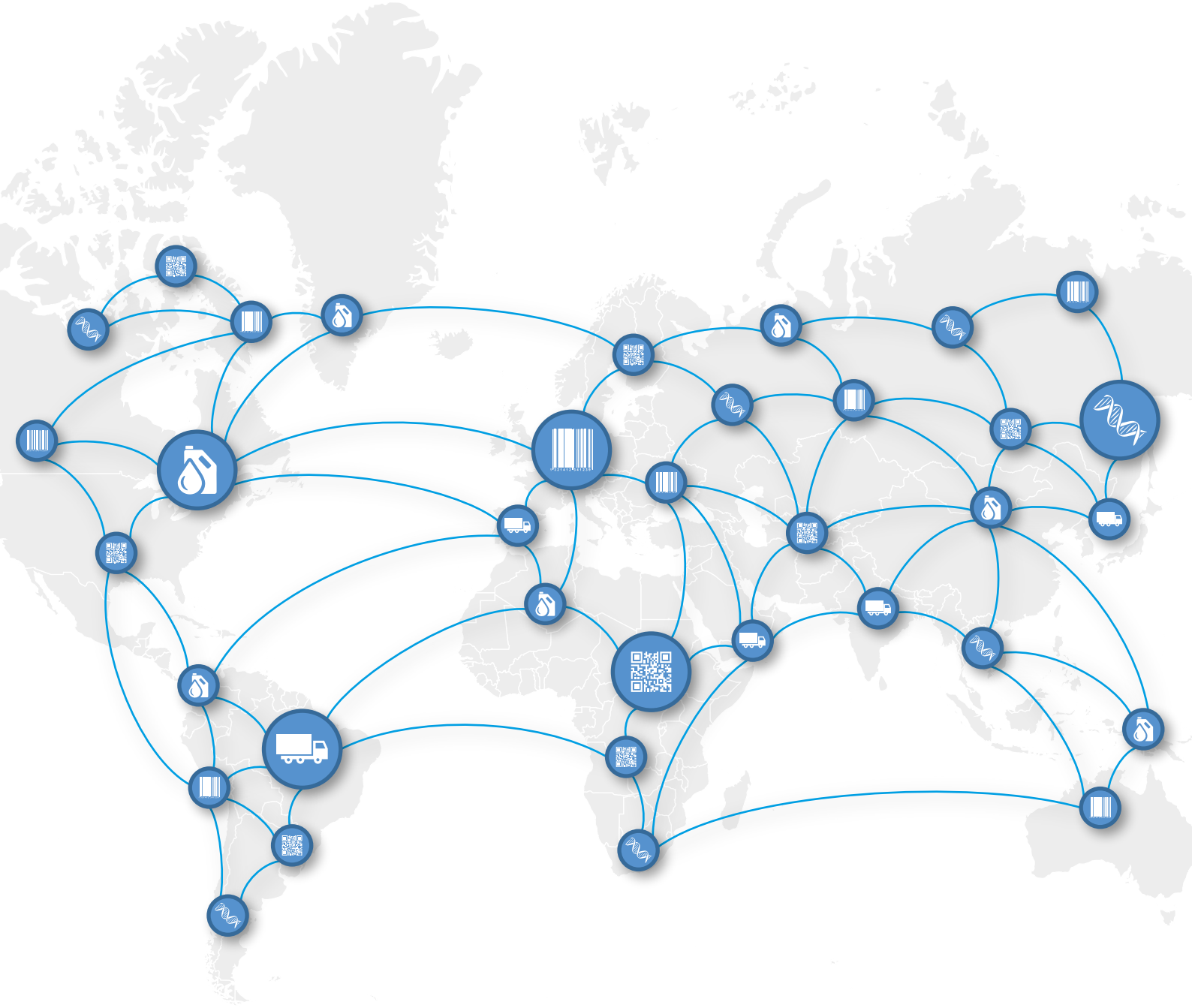
United Nations
Interregional Crime and Justice
Research Institute

TECHNOLOGY AND SECURITY:
COUNTERING CRIMINAL INFILTRATIONS IN THE LEGITIMATE SUPPLY CHAIN



TECHNOLOGY AND SECURITY: **COUNTERING CRIMINAL INFILTRATIONS IN THE LEGITIMATE SUPPLY CHAIN**

Disclaimer
The opinions, findings, conclusions and recommendations expressed herein are those of the authors and do not necessarily reflect the views and positions of the United Nations and UNICRI, or any other national, regional or international entity involved. Contents of the publication may be quoted or reproduced, provided that the source of information is acknowledged.

Acknowledgements
This Report has been prepared by Mr. Francesco Marelli, UNICRI Head of Unit, Mr. Marco Musumeci, UNICRI Programme Management Officer and Ms. Mariana Diaz Garcia, UNICRI Programme Assistant.
UNICRI would like to express its gratitude to the experts from different technological sectors that provided submissions in response to the call for innovative ideas to address counterfeiting and criminal infiltration in the supply chain, that was launched under the framework of UNICRI's Security through Research, Technology and Innovation (SIRIO) initiative. In particular, we would like to acknowledge the contributions submitted by ASMSpotter, Ashton-Potter (USA) Ltd., Australian Nuclear Science and Technology Organisation (ANSTO), Authentix, BITCLIQ, Centre for Applied Physics Dating and Diagnostics Department of Mathematics and Physics of the University of Salento (CEDAD), FOCOS, INCM – Portuguese Mint and Official Printing Office, Ion Implantation Laboratory Institute of Physics Federal University of Rio Grande do Sul, nano4u, Nornickel, ProtectedBy.AI, Scantrust, Securikett, SICPA, Singapore Synchrotron Light Source, and Tecnoalimenti. We would also like to thank the Italian Central Inspectorate of Quality Protection and Fraud Repression (ICQRF) of the Italian Ministry of Agriculture for the support provided in relation to innovative policies used to counter online infringements of protected Geographical Indications.

In addition, UNICRI would also like to thank the participants to the meeting for the creation of the risk scenarios that was held in Geneva, at the Palais des Nations on 9 – 10 July 2019 as well as those who participated to the three virtual experts' meetings that UNICRI organized on the 20th November 2020, on "Supply chain security: food fraud", 4th December, 2020, on "Supply chain security: illicit trafficking of precious metals" and the 17th December 2020 on "Supply chain security: Trafficking in Counterfeit and Substandard Pesticides, Illegal, Unreported and Unregulated (IUU) fishing, and Fuel Fraud". The list of participants can be found in Annex 1.

Table of Contents

Foreword

Organized crime continuously evolves to adapt to different circumstances and opportunities, in view of expanding its activities, increasing its profits, and ultimately strengthening its grasp on the economic, social and political sectors of countries. For criminals, the advent of market integration presented the possibility to develop global trafficking strategies and patterns, while exploiting possible loopholes, weak points and increased complexities of globally integrated supply chains that move products around the globe. In this context, the infiltration of organized crime into the legitimate supply chain is a complex issue that requires a multifaceted response, including consideration of the role that technology can play to help combat related criminal activities. This means first identifying the threats posed by organized crime to the supply chain of different products, while understanding that certain categories of products may present unique issues in terms of supply chain complexity, product authentication and vulnerability to criminal operations. This means also working with technology experts to identify how different technology solutions can respond to the identified threats.

Under the framework of the Security through Research, Technology and Innovation (SIRIO) initiative, UNICRI identifies emerging and future security risks, maps technology innovations to match security needs, raises awareness and informs policy-makers about emerging risks and innovative solutions, while enhancing cooperation between national and international authorities, industry and research institutions.

This report provides an overview of some of the main threats posed by criminal organizations attempting to infiltrate the supply chain security. It also presents possible responses that technology solutions can provide to support legitimate stakeholders seeking to protect their products and provides law enforcers with additional tools to investigate and counter organized criminal activities. This report does not intend to present technology as the sole solution to mitigate the identified risks; rather, it presents technology as an instrument to increase human capabilities and skills.

The technology solutions presented are examples to showcase different approaches that can be applied to mitigate identified threats. They integrate a wide range of innovative proposals that adopt advanced technologies, such as artificial intelligence, blockchain, big data analytics, cutting-edge authentication mechanisms, nuclear analytical techniques, protected traceability systems, and multilayered approaches where various elements are linked to increase the range of protection. Technology is being used as a tool to support the creation of new strategies, generate knowledge, and adapt responses to increase their efficiency and accuracy.

In line with its mandate in the field of criminal justice and crime prevention, UNICRI is committed to evaluating emerging criminal threats and the evolving technology solutions to combat them. We hope that this report will stimulate and encourage new discussions and developments in the area of supply chain security, leading to improved cooperation among stakeholders, while also setting the baseline for further analysis of these issues.

Antonia Marie De Meo
UNICRI, Director

Introduction

The scope of this report is to understand how technology can help to limit the threats posed by organized crime involvement in counterfeiting and food fraud, in particular in relation to the infiltration of counterfeit and fraudulent food into the legitimate supply chain.[1]

The report has been prepared by the UNICRI Knowledge Centre Security through Research, Technology and Innovation (SIRIO). The scope of SIRIO is to analyse and understand the global impacts, opportunities and challenges of technological change, including in the areas of augmented and virtual reality (AR, VR), big data analytics, digital biology and biotech, nanotech and digital printing, networks and computing systems, supply chain security and decentralized technologies such as blockchain.

To prepare this report, UNICRI has worked in close cooperation with several international and national organizations, research centres and private sector entities active in this field. UNICRI has followed a three-step approach to collect, analyse and validate data. The first element consisted in the preparation of risk scenarios related to the criminal infiltration of the food supply chain. The risk scenarios were based on different sources, including law enforcement investigations and previous research reports prepared by UNICRI and other international and national organizations. Interviews were also conducted with selected experts to fine-tune the risk scenarios.

The risk scenarios included background information on the perpetrators, their motives and capabilities. The scenarios explored possible strategies that organized crime can adopt to infiltrate the food supply chain, including the adoption of money laundering techniques as well as the infiltration of the legal economy. The use of fictional scenarios proved to be very helpful to analyse the likelihood that a concrete risk could become real and test out possible responses to foreseeable events, specific modi operandi, interlinked criminal activities as well as providing opportunities to consider potential measures to avert comparable future problems. Moreover, risk scenarios enhanced creative thinking to develop new policies and strategies that may reduce the possibility of the events taking place or that would significantly decrease their negative consequences.

The risk scenarios were validated during a workshop organized at the Palais des Nations in Geneva, Switzerland, on 9-10 July 2019. The meeting was attended by experts from international organizations, law enforcement agencies and industry who were invited to discuss (a) the feasibility of each scenario over time; and (b) the necessary capabilities (i.e., skills, knowledge, resources, equipment, etc.) to commit the crime. At the end of each scenario, a set of questions were identified in order to stimulate forward-looking proposals for technology solutions that could be applied to prevent, detect or respond to each threat. The list of participants in the meeting is included in Annex 1.

Each set of questions formed the basis for the creation of a call for technological submissions that was published on UNICRI's website in January 2020 and that constituted the second step of our approach.2 The goal of the call was to invite security experts and representatives from industry, academia, civil society and international organizations to share innovative ideas and solutions that could concretely contribute to mitigating the risks highlighted in the scenarios, which were shared with those experts who responded to the call.

The third step consisted in discussing the submissions received through the call and their correlations with the risk scenarios. This was done during a virtual experts' meeting, organized by UNICRI on 20 November 2020. The virtual meeting was attended by experts from international organizations, academia and industry. Annex 1 contains the full list of participants.

The present SIRIO report is based on results from both the risk scenarios and the technological submissions.

The report is organized in six chapters. The first chapter offers an overview of how technology has been used to protect the supply chain and identify illicit infiltrations and fraudulent activities, providing a preliminary explanation of some of the concepts that will be further analysed during the subsequent sections of the reports. Chapters 2 to 6 are each dedicated to a specific area of analysis related to criminal activities linked to the infiltration of the supply

1 In 2016, UNICRI published its first study dedicated to the role of technology solutions ensuring supply chain security. See UNICRI, Ensuring Supply Chain Security: The role of anti-counterfeiting technologies (2016) available at: http://www.unicri.it/topics/counterfeiting/anticounterfeiting_technologies/Ensuring_supply_c ain_security_report.pdf

2 http://www.unicri.it/news/article-16

chain, namely: agro-food mafia (Chapter 2); illicit trafficking of precious metals (Chapter 3); Illicit, Unreported and Unregulated fishing (Chapter 4); trafficking in counterfeit and substandard pesticides (Chapter 5) and fuel fraud (Chapter 6).

Apart from Chapter 1 on the general technological introduction, each subsequent chapter has been conceived as a standalone document and can be read without reading the other thematic-specific parts of this report. This choice has been made in view of allowing an easier reading to those interested solely in a specific thematic area. However, this also means that some repetitions will be apparent to readers who go through the whole report. Each chapter starts with a summary of the risk scenarios that we used to identify some of the threats which are specific to the various thematic areas, while the presentation of the potential support provided by technology to prevent those threats is made through the analysis of the submissions UNICRI received during the above-mentioned call for ideas. We also condensed some of these findings in the conclusions to each specific chapter, in view of stimulating further forward-looking thinking on how to create an integrated and multi-stakeholder strategy that can render the fight against criminal activities in these areas more effective.

CHAPTER 1
Introduction to Supply Chain Security

1.1 Preliminary elements on supply chain vulnerabilities and anti-counterfeiting technologies

Counterfeiting and piracy are terms used to describe a range of illicit activities linked to Intellectual Property Rights (IPRs) infringements.[1] The impact of counterfeiting goes beyond the infringement of intellectual property since it also affects the population in terms of public health and safety, tax and customs income, job losses, corruption and the expansion of organized crime. Within organized criminal groups, counterfeiting operations are usually linked to several other criminal and illicit activities, such as fraud, customs and excise contraventions, tax evasion, money laundering, several forms of illicit trade/trafficking and conspiracy/participation in crime.

The scope and scale of counterfeiting activities have been widely recorded. The 2019 joint study prepared by the Organisation for Economic Co-operation and Development (OECD) and the European Union Intellectual Property Office (EUIPO) reported that, in 2016, the volume of international trade in counterfeit and pirated products could amount to as much as €460 billion (not including domestically produced and consumed counterfeit and pirated products, and pirated digital products distributed online).[2] This represented up to 3.3% of world trade, a noticeable spike if compared to the figures reported by the OECD in 2013, when data represented an estimated value of 2.5% of world trade. Moreover, imports of counterfeit and pirated products into the EU amounted to as much as €121 billion.[3] This represented up to 6.8% of EU imports, compared to 5% of EU imports in 2013.

Counterfeiting is an extremely complex phenomenon. Repression in itself, be it through civil, criminal or Customs' remedies, is not sufficient to significantly reduce the problem, and there is a strong need to develop a comprehensive counter strategy. This strategy, while considering the adoption of higher criminal sanctions to step up deterrence, should also include the active participation of a wide range of actors that could contribute to a multi-disciplinary response to the problem, each one contributing with its own expertise and within its specific area of work. In particular, private sector stakeholders and technology providers can offer significant contributions for curbing counterfeiting. Their involvement in discussing how to jointly advance the fight against counterfeiting and organized crime may significantly contribute to the identification of innovative and shared strategies to support governments and the international community.

Recent advancements in innovation in the technology sector combined with digital transformation have re-shaped the realm of supply chain security, enabling the adoption of new techniques that have exponentially reinforced existing security mechanisms in order to protect products from ever-developing threats. New technology solutions have been developed to address the vulnerabilities of the various stakeholders in the supply chain. These vulnerabilities can be found in both the supply and production nodes, where the extreme fragmentation of the supply chain creates difficulties for monitoring purposes. Supply chain fragmentation has accentuated the need to integrate information from multiple production facilities, transportation modalities, materials' providers, points of exchange and inspection, adding dynamic and detailed complexity to supply chain management.[4]

1 According to the Trade-Related aspects of Intellectual Property Rights (TRIPS) Agreement, the term counterfeit is defined as: "any goods, including packaging, bearing without authorization a trademark which is identical to the trademark validly registered in respect of such goods, or which cannot be distinguished in its essential aspects from such a trademark, and which thereby infringes the rights of the owner of the trademark in question (...)."
In the same spirit, EU Regulation 608/2013 differentiates products infringing on a patent from counterfeited items, qualified as "goods which are the subject of an act infringing a trademark in the Member State where they are found and bear without authorization a sign which is identical to the trademark validly registered in respect of the same type of goods, or which cannot be distinguished in its essential aspects from such a trademark (...)."

2 OECD/EUIPO (2019), Trends in Trade in Counterfeit and Pirated Goods, Illicit Trade, OECD Publishing, Paris/European Union Intellectual Property Office. https://doi.org/10.1787/g2g9f533-en

3 Ibid.

4 Watson, J. (2015). Essays on deceptive counterfeits in supply chains: A behavioural perspective.

Nowadays, supply chain security technology offers a great variety of solutions which in themselves are very flexible and can be applied to a great number of products and categories. These technologies evolved in recent years to progressively respond to a series of factors which directly impacted on how security in the supply chain had to be implemented. Some of these factors include increased complexity and globalization, cross-border interdependency, digitized management of supply chains and expanding security implications.[5]

While these trends have created serious challenges for the overall management of the supply chain, this complexity has also been exploited by organized crime to infiltrate counterfeit, substandard and/or illicit products into the supply chain. Within the overall picture of the supply chain functioning, the following are some of the aspects which are becoming increasingly complex, rendering supply chain control more and more challenging:

- Visibility. The network of buyer-supplier relationships at the level of raw materials and components used for the production of finished goods is becoming more complex. This may create a lack of visibility of raw material movements and of their incorporation into the final product. This complicates the assessment of the integrity of procured parts and subsequently the distribution of the final product.[6]

- Traceability. Tracking data can be fragmented when it circulates among the involved actors, which makes it difficult to uniquely identify each procured item and trace its history. This is also valid for final goods and may lead to shortage of data that can be used for forensics investigations.[7]

- Accountability. Fraudulent conduct of criminals can be noticeably facilitated in a context with poor visibility and a lack of traceability, which leads to a deficiency in accountability. These factors can also complicate the identification of a breach in a part of the supply chain.[8]

Within this framework, an increased awareness on the involvement of organized crime in counterfeiting activities, as well as on the threats and negative consequences created by this crime, is leading governments, international organizations and industry groups to increase cooperation aimed at developing and improving the enforcement of related criminal penalties and reduce the distribution of counterfeit products. Public-private partnerships between governments and industry have also been established to use supply chain security technology to protect the marketing of several products' categories. Existing technology solutions have been developed with the aim of responding to the challenges presented by criminal activities and proposing single and combined options to target vulnerabilities in the supply chain.

In this regard, anti-counterfeiting technologies are aimed at protecting governments' revenues, public safety, brand owners' rights, and suppliers' reputations.[9] In general, and with some exemplifications, these solutions may include overt or covert technology and/or a combination of the two. According to ISO standard 12931, an overt authentication element "is detectable and verifiable by one or more of the human senses without resource to a tool", while a covert authentication element is "hidden from the human senses until the use of a tool by an informed person reveals it to their senses or else allows automated interpretation of the element".[10] As there can be some confusion on the meaning of 'covert', it is important to note that a covert authentication element can be visible, however, the verification of its authenticity always requires a tool and cannot be accomplished by the human senses alone.

5 Demidov, O.; Persi Paoli, G. (n.d.). Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses (Publication). Retrieved 2020, from United Nations Institute for Disarmament Research website: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/UNIDIR_Supply-Chain-Security-in-the-Cyber%20Age.pdf

6 Hohenstein, et al. in Aniello, L., Halak, B., Chai, P., Dhall, R., Mihalea, M., &; Wilczynski, A. (2019, September 04). Towards a Supply Chain Management System for Counterfeit Mitigation using Blockchain and PUF (Publication). Retrieved August 18, 2020, from University of Southampton website: https://arxiv.org/pdf/1908.09585.pdf

7 Khojasteh-Ghamari et al. in Aniello, L., Halak, B., Chai, P., Dhall, R., Mihalea, M., &; Wilczynski, A. (2019, September 04). Towards a Supply Chain Management System for Counterfeit Mitigation using Blockchain and PUF (Publication). Retrieved August 18, 2020, from University of Southampton website: https://arxiv.org/pdf/1908.09585.pdf

8 Hartmann et al. in Aniello, L., Halak, B., Chai, P., Dhall, R., Mihalea, M., &; Wilczynski, A. (2019, September 04). Towards a Supply Chain Management System for Counterfeit Mitigation using Blockchain and PUF (Publication). Retrieved August 18, 2020, from University of Southampton website: https://arxiv.org/pdf/1908.09585.pdf

9 Ling Li, Technology designed to combat fakes in the global supply chain, Business Horizons (2013) 56, pp. 168-171.

10 International Organization for Standardization (ISO). (n.d.). ISO 12931:2012. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:12931:ed-1:v1:en

'Covert' security elements were traditionally restricted to authorized stakeholders such as producers, brand owners, or enforcement officials, yet an increasing number of security elements can be authenticated by smartphones (for example, digital watermarks, copy detection patterns, Near Field Communication (NFC)). As a result, it has become common practice to let consumers, as well as other supply chain intermediaries and retailers, verify the authenticity of covert authentication elements.

The above technologies mainly serve the purpose of authenticating a product or, more often, its packaging, telling if it is genuine or not. To control products' movements along the supply chain, track and trace technologies are needed and the combination of authentication and track and trace may serve as a more effective barrier to the infiltration of fake and illegitimate products within the legal supply chain.

Several types of authentication elements can be used to distinguish authentic goods from phony items, including holograms, colour-shifting inks, security threads, QR codes, data matrix codes, micro-printing, anti-forgery inks, bar-code technology, digital watermarks and copy detection patterns, to mention a few. On the other hand, tracking and tracing mainly relies on two identification methods: optical barcodes (e.g. QR codes, data matrix) and radio frequency identification (RFID), which can be applied either separately or jointly and with optical identification methods being more widespread. QR codes and data matrix codes may however be used for authentication if used in combination with an authentication element which is verified simultaneously.[11]

Operationally, and for both optical and RFID technology, the process of securing and controlling the movement of products with authentication and track and trace may start as early as the manufacturing stage and may continue in the distribution and retail phases, depending on the type of product, the producer/government's requirements, and the relevant regulations in place[12].

1.2 An introduction to the evolution of technology solutions for securing the products' supply chain

The technological evolution in supply chain security mechanisms has been combined with the progressive transformation of industries which were facing the need to quickly circulate mass market products globally while controlling their location and protecting from a series of evolving threats posed by criminals to the integrity of the supply chain.

Two examples can be briefly mentioned to show how technology evolved in the area of supply chain security. The first one relates to rapid technology evolution in relation to tools to authenticate and subsequently track and trace products. The second one refers to the possibility of adapting tools initially created for specific purposes (tax collection in this specific case) to a modified criminal environment, where the purpose of collecting taxes progressively met the purpose of protecting the integrity of the supply chain.

11 For more information see: The European Observatory on Infringements of Intellectual Property Rights (EUIPO). (2021). Anti-Counterfeiting Technology Guide. Retrieved from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Anti_Counterfeiting_Technology_Guide/2021_Anti_Counterfeiting_Technology_Guide_en.pdf

12 A complete overview of these elements can be found in the 2016 report "Ensuring supply chain security: the role of anti-counterfeiting technologies". The report was published in 2016, consequently, the information presented might not consider the latest developments in technology. The present report focuses on current risks and possible responses, including the presentation of innovative submissions based on up-to-date technology solutions. To access the previous report, see: UNICRI (2016), "Ensuring supply chain security: the role of anti-counterfeiting technologies", http://www.unicri.it/index.php/ensuring-supply-chains-security-role-anti-counterfeiting-technologies

Example 1

In 1952, with the patent of the barcoding system, technology had already begun to play a decisive role for the control of the production of goods and for securing the supply chain. In this period, barcodes progressively became an innovative solution to manage operations in the manufacture and distribution of products, and eventually they facilitated the integration of other technology solutions to consolidate information. The relevance of data management increased in 1960 with the invention of computer systems that were able to transfer data between devices, enabling the exchange of electronic business documents. Globalization and the growth of the scale in production also led to the creation of a new computerised tracking system that provided near real time information about packages for delivery by FedEx in 1985. This end-to-end visibility system enabled drivers to use portable handheld computers to scan pickups and deliveries, allowing the monitoring of the status of a shipment through the stages of the supply chain.

The development of more secure code systems continued, and in 1987, David Allais developed the first 2D barcode, enabling a larger amount of data storage and better encryption. Later, in 1994, the QR code system was invented by Masahiro Hara from the Japanese company Denso Wave to track vehicles during manufacturing. The company has held the patent rights since its creation but has decided not to exercise them, which allowed the widespread adoption of the technology. These improvements were highly relevant since coding plays a central role in the current authentication and monitoring technology.

In 2000, another major development occurred when radio-frequency identification (RFID) was developed at the MIT Auto-ID Centre. The code-carrying technology uses data stored in a microchip where the tag's antenna receives electromagnetic energy from an RFID reader's antenna, and eventually, the tag sends the frequency waves back to the reader to be interpreted. The integration of RFID to objects was essential to generate track-and-trace solutions using a database and to establish the technology for automatic identification and data capture (AIDC).

Furthermore, monitoring of the processes and information security went through important changes. In 2009, technology security solutions had a breakthrough when a developer or developers working under the pseudonym Satoshi Nakamoto published a white paper establishing the model for a blockchain and a blockchain database. The use of blockchain in the supply chain adds a layer of security in the peer-to-peer interaction and exchange of data by eliminating intermediaries and by storing data which are immutable.

Example 2

Governments have also directly taken measures to protect national commerce and tax revenue. To achieve this, they developed the tax stamp system in the 17th century. A tax stamp is an easily recognizable government-approved mark, applied to a product to guarantee that the correct amount of taxes has been paid. Tax stamps are required by many countries as a way of ensuring taxpayers' compliance by monitoring production. The rationale for tax stamps stems from the primary goal of tax administration, which is to "collect taxes and duties payable in accordance with the law."[13] Tax administrations put in place strategies and structures to guarantee that non-compliance with tax obligations is kept to a minimum.

With the evolution of illicit trade and the rise of counterfeiting and smuggling, tax stamps have progressively acquired a new function, namely contributing to products' authentication and allowing for the tracking and tracing of products to which they are affixed. In simple terms, tax stamps are nowadays one of the means used by governments to ensure that an excisable item is original and is put into commerce via authorised channels.

13 Centre for Tax Policy and Administration (2008), Forum on Tax Administration: Compliance sub-group, final report, "Monitoring taxpayers' compliance: A practical guide based on Revenue body experience", available at: http://www.oecd.gov

To this end, governments started cooperating with several providers of anti-counterfeiting technology, purchasing increasingly sophisticated tax stamp protection systems. In some cases, and especially for companies already active in the areas of banknote security, these systems were usually based on the same high security features already applied to the protection of banknotes from counterfeiting. These security features have been progressively tailored in view of their specific application to tax stamps. Other enterprises that entered the market at a later stage usually offered a combination of new security products and innovative technologies. To this end, product protection systems have been developed to prevent the unauthorized and/or illegal manufacturing and selling of protected products.

The protection of both excisable and non-excisable products follows similar principles. A wide range of technologies are currently available to authenticate them and/or their packaging, as well as to track and trace these products as they move along supply chains. The examples provided above show that existing technology solutions to identify counterfeit products and any other security disruption in the supply chain are the result of the evolution of different elements. The improvement of technology created the possibility of combining several mechanisms to create integral product protection systems that are able to increase security in several stages of the supply chain with multilayer protection techniques.

Finally, existing technology solutions aimed at securing the supply chain of products at different stages are nowadays coupled by other solutions aimed at analysing suspect counterfeit/fraudulent/substandard products to verify their originality, with the view of collecting forensic evidence that can be subsequently used during civil or criminal proceedings. This report provides an overview of both categories, presenting how they can contribute to identifying and limiting criminal activities in the area of food fraud and food counterfeiting.

1.3 From supply chain security to the collection of forensic evidence

Several technologies can contribute in various ways to increase the security of the supply chain and respond to threats posed by criminals. In particular:

- From the perspective of governments, commodities' producers and supply chain stakeholders, one of the primary goals is to avoid illicit products infiltrating the legitimate supply chain. In this case, supply chain security technologies can support this goal to uniquely identify original products, follow them on their journey to the final customers, and avoid that unidentified products infiltrate the legitimate supply chain.
- However, in the case in which an infiltration occurred, then the primary goal is to identify the breach and the infiltrated products, by analysing their nature and composition to determine if they are genuine or not and then trace them back to the origin of the infiltration. Forensic analysis and related technologies can support this goal.

a) Securing the supply chain

For what concerns supply chain security, some basic concepts are similar across different sectors and different solutions which have been developed by a variety of providers. However, this does not mean that anti-counterfeiting and supply chain security technology is the same across all sectors and across all providers. In reality, the same technological concepts – being it authentication through optical means or integrated track and trace solutions – can and have been applied in a variety of different ways by the various stakeholders which are active in this field. This report will consequently focus on describing the potential benefits to the security of the supply chain of food products created by specific technological categories, while also delving into concrete examples obtained through the responses to UNICRI's call for ideas. The aim is to present the potential contribution of technology to counter

criminal activities in this field through the use of practical examples, showing how several providers developed solutions or ideas to improve the effectiveness of anti-counterfeiting and supply chain security technology.

In general terms, technology options to increase security in the supply chain can target the external packaging of a product and/or the product itself, by designing, integrating and/or affixing tools for the authentication of the product. These tools have the primary function of telling the user if the product is authentic or not. Furthermore, it is becoming more and more common for authentication technology on the products to be coupled with the implementation of track and trace systems that allow the monitoring of the authenticated goods throughout the different stages of the supply chain and secure the latter from infiltration of unauthorized products. As it will be shown, combining these two technologies is very often at the core of ideas for securing the supply chain of products.

- Authentication

Authentication solutions are defined by specific characteristics that allow the differentiation of an entity (a product in the current case) from another one on the basis of specific features. Defining the characteristics of an original product helps the different stakeholders of the supply chain, and possibly consumers, to identify the presence of counterfeit versions. To define what an original product is, it is possible to refer to certain intrinsic features of the product itself or to apply specific technology on the product, which will provide for the distinction between original and counterfeit (a hologram or a code, for instance). The intrinsic features of a product can be the result of the production environment, the distribution environment, the composing elements of the product or of other factors.[14] However, in most cases, these characteristics cannot be easily identified, therefore, technology solutions are used to apply authentication mechanisms on the product during its production or distribution phases. As previously described, the solutions can be overt[15] (using the sensorial capability of the individual) or covert[16] (that require a device or an additional tool to be revealed) or a combination of both.

Authentication technologies are usually linked to the packaging process. Primary packaging is usually the means through which implementing overt technologies can be accessed without the need to rely on a particular device or tool to perform the authentication. These applications are also easy to recognize for consumers. An overt device can also be incorporated within a tamper-evident feature for added security.[17] Some of the possible overt authentication options include tamper-evident/tamper-resistant packing (micro cut labels, VOID labels, multi-destructible vinyl labels), holograms, optically variable devices, colour shifting security inks and films, fugitive inks, security graphics, scratch-off technologies, among others. The evident manipulation of the security measures gives the supply chain actor or the final consumer a clear warning indicating that the product is no longer safe. The adoption of VOID elements tries to respond to the fact that overt solutions have been imitated by criminal organizations in the past, especially if they are widely used. Furthermore, authentication has evolved to provide authentication of the product itself, beyond the use of labels or codes engraved on paper, packaging or other materials. As it will be discussed in the following parts of this report, these new developments have made the reuse or imitation of labels, stamps and packages harder for criminal organizations.

Coming back to packaging, it can also be used to carry covert authentication elements as a security measure in the supply chain. Covert technology requires a device for authentication and covert devices enable a producer or a brand owner to identify the original product against a counterfeit one.[18] The covert solution may be visible or invisible. When an invisible security element is applied to the packaging, it can safeguard the product since only holders of an authorization and specific stakeholders in the supply chain are aware of the presence of a security measure, making it harder for criminals to identify it as easily as a visible solution. Some options, such as invisible inks, need

14 Baldini, G., Fovino, I. N., Satta, R., Tsois, A., Checchi, E. (2015). Survey of techniques for fight against counterfeit goods and Intellectual Property Rights (IPR) infringing. Retrieved, 2020, from https://ec.europa.eu/jrc/en/publication/survey-techniques-fight-against-counterfeit-goods-and-intellectual-property-rights-ipr-infringing

15 Some examples include holograms, inks, security threads, watermarks, sequential product numbering, fibres, among others.

16 Some examples include security inks, digital, watermarks, biological taggants, chemical or microscopic taggants, microprinting, NFC, copy detection patterns, among others.

17 World Health Organization. (n.d.). Appendix 2: Available Authentication Technologies for the Prevention and Detection of SSFFC Medical Products. Retrieved 2020, from https://www.who.int/medicines/regulation/ssffc/Available_Authentication_Technologies_for_Prevention_and_Detection_of_Substandard_and_Falsified_Medical_Products.pdf?ua=1

18 The main covert devices include security inks/coatings, reactive inks, UV inks, IR inks, and thermochromic inks, hidden printed messages, digital watermarks and taggants.

special "developers" to reveal the security mark.[19] The covert technologies usually include invisible printing (using luminescent, reactive, "rub and reveal"/ "coin reactive", photochromic, or thermochromic inks and infrared fluorescent pigments), three-dimensional (3D) intaglio printing, embedded images, filigrees, digital watermarks, microprinting, anti-scan designs, safety fibrils, marks in a die-cut profile, substrates and odour.[20] Other solutions include the use of micro taggants, which enable on-the-spot, non-destructive field testing, allowing for the instant identification and verification of materials with readers and detectors such as microscopes, UV lights and laser pens.[21]

Packaging may also carry covert authentication elements which can be authenticated by using a smartphone, for example, digital watermarks, NFCs or copy detection patterns. In such cases, authentication can be opened up to a much larger audience, including supply chain intermediaries, retailers and consumers "crowd-sourcing" the brand-protection activities. Compared to covert authentication solutions that are only authenticated by the brand owners or inspectors, the number of verified products may be increased by orders of magnitude. This has two resulting positive effects; as products are routinely checked, it becomes harder for counterfeiters to infiltrate the legitimate supply chain, and as each authentication usually generates data points that are captured by a connected product cloud, brand owners get real-time visibility on illicit activities in the supply chain.

Packaging solutions, in both primary and secondary packaging, can also include track and trace technologies in order to follow the product on its journey from the producer to the various distributors and, eventually, the final consumer, increasing the security level in the supply chain beyond the authentication of the product.

- Track and trace technology

Authentication solutions tackle some of the common issues related to counterfeiting, yet organized crime is using more and more advanced techniques to infiltrate the legal economy, control operators in the supply chain and make it more difficult to distinguish original products from imitations. Criminal organizations have adopted new techniques to breach the security measures established by the initial authentication solution. Frequently, expired or low-quality products are repacked and relabelled with falsified dates, dosage and brand information. If the overt mechanisms are imitated and the new package can mimic the original one, consumers and supply chain operators may not be able to identify counterfeit merchandise or may find it more difficult if they do not apply all needed identification measures. In addition, machinery used to repackage these products is often the same used by original manufacturers or it is as sophisticated as the ones they use, adding a layer of complexity in the identification of counterfeit or fraudulent products. In order to combat these challenges, coupling track and trace with authentication can provide an additional measure to ensure that there is no interruption and infiltration in the supply chain and that no actor or product external to the authorized ones becomes involved without being noticed.

Traceability mechanisms are characterized by the application of a unique identifier to the product[22] or to a batch of products, which is then used to track its movements throughout the different stages of the supply chain. The adoption of these technology solutions is linked to the use of a back-end database within which each movement of goods along the supply-chain is recorded.[23] This type of technology solution helps in the enhancement of visibility of the product during the different stages of the supply chain. However, if not coupled with authentication measures, these solutions alone cannot really certify the authenticity of a product, although they can contribute to tracking the products along the supply chain. Additionally, if the reference applied to a batch of products does not exist in the producer's database, then the system can warn that a particular batch is not part of the original production. Likewise, the track and trace system can alert different stakeholders when the products are no longer in the supply chain.

However, simple supply chain management tools lack strong authentication features which are difficult to copy and allow for the attribution of a unique and strong secure identifier to each product, rendering counterfeiting opera-

19 "Developers" include ultraviolet or infrared light, heat, cold and iodine vapour.

20 World Health Organization. (n.d.). Appendix 2: Available Authentication Technologies for the Prevention and Detection of SSFFC Medical Products. Retrieved 2020, from https://www.who.int/medicines/regulation/ssffc/Available_Authentication_Technologies_for_Prevention_and_Detection_of_Substandard_and_Falsified_Medical_Products.pdf?ua=1

21 Microtrace (n.d). Microtaggant Identification Particles. Retrieved 2020 from: https://www.microtracesolutions.com/solutions/implement-independently/microtaggant-identification-particles

22 Identifiers include tags, labels, and codes.

23 Baldini, G., Fovino, I. N., Satta, R., Tsois, A., Checchi, E. (2015). Survey of techniques for fight against counterfeit goods and Intellectual Property Rights (IPR) infringing. Retrieved, 2020, from https://ec.europa.eu/jrc/en/publication/survey-techniques-fight-against-counterfeit-goods-and-intellectual-property-rights-ipr-infringing

tions much more difficult. The combination of track and trace with authentication technology creates the possibility of using a secure unique identifier to trace the movement of each individual good and verify its authenticity at every step of the distribution chain, strengthening the security of the supply chain.

Track and trace solutions help provide visibility of the product within the supply chain to the multiple stakeholders involved in the process, while at the same time avoiding the infiltration of unauthorized goods. As anticipated, they rely mainly on optical and/or on RFID mechanisms. In the case of optical technologies, a code containing information on the product is generated and then affixed on the product itself, usually via a label.[24] The label containing the code is then read along the production and the distribution chain. The information contained in the code is therefore acquired by the system and inserted into a dedicated and secured database and will serve to authenticate and track the product along the distribution steps and monitor its movements. The barcoding system invented in the 1950's has evolved to create more complex linear and matrix 2D barcodes, such as the Data Matrix code, as well as the widely available QR code and the Cronto Visual Cryptogram. The current available codes are highly encrypted and use different patterns and technology to ensure the integrity of the data. They may include encrypted data, or randomly generated unique identifiers; they often contain a unique URL, enabling the creation of a digital connexion when they are scanned. They also include improved characteristics such as a larger storage capacity, a smaller size, the capacity of being read from any angle, the possibility to encode numeric, alphanumeric, binary, and Kanji characters, and error correction for better scannability.

Traceability options can also use space technologies as a proof of origin as well as for monitoring purposes. The images taken from drones and satellites can be used to link products to their place of origin, but also enable the calculation of production volumes to check whether the quantity of products in circulation varies from the original quantity. Secure communication and data exchanges between drones, satellites and ground Internet of Things (IoTs) are key developments for supply chain auditability.

Technology is also evolving in view of facilitating some of the steps presented above, as can be seen in the example below.

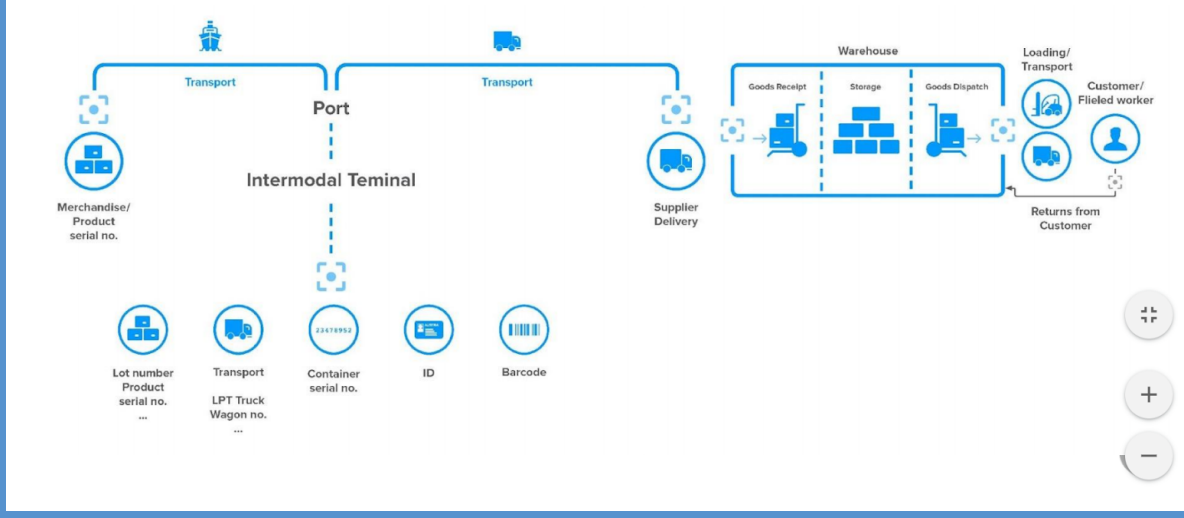
Smart data capture capability, beyond Optical Character Recognition (OCR)

End-to-end (E2E) traceability with smart data capture can be a useful and highly efficient technology tool to support the extraction and registration of information from multiple sources, such as license plates, IDs, passports, driving licenses, "any" serial number, various symbols and 2D codes and containers documents.

The smart, mobile and contact-free technology allows the stakeholders to capture the goods on any step of the supply chain by reading any visuals and data using a standard consumer smartphone. This provides a fast, accurate, and secure method by eliminating manual typing. Machine learning is used to improve the detection of information and it is constantly trained with data to provide a higher level of accuracy with the adoption of convolutional long short-term memory networks. The data captured then goes to the secure app or platform that is used by the authorities to perform inspections.

The system is secure since it does not transmit data and can work offline. The on-device processing means all data captured stays safe in the stakeholder's closed system. This technology can be used throughout the different processes in the supply chain to corroborate the information that is shared in documents, lots, and transportation.

24 Information can be stored in different types of codes, as barcodes, 2D codes, or QR codes, to list some examples.



Technology developed by Anyline

- Enhancing security through blockchain

A recent development to enhance security in traceability solutions has come through the adoption of additional tools that minimize the risks of compromising information or the lack of visibility in certain parts of the chain. Blockchain is a type of distributed ledger technology (DLT) that can connect and enable efficiency, transparency, and accountability among participating actors. Blockchain can connect the different parties in the supply chain that have not established trusted relationships with each other, by ensuring transparency due to its tamper-evident nature. Blockchain stores every transaction or exchange of data that occurs in the network, reducing the need for intermediaries by providing a means by which all the actors in the network may share access to the same information, including what is added to the data, by whom, and the date and time of the submission.[25]

Once the data is registered, it cannot be removed or modified. Reconciliation of all the parties involved is achieved by enabling the actors to see the same data in real time.[26] Some of the security measures that can be used to facilitate the automated data collection and tracking along with the blockchain solution include product tagging (RFID, NFC-embedded ID chips), digital quality assurance checklists, GPS-enabled smart logbook, IoT devices – scanners, sensors, cameras, smart packaging and digitized labelling, tamper-evident seals or security stickers – and identity management of devices, commodities and users.[27]

25 Accenture. (2019, January 15). Tracing the Supply Chain. Retrieved August 23, 2020, from https://www.accenture.com/_acnmedia/pdf-93/accenture-tracing-supply-chain-blockchain-study-pov.pdf

26 Ibid.

27 Ibid.

b) Forensics

Forensic science works off of the physical remnants of past criminal activity, and, therefore has certain native and non-native principles that guide its operation, application, and interpretation. One of the implicit precepts in this view of forensic science is that the production history of mass-produced goods is embedded in the finished product. This production history sets in large part the specificity and resolution of the evidentiary significance of that item. In some cases, certain evidence types are analysed without a concrete focus on the product's origins or production history, which could be essential to identify critical information. Supply chains can generate numerous variations encountered in most mass-produced items, therefore, the foundation for the potential significance of those items encountered as evidence in forensic investigations and casework.[28]

In the field of supply chain management, forensic science has been able to identify the particular parameters of any product to determine how or if it can be differentiated from other similar products. A product resulting from the supply chain process can be seen as the culmination of certain contingencies (nodes in the supply chain) and continuities (production
methods) intrinsic in its manufacture.[29]

The techniques used to analyse the goods occasionally overlap with chemistry methods that are employed by the supply chain stakeholders to verify the quality and security standards of the products. In this regard, forensics can be used to analyse a product which has already reached the market to verify if it is counterfeit or not. The comparison of the physical and chemical characteristics of a suspected counterfeit product can determine if the analysed good is, in effect, a counterfeit. This evidence can even be brought in court to support allegations of counterfeiting since it may also serve as a tool for tracing back to the origin of the incident. In addition, it is possible to trace back the composition to its source or compare other counterfeits to verify if they have the same origin.

28 Houck, M. M. (2010). An Investigation into the Foundational Principles of Forensic Science (doctoral dissertation). Curtin University of Technology. Retrieved 2020, from https://espace.curtin.edu.au/bitstream/handle/20.500.11937/1568/146239_Houck%20M%202010%20Full.pdf?sequence=2

29 Ibid

CHAPTER 2
Agro-food mafia

Organized crime has always demonstrated a great interest in controlling legitimate economic activities by combining money laundering operations with the diversification of profits and investment possibilities. This is one of the main reasons pushing criminal organizations to infiltrate the legal economy. This infiltration can take different forms. While it mainly results in the direct or indirect control of legal businesses, companies can be acquired, administered or controlled in different ways; one of the most common being through the fictitious interposition of third persons to circumvent the effects of freezing orders or asset seizure measures against criminal assets. Criminal reinvestments may also target whole business entities operating within the supply chain, from wholesale distribution to supermarkets and retailers. This strategy involves, if necessary, the use of violence against businesses resisting intimidation, and ultimately aims at creating monopolies in specific sectors to maximize profits and disrupt fair competition.

Over the last few years, the involvement of organized criminal groups in the agro-food sector has become more prominent and is commonly referred to as "agro-mafia". In Italy, where a strong agro-food sector stands alongside the consolidated presence of organized crime, the food fraud business has flourished since the early 2000s, with a constant increase in revenue lost to criminals. The potential health and safety consequences for unsuspecting consumers have prompted the European Union (EU) Member States to increase vigilance against criminal food fraud. In Germany – one of Italy's main trading partners – law enforcement authorities have confirmed the existence of a *modus operandi* of Italian "agro-mafia". This strategy operates by peddling counterfeit food to catering businesses in the German territory through a network of door-to-door sales agents. Similar criminal activities are also present in other countries.

From a broader perspective, the prevalence and success of this criminal *modus operandi* points at the emerging risk of criminals acquiring control and/or infiltrating the supply chain for mass-market food products – which are usually not a priority for law enforcement operations. In this respect, an issue of special concern is the online sale of counterfeit and substandard food products, which can easily escape detection. Since the market share of products bought via the World Wide Web is extensively growing, this has also attracted the interest of organized crime as an unmissable opportunity for profit. But while the electronic market provides cover for illegal activities, online activities will also usually leave traces which can be found and used during an investigation to monitor and trace the illegal acts.

In some cases, governments are also directly intervening to ensure the enforcement of IP-protected food and beverages across the Internet, as in the case of the activities performed in relation to Geographical Indications (GI) by the Italian Ministry of Agriculture and presented in the box below.

Department of central inspectorate for fraud repression and quality protection of agri-food products and foodstuffs (ICQRF)

The ICQRF developed a unique approach in relation to e-commerce, in view of protecting the intellectual property rights related to geographical indications. ICQRF conducts constant searches for relevant IP related products in online marketplaces and identifies what kind of infringements should be investigated (unlawful use of the registered name, false advertising, misuse, usurpation, imitation, evocation) in order to take further actions for the removal of products' offers.

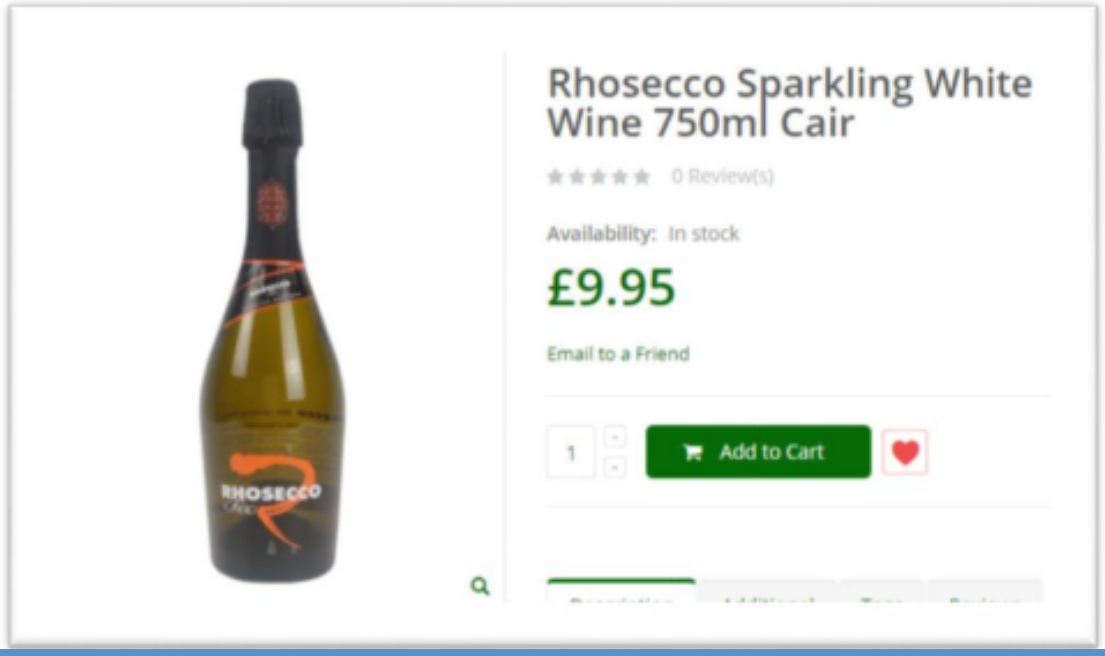
The protection of the geographical indication of the product is obtained through a model where ICQRF acts as the representative for the protection of GIs, enabling strong direct cooperation with the marketplaces. Cooperation is also achieved through the stipulation of memorandum of understanding (MoU) with marketplaces to allow quicker and more effective takedowns for offers related to products that are infringing GIs. In addition, there is further collaboration with other Member States to remove online content.

The activity has been performed over a number of years, and the following are some cases which show how GIs are infringed online and where ICQRF has operated.

Evocation of Parmigiano Reggiano DOP at ANUGA exhibition in Cologne (Germany)

Source: ICQRF Activity Report 2019

Sparkling white wine on tap sold on the web as Prosecco

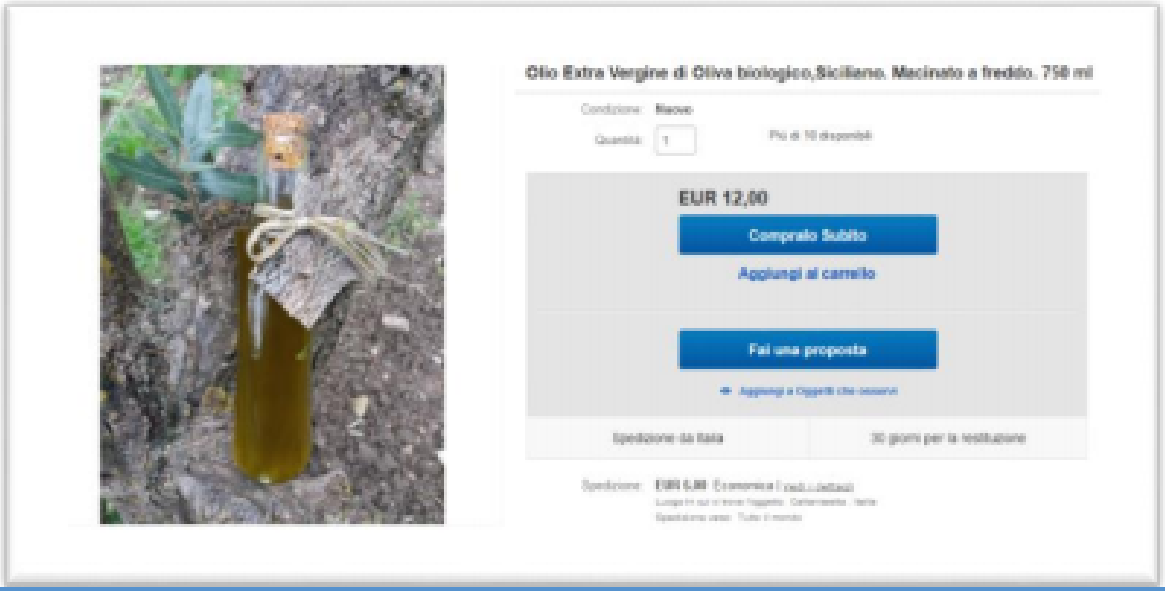


Source: ICQRF Activity Report 2019

White vinegar sold on the web as Aceto balsamico di Modena

Source: ICQRF Activity Report 2019

Evocation of PGI "Sicilia" for a generic extra virgin olive oil



Source: ICQRF Activity Report 2019

This section of the report describes three different risk scenarios related to agro-mafia, to show how organized crime can explore vulnerabilities in the food sector. The scenarios are dedicated respectively to the infiltration of the dairy supply chain, parallel market for catering supplies, and the criminal infiltration of online supermarket chains for home delivery of fake food. Subsequently, the report analyses possible technology-based solutions aimed at limiting risks highlighted by the scenarios.

2.1 Risk scenarios

Three risk scenarios have been elaborated in the area of agri-food mafia.

Risk Scenario 1: Infiltration of Dairy Supply Chain (milk and products made from or containing milk)

Always on the lookout for high profits at low risk, the ringleader of a well-structured organized crime group is operating in a country in which renowned vegetables are grown, and different types of cheese are produced. The criminal group intends to infiltrate the dairy supply chain. To do so, it develops and implements the following criminal business model:

Step 1. Control of the distribution market: the criminal group takes over numerous restaurants and supermarkets. By entering into contact with businesses facing economic difficulties, the criminal group offers loans at extremely high interest rates with violent terms of collection upon failure (loan sharking). When the owners are unable to pay back the loan, the criminal group entrusts their businesses to a network of frontmen with no criminal record. They are now under the control of organized crime.

Step 2. Control of the supply chain: the criminal group uses original packaging of the businesses it controls to market substandard and fraudulent products. Consumers are unaware of the change in ownership of the companies and continue to purchase their products.

Step 3. Copying local producers' design: a clandestine sweatshop (a small factory, in which workers are paid meagre amounts and work many hours in very bad conditions) is installed. The associates copy the design, packaging and trademark of well-known local producers. This step adds to the infiltration of substandard products into the supply chain highlighted in step 2.

Step 4. Procurement of low-level milk or dairy products: through its contacts with other criminal associates operating in the neighbouring countries, the criminal group obtains low-cost dairy products, produced under unsanitary conditions or with the use of contaminated raw milk. The criminal group packages the low-cost dairy products with falsified labels that imitate the design of legitimate and well-known local producers. This step will also allow the criminal group to pass the blame for unsafe products onto its legitimate competitors.

Step 5. Distribution of the falsified goods: the criminal group uses its comprehensive and well-structured network, which includes dozens of wholesalers and supermarkets controlled by its frontmen, to infiltrate the distribution of dairy products. As a result, counterfeit and substandard products are delivered to unsuspecting retailers.

After a year, the infiltration of the dairy supply chain allows the group to generate several million euros in illicit profits. The criminal group infringe the intellectual property rights of the country's legitimate dairy producers, while disrupting fair competition and reducing fiscal revenues. In the same period, the National Health Service reports an inexplicable surge in cases of food poisoning.

Risk Scenario 2: Parallel Market for Catering Supplies

The same criminal group, operating in the same territory, intends to increase its control over the legal economy and fully exploit the opportunities created by their grasp over licit businesses in the catering industry, by implementing the following business model:

Step 1. Control over legitimate businesses: use of loan sharking and violent intimidation against several businesses in the catering and hospitality sectors. When the owners are unable to pay back the loan, the group takes control of numerous producers and actors of the food supply chain, restaurants, and supermarkets as compensation. The criminal group entrusts them to a network of frontmen with no criminal record to ensure a pretence of legitimacy for its incoming funds.

Step 2. Control of the anti-counterfeiting solutions: with the acquisition of the producers and actors in the supply chain, the group gains access to anti-counterfeiting solutions that are used to authenticate selected foodstuffs and that are integrated into the businesses' production lines. They use the original packaging and the businesses' production lines to produce substandard and fraudulent products. Consumers are unaware of the change in ownership of the companies and continue to purchase their favourite products.

Step 3. Develop a fully-fledged supply chain for vegetables and dairy products: the group decides to scale up the operations beyond the domestic market, targeting catering businesses operating in a neighbouring State.

Step 4. Procurement of materials: low-priced farmland, located in areas with significant level of soil pollution, is acquired in the neighbouring State. Local people are illegally employed on these farms to grow a variety of vegetables. To increase the harvest and reduce costs, crops are sprayed with illegal pesticides. The criminal group also takes over a canning company to operate as a legitimate agro-food business and starts importing tomatoes from developing countries in the form of tomato high concentrate. The concentrate is diluted with water, canned by the company and then labelled as premium local produce. The operation is a cover-up for importing low quality tomato concentrate, canning it in the neighbouring country and giving the appearance that it originates from there.

Step 5. Building a parallel market for catering food supplies: the criminal groups dispatch its members to operate as sales agents in the neighbouring country. They rent light-duty trucks and load them with counterfeit foodstuffs, intended for restaurants and grocery stores, promoting the local premium food and cuisine.

Step 6. Distortion of competition: the criminal group fixes the prices of its products, which are considerably lower than the goods of its local competitors in the neighbouring State, while customers are offered discounts up to 30 to 50% less than the price for authentic goods sold on the domestic market. Many grocers are attracted by the offer, which appears to be coming from a reputable holding based in the country. Grocers are thus forced to choose between giving up their former suppliers to match their competitors' prices or fighting the price war and being driven out of the market.

By disregarding food safety standards, the criminal group puts the safety of consumers at risk by peddling hazardous and substandard products. Moreover, the rental of transport vehicles shelters the criminal group from asset seizures, makes police investigations harder and ensures the resilience of the distribution network. The criminal business model proves highly successful. After the first year, the revenues from the exportation of counterfeit and substandard food are already exceeding profits from domestic sales.

Through a mixture of pressures and implicit threats against uncooperative grocers, the group consolidates its position in both its local and the neighbouring State's catering market, supplying thousands of unsuspecting customers through a parallel supply chain and thus generating millions of euros per year in profits. Over the months, a sudden wave of food poisoning cases starts affecting both countries.

Risk Scenario 3: E-commerce: Criminal Infiltration of Online Supermarket Chains for Home Delivery of Fake Food

The same country of the previous scenarios has become the leading country in e-commerce. In its largest cities, nearly 50% of the total supermarket food supply is covered by the food e-market, 70% of this is via on-demand delivery. The expansion of e-commerce has attracted the attention of criminal groups, some of which have successfully hacked e-commerce platforms and stolen the personal data of customers, including credit card numbers. Always on the lookout for high profits at low risk, the ringleader of an organized crime group that operates in the most populated cities of the country, infiltrated the e-market of car parts and now plans to extend his operations to the selling of fraudulent food online.

In order to achieve this goal, the criminal group implemented the following criminal business model:

Step 7. Control of legitimate e-operators: through one of the companies that it partially controls, the criminal group infiltrates two popular e-supermarkets which fall under its control. The well-established reputation of these two e-supermarkets will help the group to gain competitive advantage in the e-market of food, given that customers are becoming increasingly concerned by the risk of online fraud, especially with the smaller online shops.

Step 8. Selling fraudulent food as genuine: the criminal group uses the e-supermarkets to sell fraudulent products. First, it copies the design, packaging and trademark of well-known producers. Then it replaces the authentic products with low-cost products that disregard any food safety standards; or with food products that have expired or nearly expired.

Step 9. Expansion of e-commerce market: the criminal group develops a Super E-food app, which is encrypted to the highest level. Customers believe that the app (awarded with the Invincible App Certificate) will protect them from online fraud. Unbeknownst to them, they use a secure app to purchase fraudulent food.

Step 10. Creation of dedicated social network groups/pages: the group creates dedicated pages and groups on social media to promote and sell their products, leveraging on the reputation of the acquired e-supermarkets.

In one year, the infiltration of the e-food sector reached a market share of nearly 5%, 10% of the sales are related to fraudulent food and they generate profits of several million euros. In the same period, a sudden wave of food poisoning cases starts affecting the country.

2.2 Supply Chain Security Solutions to address the risk scenarios

This part of the report presents possible solutions to the challenges posed by the three risk scenarios described in the previous section. It describes the main aspects of the technology submissions, their relevance to the risk scenarios and possible advantages and limitations.

Advantages and limitations in the use of supply chain security technology are also discussed in this section. They usually refer to the technology categories in general (authentication and track and trace). However, in some cases, reference will be made to some of the specific submissions we received; this will be done solely in view of providing a specific example of technology application.

The issue of supply chain security in the area of food fraud is fundamentally framed by the notion that these traded products are consumed by humans, posing a significant threat to human health and safety and the existing food system. Security in the food supply chain is widely based on overt and covert security authentication solutions, that are incorporated into layered protection systems, which incorporate additional levels of security such as traceability mechanisms and sample testing.

In general terms, by analysing the various submissions received, it can be observed that technology solutions applied to combat supply chain related threats have been developed to be flexible and easily adaptable to different products and various stages of the supply chain. Available technology options can be integrated to enhance the protection of the production and distribution process, especially since technology can be adapted to multiple approaches such as the authentication of the package, the monitoring of the product through the supply chain, the chemical composition of the goods, or the combination of several techniques.

Several available technology options are based on tagging or modifying the package by using stamps, seals or labels that are attached to the products and that are usually tamper evident. The authentication technology can also be embedded in the material, in microtaggants or nano-structured security features such as holograms and codes, which make the solution non-removable. The information to validate the authenticity of the product is frequently read with machines developed to specifically perform this task and work in combination with the authentication and track and trace technology. The codification and decodification of the data that is saved in the product provides stakeholders of the supply chain with a secure mechanism to corroborate the authenticity of the merchandise.

Moreover, if the stamps or labels are part of an overt solution, consumers may have a tool at their disposal to corroborate that the product bought is authentic.

After further studying the potential benefit of authentication and track and trace technology to limit the risks highlighted by the scenarios, the following was confirmed. The first element to be considered, which is also confirmed by the submissions we received, is that in order to be effective, technology solutions aimed at protecting the supply chain are nowadays combining secure authentication of the product with secure track and trace along the supply chain. Even if operating in different ways, all the submissions we received showed ways in which specific threats presented by the risk scenarios can be addressed. These include:

- repacking operations and substitution of original products with counterfeits,
- the creation of clandestine sweatshops and production centres,
- the lack of full monitoring and data exchange in the supply chain,
- the lack of control over the distribution of the product, and
- the fact that consumers may be unaware of buying a fraudulent product.

These results are achieved thanks to the creation of a strong and unique digital identity for each product which usually serves a double purpose: 1) it permits the product's authentication; and once included into a dedicated database, 2) it can be used as the unique identifier thanks to which the product itself can be tracked and traced along the supply chain.

Secure authentication and track and trace technology present a series of interesting features that show promise in relation to the limitation of risks highlighted in the scenarios.

In particular, all the submissions we received included the following interesting features:

Clear identification: Overt authentication solutions can be designed to be easily identified by individuals when using their senses, this includes by consumers. The physical characteristics that can be added to the package or the product provide a mechanism to differentiate original from counterfeit goods.

Monitoring: Track and trace technology is used to monitor the product through the different processes in the supply chain, limiting diversion and infiltration possibilities. Traceability can be integrated with authentication solutions to provide an additional layer of security.

Customization possibilities: Codes, tags and labels can be widely modified to create unique and personalized options, showing great adaptability to products and surfaces. Customized codes, tags and labels can be harder to imitate since they are not widely available for a large range of products.

Codes are non-reproductible: Codes can hardly be reproduced without knowing the cryptographic key, this is essential to: authenticate the original product, monitor its movement along the supply chain and prevent infiltration of non-authenticated and non-original products.

Tamper-evident codes: Most solutions have tamper-evident mechanisms that facilitate the identification of any issue with the product, including easy spotting of manipulation attempts and/or infiltration of non-original products into the supply chain. A tamper-indicating device can also be used and is designed to leave non-erasable, unambiguous evidence of unauthorized access to packaging, facilitating the identification of any suspicious handling.

Codes can be easily read by consumers: Codes with encrypted information can be made to be machine-readable by smartphones and ubiquitous devices. In some options, validation is easy and fast and can be made offline.

Uniqueness of codes: Codes, labels and tags create an identity for every object or product. Furthermore, codes can usually be fully customized to imitate specific patterns and images, providing an additional unique characteristic to the code in view of avoiding its reproduction.

Large data storage: Available codes and tags can encode large amounts of information.

Adaptability: Authentication and track and trace can be adapted to different products and industries.

Non-intrusive: Identification of the product can be performed, without opening the package or testing the contents, through the use of scanners or special readers, in addition to tracking mechanisms that provide updated information about the status of the product in the supply chain without the need of physically checking the product.

Several submissions we received also use blockchain (or are ready to integrate this technology) for storing, securing and exchanging data used for authentication and track and trace purposes. The use of blockchain adds some interesting features to the ones presented above, in particular:

Immutability of data: The information about the product and its movement in the supply chain are recorded in the blockchain and cannot be modified. This is achieved through the ability of a blockchain ledger to remain unchanged, unaltered and indelible.

Auditability and accountability: Accountability is verified as a part of timestamps established by the blockchain system. This system allows every stakeholder to confirm whether the service operates in the intended way. If the product fails the verification process, then the stakeholders have proof of malicious behaviour which could be used to hold the responsible entity accountable.

Transparency: Blockchain technology allows stakeholders to monitor the supply chain with openness, communication, and accountability. The stakeholders included in the chain can access the information at any point to corroborate the status of the products and the processes.

Some common limitations to supply chain security technologies include:

- *Package-dependant*: Several solutions are implemented at the packaging-level. This means that, even if linked to a secure and immutable tracking system, the original food does not have an authentication option "in itself", therefore, the traceability begins at the first packaging point and is linked to the package, not the product. As we will see later on, some technology options are trying to steer away from this element, by adding certain information to the authentication on the chemical/organic/DNA composition of the food product.

- *Reproduction*: Overt solutions can be sufficiently replicated to trick the client, in the case in which he/she does not perform an authentication via scanning. If a specific code, seal, tag, or label is widely used, it is easier and cheaper to invest in the reproduction of the authentication solution. However, all the submissions we received are also based on covert and secure marking methods, coupled with additional layers of security. One of the submissions also presents the possibility of engraving the code directly on the packaging, a technology which would make its copying much more difficult.

- *Consumer education*: When consumers are given the possibility to perform a check on the authenticity of the product at the time of purchase, they need to be aware of the security measures applied to the product and of how to scan the code or tag to obtain the information. If the consumer has no information about the mechanism, then this specific part of the solution might not serve their objective.

- *Interoperability*: Achieving interoperability between the different systems can be a challenge. However, once the initial interoperability is achieved, it becomes an advantage since it allows the integration of the different systems used by the solution.

- *Data complexity*: The new flow of data requires personnel who are able to interpret the information that is received. Most options include tools that facilitate the interpretation of results through graphs and data simplification, yet in order to have a full analysis of all the information received, it is necessary to have specialized individuals.

We will now provide some practical examples using the submissions we received to show how the combination of all these elements can limit some of the risks highlighted by the scenarios. The use of the submissions will also allow us to appreciate the different approaches that can be followed to ensure supply chain security as well as some innovative and potentially interesting features that contributors include to better respond to the risks presented by the scenarios. Some of these features could already be implemented in the market while for others, additional research and development may be needed.

2.2.1 Product authentication and track and trace: unique visual identity

Technology submission 1

This submission focuses on the use of a machine-readable unique code and its subsequent coding, decoding and validation system. The solution is based on printing of stamps, seals or labels that are attached to the products and that are tamper evident. The authentication component of this technology is quite innovative, as it merges different elements to authenticate the product, namely a machine-readable 2D barcode (using symmetric and asymmetric cryptography), security holograms and glitter inks with unique patterns. The objective of the solution is to code information in a unique identifier that combines several layers of security measures by combining the physical characteristics of the product with a digital identity that is stored in a code that is fully customizable and adaptable to any product. The code is readable via a mobile app, enabling authorities, stakeholders and customers to read the code at any point. Coded information can be performed via several layers of security, such as private, public and encrypted. The code can be hidden in the aesthetics of the design and has high capacity to store a great amount of information.

One of the most interesting aspects of this option relates to the creation of a unique visual identity of the product to be authenticated and then tracked and traced. The code provided by this solution is composed of a graphic and a physical component. The graphic code is the printed part of the solution (a bidimensional code composed of cells that can be filled with a grid of pixels) and is designed to be validated by using images acquired by most cameras. Additionally, the presence of a hologram increases the security of this code by providing a specific optically variable response to improve visual identity, with design features and a geometric description that are unique for the specific hologram cut. This is the physical part of the code. By having the graphic code and the hologram working together, the test of authenticity of the visual identity can be improved through a cross validation between the graphic code and the hologram. The random-generated geometric coordinates of the hologram can be coded in the graphic code part. After this, they are photographed and registered at the production line, linking the physical product to their digital identity. The unique random position of the hologram is almost impossible to reproduce, and its validation can be made offline.

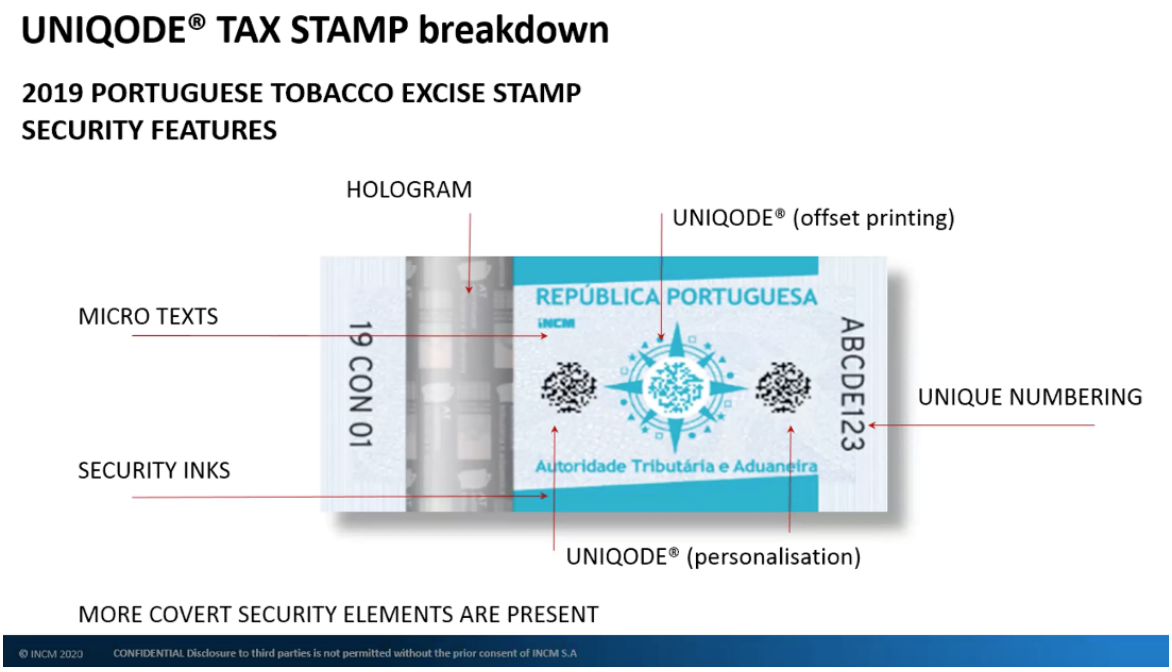
In a nutshell, the complete authentication solution can be divided into different security layers: 1) the printed-graphic code, 2) holographic Optical Variable Devices (OVD), and 3) the glitter inks; all which have a unique and irreproducible pattern.

Furthermore, glitter-ink patterns unique to each code can also be used for authentication purposes and as unique product identifiers due to their physical unclonable function (PUF). Glitter inks produce a random permanent pattern when printed. It is a printing process defined as “chaotic” and guarantees a unique pattern each time it is produced. The brightness of glitter particles provides an additional mechanism to prevent the reproduction of the authentication method since each particle reflects light in a specific direction. This unique characteristic of a printed pattern with glitter inks is unclonable and irreproducible. Validation of this complex visual identity can be performed by means of an app that identifies all the parts, decodes and validates them. The decodification can also be performed through a mobile app while offline. During the validation process through the app, several elements are analysed, such as: the stamp structure and colour, the graphic code reading, the hologram features and colour shifting, the Unique Identifier (UID) registration, the brand, the producer, and the stamp activation time. The system has capabilities to be used as a track and trace (T&T) framework, either implementing one or being integrated with an external T&T. It is also possible to integrate blockchain technology.

In addition to this, INCM is currently conducting a project which endeavours to validate the integrity of wine already bottled by analysing its composition without the need to open the wine bottles. This idea can be also applied to other already packed food and beverages. This project would be a complement to the existing UniQode technology, developed and patented by INCM, that is able to authenticate the packaging.

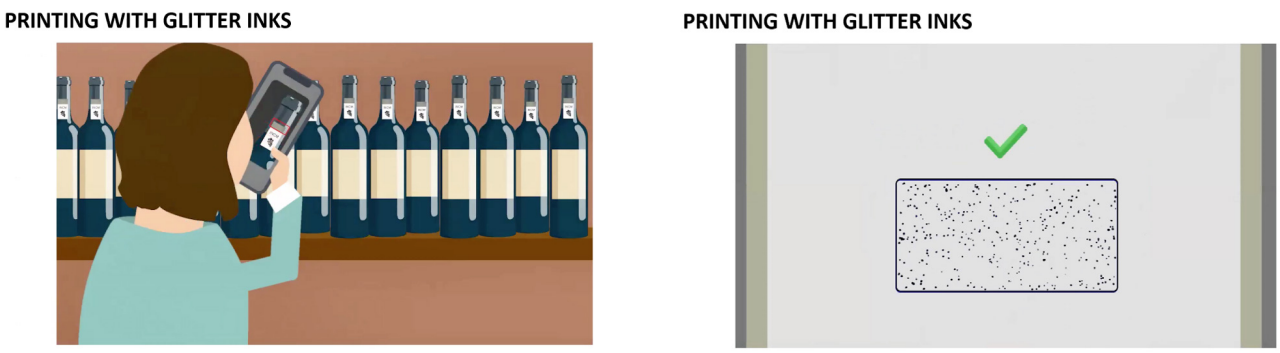
Submission received from INCM – Portuguese Mint and Official Printing Office

This submission presents several interesting features, and these elements together are used to increase the security of objects, products or services, helping in their traceability and in the identification of counterfeiting activities and criminal infiltrations in the supply chain. Furthermore, for what concerns the clear identification of the code, this solution offers multiple options, as the use of: 1) a printed-graphic code, 2) a holographic OVD, and 3) glitter inks, are combined to provide different layers of security. The codes can be shaped into different icons, depending on the product. The labels can be fully customized to fit the needs of the producer. They contain a unique sequence of codes and data that provide specific information about the individual product.



Source: INCM

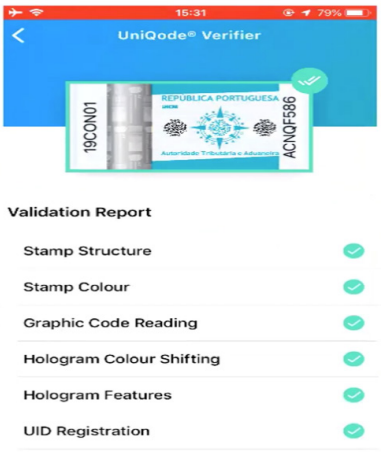
The use of a dedicated app also shows how monitoring can be done in practice, since the app provides information that is taken directly from the traceability system, such as the origin and time/location stamp. The app would recognize if the product was manipulated, generating a red cross when scanning the code. This is useful for tamper-evident purposes, while this kind of monitoring is not intrusive.



Source: INCM

This submission allows us to discuss how authentication and track and trace technology in general can target some of the issues identified in the three risk scenarios related to food fraud. In order to prevent the copy of designs and the repacking operations and the sale of fraudulent food as genuine, the adoption of authentication options like codes, tags, labels or seals offer a set of tools that provide an initial security layer. The tamper-evident solutions and the unique identifiers also aim at minimizing the possibility of having counterfeit products in the market. The overt and covert options allow the stakeholders and the clients to recognize original products, especially to avoid the possibility that consumers are unaware of fraudulent purchases.

The use of traceability systems not only provides an additional layer of security, but it also targets other issues presented in the scenarios, such as the distribution of the falsified goods, the use of clandestine sweatshops and production centres, and the lack of full monitoring and control of the production and distribution chains. The track and trace solutions enable the monitoring of the processes involved in the supply chain, granting visibility to identify illicit activities related to the deviation of the products from the supply chain or unauthorized insertions into it.



Source: INCM

In particular, for what concerns **risk scenario 1** (infiltration of the dairy supply chain), the described technology can support a risk reduction in several steps of the criminal business model. In particular, risk is reduced thanks to the use of non-replicable codes that are recognizable both visually and via the use of specific tools. As seen before, these codes create the visual identity of each product and contain various technologies whose combinations create the uniqueness of each product identity and renders its duplication extremely difficult. In many cases the replication of these codes, even if possible, in theory, would involve a great investment from organized criminals, limiting their business case. In addition, the replication would only be visual; the mobile app would not read the non-original code. Furthermore, the visual identity is used to track and trace the product along the distribution chain, in effect securing the existing legitimate supply chain from infiltration of products that are not recognized at one of the various control stages of the distribution.

This can limit risks related to the following steps of the criminal plan:

- Copying of local producers' packaging design by using sweatshops and subsequent infiltration of these products into the legitimate supply chain.
- Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.
- Distribution of the falsified goods via the criminal group's comprehensive and well- structured network, which includes dozens of wholesalers and supermarkets controlled by their frontmen, to infiltrate the distribution of dairy products and deliver them to unsuspecting retailers.

In **risk scenario 1**, some steps of the criminal plan are still difficult to limit, in particular step 2) control of the supply chain by using original packaging of the businesses which fell under the control of organized crime and step 1) on the acquisition of criminal control over sectors of the legal economy. The technology proposed partly mitigates the distribution of the falsified goods via the criminal group's comprehensive network since, in the case in which the whole supply chain is controlled by organized crime, it can provide a check point for stakeholders or consumers only at the ultimate point of sale.

The difficulty for supply chain security technology to limit these risks is valid for the majority of the submissions received.

For what concerns **risk scenario 2** (parallel market for catering supplies) the same considerations presented for risk scenario 1 also apply in this case. The combination of authentication via a strong digital identity with track and trace technology, can limit the following steps of the criminal plan:

- Building a parallel market for catering food supplies.
- Develop a fully-fledged supply chain for vegetables and dairy products.

With reference to step 3 "Develop a fully-fledged supply chain for vegetables and dairy products" and step 5 "Building a parallel market for catering food supplies", if shops also use technology to perform a final check of products they receive and then sell to the final customer, then infiltration of unauthorized goods at final selling points is made much more difficult. Of course, in this case technology also relies on the honesty of final sellers and does not apply to those cases in which the criminal group controls these shops. In this case, the possibility given to consumers to check the products they buy could assist in making the distribution more secure.

Also, for risk scenario 2, the same steps identified for risk scenario 1 cannot be mitigated by the use of supply chain security technology. Once again, this is common to many submissions.

For what concerns **risk scenario 3** (e-commerce: criminal infiltration of online supermarket chains for home delivery of fake food), this submission can partly support securing online markets, especially considering that, also in the food sector, products will have a physical distribution component and they will necessarily pass through a series of distribution elements. Securing these elements could be the key to limit some of the steps of the criminal plan highlighted in this scenario, especially:

- Selling fraudulent food as genuine via the control of well-known e-supermarkets and by copying the design, packaging and trademark of well-known producers.

The same considerations presented for the previous risk scenarios apply in this case, in relation to the mitigating effect on this step that can be created by the combination of authentication via a strong digital and physical identity with track and trace technology. Considerations of the role of consumers also apply in this case and are possibly even more relevant, since online purchases may involve a direct relationship and line of shipping from the seller to the purchaser.

Also, in the case of risk scenario 3, other technological resources should be used to mitigate other steps of the criminal plan, which cannot be limited through supply chain security technology.

As seen in the case of risk scenarios 1 and 2, this corresponds with the majority of the submissions received.

Summary table submission 1: possible application to limit risks highlighted by the scenarios

Scenario	Applicability of the solution
Scenario 1: *Infiltration of the dairy supply chain*	
Step 1 – Control of the distribution market by owning or controlling legitimate operators.	
Step 2 – Control of the supply chain using the technology owned by the controlled legitimate operators.	
Step 3 – Copying local producers' packaging design and subsequent infiltration of these products into the legitimate supply chain.	Risk is reduced thanks to the use of non-replicable codes that are recognizable both visually and via the use of specific tools and, by using track and trace technology to secure the supply chain. The identity of each product is created by using a unique tamper-evident code merging a graphic and a physical component. Furthermore, the graphic and the physical part of the code can also cross-validate for increased security. The flows of products along the supply chain can be checked using an app, giving consumers the possibility of performing an offline check.
Step 4 – Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.	The technology solution offers a combination of a graphic code and a hologram as verification of authenticity. The code is easily readable, moreover, a falsified label would not be read by the app if the stakeholders or customers attempt to scan it. The risk of insertion of counterfeit products into the supply chain is reduced with the use of track and trace technology.
Step 5 – Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.	If the whole supply chain is controlled by organized crime, then only checks performed at the ultimate point of sale or performed by consumers could spot the illicit product.

Scenario	Applicability of the solution
Scenario 1: *Infiltration of the dairy supply chain*	
Step 1 – Control of the distribution market by owning or controlling legitimate operators.	
Step 2 – Control of the supply chain using the technology owned by the controlled legitimate operators.	

Scenario	Applicability of the solution
Scenario 1: *Infiltration of the dairy supply chain*	
Step 1 – Control of the distribution market by owning or controlling legitimate operators.	
Step 2 – Control of the supply chain using the technology owned by the controlled legitimate operators.	
Step 3 – Copying local producers' packaging design and subsequent infiltration of these products into the legitimate supply chain.	Risk is reduced thanks to the use of non-replicable codes that are recognizable both visually and via the use of specific tools and, by using track and trace technology to secure the supply chain. The identity of each product is created by using a unique tamper-evident code merging a graphic and a physical component. Furthermore, the graphic and the physical part of the code can also cross-validate for increased security. The flows of products along the supply chain can be checked using an app, giving consumers the possibility of performing an offline check.
Step 4 – Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.	The technology solution offers a combination of a graphic code and a hologram as verification of authenticity. The code is easily readable, moreover, a falsified label would not be read by the app if the stakeholders or customers attempt to scan it. The risk of insertion of counterfeit products into the supply chain is reduced with the use of track and trace technology.
Step 5 – Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.	If the whole supply chain is controlled by organized crime, then only checks performed at the ultimate point of sale or performed by consumers could spot the illicit product.
Step 6 – Distortion of competition.	If the supply chain is secured, then in that specific market criminals may find it more difficult to implement their criminal plan and distort competition. This can be seen as a by-product of the implementation of the technology.
Scenario 3: *E-commerce: criminal infiltration of online supermarket chains for home delivery of fake food*	
Step 1 – Control of legitimate e-operators.	
Step 2 – Selling fraudulent food as genuine through the controlled e-supermarkets.	If the whole online supply chain is controlled by organized crime, and since the e-supermarkets sell directly to the final consumer, then only checks performed by the latter could spot the illicit product.
Step 3 – Expansion of e-commerce market through the creation of a Super E-food app.	
Step 4 – Creation of dedicated social network groups/pages to sell fraudulent products to final customers.	

2.2.2 Using metameric inks

Technology submission 2

This submission can be described as a food packaging authentication system based on security inks and Information and Communications Technologies (ICT). In particular, it uses metameric, invisible or other types of security inks that give a digital identity to each item that needs to be authenticated by the customer. These create a hidden graphical code that is readable through a digital algorithm (using a mobile phone camera, for instance). These hidden codes can be applied using the standard printing technology of a production/packaging company, facilitating the implementation of the solution.

Metameric inks combine two colours that match under certain lighting conditions, allowing the possibility to show features that are not visible in other conditions. For instance, a certain illumination by a lighting tool or the use of a colour filter can show the appearance of a number on a label using metameric inks. The same number would not be visible in different lighting conditions or without the colour filter. The use of metameric inks for the creation of the product's digital identity can potentially allow for a more secure management of distribution logistics throughout the supply chain. On the other hand, invisible inks combine components to produce a fluid that is transparent and invisible to the naked eye, but visible under certain operating conditions.

The metameric inks and invisible inks are applied on the food packaging to uniquely encode the product and work in combination with other tools, in particular: 1) a smart phone app equipped with a specific algorithm for the digital decoding of the hidden printed code, 2) a web-based interface for the management of information connected with the production in the supply chain, and 3) ICT communication infrastructure for product authentication.

One of the important benefits of this technology submission lies in the combination of all these elements and in the way in which the unique digital identity of the product is created. Another technology option that can be used in authentication is microtaggants. A taggant refers to a chemical or physical marker added to materials to enable various forms of testing. Physical taggants are highly variable but are typically microscopic in size, included at low levels, and simple to detect. The use of microtaggants allows for the creation of a potentially unlimited number of codes while, according to the submission received, their use would also be economical, especially if the tagging is performed on bulk products and if the existing printing infrastructure can be used to adopt the technology.

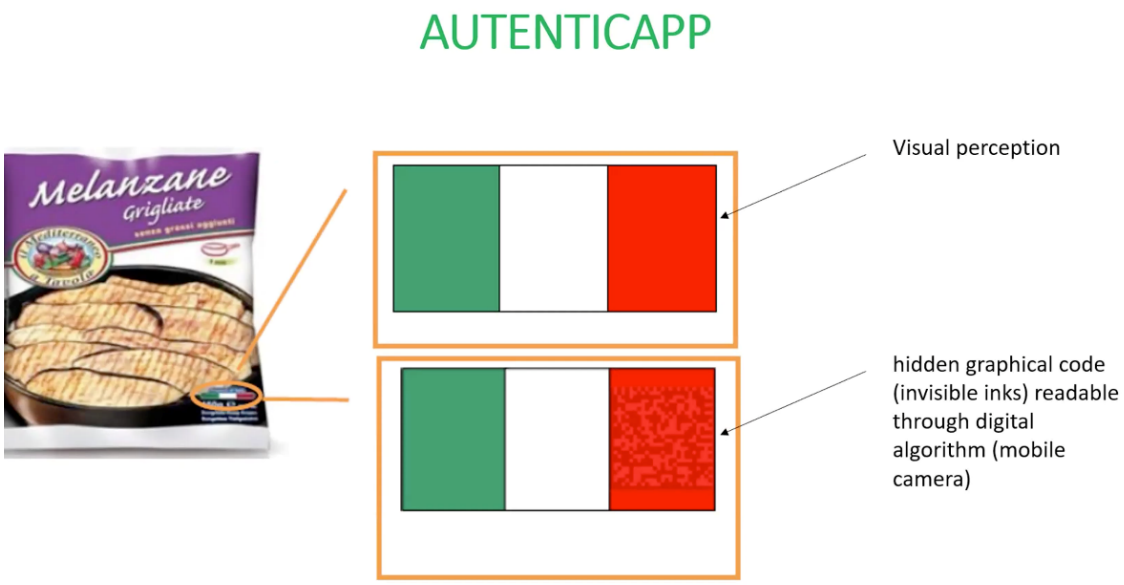
Submission received from Tecnoalimenti

This submission presents all the interesting features previously highlighted and can be used to show a different way in which secure coding can be achieved, in particular through the use of metameric inks. The code is coupled with a secure track and trace system which also uses an app to monitor the movement of products along the supply chain and for their authentication.

For what concerns covert identification, the solution offers a clear identification method through the use of metameric inks – where two colours matching under one set of lighting conditions can make the identification element appear and look quite different under another set – and of invisible inks. However, in these cases the customer needs to know in advance how to find and decode the hidden code. The codes can be adapted to different shapes and designs, making them easy to hide.

The use of metameric inks is important for the security of this option. First of all, it renders the codes difficult to imitate, since a special pigment series is needed to produce them. In addition, they have good durability, and after a certain period of time, the colour development characteristics will not change or become affected by outside factors. Additionally, since the metameric inks are invisible and printed directly on the package, they cannot be removed from the packaging.

This technology option encodes each product, only allowing decodification by using the specific app. The app validates the product by displaying a green tick box on the screen if it is authentic.



Source: Tecnoalimenti

For what concerns the application to the risk scenarios, the results are very similar to what was described for Submission 1. Since each submission can be read as a standalone example, we will repeat the findings.

The technology solution targets some of the issues identified in the three risk scenarios related to food fraud. The implementation of this option would help to prevent the copy of designs as well as unauthorized repacking operations and the sale of fraudulent food as genuine. This can be achieved through the adoption of authentication options (like codes or inks) that can be easily verified by a scanner. Furthermore, the possibility to scan and authenticate the codes via a smartphone app creates the possibility for consumers to check their purchases.

Regarding the threats presented in **risk scenario 1** (infiltration of dairy supply chain), the technology option can support a risk reduction for several steps of the criminal business model. In particular, risk is reduced thanks to the use of non-replicable codes that are recognizable by using the mobile app. As seen before, these inks create a specific visual identity for each product, while the use of encoded characteristics that are revealed by a customized app builds an extra security layer. This can limit risks related to the following steps of the criminal plan:

- Copying local producers' packaging design by using sweatshops and subsequent infiltration of these products into the legitimate supply chain.
- Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.
- Distribution of the falsified goods via the criminal group's comprehensive and well- structured network, which includes dozens of wholesalers and supermarkets controlled by their frontmen, to infiltrate the distribution of dairy products and deliver them to unsuspecting retailers.

The points mentioned in the previous submission related to **risk scenario 1** also apply to this submission. Some steps are still difficult to limit, especially: 1) Control of the distribution market by owning or controlling legitimate operators, 2) Control of the supply chain by using original packaging of the businesses which fell under the control of organized crime. To a certain extent, these considerations also apply to step 5) Distribution of the falsified goods via the criminal group comprehensive and well-structured network, which is difficult to be limited in its entirety.

For what concerns **risk scenario 2** (parallel market for catering supplies) the same considerations presented for risk scenario 1 apply. The authentication via a strong digital identity can limit the following steps of the criminal plan:

- Building a parallel market for catering food supplies.
- Develop a fully-fledged supply chain for vegetables and dairy products.

For these steps, the considerations listed in the previous submission apply. The technology can be used by shop owners to perform a final check before selling them to customers to minimize the risk of infiltration, however, it cannot prevent infiltration in cases where criminal groups control these shops. The client is also able to scan the code of the product to do a final verification of its authenticity.

Also, for risk scenario 2, the steps of the criminal plan identified for risk scenario 1 cannot be mitigated by the use of supply chain security technology. In addition to those threats, the use of low quality and diluted materials and the distortion of competition are issues that would remain as threats.

For what concerns **risk scenario 3** (e-commerce: criminal infiltration of online supermarket chains for home delivery of fake food), the technology can be used to protect the physical distribution of products. Securing these elements could be the key to limit risks highlighted in this risk scenario, especially the following step:

- Selling fraudulent food as genuine via the control of well-known e-supermarkets and by copying the design, packaging and trademark of well-known producers.

The same considerations presented for the previous risk scenarios apply in this case, in relation to the mitigating effect on this step that can be created by the combination of authentication via a strong digital identity with track and trace technology. The role of consumers is relevant since online purchases may involve a direct relationship and line of shipping from the seller to the purchaser.

As also seen in the case of the previous submission, the other steps of the criminal plan are more difficult to limit.

Summary table for submission 2: possible application to limit risks highlighted by the scenarios

Scenario	Applicability of the solution
Scenario 1: *Infiltration of the dairy supply chain*	
Step 1 – Control of the distribution market by owning or controlling legitimate operators.	
Step 2 – Control of the supply chain using the technology owned by the controlled legitimate operators.	
Step 3 – Copying local producers' packaging design and subsequent infiltration of these products into the legitimate supply chain.	The metameric and invisible inks provide an authentication method that differentiate the original products from counterfeit ones. Furthermore, the app allows the customer to scan the package of the product in order to corroborate that it is an original.

Step 4 – Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.	The use of invisible inks and hidden codes on the food package protect the original product by providing an authentication method that can be used by both stakeholders and customers. A falsified label, even if it included a copy of a code, would not be read by the app.
Step 5 – Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.	If the whole supply chain is controlled by organized crime, then only checks performed at the ultimate point of sale or performed by consumers could spot the illicit product. The scanning app provides an easy tool for customers to check the product before consuming. However, if the original product is altered or replaced by using the original package at some point in the supply chain, it would not be possible to corroborate that the product inside the package is authentic.
Scenario 2: *Parallel market for catering supplies*	
Step 1 – Control over legitimate businesses.	
Step 2 – Control of the anti-counterfeiting solutions used by the infiltrated businesses.	
Step 3 – Develop a fully-fledged supply chain for vegetables and dairy products.	As seen in other submissions, only if the criminal supply chain attempts to infiltrate the legitimate one at a certain stage. The same considerations explained in step 5 of scenario 1 apply.
Step 4 – Use of low quality and diluted materials.	The solution targets the packaging and not the food itself. It comes into play at the first packaging point. Consequently, criminals capable of infiltrating companies working at the production level can package fraudulent goods using original packaging.
Step 5 – Building a parallel market for catering food supplies targeting small shops.	The risk is mitigated thanks to the use of non-replicable codes that are scanned with the mobile app to corroborate the authenticity of the product. However, small shops and consumers must have the knowledge of the authentication measures and how to use the mobile app to read the code.
Step 6 – Distortion of competition.	If the supply chain is secured, then in that specific market criminals may find it more difficult to implement their criminal plan and distort competition. This can be seen as a by-product of the implementation of the technology.
Scenario 3: *E-commerce: criminal infiltration of online supermarket chains for home delivery of fake food*	
Step 1 – Control of legitimate e-operators.	
Step 2 – Selling fraudulent food as genuine through the controlled e-supermarkets.	If the whole online supply chain is controlled by organized crime, and since the e-supermarkets sell directly to the final consumer, then only validation through the scanning of codes performed by the latter could spot the illicit product.

Step 3 – Expansion of e-commerce market through the creation of a Super E-food app.	
Step 4 – Creation of dedicated social network groups/pages to sell fraudulent products to final customers.	

2.2.3 Focus on labels – the "all in one label"

Technology submission 3

One of the submissions received combines the initial unique identification of the product with a traceability system that is protected by blockchain technology. Multilayer security is presented as a combination of authentication, tamper evidence and digital security.

In the specific case of food traded online, this multilayer security technology starts at the basic protection element, using VOID labels for packaging. A VOID label is type of security label that is designed to indicate that a label has been tampered with by displaying a "VOID" message on the substrate (total transfer), on the back of the label (non-transfer), or both (partial transfer) when the label is removed. These seals can use covert, overt or semi-covert authentication and anti-tampering technology and can consequently also be used to create the digital identity of the product in the track and trace database to follow its movements along the supply chain. There is a wide range of proprietary VOID effects that can be applied, for example, three-colour VOID, integrated micro texts, variable codes, VOID effects visible on light and dark backgrounds. With transparent VOID tapes, underlying texts remain legible. If no transparency is required, a VOID effect can also be created from a multi-coloured image.

These labels are also "consumer friendly", since the VOID effect reveals a previously invisible, irreversible pattern as soon as the tape is removed or peeled off. VOID labels for packaging can be customized for each customer.

In the case in which food is packaged in reusable packaging, returned by the consumer, this submission takes into consideration that there will be specific issues to solve. The standard VOID label with different security features could not be used in this case, since it would be difficult to remove from the packaging in view of its new use. For this reason, the submission is proposing to use a special dry-peel VOID that has been developed. This label is a 2-layer construction, allowing both identification of tampering and reusability of packaging after usage. When an attempt is made to remove the label, a VOID effect is triggered between two layers. The bottom layer of the label remains on the returnable packaging. The bottom layer can be removed without leaving residues, since if the label is peeled off again, a security punch is triggered, and the label is destroyed into individual parts. In case of legitimate reuse of the packaging, the supply chain operator will affix a new VOID label while in the case of criminal manipulation, the label will be destroyed and further actors of the supply chain, including consumers, will be alerted by its absence. As in the case of the traditional VOID labels, these dry-peel labels can also be equipped with different authentication measures that allow each of them to have its own ID and consequently to be followed and checked along the supply chain.

In addition to the physical product security, a dry-peel VOID can be equipped with serialised ID and a related traceability function. That means that each label has its own ID and can be managed and tracked individually. The main features include the online authentication of each code, personalisation at item level, creating response pages driven by algorithms, GEO tracking with full track and trace for the entire supply chain and global distribution chain, management of packaging aggregation, consumer engagement. The solution can be divided into:

1) Security labels with tamper evidence and unique codes (serialization),

2) Real-time monitoring of traceability, inventories and distributors,

3) Individual content for the end-users and supply chain stakeholders in the user's language,

4) Business data analytics and measures.

In addition, all information is protected with blockchain technology.

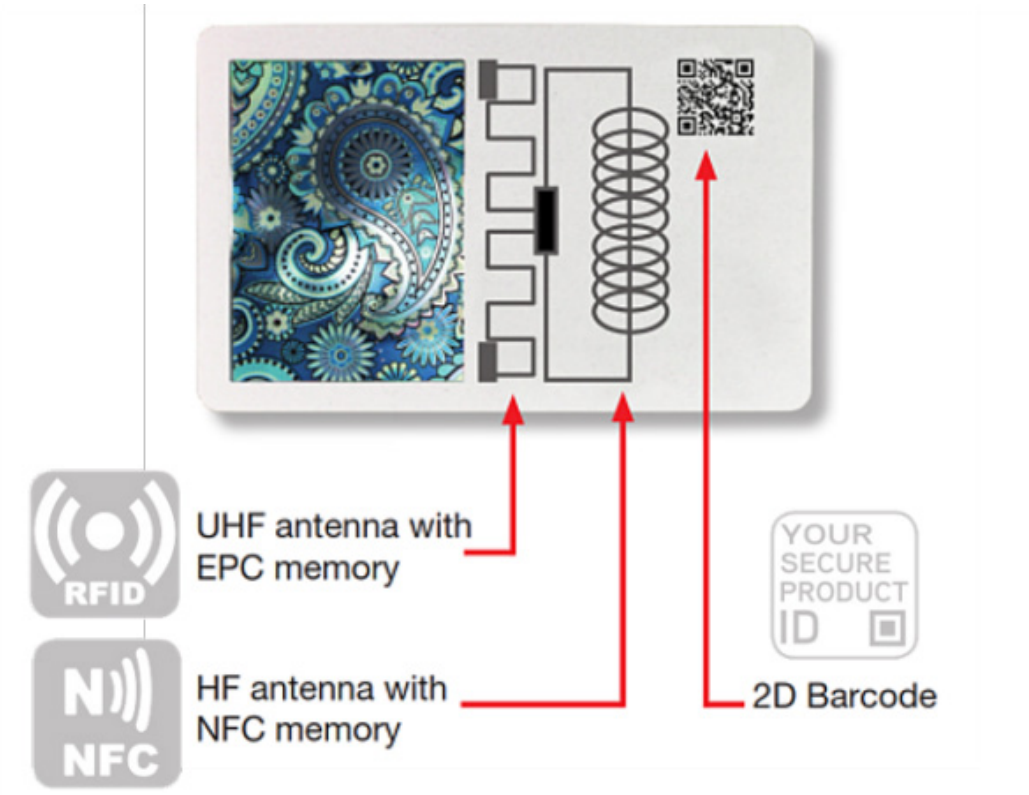
In the case in which they are equipped with QR codes, consumers also have the possibility of scanning the labels via the usual smartphone apps. RFID can also be used for the purpose of creating the product ID and then tracking and tracing it. This proposal uses both NFC and Ultra High Frequency (UHF) RFID types. The first also allows consumers to check the product, since many smartphones nowadays are equipped with NFC. UHF, on the other hand, supports long range reading of multiple labels/products at a time and is used for inspection purposes. The label proposed by this submission can combine both types of RFID at the same time.

Submission received from Securikett

This submission can be used as an example of multilayer security achieved through the combination of several elements. Starting from basic elements of securing the original product, this submission focuses on involving all actors of the supply chain, including those responsible for final delivery to consumers as well as consumers themselves. Given this aim, some of the authentication technology also needs to be easily readable and usable by consumers, while for other actors of the supply chain, more complex technological solutions can be used, including overt, covert and semi-covert security features. Apart from the relevant features already analysed in the introduction to this section of the report, the interesting elements of this technology can be found in its complex label, combined with the use of blockchain and business data analytics. The label, in particular, is capable of integrating VOID tamper-evident features which can also be applied to package that will be recycled and which also include RFID technology for verification by consumers. The labels can be fully customized to fit the needs of the producer. The different authentication options available can be modified to create a unique label or VOID tape for a specific producer.

Customization of the VOID labels is also possible. This is a very important step since using generic VOID labels that can also be purchased online greatly reduces security. It would be sufficient for a malicious actor in the supply chain that wants to infiltrate counterfeit products to open the packaging, remove the old generic VOID label, insert the counterfeit product in the original packaging, and then use a new generic VOID label of the same type.

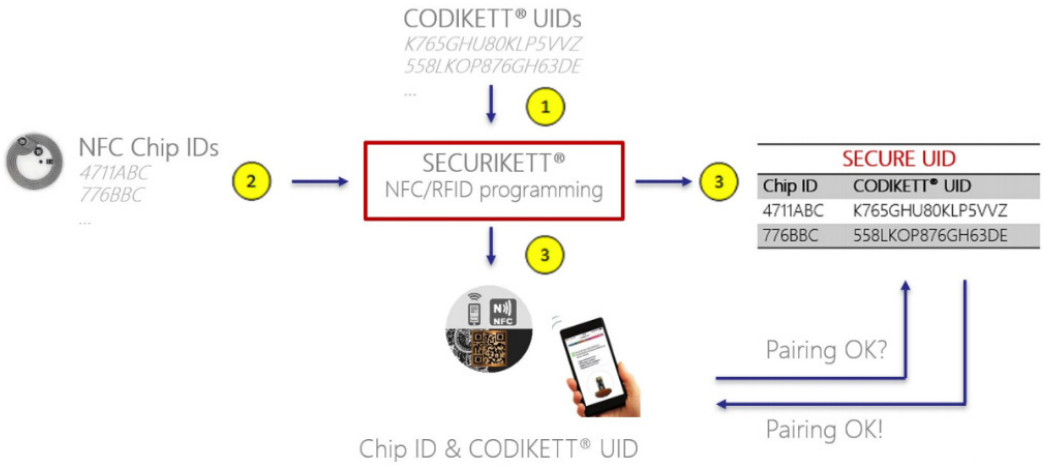
This results in different options which are available for identification purposes as well as in the possibility to combine them to provide different layers of security. These options include different and customizable VOID tapes, dry-peel VOID as a 2-layer construction for reusable packages, QR code or human readable code, RFID (NFC) technology, and an All-in-One label, consisting of secure ID, RFID (NFC) and RFID (UHF) in one.



Source: Securikett

Apart from the use of VOID labels for tamper evidence, this submission also shows the possibility of using tamper-indicating devices, which are designed to leave non-erasable, unambiguous evidence of unauthorized access to packaging, facilitating the identification of any suspicious handling. When the code is scanned by the client or the stakeholders in the supply chain, a response page is opened to identify if the product was manipulated, displaying a green or red text with a clear message that indicates if the product was open.

Two further elements need to be highlighted: the possibility to use geo-tracking as well as data analytics features. These features enable the identification of the current physical location of the product by obtaining GPS data from using smartphones or other GPS-enabled devices. This characteristic is combined with a full track and trace for the entire supply chain. Data can also be used to analyse the flow of goods and, in case of anomalies, alert any possible infringements of the supply chain.



Source: Securikett

For what concerns the application to the risk scenarios, this submission targets some of the issues identified in the three risk scenarios related to food fraud. In order to combat the copy of designs, the repacking operations and the sale of fraudulent food as genuine, the adoption of authentication options like codes, tags, labels or seals offer a set of tools that provide an initial security layer. The tamper-evident solutions and the unique identifiers also aim at minimizing the possibility of having counterfeit products in the market. The overt and covert options allow the stakeholders and the clients to recognize original products, especially to avoid the possibility that consumers are unaware of fraudulent purchases.

The use of traceability systems not only provides an additional layer of security, but it also targets other issues presented in the scenarios, such as the distribution of the falsified goods, the use of clandestine sweatshops and production centres, and the lack of full monitoring and control of the production and distribution chains. The track and trace solutions enable the monitoring of the processes involved in the supply chain, granting visibility to identify illicit activities related to the deviation of the products from the supply chain. The capability of the solution of monitoring data and the adoption of blockchain technology create a platform where any anomalies in the process would be pointed out immediately. Furthermore, the data introduced to the system would automatically be immutable and transparent for all the stakeholders, enabling auditability and accountability. The code is made by using serialization, creating a unique, non-replicable identification. Geo-tracking is used through the monitoring process to obtain an accurate location of the product within the track and trace system.

In particular, for what concerns **risk scenario 1** (infiltration of the dairy supply chain), the described technology can support a risk reduction for several steps of the criminal business model. In particular, risk is reduced with the use of non-replicable codes, tags, and customized labels on the package that serve as an authentication mechanism and that can be read with a smartphone camera. As seen before, these codes and tags create the visual identity of each product and contain various technologies whose combinations create the uniqueness of each product identity and render its duplication extremely difficult. In many cases the replication of these codes, even if possible in theory, would involve a great investment from organized criminals, limiting their business case. In addition, the replication would only be visual; the mobile camera would not read the non-original code. When attempting to scan the falsified code, the response page will not open to indicate if the product has been tampered with. Furthermore, the code or label is used to track and trace the product along the distribution chain, basically securing the existing legitimate supply chain from infiltration of products that are not recognized at one of the various control stages of the distribution.

This can limit risks related to the following steps:

- Copying local producers' packaging design by using sweatshops and subsequent infiltration of these products into the legitimate supply chain.
- Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.
- Distribution of the falsified goods via the criminal group's comprehensive and well- structured network, which includes dozens of wholesalers and supermarkets controlled by their frontmen, to infiltrate the distribution of dairy products and deliver them to unsuspecting retailers.

In **risk scenario 1**, some of the steps are still difficult to limit, and the same considerations presented for previous submissions also apply in this case.

For what concerns **risk scenario 2** (parallel market for catering supplies) the same considerations presented for risk scenario 1 also apply in this case. The combination of a unique authentication mechanism with track and trace technology can limit the following steps of the criminal plan:

- Develop a fully-fledged supply chain for vegetables and dairy products.
- Building a parallel market for catering food supplies targeting small shops.

The same considerations regarding steps 3 and 5 explained in previous submissions apply to this technology. Shops can verify the authentication code before selling it to customers, who can also validate the code, but it does not apply to those cases in which the criminal group also controls these shops.

For what concerns **risk scenario 3** (e-commerce: criminal infiltration of online supermarket chains for home delivery of fake food), this submission can partly support securing online markets, since it can be adopted in the physical distribution of products. Securing these elements could be the key to limiting some of the risks highlighted in this scenario, especially the following step:

- Selling fraudulent food as genuine via the control of well-known e-supermarkets and by copying the design, packaging and trademark of well-known producers.

The same considerations presented for the previous risk scenarios apply in this case, in relation to the mitigating effect on this step that can be created by the combination of authentication via a strong unique digital identity with track and trace technology. The role of consumers is highly relevant, considering that online purchases usually include a direct relationship and line of shipping from the seller to the purchaser. The use of VOID labels as described in this submission is an interesting approach. As mentioned before, this technology submission offers two specific solutions to protect food that is being sold and distributed through online markets; by 1) protecting single-use shipping units and cartons for non-perishable food with customizable VOID tape and by 2) protecting reusable packaging for fresh food with customized security seals with overt, covert and semi-covert security features as well as digital security features, indicating tampering with a package or counterfeited package.

Summary table for submission 3: possible application to limit risks highlighted by the scenarios

Scenario	Applicability of the solution
Scenario 1: *Infiltration of the dairy supply chain*	
Step 1 – Control of the distribution market by owning or controlling legitimate operators.	
Step 2 – Control of the supply chain using the technology owned by the controlled legitimate operators.	
Step 3 – Copying local producers' packaging design and subsequent infiltration of these products into the legitimate supply chain.	Specific features are used to increase the security of the code, such as the All-in-One label that combines several features. Furthermore, the graphic element that is linked to the digital identity of the product and the physical characteristics of the code can also cross-validate for increased security. The flow of products along the supply chain can be checked using a mobile scanner giving stakeholders and consumers the possibility of performing a check. In addition, the use of blockchain technology protects the exchange of information in the supply chain.
Step 4 – Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.	The previous considerations apply to this step. The code that links the specific product with the digital identity is essential to provide an accurate reading when the customer or any stakeholder performs the check with the app. The link between the code and the unique serialization that is protected by blockchain creates an important security mechanism.

Step 5 – Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.	If the whole supply chain is controlled by organized crime or if they control legitimate operators, then an analysis of the product might be complicated to make, since the only way in which this could be achieved is through an investigation after the products are sold. If the criminal group infiltrates the supply chain, an alert can be sent to inform the stakeholders about the security breach thanks to the use of blockchain technology to protect the traceability system. By scanning the code, the information about the composition of the product can be accessed. The opening status of a product is indicated on the response page.
Scenario 2: *Parallel market for catering supplies*	
Step 1 – Control over legitimate businesses.	
Step 2 – Control of the anti-counterfeiting solutions used by the infiltrated businesses.	As previously clarified, the technology solution targets the packaging and not the food itself or its unique chemical composition. It comes into play at the first packaging point. Consequently, criminals capable of infiltrating companies working at the production level can package fraudulent goods using original packaging.
Step 3 – Develop a fully-fledged supply chain for vegetables and dairy products.	As seen in other submissions, only if the criminal supply chain attempts to infiltrate the legitimate one at a certain stage. The elements that have been previously described 1) unique identification, 2) track and trace system, 3) blockchain technology) play an important role in the protection of the supply chain.
Step 4 – Use of low quality and diluted materials.	This technology is focused on providing protective elements to the package and its movement through the supply chain, yet it does not target food itself. Consequently, criminals could infiltrate companies working at the production level and can package fraudulent goods using original packaging.
Step 5 – Building a parallel market for catering food supplies targeting small shops.	The use of scannable codes, track and trace technology and blockchain mitigate this risk. The solution provides an easy-to-use tool for customers to verify the authenticity of the product. Both the owner of the small shop and the customer can use the mobile scanner to check the code.
Step 6 – Distortion of competition.	If the supply chain is secured by adopting this technology solution, criminals may find it more difficult to implement their criminal plan and distort competition. This can be seen as a by-product of the implementation of the technology.
Scenario 3: E-commerce: criminal infiltration of online supermarket chains for home delivery of fake food.	
Step 1 – Control of legitimate e-operators.	
Step 2 – Selling fraudulent food as genuine through the controlled e-supermarkets.	If the whole online supply chain is controlled by organized crime, and since the e-supermarkets sell directly to the final consumer, then only checks performed by the latter could spot the illicit product. The submission proposes two different approaches to e-commerce security: 1) by protecting single-use shipping units and cartons for non-perishable food with customizable VOID tape and 2) by protecting reusable packaging for fresh food with customized security seals with overt, covert and semi-covert security features as well as digital security features, indicating tampering with packaging or counterfeited packaging.
Step 3 – Expansion of e-commerce market through the creation of a Super E-food app.	
Step 4 – Creation of dedicated social network groups/pages to sell fraudulent products to final customers.	

2.2.4 DNA ID, mass balance products' flow reconciliation and satellite integration

Technology submission 4

One of the submissions received incorporates several security layers for the creation of the digital identity of the product and for controlling its movements along the supply chain. The overall process can be divided in different stages:

Creating a unique identity for the product using its biometry and biography and initiating physical traceability,
Transferring the identity into a secure database creating the digital one and initiating digital traceability,
Monitoring the life of the product along the supply chain and
Providing data analytics.

The starting point of this technology is that, to secure the supply chain, it is necessary to link the physical journey of a product to the digital to guarantee integrity and auditability and to fight against fraud or diversion. This submission proposes initiating physical traceability by recording the biometry and biography of the product in different forms. In the case of products, and especially for food, the initial identification of the raw materials is essential, as it captures and records the fundamental characteristics of the products. This includes the true DNA of the product (genomics through polymerase chain reaction (PCR), as well as the "environmental DNA" (the conditions in which the product is grown) of the goods.

This element provides a unique and innovative way to establish the product's identity at its very first point of authentication. This first "DNA" capture identifies and contains the biometrics of the products and is further enriched with secure marking (active or passive) of the packaging. This marking also includes the biography of the product, which provides the product description and credentials, including for instance its ingredients.

The information allows for the creation and management of "physical reference" databases, which are integral parts of this proposed solution. These databases are used to secure the aforementioned complex identity. The data (transaction and process data) is then inserted into an immutable digital storage. This is a crucial step since the biometrical information of the product then has to be connected to a platform of integrity that will enable tracking through the supply chain. At this step, the physical identification is connected to the digital one.

Checks along the supply chain can be randomly performed to verify that the chemical composition of the product matches the recorded biography of the product. One of the tools that can be used for this purpose is a Portable Authentication Device (PAD) encompassing a Fourier Transform Near-Infrared (FT-NIR) spectrometer produced by the company itself. Spectrometers are used to identify and characterize chemicals and compounds in a test sample. These devices are based on the characteristic absorption spectra determined by the chemical bonds in organic materials, which can be used to identify organic compounds, the same method fingerprints are used for identification. FT-NIR provides a useful complement to or replacement of screening methods before the laborious chemistry tests and chromatographic methods. FT-NIR is non-destructive, needs little or no sample preparation as well as being fast, safe and dependable, as it doesn't need dangerous chemicals.

The PAD SICPA FT-NIR spectrometer can be used to detect on site at import points or at points of sale of the non-conformal food products. The PAD in its present form cannot determine whether the deviation from the genuine signature is due to counterfeiting, adulteration, or a quality related problem. However, coupled with the rest of the technology included in this submission, it complements the proposed approach. This gives field inspectors a useful screening tool to rapidly check if the biography information included in the identification and traceability code matches the detected spectral signature without the need to perform a lab test.

To begin the digital traceability, the initial biography is linked to the biometry and stored in an immutable manner using blockchain technology to achieve a controlled monitoring of the processes in the supply chain, through the use of the platform of integrity. Product packages will be marked using information on

the biography of the product. Where possible, in-product marking can also be used. Biography and biometry can be checked at any point of the chain.

Storage in a blockchain ensures immutability and auditability. Integer and immutable data are used to control processes and perform mass balance calculations to detect fraud, diversion and malfunction during the trace of the product in the chain. This is a very interesting element of this technology, since it compares data related to the volume of traded goods at their point of origin with volume of the same goods at their point of destination.

Variations in volume, that cannot be justified by possible losses happening in the normal course of trade, will trigger an alarm and can be a sign of smuggling, diversion or counterfeiting operations. Data analytics and artificial intelligence algorithms provide additional means of predicting and checking the overall balance along the supply chain.

In particular, this input foresees three main applications for space technologies:

Use for proof of origin and mass balance verification: images from drones and satellites can be used to link products to their place of origin. They make it possible to calculate production volumes and to anticipate and facilitate reconciliation.

Use for ensuring product quality: products' quality (Genetically Modified Organism (GMO)-free, pesticides and fertilisers content, soil quality…) can be assessed using specific imaging technologies, including hyperspectral cameras, linking to the origin of the product and of its ingredients.

Use for monitoring and communication: spatial monitoring of land can also be used to detect criminal operations. Together with proof of origin, it can provide for additional data to check mass balance along the supply chain.

This submission stresses the fact that secure communication and data exchanges between drones, satellites and ground IoTs are key for supply chain auditability. Therefore, it is also important to secure images, transmissions and positioning of devices (IoTs and software).

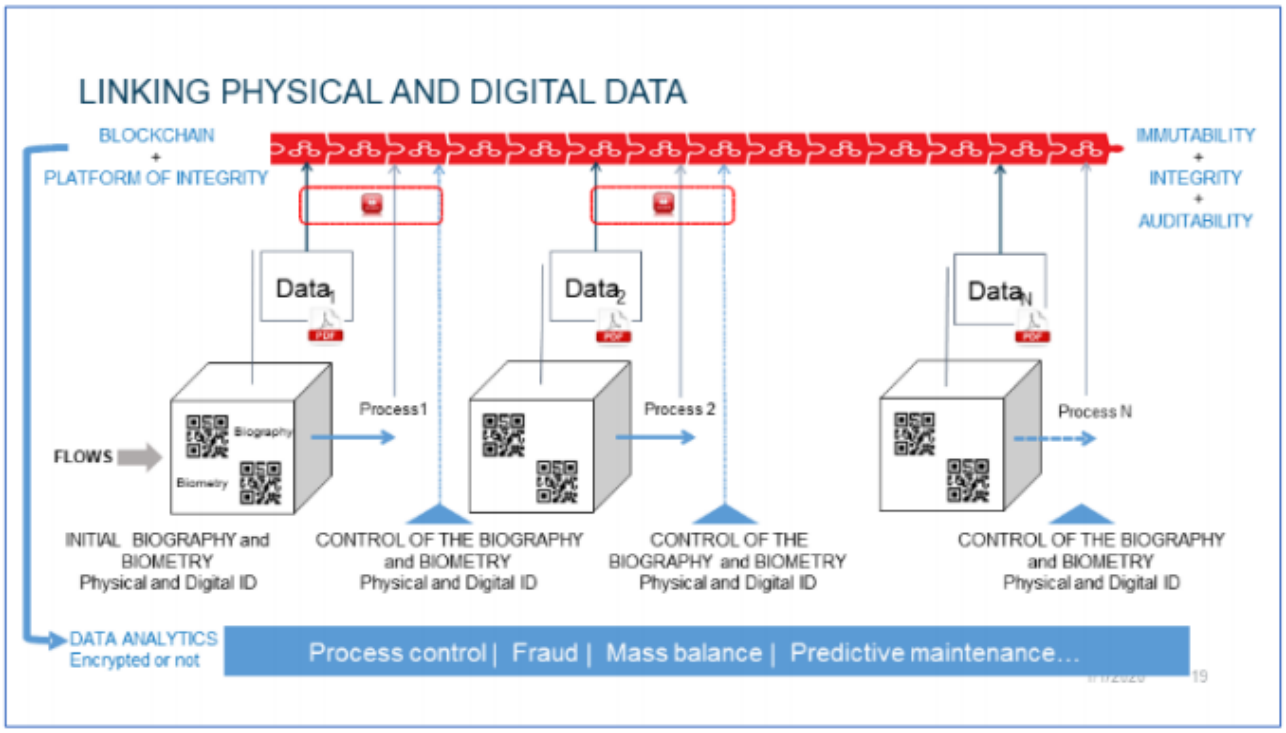
Space data will be used for continuous and ulterior controls along the supply chain and, consequently, data and processes will also be certified and timestamped in a blockchain to improve security and avoid falsification. According to the submission, in the near future compressed spatial images with their embedded unforgeable signatures and localisations through quantum-derived technologies will be used for this purpose.

Satellites can already be used and make the collection of relevant data possible thanks to their large-scale coverage, while various spectrometers can be used for product and ingredients identification, time series, connection with ground data, work on land and sea, communication and collection of large data sets. Drones may also have a role to play, since they have the same advantages but often with a better spatial resolution at a cheaper cost and their use can be complementary to satellites.

Submission received from SICPA SA

This submission is useful to show how approaches to supply chain security are constantly evolving, incorporating several elements to render the authentication and track and trace process less dependent on the packaging alone, while incorporating additional features to identify possible criminal activities related to supply chain infiltration. In this case, these features are satellite integration and products' flow mass balance reconciliation.

The combination of all these elements creates an innovative approach for what concerns the identification of the product, since the DNA elements, biometry and biography of the product are included in the authentication code. In case of verification, this feature not only allows stakeholders to authenticate a product through the scanning of the code on the packaging, but also to verify if the very composition of the food product contained by the packaging is genuine.



Source: SICPA

This will of course require a separate DNA analysis, but it is an important step forward that can facilitate rapid on-field testing. Since the DNA information of the food product is already included in the authentication code, personnel running the field test will not need to be connected to a separate database containing all DNA profiles of the specific category of product. The field test will simply verify that the composition of the analysed product corresponds with the DNA indication included in the code. Field testing can be performed by using the FT-NIR spectrometer produced by the same company, without the need to perform a more time-consuming lab test.

Apart from field testing, this kind of analysis could be performed at established checkpoints along the supply chain, further strengthening its security. Since the DNA is captured at the very beginning of the manufacturing process, monitoring starts very early in the chain and, thanks to the use of the blockchain, data inserted in the database will be immutable and secure. The idea is to use them for proof of origin as well as for track and trace, by generating data that, when added to those directly obtained from the products, can guarantee an increased level of assurance of the quality of the products and the integrity of their transactions along the supply chain. Furthermore, they can also be used for improving the aforementioned mass balance calculations and reconciliations on trade volumes.

This submission can be further used to introduce the possible advantages deriving from the use of space technology and of mass balance reconciliation related to the flow of tracked and traced goods. In this specific case, these two elements are also intended to work in combination. The volume of products or substances entering the supply chain can be measured and the volumetric balance between departure and arrival points can be used to verify if any suspicious activity was performed.

The integration with space technology can be used for proof of origin as well as for track and trace purposes and can be seen as a tool to create fully-fledged auditable supply chains. Images from drones and satellites can be used to link products to their place of origin. They make it possible to calculate production volumes, to anticipate and facilitate reconciliation, check whether the quantity of products in circulation is bigger/smaller than the effective and verified original quantity. As space data is used for continuous and ulterior controls along the supply chain, data and processes are certified and timestamped in a blockchain to avoid falsification.

These elements may allow stakeholders, for instance, to detect frauds related to Geographical Indications, ensuring that the origin of the product is the correct one. When working in combination with the DNA ID, this represents an additional layer of security.

For what concerns the application to the risk scenarios, the unique features presented by this submission open some doors for supply chain security technology to also protect from additional risks highlighted by the scenarios, including the use of original packaging filled with fraudulent food products.

The unique identification of the product, as well as of its ingredients, by biometric information linked to its nature, represents an additional layer of security in the authentication process. The encrypted information provides a clear description of the specific product, exponentially complicating the imitation of the authentication solution. The physical authentication mechanism is immediately connected to the second layer of protection by linking the product to the track and trace system. This way, the unique identifier is providing a secure mechanism to easily recognize the product, while at the same time the information is protected with blockchain technology during the monitoring through the traceability solution to combat the lack of control over the product quality once it is packed.

The blockchain technology also protects the data exchange that is made through the monitoring. In addition, the immutability of the blockchain targets the use of illegal production methods and illicit operations, as well as the substitution of products with lower-quality or cheaper versions, by ensuring that no one can intrude in the system or alter the data saved to the block.

In particular:

For what concerns **risk scenario 1**, using biometric elements of food that is being traced along the supply chain (including chemical and physical properties) for the production of its ID creates a strong layer of security capable of responding to several steps of the criminal plan presented in this scenario. This also includes ingredients in the case of processed food. This creates a certain barrier to these illegal activities, because the systems will not recognize any correspondence with the identity of the fraudulent food, given that its biometry is radically different. Analysis of data related to flow balance of products from origin to destination can also trigger an alarm in the case in which one actor of the supply chain, for instance, starts inserting a higher number of food products in the chain. All these elements are integrated with the use of space technology to verify and timestamp the origin and movement of products. Consequently, and as described in the summary table, this submission can mitigate several steps of the criminal plan:

- Copying local producers' design by setting up a clandestine sweatshop to copy the design, packaging and trademark of well-known local producers.
- Procurement of low-level milk or dairy products and marketing them as original.
- Distribution of falsified goods through the criminal group's comprehensive and well- structured network, which includes dozens of wholesalers and supermarkets controlled by their frontmen.
- Control of the supply chain by using original packaging of the businesses controlled by organized crime to market substandard and fraudulent products, fooling consumers who are unaware of the change in ownership.

Also, for this submission, in **risk scenario 1**, one of the steps is still difficult to limit, step 1) Control of the distribution market by owning or controlling legitimate operators. As previously clarified, this is a complex step which needs technology to support law enforcement in better understanding and monitoring organized crime strategies related to the acquisition of legitimate businesses or to the gaining of control over their operations.

Similar considerations can be made for **risk scenario 2**, and the submission can support mitigating the following steps of the criminal plan:

- Development of a fully-fledged supply chain for vegetables and dairy products.
- Using and marketing low-quality, diluted and polluted raw materials and food products.
- Building a parallel market for catering food supplies.
- Control of the anti-counterfeiting solutions used by the producers and actors of the supply chain controlled by organized crime.
- Distortion of competition.

In particular, and as seen in the case of the previous risk scenario, the creation of an ID based on the biometry and biography of a product is an important step to avoid infiltrations of the food supply chain. Even in the case in which criminals would be able to use the packaging technology of legitimate producers, the biometric ID of the food product would not be verified and would trigger an alert at checkpoints or in case of a field test. This can happen at any stage of the supply chain. The use of space technology to verify the origin of the product and of its ingredients adds a layer of security capable of mitigating several steps of the criminal plan presented by the risk scenario. Data analysis on trade flow balance, supported by the use of space technologies, can also support triggering alerts in this risk scenario.

Finally, for what concerns **risk scenario 3**, the following considerations can be made when using this submission to limit the following step of the criminal plan:

- Selling fraudulent food as genuine through controlled e-Commerce operators by copying the design, packaging and trademark of well-known producers and replacing authentic products with low quality or expired ones.

Once again, the strong ID creation of the product through its biometric properties and then the control of its movements, represents an interesting element to prevent this step. However, in the case in which the product is shipped directly to the consumer, an authentication method for the consumer themselves is also needed.

As in the case of previous submissions and examples, for all the three risk scenarios, organized crime activities aimed at infiltrating supply chain stakeholders before starting to practically market fraudulent products need to be controlled and monitored through different technology.

This calls for an integrated approach between different technology options to support investigators, law enforcement agencies and Customs Agencies on the one side as well as supply chain operators and consumers on the other. Similarly, a strategy needs to be built in relation to marketing strategies of illicit products through misuse of social media.

Furthermore, and as in the case of the other submissions, in the case of risk scenario 3, other technological resources should be used to mitigate other steps, which cannot be limited through supply chain security technology.

Summary table for submission 4: possible application to risk scenarios

Scenario	Applicability of the solution
Scenario 1: *Infiltration of the dairy supply chain*	
Step 1 – Control of the distribution market by owning or controlling legitimate operators.	
Step 2 – Control of the supply chain using the technology owned by the controlled legitimate operators.	If the legitimate business is infiltrated at any point by the criminal organization, then this technology would trigger an alarm to indicate that something has changed, thanks to the protection provided by blockchain technology. However, if the supply chain is fully controlled by the criminal organization from the beginning, then they can control the information that is introduced into the database. The system would need an independent body to validate the authenticity of the product, such as National Food and Health Authorities. This submission adds layers of security, such as: 1) use of biometry to identify the product and to monitor it along the supply chain, 2) easy and quick field testing through the FT-NIR spectrometer, 3) data analysis of flow mass balance of products, and 4) use of space technology.

Step 3 – Copying local producers' packaging design and subsequent infiltration of these products into the legitimate supply chain.	For the same reasons as the previous step, the strong product ID and the way in which it is monitored throughout the supply chain, will make it extremely difficult if not impossible to insert fraudulent products by simply imitating the original packaging. The mass balance calculations and the link with space technology provide additional layers of security.
Step 4 – Procurement of low-quality milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.	Once again, for the same reasons as presented above. In addition, it is important to point out that the use of the biography and biometry of the product for creating its unique ID, along with space technology and mass balance reconciliation, will even greatly reduce the risk of using low-quality ingredients for the production of the food and then inserting it into the supply chain.
Step 5 – Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.	All the previous considerations also apply to this step.
Scenario 2: *Parallel market for catering supplies*	
Step 1 – Control over legitimate businesses.	
Step 2 – Control of the anti-counterfeiting solutions used by the infiltrated businesses.	If an infiltration occurs, then this technology would trigger an alarm due to the use of blockchain. However, it would not be possible to detect if the supply chain is fully controlled by the criminal organization from the beginning. As mentioned before, the combination of biometry, monitoring, field testing through the FT-NIR spectrometer, data analysis of flow mass balance of products, and space technology provide a multilayer solution to protect the supply chain from any infiltration.
Step 3 – Develop a fully-fledged supply chain for vegetables and dairy products.	As seen in other submissions, only if the criminal supply chain attempts to infiltrate the legitimate one at a certain stage. In the case in which the criminal supply chain targets the final consumer directly or small shops, it has to be ensured that even small shops are using the technology and that consumers have the possibility of checking the products they bought. However, analysis of mass flow of products can trigger alerts if applied also between different countries.
Step 4 – Use of low quality and diluted materials.	The same considerations presented for the previous step also apply here, in addition to the fact that the use of the biography and biometry of the product, along with space technology and mass balance reconciliation, will even greatly reduce the risk of using low-quality ingredients for the production of the food and then inserting it into the supply chain.
Step 5 – Building a parallel market for catering food supplies targeting small shops.	The same considerations made for step 3 of this risk scenario apply here.

Step 6 – Distortion of competition.	If the supply chain is secured through the use of this multilayer technology solution, criminals may find it more difficult to implement their criminal plan and distort competition. This can be seen as a by-product of the implementation of the technology.
Scenario 3: *E-commerce: criminal infiltration of online supermarket chains for home delivery of fake food*	
Step 1 – Control of legitimate e-operators.	
Step 2 – Selling fraudulent food as genuine through the controlled e-supermarkets.	Through the creation of a strong ID for the product through its biometric properties and the control of its movements. However, since in many cases the product is directly sold to the final consumer avoiding any other intermediary passages, consumers may also have a role to play in this case.
Step 3 – Expansion of e-commerce market through the creation of a Super E-food app.	
Step 4 – Creation of dedicated social network groups/pages to sell fraudulent products to final customers.	

2.2.5 Innovative marking methods and satellite integration

Technology submission 5

Multilayer security linked to the use of blockchain is also a key element in a different submission received. The proposed technology solution comprises a blockchain with a bridge-database, combined with accurate time and position data from satellite navigation, and an option to digitally encrypt data from a product-level food signature at origin to verify against printed packaging codes, using cryptographic keys. The blockchain can be public or private, or a combination of both, depending on the user groups involved. A trusted computing platform is used to secure interfacing to the internal systems of manufacturers. The different processes offered by this technology solution can be divided into:

1) Product fingerprint: The unique identification of the product (characteristics or chemical fingerprint) is obtained and linked to the traceability system. It can be read by using a smartphone or through a fast µ-level-3D scan if the digital fingerprint is on the product. At its current stage, the use of a chemical fingerprint is a proposal that can be adopted in this technology option if a partnership is created with other providers that have developed the technology or if it will later be developed by the company.

2) Primary packaging: The initial digital fingerprint is linked to the primary packaging using cryptography to create a code. This code is verifiable by scanning it with a smartphone.

3) Further package: If the product needs further packaging, the process can be repeated. The code on the new package is linked to the other different codes used, starting with the product-linked code. All barcodes are uploaded to the blockchain.

4) Blockchain tracking: Blockchain is used to protect the product fingerprint and the rest of the cryptographically secured codes that were used for packaging. The data is logged in a "bridge-database"

between the data collection and the blockchain. This enables visibility in the changes of ownership, aggregation and disaggregation from the product-level encoding.

5) Apps: A tablet verification app and a blockchain app are used as tools. The tablet verification app enables the customer to check the authenticity of the product, whereas the blockchain app tracks changes in ownership (aggregation and disaggregation) in the supply chain.

The creation of the unique digital identity of the product is especially interesting since, in the case of food, it can be created by including a signature related to the physical or chemical properties of the product. This process is still an option for future development at this stage, but the submission describes it as using a combination of high-speed 2D and 3D digital imaging that is then encrypted and recorded via printing on the first layer of packaging and in the database and blockchain. Depending on the materials, the digital mark can be printed on the package itself by using laser engraving. The 3D scanning capability has the resolution of an atomic force microscope. These systems can create the digital fingerprints that can be scanned on a production line to identify unique properties of products (on a packaging line for example). Scanning along the supply chain happens at two levels: non-forensic with a smart-phone or with a hand-held scanner, or, on the forensic level using 3D scanners in reference labs along supply chains.

Digital information from the original product can be combined with a precise time and location stamp (provided by satellite information) to make each set of product data unique and to allow precise identification of the origin. The precise location and time data from satellite navigation and communications can be inserted into a blockchain based database and be used for tracking and authentication purposes. The combination of all these elements results in a unique cryptographic stamp linked to the printed codes that makes each code unique. Therefore, barcodes with location and time stamping are used to track each step of the repackaging process. The data is logged in a "bridge-database" between the data collection and the blockchain. The use of a bridge-database allows data to be stored for later reference and easy checking, but groups of data are uploaded in a "hashed" form into the blockchain so that no changes to the data can be made. A transaction can only be made when both the sender and receiver are authorised through the private and public key system.

In the case in which the optional part of this proposal is developed, authentication at the various stages of the supply chain will also use the signature data from the food product at origin, which will be uploaded to the blockchain and then verified by a scan at the first packaging point. If the signature verifies, then the packaging code can be cryptographically signed. If not, the code will be recognised as wrong the next time that it is scanned.

Cryptographic keys are exchanged, allowing the receiver to become the new owner of each item when authorized to do so by the sender. Each transaction is recorded as a new block in the blockchain. Furthermore, through this approach the blockchain technology can be used to corroborate the amount of product exchanged between the different checkpoints in the supply chain. For instance, if the amount of packaging and legitimate food submission in a distribution node was monitored (the use of geographical satellite data can strengthen this element), then it should match a particular amount of packaged food output. If the same output is happening but with less authorised food submission, this suggests an issue.

For what concerns the security of the database, only authorized users have access to it. If anyone breaks into the database, no data can be changed, because it would change the blockchain. Such a change can be flagged in different ways depending on security needs.

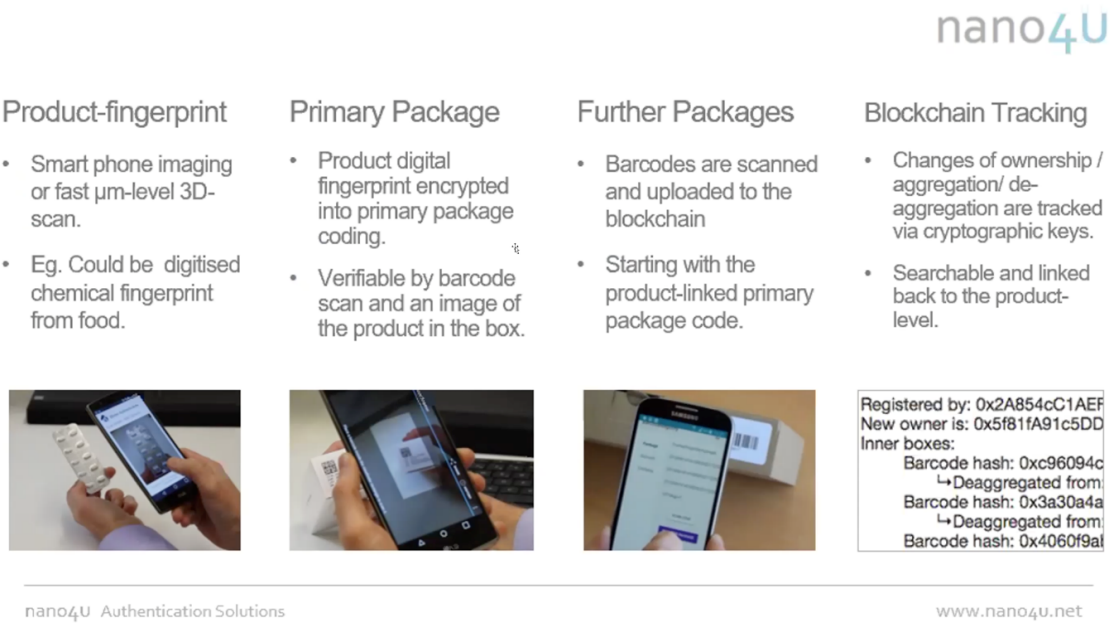
Submission received from Nano4U

This submission presents certain similarities with the previous one, which demonstrates how interesting some technology areas may be for increasing the food products' supply chain. However, this submission can also be used to show how similar approaches may in reality be implemented in different ways. The unique element of this submission is probably the possibility to print the authentication codes directly on the primary package of the product by engraving the code on the package itself. This technology can also be used to control repackaging operations,

since changes in ownership of the product and aggregation and de-aggregation of packaging are recorded immutably in the blockchain. For example, the code can be engraved on the glass bottle of a beverage instead of using a label or printed code over the surface of the bottle. This creates a strong defence against the possibility of modifying codes or replicating them because the investment for technology to engrave a code directly on the packaging will very probably limit the business case for criminals. The authentication of the codes can be performed through an app, providing customers with a mechanism to differentiate original from counterfeit goods.

As in the case of submission 4, this submission also adds layers of security based on satellite integration and on the possibility to include the organic/chemical properties of the product in its ID. The latter element is not yet fully developed by the company, but it could be integrated later by establishing cooperation with other stakeholders or by conducting its own research and development. The considerations presented in the case of submission 4 with regards to the use of the organic/chemical properties of the product for its authentication can also be used for this submission, and when fully developed will represent an increased barrier to criminal infiltrations into the supply chain.

This submission can also be used to show the various possibilities deriving from the combination of satellite integration and use of its data in the blockchain. Once again, some similarities exist with submission 4 for what concerns the possibility of using mass balance verification between the different nodes of the supply chain in view of identifying possible suspicious activities. In particular, in this case the information about the total weight of parcels or packages received and sent at each node is stored in the blockchain and the change in the volume measurement would trigger an alert. Introducing falsified products in the authorized distribution chain would not be possible because each transaction is locked in the blockchain through cryptographic key authorisation. The supplier must have an authorised key and be connected cryptographically to the receiver. Furthermore, the signature from the original food authentication would not match, in the case in which this option is implemented. Recorded product and time/location data is stored for easy data access in the bridge-database but cannot be adulterated in any way because it is locked to the cryptographic hashing in the blockchain, and a change would immediately be visible.



Source: Nano4U

For what concerns its application to the risk scenarios, the solution targets some of the issues identified in the three risk scenarios related to food fraud. In order to combat copying of designs and the repacking operations and the sale of fraudulent food as genuine, the adoption of authentication options, such as the code that encrypts specific information related to the characteristics of the products and its components, offer a tool that provides an initial security layer. However, it has to be noted that this element is still not fully developed by this submission and

will have to be integrated thanks to partnership with other suppliers or will have to be the result of further R&D. The unique identifiers also aim at minimizing the possibility of having counterfeit products in the market. The overt and covert options allow the stakeholders and the clients to recognize original products; this is especially important for avoiding the possibility that consumers are unaware of fraudulent purchases.

The use of traceability systems not only provides an additional layer of security, but it also targets other issues presented in the scenarios, such as the distribution of the falsified goods, the use of clandestine sweatshops and production centres, and the lack of full monitoring and control of the production and distribution chains. The traceability is greatly supported by satellite navigation and communication, which supplies precise location and time data and provides a unique cryptographic stamp for printed codes that makes each code unique. Space-related data is also used by this submission to track the origin and the location of products as they are packaged or repackaged.

In particular, for what concerns **risk scenario 1** (infiltration of the dairy supply chain), the described technology can support a risk reduction for several steps of the criminal business model. In particular, when this option is fully developed, risk is reduced due to the use of a non-replicable code that contains information about the specific product or if the technology is developed, of its composition. As previously analysed, these codes create the visual and digital identity of each product, making its duplication extremely difficult or nearly impossible. In the case in which the optional element of the submission is developed/integrated, even if the code is imitated, by attempting to scan it, it would be clear that it is not an original product since it would probably not show the information related to the characteristics of the product. Furthermore, the authentication codes are linked to the traceability system and with a blockchain-based database to follow the product along the distribution chain, securing the existing legitimate supply chain from infiltration of products that are not recognized at one of the various control stages of the distribution.

This can limit risks related to the following steps:

- Copying local producers' packaging design by using sweatshops and subsequent infiltration of these products into the legitimate supply chain.
- Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.
- Distribution of the falsified goods via the criminal group's comprehensive and well- structured network, which includes dozens of wholesalers and supermarkets controlled by their frontmen, to infiltrate the distribution of dairy products and deliver them to unsuspecting retailers.

If the use of the chemical fingerprint of the product for the creation of its ID is added to the current solution, then the technology could be used to mitigate the following step:

- Control of the supply chain by using original packaging of the businesses controlled by organized crime to market substandard and fraudulent products, fooling consumers who are unaware of the change in ownership.

In **risk scenario 1**, some of the steps are still difficult to limit, in particular element 1) Control of the distribution market by owning or controlling legitimate operators. The same considerations regarding the support of law enforcement explained in previous submissions apply to this technology. Furthermore, the current version of the technology does not address the threat presented in step 2) Control of the supply chain using the technology owned by the controlled legitimate operators. In order to mitigate this risk, it would be necessary to integrate the chemical fingerprint to the existing option, which would enable the blockchain-protected code to carry the unique chemical properties of the product, making it almost impossible to change or replace the original product without creating an alert in the system.

For what concerns **risk scenario 2** (parallel market for catering supplies) the same considerations presented for risk scenario 1 also apply in this case. The combination of authentication via a strong digital identity with track and trace technology can limit the following steps of the criminal plan:

- The development of a fully-fledged supply chain for vegetables and dairy products as well as the building of a parallel market for catering food supplies targeting small shops.
- Building a parallel market for catering food supplies targeting small shops.
- Distortion of competition.

If the use of the chemical fingerprint of the product for the creation of its ID is added to the current solution, then the technology could be used to mitigate the following steps:

- Control of the anti-counterfeiting solutions used by the infiltrated businesses.
- Use of low quality and diluted materials.

For what concerns **risk scenario 3** (e-commerce: criminal infiltration of online supermarket chains for home delivery of fake food), the technology solution partly supports securing online markets considering the physical distribution of products and the series of distribution steps. If the option is developed, the use of encrypted chemical composition or other characteristics of the product in a code can create a security layer from the start of the supply chain to the customer. Securing these elements could be the key to limit the following step of the criminal plan:

- Selling fraudulent food as genuine via the control of well-known e-supermarkets and by copying the design, packaging and trademark of well-known producers.

The same considerations presented for the previous risk scenarios apply in this case, in relation to the mitigating effect on this step that can be created by the combination of authentication via a unique code with a connection to the traceability system that is protected by blockchain technology. Once again, consumers have a central role since online purchases may involve a direct relationship and line of shipping from the seller to the purchaser. In this case, the app enables the customers to verify the authenticity of the product.

Also, in the case of risk scenario 3, and as seen for all the previous submissions, other technological resources should be used to mitigate other steps of the criminal plan, which cannot be limited through supply chain security technology.

Summary table for submission 5: Possible application to limit risks highlighted by the scenarios

Scenario	**Applicability of the solution**
Scenario 1: *Infiltration of the dairy supply chain*	
Step 1 – Control of the distribution market by owning or controlling legitimate operators.	
Step 2 – Control of the supply chain using the technology owned by the controlled legitimate operators.	Not at the current stage. However, the submission presents an option to mitigate this risk by integrating the chemical fingerprint to the existing authentication methods, traceability systems and blockchain technology to protect the supply chain. The blockchain-protected code could carry the unique chemical properties of the product, making it almost impossible to change or replace the original product without creating an alert in the system.

Step 3 – Copying local producers' packaging design and subsequent infiltration of these products into the legitimate supply chain.	Risk is reduced with the integration of the technology solution that combines the authentication mechanism based on a unique code with the blockchain-protected track and trace system. The identity of each product is created by using a unique non-removable code. In this case, if the optional component is developed or integrated, the code will also include encrypted information about the characteristics of the specific product, creating a unique identification that is linked to the blockchain-protected traceability system.
Step 4 – Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.	The same considerations mentioned in the previous step apply.
Step 5 - Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.	As previously stated, if the whole supply chain is controlled by organized crime or if they control legitimate operators, then an analysis of the product might be complicated for corroborating the quality of the products or the criminal network behind them. However, this risk could be greatly mitigated by the development or integration of the foreseen option using the chemical properties of the product in the code that is linked to the traceability system. Furthermore, the described use of space technology and of submission and output product calculation at all nodes can mitigate this risk.
Scenario 2: *Parallel market for catering supplies*	
Step 1 – Control over legitimate businesses.	
Step 2 – Control of the anti-counterfeiting solutions used by the infiltrated businesses.	The same considerations explained in step 2 of the first risk scenario apply.
Step 3 – Develop a fully-fledged supply chain for vegetables and dairy products.	As seen in other submissions, only if the criminal supply chain attempts to infiltrate the legitimate one at a certain stage. The elements that have been previously described – 1) unique identification, 2) track and trace system, 3) blockchain technology – mitigate the risk. In the case in which the criminal supply chain targets the final consumer or small shops directly, it has to be ensured that even small shops are using the technology and that consumers have the possibility of checking the products they bought through the app.
Step 4 – Use of low quality and diluted materials.	The same considerations explained in step 2 of the first risk scenario apply.
Step 5 – Building a parallel market for catering food supplies targeting small shops.	The code may include encrypted information about the characteristics of the specific product in the future, creating a unique identification that is linked to the blockchain protected traceability system. But only if small shops are also part of the supply chain security technology. Consumers also have a role to play in this case, since they check the originality of the product through the app.
Step 6 – Distortion of competition.	If the supply chain is secured, then in that specific market criminals may find it more difficult to implement their criminal plan and distort competition. This can be seen as a by-product of the implementation of the technology.

Scenario 3: *E-commerce: criminal infiltration of online supermarket chains for home delivery of fake food*	
Step 1 – Control of legitimate e-operators.	
Step 2 – Selling fraudulent food as genuine through the controlled e-supermarkets.	Through the use of strong authentication measures in the product and then the control of its movements. The code provides an important security layer, which can be improved in the future if it includes encrypted information about the characteristics of the specific product that is linked to the blockchain protected traceability system. However, since in many cases the product is directly sold to the final consumer, avoiding any other intermediary passages, consumers may also have a role to play in this case. This requires the consumer to be fully aware of the authentication method and of how to identify a counterfeit.
Step 3 – Expansion of e-commerce market through the creation of a Super E-food app.	
Step 4 – Creation of dedicated social network groups/pages to sell fraudulent products to final customers.	

2.2.6 Focus on authenticating, tracking and tracing ingredients

Technology submission 6

One of the submissions received focuses on the application of an advanced Manufacturing Execution System (MES) that provides the ability to track the manufacturing of products and their movement through the supply chain anywhere in the world via a web-based tracking data management system. The solution secures products through tamper-proof labelling solutions that assign unique, serialized identities to each crop, ingredient, product, and batch. This is combined with total traceability and control throughout the food and beverage supply chain—from seed, to harvest, production, distribution, sale, and after sale. This technology option is based on assigning serialized identities to every product, starting in the field, providing stakeholders with a highly detailed record of every product's genealogy. With a single scan, this detail can be instantly accessed by key stakeholders throughout the supply chain, providing insight into where a product came from, what ingredients were used, and who interacted with it at every stage of the supply chain. The solution creates and assigns unique codes (paired with security labelling). The codes are associated with all aspects of the process and items used in the process. It starts with the codes that are associated with raw materials and ingredients, product, and materials produced. The raw material and ingredient codes are embedded in the product along with other process data such as user information, operational data, and specific intrinsic data such as temperatures, pressures, and dwell times, among others. These codes are aggregated to pallets, skids, and cartons, allowing the solution to easily track the shipping information.

By using the system, stakeholders can have a complete overview of what is produced, where it came from, and where it went.

The system uses tamper-proof labelling solutions to create the digital identity of the product, which is subsequently integrated into the supply chain management database to enable the product serialization, authentication, and traceability. Furthermore, authentication is offered through a large variety of options that can be adapted to different products designs, such as nano and micro printing; other anti-counterfeit features that include liquid crystals, taggants, colour-shift inks, holographic features, and tamper-evident adhesives. In addition, the use of blockchain technology for storing the data in the database allows for data to be processed through the system in an unalterable way when entered into the blockchain.

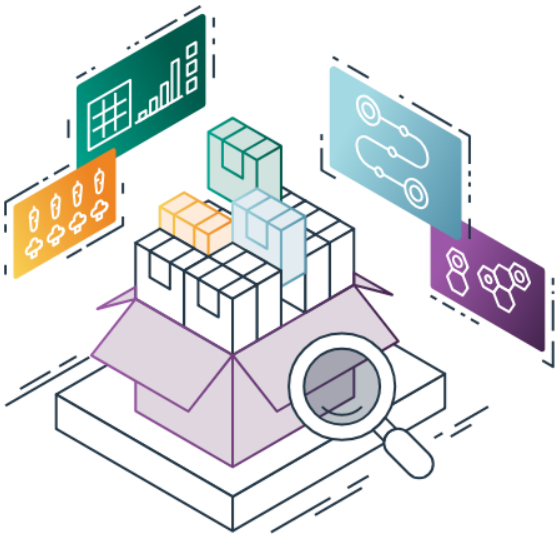
An interesting feature lies in the fact that, apart from the proprietary secure marking method, the software of this technology option is able to integrate different existing data systems to create the digital identity of the product, since data can also be collected, for instance, through barcodes or QR codes. Furthermore, it is interesting to note that the monitoring of the product along the supply chain can begin as early as the manufacturing of components or their harvest in the field.

A relevant element of this technology also relies on the capabilities for analysis of products' movements along the distribution chain. Thanks to the use of dashboards, this option allows the user to obtain traceability reporting.

Alerts in the system can be set by location or single scan ability by vendors for authentication purposes. In the case in which values scanned or entered into the system are outside parameters, the system would red flag the data allowing for investigation by the authorities.

Submission received from Ashton-Potter (USA) Ltd.

The last example within the area of supply chain security allows us to present an interesting approach based on authenticating, tracking and tracing not only the food product but also its ingredients. This may create an additional layer of security for those cases in which criminal operations are targeting low quality products or food products produced using low quality ingredients. If fully integrated in the whole supply chain, including all possible ingredients of a food product, criminals will need to control the whole of the supply chain of ingredients in order to bypass the system, increasing the complexity of criminal operations.



Source: Ashton-Potter (USA) Ltd.

This solution provides serialized identities assigned to each product and to its subcomponents, which are integrated into the traceability system. The authentication is established through a highly detailed digital genealogy down to the individual component, giving detailed insight to each product in circulation.

For what concerns the authentication and track and trace solution, most solutions have tamper-evident mechanisms that facilitate the identification of any issue with the product, including easy spotting of manipulation attempts and/or infiltration of non-original products into the supply chain. A tamper-indicating device can also be used and is designed to leave non-erasable, unambiguous evidence of unauthorized access to packaging, facilitating the identification of any suspicious handling. The submission also provides the option of data analytics through dashboards. These dashboards, their use as well as access to them are configurable based on the clearance or role of each user and could create alerts and notifications to be set to monitor an increase, decrease or dramatic change in flow on reported data on products for what concerns the supply chain or on ingredients for what concerns the production chain. Movements of products through the supply chain are recorded via scan or data submission. The solution is highly adaptable to existing systems and processes, providing a centralized reporting base, including production monitoring.

Finally, this submission can also be used to show the benefits of blockchain integration, including timestamping related to production and movement of food products as well as of their ingredients. As seen in submissions 4 and 5, this submission also includes the possibility of analysing the flow of goods and of their ingredients between supply chain nodes, triggering alerts in case of discrepancy of data.

For what concerns the application to the risk scenarios, in order to combat copying of designs and the repacking operations and the sale of fraudulent food as genuine, the adoption of authentication options like codes, tags, labels, seals, nano and micro printing, taggants, colour-shift inks, holographic features, and tamper-evident adhesives offer a set of tools that provide an initial security layer. The tamper-evident solutions and the unique identifiers also aim at minimizing the possibility of having counterfeit products in the market. The overt and covert options allow the stakeholders and the clients to recognize original products; this is especially important for avoiding the possibility that consumers are unaware of fraudulent purchases. Scanning the codes, tags and labels enable the stakeholders and consumers to access the information about that specific product (highly detailed records that provide insight into field conditions, pesticide use, exposure to allergens, and more), which provides an additional level of security to confirm that the authentication mechanism is original.

The use of traceability systems not only provides another layer of security, but it also targets other issues presented in the scenarios, such as the distribution of the falsified goods, the use of clandestine sweatshops and production centres, and the lack of full monitoring and control of the production and distribution chains. The track and trace solutions enable the monitoring of the processes involved in the supply chain, granting visibility to identify illicit activities related to the deviation of the products from the supply chain or introduction of illicit/unauthorised ones into it. In this case, the submission secures products through tamper-proof labelling solutions that assign unique, serialized identities to each crop, ingredient, product, and batch. This is combined with total traceability and control throughout the food and beverage supply chain —from seed, to harvest, production, distribution, sale, and after sale. The capability of the solution of monitoring data and the adoption of blockchain technology create a platform where any anomalies in the process would be pointed out immediately. Furthermore, the data introduced to the system would automatically be immutable and transparent for all the stakeholders, enabling auditability and accountability. With scanning, the stakeholders can access highly detailed records of every product's genealogy.

In particular, for what concerns **risk scenario 1** (infiltration in the dairy supply chain), the described technology can support a risk reduction in several steps of the criminal business model. Specifically, risk is reduced thanks to the use of authentication mechanisms (codes, tags, labels, seals, nano and micro printing, and others) that are recognizable both visually and through the use of a scanner. As seen before, these codes create the visual identity and renders its duplication extremely difficult. As previously explained, the replication of these codes would involve a great investment from organized criminals, limiting their business case. The customization of the authentication methods complicates their replication; a higher investment would be required to be made by a criminal organization if they want to copy a customized code, tag, or label than just investing in a widely used one. Moreover, the code can be linked to a traceability system, securing the existing legitimate supply chain from infiltration of products that are not recognized at one of the various control stages of the distribution. The information is protected with blockchain technology. Once the information of the product is introduced in the code, it can be tracked through the supply chain.

This can limit the following steps of the criminal plan:

- Copying local producers' packaging design by using sweatshops and subsequent infiltration of these products into the legitimate supply chain.
- Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.
- Control of the supply chain using the technology owned by the controlled legitimate operators.
- Distribution of the falsified goods via the criminal group's comprehensive and well- structured network, which includes dozens of wholesalers and supermarkets controlled by their frontmen, to infiltrate the distribution of dairy products and deliver them to unsuspecting retailers.

In **risk scenario 1**, as seen in the case of several previous examples, some of the steps are still difficult to limit, in particular step 1) Control of the distribution market by owning or controlling legitimate operators, and to a certain extent step 2) Control of the supply chain using the technology owned by the controlled legitimate operators and step 5) Distribution of the falsified goods via the criminal group's comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen. These are more complex risks which need, first of all, technology to support law enforcement in better understanding and monitoring organized crime strategies related to the acquisition of legitimate businesses or to the gaining of control over their operations. Nonetheless, this technology is still package dependent and it should be considered that if the criminal organization owns the production facility, they can easily access the technology. Criminal groups would need to control the whole supply chain since traceability starts early (from the harvest) to avoid triggering an alarm.

Step 2) should then be read in conjunction with step 1) on the acquisition of criminal control over sectors of the legal economy and step 5) related to the distribution of the goods. This technology solution offers a multilayer security option that would complicate any type of infiltration to an established supply chain by securing the detailed information about a product and its ingredients from the harvest point in a traceability mechanism that is protected by blockchain technology, yet it cannot fully mitigate these risks since the criminal organization can access the technology or prevent its use if it controls the entire supply chain.

For what concerns **risk scenario 2** (parallel market for catering supplies), the same considerations presented for risk scenario 1 also apply in this case. The combination of authentication via a strong digital identity with track and trace and blockchain technology, can limit the following steps of the criminal plan:

- The development of a fully-fledged supply chain for vegetables and dairy products as well as the building a parallel market for catering food supplies targeting small shops.
- Control of the anti-counterfeiting solutions used by the infiltrated businesses.
- The use of low quality and diluted materials.
- Building a parallel market for catering food supplies.
- Distortion of competition.

With reference to step 3) Develop a fully-fledged supply chain for vegetables and dairy products, step 4) Use of low quality and diluted materials, and step 5) Building a parallel market for catering food supplies, the stakeholders in the supply chain can monitor the different processes and would receive an alert if an anomaly is presented. Furthermore, the multilayer approach makes it harder for criminals to forge the security measures. In addition, if shops also use technology to perform a final check to products they receive and then sell to the final customer, then infiltration of unauthorized goods at final selling points are made much more difficult. As explained in other submissions, in this case technology also relies on the honesty of final sellers and does not apply to those cases in which the criminal group controls these shops. The possibility given to consumers to check the products they buy could assist in making the distribution more secure.

As in the case of risk scenario 1, regarding step 2) Control of the anti-counterfeiting solutions used by the infiltrated businesses, the solution can only partially mitigate the risk, since it will not prevent it if the criminal organization controls the entire supply chain. However, this solution offers an anti-counterfeit technology that is multi-layered and complicated to imitate. The investment to use the technology would be high and would probably need the involvement of outside parties to be implemented, representing a barrier for organized crime operations.

For what concerns **risk scenario 3** (e-commerce: criminal infiltration of online supermarket chains for home delivery of fake food), this submission can partly support securing online markets, especially considering the distribution component. Securing these elements could be the key to limit the following step of the criminal plan highlighted in this risk scenario:

- Selling fraudulent food as genuine via the control of well-known e-supermarkets and by copying the design, packaging and trademark of well-known producers.

The same considerations presented for the previous risk scenarios apply in this case. It is relevant to highlight that this submission provides a technology option that secures the detailed information about a product and its composition from the harvest point in a traceability mechanism that is protected by blockchain technology. The code is additionally protected by tamper-evident technology, providing a secure authentication mechanism. Any change during the process is immediately noted and the stakeholders are alerted. The flows of products along the supply chain can be checked using a scanner.

Also, in the case of risk scenario 3, other technological resources should be used to mitigate other steps of the criminal plan, which cannot be limited through supply chain security technology.

Summary table for submission 6: Possible application to limit risks highlighted by the scenarios

Scenario	**Applicability of the solution**
Scenario 1: *Infiltration of the dairy supply chain*	
Step 1 – Control of the distribution market by owning or controlling legitimate operators.	
Step 2 – Control of the supply chain using the technology owned by the controlled legitimate operators.	This submission provides a technology option that secures the detailed information about a product in a tamper-evident code and its ingredients from the harvest point in a traceability mechanism that is protected by blockchain technology. However, this technology is still package dependent and if the criminal organization owns the production facility, they can easily access the technology. Still, criminal groups would need to control the whole supply chain, including the ones related to ingredients, since traceability starts early (from the harvest of ingredients).
Step 3 – Copying local producers' packaging design and subsequent infiltration of these products into the legitimate supply chain.	Risk is reduced with the integration of scannable and tamper-evident authentication mechanisms that contain specific information about the product and by using blockchain protected track and trace technology to secure the supply chain. Any change during the process is immediately noted and the stakeholders are alerted. The flow of products along the supply chain can be checked using a scanner. This also gives consumers the possibility of performing a check.
Step 4 – Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.	The previous considerations apply to this step. The code contains specific information about the product, which is protected by the blockchain technology used in the track and trace system.

Step 5 – Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.	If the whole supply chain is controlled by organized crime or if they control legitimate operators, then an analysis of the product might be complicated to make since the only way in which this could be achieved is through an investigation after the products are sold. If the criminal group infiltrates the supply chain, an alert can be sent to inform the stakeholders about the security breach thanks to the use of blockchain technology to protect the traceability system. By scanning the code, the information about the composition of the product can be accessed.
Scenario 2: *Parallel market for catering supplies*	
Step 1 – Control over legitimate businesses.	
Step 2 – Control of the anti-counterfeiting solutions used by the infiltrated businesses.	This submission provides a technology option that secures the detailed information about a product and its ingredients in a tamper proof code from the harvest point in a traceability mechanism that is protected by blockchain technology. As clarified previously, this technology is still package dependent, but criminal groups would need to control the whole supply chain, including the ones related to ingredients.
Step 3 – Develop a fully-fledged supply chain for vegetables and dairy products.	As seen in other submissions, only if the criminal supply chain attempts to infiltrate the legitimate one at a certain stage. In this case, all the security elements highlighted in the description of the technology and its advantages will come into play to avoid this happening. In the case in which the criminal supply chain targets the final consumer or small shops directly, it has to be ensured that even small shops are using the technology and that consumers have the option to check the products they bought.
Step 4 – Use of low quality and diluted materials.	By using authentication methods, traceability systems and blockchain technology to protect the supply chain, the stakeholders would immediately receive an alert if there were an attempt to infiltrate the chain. In addition, criminal organizations would hardly use the multilayer security approach that combines these technology options. However, as mentioned above this technology is still package dependent.
Step 5 – Building a parallel market for catering food supplies targeting small shops.	The same features and limitations described in the previous stages apply for this step. Criminal groups would need to control the whole supply chain to avoid triggering an alarm since traceability starts early (from the harvest).
Step 6 – Distortion of competition.	If the supply chain is secured, then in that specific market criminals may find it more difficult to implement their criminal plan and distort competition. This can be seen as a by-product of the implementation of the technology.
Scenario 3: *E-commerce: criminal infiltration of online supermarket chains for home delivery of fake food*	
Step 1 – Control of legitimate e-operators.	
Step 2 – Selling fraudulent food as genuine through the controlled e-supermarkets.	Through the use of strong authentication measures in the product and then the control of its movements. However, since in many cases the product is directly sold to the final consumer avoiding any other intermediary passages, consumers may also have a role to play in this case. This requires that the consumer is fully aware of the authentication method and how to identify a counterfeit.

Step 3 – Expansion of e-commerce market through the creation of a Super E-food app.	
Step 4 – Creation of dedicated social network groups/pages to sell fraudulent products to final customers.	

2.3 Nuclear and other analytical techniques

This part of the report is dedicated to analysing the potential contribution to the fight against food fraud and food counterfeiting which can be achieved by using technologies aimed at examining the composition of the food product itself. By looking into its organic and chemical properties, these technologies are capable of telling if the food product is genuine or not.

If compared to supply chain security solutions, these technologies come into play at a different stage, when the supply chain has already been breached or when there is suspicion that a breach occurred. The result of the analysis can not only determine if the breach happened but can also provide important indications on the composition of the fraudulent product. The latter, when coupled with a series of analysis on suspect infringing goods, can help tracing back the origin of the fraud, while results can also be brought in court by forensic experts to provide evidence of who was responsible for the illegal actions.

Also, in this case, the discussion on the possible use of these technologies will be done through concrete examples that were collected by UNICRI through its call for submissions. As will be presented in the next paragraphs, there is a wide range of technologies that can be used to analyse food composition for forensic purposes. These include a stable isotope analysis and X-ray fluorescence (XRF), Accelerator Mass Spectrometry (AMS), PIXE (Particle-Induced X-ray Emission), RBS (Rutherford Backscattering Spectrometry), Ion Microprobe and MeV- SIMS (Secondary Ion Mass Spectrometry with MeV ions), Fourier Transform InfraRed (FTIR) spectroscopy O-PTIR (Optical-Photothermal InfraRed) spectroscopy, portable Near InfraRed (NIR) or RAMAN spectrometers.

Notwithstanding this, it is already possible to present some general interesting features which are intrinsic to these solutions, such as:

Unique result of the analysis: Geographical and environmental conditions ultimately control the elemental and isotopic makeup of a product. Nuclear techniques can determine the intrinsic isotopic and elemental fingerprints in the samples, with greater detail and accuracy than conventional methods (i.e., morphological traits, fatty acid analysis, DNA profiling, etc.).

Accountability: These techniques provide accountability through the analysis of the origin and quality of the product, which may act as a deterrent to fraudulent practices.

Detection: In the case of non-targeted methods, they are particularly useful for the detection of food adulteration because of the high number of potential adulterants that a sample can contain and because they may be adulterated with compounds not yet discovered. New adulterants that were previously unknown can be discovered simply based on an aberration of the spectrum, that is then investigated to identify what caused the aberration.

Accurate and well-established techniques: The methodology used by these techniques is highly sensitive, accurate and has been validated by a wide scientific literature. The use of the technology in other areas

provides corroboration of the usefulness and accuracy of the method. Furthermore, some methods, such as radiocarbon AMS, are bound to existing international protocols that can be applied.

Non-imitable: Isotopic signatures are very difficult to mimic. Biomarkers are compounds that have a biological specificity in the sense that they are produced only by a limited group of organisms.

Small sample handling: The sample required in order to perform the analysis is small, facilitating the process.

Multi-elemental capability: The solutions allow for multi-molecular analysis.

Non-destructive: Techniques are non-destructive, allowing the samples to be stored for new measurements if required.

Simple detection: Information of the elements present in the sample can be obtained with a limit of detection as low as a few parts per million. Sample preparation protocols demand little sample handling.

Encompassing analysis: Different kinds of materials like liquids and solids can be analysed by a single technique, thus enhancing the effectiveness and results of the analysis.

Routine applications: It is possible, in general, to make routine applications if needed.

Some possible limitations for these techniques, with some exceptions, that will be analysed later on, include:

Space: The size of a laboratory is large, therefore, in order to apply this technique, it is necessary to have considerable space to build related facilities.

Cost: The cost of the equipment is elevated (the use of a particle accelerator, usually electrostatic accelerators or cyclotrons, and ancillary equipment), which means that the initial investment is high. Other costs related to the equipment after the initial investment, such as maintenance and replacement of parts, can be significantly high.

Data dependant: The identification of different geographical origins requires the set-up of proper, solid databases. However, this limitation can transform to an advantage when the databases are created.

Time-consuming in some cases: Sample preparation can be complex and time-consuming.

Identical chemical markers: Some products have identical chemical markers, even if their origin is different. This could complicate the identification of the authentic product from a cheaper version if they both share chemical markers.

Maintenance: The results of some methods depend on the state of the instruments and their maintenance. For example, X-ray fluorescence analysis must be routinely calibrated using industry-standard reference material to maintain accuracy over repeated use cycles.

We will now use some practical examples using the submissions we received to show how the combination of all these elements can limit some of the risks highlighted by the scenarios. The use of the submissions will also allow us to appreciate the different approaches that can be followed, given the different types of technologies used.

2.3.1 Focus on portable devices

Technology submission 7

Food analysis has to consider the thousands of ingredients and additives with different chemical compositions, as well as how different food manufacturing processes affect them. The existing portable devices can essentially be grouped into two categories:

1) devices to specifically analyse one or a few analytes and,

2) devices that generate fingerprint profiles, which are typically used for screening analysis.

The increasing number of analytes make it practically and economically impossible to test for every single compound in a targeted analysis. However, there is a different approach known as non-targeted analysis also referred to as untargeted, in which the analytical technology does not test for specific compounds but generates composition fingerprints. Typical fingerprints for ingredients are stored in databases. Sample fingerprints are then compared with the typical fingerprints stored in the database. Variations proven to be statistically different from the typical profile are called abnormal samples. One of the main advantages of non-targeted analysis is the fact that one can potentially discover new adulterants that were previously unknown, simply based on an aberration of the spectrum. The aberration is then investigated to identify the cause of it. The cause for the abnormality is often not known in non-targeted analysis, requiring additional analytical investigation with targeted methods to identify the identity of the compound(s) causing the deviation. Yet, most of the devices have the algorithms already adjusted to detect some of the compounds based on their spectrum.

The technology enables the so-called Smart Sampling, a procedure where the decision of which sample to take is supported by a device (e.g., a portable NIR or RAMAN spectrometer). The approach consisting of a portable device allows the stakeholders to perform an on-site screening of the product. Screening locally would provide a quick detection of products with deviating profiles, allowing the examination of a larger quantity of products with aberrant profiles. Samples would then be taken from those products and sent to the laboratory for confirmatory analysis. This would identify the substance causing the deviation, i.e., the potential adulterant.

Cases of Smart Sampling can be observed in different situations. The portable device can perform a Near Infrared (NIR) analysis, which is a spectroscopic technique that uses the naturally occurring electromagnetic spectrum. NIR is considered an accurate and rapid analysis method that is adequate for the quantitative determination of the main constituents in most types of food and agricultural products. For example, it can be used to test the freshness of fruit, to differentiate farmed from wild fish, or to identify a variety of types of a product, such as rice.

Furthermore, the mid-infrared portable spectrometer is another type of device that can be placed in any location with a fairly small footprint to perform an analysis on the composition of food. This is not a hand-held-point device, but it can be placed on a table at a factory site. As an example, this device can be used to perform a trans-fat analysis.

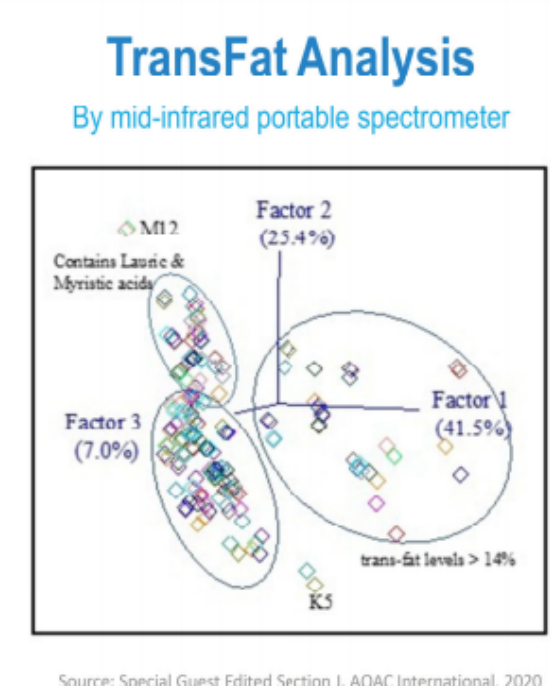
Another possible option is to adopt a multi sensor approach, where different techniques are applied to perform a comprehensive study of the product. In this case, a combination of sensors measures fluorescence, visible and UV light, as well as light in the near infrared range. This can be used to determine the authenticity of the product, e.g., the authenticity of extra virgin olive oil.

These devices do not require a scientist to operate them nor to read the results, facilitating the implementation of these technology options. Moreover, they will enable a risk-based sampling (Smart Sampling). The advent of these decision-support devices will ultimately shift the first line of analytical defence from laboratories to the food manufacturing sites, enabling risk-based sampling that will contribute to identifying quality issues and adulteration at an earlier stage than is now possible.

Submission received from FOCOS.

This technology submission allows us to discuss the interesting role that can be played by on-field portable testing devices which can provide a rapid analysis of the composition of the product.

This submission presents some unique elements if compared to the other technologies discussed in this chapter. These basically derive from the fact that, as anticipated, this submission has been designed as a portable technology for fast field testing. A field-site screening portable device permits the rapid identification of suspect samples which would have otherwise been taken randomly and sent to a laboratory. This approach saves both time and cost. Many of these portable devices require little or no sample preparation, which is another advantage. This approach will shift the first line of analytical defence from the laboratories to the food manufacturing sites or to the place where the control is performed, enabling risk-based sampling that will contribute to identifying quality issues and adulteration at an earlier stage.

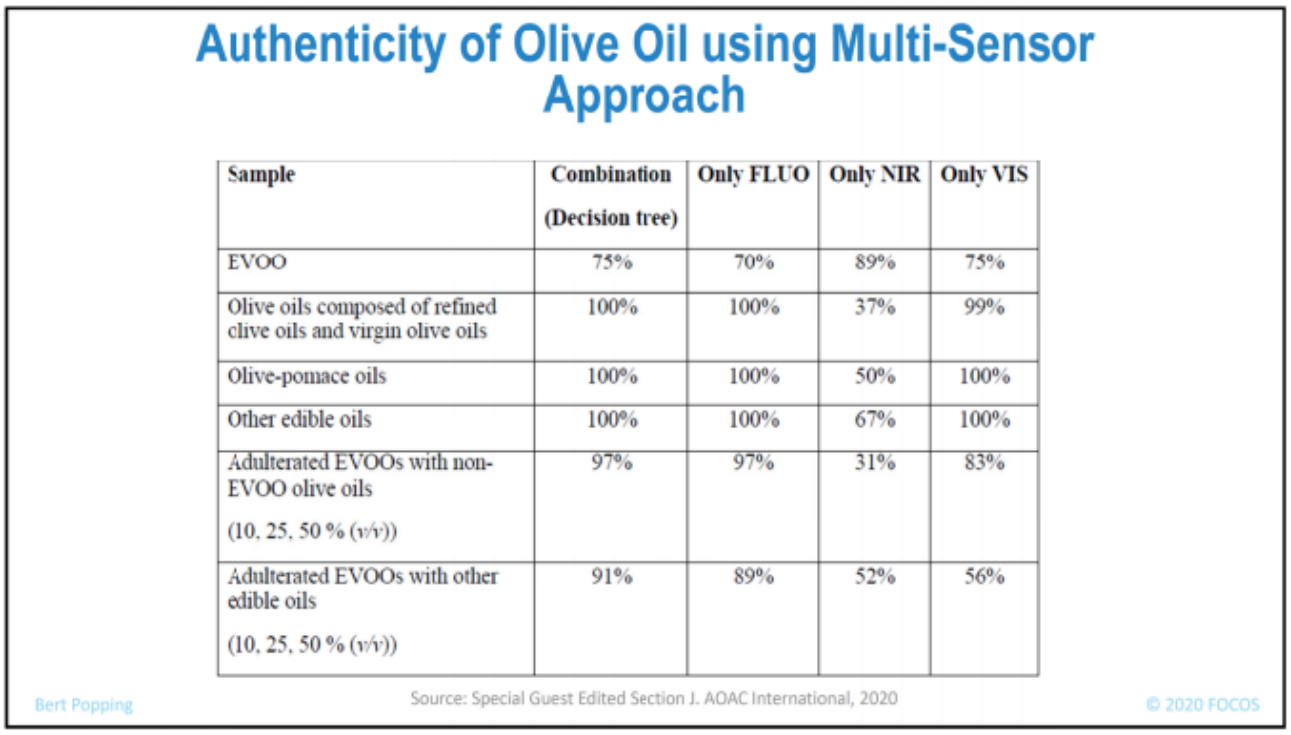


Source: Special Guest Edited Section I, AOAC International, 2020

The technology option does not require scientific expertise to be operated. Developed devices have easy-to-use user interfaces making them suitable for non-experts, for example trained factory workers, quality control managers and law enforcement agencies. When combined with some of the submissions presented in the chapter dedicated to supply chain security technology, this technology can complement rapid DNA analysis to check the information contained in the DNA ID of the food, improving the effectiveness of controls and law enforcement response against food frauds.

Source: FOCOS

For portable (as well as for laboratory) devices using non-targeted methodologies like NIR or FT-IR, appropriate reference databases are needed for the correct identification of aberrations from a reference profile. Some of these databases already exist, others will need to be built.
A second important aspect that needs to be considered for such portable devices which are operated by non-scientific staff is that the validation needs to be extended. Current validations only evaluate the method in a laboratory environment. For portable devices, the validation needs to include use by non-scientific staff under field conditions (i.e. at food manufacturers' sites or at port of entry).



Source: FOCOS

For what concerns the application to the risk scenarios, and given the focus on the composition of the food itself, the use of the technology can mitigate risks related, in particular, to repacking operations and the substitution of original products with counterfeit ones and the mislabelling of packaging to promote false claims related to the origin process or composition of the product. Furthermore, it can be used to identify if the product has been diluted or if there are adulterants in its composition. XFR can be used to identify the mineral composition of a product, which can be used to get an idea of if the product is more likely to come from the same place where it usually comes from, however, a specific "origin" identification like the one that can be obtained from a stable isotope ratio analysis is currently out of the scope of portable devices. XRF provides a multi-component, however, some of the main problems of XRF include the limited sensitivity for high mass elements and the need for pure samples. Even when an ultrapure reagent is used, impurities can appear, therefore it is mandatory to carefully measure the reference samples.[1] At the current stage, XRF is a support tool for when reference materials from one location are available and need to be compared to another, but as mentioned, this cannot be executed on a global scale at this point due to lacking databases and sensitivity.

With regard to the three risk scenarios, the solution targets some of the issues, in particular:

For what concerns **risk scenario 1**, the forensic analysis element is capable of unequivocally identifying the geographical origin of the products as well as its components. However, it has to be taken into account that these technologies will come into play once an incident occurs or once a suspicion arises. In the case of portable devices, it would be feasible to make frequent analysis of the products during their processing in the supply chain. Portable devices can be used throughout the supply chain, and identify fraud early, before it reaches consumers, and potentially even before it reaches food manufacturers. They cannot be used to prevent the criminal activity from happening (unless their continuous use over time creates a dissuasive effect on criminals), but they can be used to unequivocally identify the adulteration of a product or the fraudulent behaviour of criminals involved in food fraud. For example, if there is a person checking every bag in the incoming raw materials department, criminals would likely realize that it is complicated to infiltrate the supply chain through this means. Therefore, the portable device would also have a deterrent effect once in operation. Another possible advantage can be attained if people in one supply chain use the same technology and scan every batch. In this case, the stakeholders would be able to

1 Katerinopoulou, K., Kontogeorgos, A., Salmas, C. E., Patakas, A., & Ladavos, A. (2020). Geographical origin authentication of agri-food products: A review. Foods, 9(4), 489. doi:10.3390/foods9040489

literally trace the material, based on its NIR profile (or SERS profile), through the supply chain. Consequently, these technologies may play a role in uncovering the following steps of the criminal plan:

- Control of the supply chain by using original packaging of the businesses controlled by the criminal group to market substandard and fraudulent products.
- Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.
- Copying local producers' packaging design and subsequent infiltration of these products into the legitimate supply chain.
- Use of low-quality milk or dairy products.

By analysing the products marketed by the criminal group with the proposed technologies, it will be immediately visible that they are of low quality and that they do not originate from the correct geographical location. Adulterations and possible toxic/poisonous substances will also be revealed. On-field analysis with the portable device would enable stakeholders to perform a risk-based sampling that will contribute to identifying quality issues and adulteration at an earlier stage. The different analysis methods that can be adopted in portable devices for smart sampling offer a variety of options to examine a wide range of products. The analysis of specific elements in the composition of a product enables the clear authentication of the goods. Furthermore, by progressively analysing samples in the supply chain, it will also be able to trace back the source of the incident and present this evidence in court.

In the case of **risk scenario 2**, the technology may reduce the following steps of the criminal plan:

- Control of the anti-counterfeiting solutions to market fraudulent products using original packaging bearing authentication technology.
- Procurement of low-quality materials from areas with high levels of pollution, marketing vegetables grown using illicit pesticides as well as low-quality and diluted tomato concentrate.
- Develop a fully-fledged supply chain for vegetables and dairy products.
- Building a parallel market for catering food supplies targeting small shops.

If suspicions of criminal operations arose, the technology could be used to confirm what the criminal group was marketing using the original packaging or what elements do not correspond to the original composition of the product, and this element can also be brought in court as evidence.

The considerations already made in the case of risk scenario 1 are also valid for mitigating these steps of the criminal plan, since the technology is capable of recognizing the geographical origin of food products as well as their composition, including the presence of toxic ingredients and if they have been diluted. The technology cannot prevent infiltration but can be used to identify counterfeit products and their characteristics after the security breach occurs.

For what concerns risk scenario 3, the technology can limit the following steps:

- Selling fraudulent food as genuine via the e-supermarkets controlled by the criminal group.

The same considerations presented for the previous risk scenarios also apply in this scenario in relation to analysis that can be performed in the case of incidents or following investigations to determine the nature of products marketed by the criminal group.

Other steps of the criminal plan highlighted by the risk scenarios cannot be prevented by using this type of technology.

Summary table for submission 7: possible application to limit risks highlighted by the scenarios

Scenario	Applicability of the solution
Scenario 1: *Infiltration of the dairy supply chain*	
Step 1 – Control of the distribution market by owning or controlling legitimate operators.	
Step 2 – Control of the supply chain using the technology owned by the controlled legitimate operators.	The technology will be able to analyse the marketed products and determine if they are fraudulent and/or of low quality.
Step 3 – Copying local producers' packaging design and subsequent infiltration of these products into the legitimate supply chain.	The technology solution is able to detect counterfeit products. However, it is relevant to highlight that this technology cannot prevent infiltration, rather it works as a mechanism to identify counterfeit products and their characteristics after the security breach occurs. Criminal activity cannot be prevented unless their continuous use over time creates a dissuasive effect on criminals, but they can be used to unequivocally identify the adulteration of a product or the fraudulent behaviour of criminals involved in food fraud.
Step 4 – Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.	Adulterations and the presence of possible toxic/poisonous substances can be revealed by the technology. If the product is a milk powder, it may be possible to test with NIR-based devices which are handheld. The authentic spectra of the original is required – high quality milk powder (ideally across seasons to capture variation) and potentially adulterated, lower quality milk powder – to also train the system to distinguish the differences. If the product is liquid milk, options include: a top-level scan done by portable XRF to determine the minerals and metals in a dairy product. If it has been adulterated with a lower quality one, the mineral composition is likely to be different. This is not the most sensitive method, but it is handheld. The second option is the use of FT-IR devices. They can determine if milk has been diluted, if the protein level is lower or if other materials have been added. However, this is not handheld, even if it has a small size footprint. Again, it would be important to have authentic reference samples. These could be samples pulled directly from the farmers when they are milking the cattle.
Step 5 – Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.	The previous considerations apply to this step. The solution can identify products that are fraudulent, of low quality and whether they do not originate from the correct geographical location.

Scenario 2: *Parallel market for catering supplies*	
Step 1 – Control over legitimate businesses.	
Step 2 – Control of the anti-counterfeiting solutions used by the infiltrated businesses.	In case of proven or suspected criminal operations, the technology can be used to confirm what the criminal group was marketing using the original packaging, and the anti-counterfeiting features and this element can be brought in court as evidence. For solid products, NIR can be used to test authenticity and composition, including the fat, protein, and sugars of a product – any changes may be an indication of adulteration. However, for composite products this may be more complicated. For example, if you have pure minced meat, you will obtain similar profiles every time. If you have a sausage with varying ingredients, your profile will significantly differ. Therefore, NIR is useful for single ingredient (solid) products, but less useful if you test ready meals.
Step 3 – Develop a fully-fledged supply chain for vegetables and dairy products.	The same considerations described in step 3 of risk scenario 1 apply to this step.
Step 4 – Use of low quality and diluted materials.	Since the technology is capable of recognizing the geographical origin of food products as well as their composition, including the presence of toxic ingredients and if they have been diluted. Dilution can be tested by FT-IR in a similar way to how the dilution of milk is detected. Tomato concentrate may be tested with NIR and XRF, applying two tools that are handheld.
Step 5 – Building a parallel market for catering food supplies targeting small shops	As previously stated, the analysis would detect fraudulent or low-quality products as well as their origin. Yet, it cannot prevent infiltration, rather it works as a mechanism to identify counterfeit products and their characteristics after the security breach occurs. Criminal activity cannot be prevented, but they can be used to unequivocally identify the adulteration of a product.
Step 6 – Distortion of competition.	

Scenario 3: *E-commerce: criminal infiltration of online supermarket chains for home delivery of fake food*	
Step 1 – Control of legitimate e-operators.	
Step 2 – Selling fraudulent food as genuine through the controlled e-supermarkets.	The technology solution can be used to identify counterfeit products. Single component products are suitably analysed by NIR and potentially XRF, while liquids can be analysed by RAMAN, XRF (if they have minerals) and FT-IT.
Step 3 – Expansion of e-commerce market through the creation of a Super E-food app.	
Step 4 – Creation of dedicated social network groups/ pages to sell fraudulent products to final customers.	

2.3.2 Accelerator Mass Spectrometry

Technology submission 8

This submission focuses on the analysis of food components through the use of isotopes to identify the geographical origin of products. Stable isotope signatures of elements related to life (traditionally C, N, S, Fe; but most recently also Ca, Cu, Zn, Mo and Cl) are important biomarkers since they enable the acquisition of key information on the biological origin of organic remains, the metabolic pathways of formation and degradation of organic matter and related biominerals, as well as environmental conditions at the time of deposition.

Food is typically formed by bio-organic materials whose elemental constituents (mainly carbon, oxygen, nitrogen and sulphur) have different stable isotopes. Though different isotopes of the same element have the same number of electrons (and then form the same compounds), fractionation effects are possible during biochemical/biological/geochemical processes. Different isotopes of the same elements can show different relative partitioning between two coexisting phases in a natural system.

The accurate measurement of the abundance of a certain isotope can then provide important information about the underlying biological/biochemical/geochemical processes. For instance, carbon isotopic ratios in animal tissues and derived products are strongly influenced by animals' diet. Nitrogen isotopic values can be used to obtain information about soils, the kind of vegetation and the climate of the area where animals lived, and derived food products were obtained. Oxygen and hydrogen isotopes determined in animal tissues and products supply information about water sources and geographical origin. Different isotopes can give different information about the product (e.g., oxygen to identify the dilution of beverages and origin, carbon to identify adulteration, nitrogen to identify the origin and the use of fertilizer, sulphur to identify the origin, hydrogen to identify dilution and origin, and C-radiocarbon to identify dating).

The solution is based on the development and use of a multi-isotope approach, based on the simultaneous determination of the isotopic signature for different isotopes (H, C, N and S) to develop a powerful tool to assess the quality and the provenance of food products and to identify isotopic fingerprints for different types of food products and their geographical origin. For this purpose, techniques based on stable isotope determination are complemented with those based on the measurement of the content of 14C (radiocarbon) by using Accelerator Mass Spectrometry (AMS). The large difference in terms of isotopic signature between fossil-derived and bio-derived carbon-based products can be effectively used to identify the presence of illicit fossil sources of carbon in food products. The multi-isotope approach can be used to:

1) Assess the quality of the products.

2) Assess or certify the geographical origin of the products.

3) Identify contaminations (synthetic substances/compounds).

4) Identify dangerous agents.

In this context, the isotopic fingerprint can be used to identify and trace the origin of fraudulent products and then provide a solid basis for investigators to trace back the actors of the fraud, serving as a tool for control and investigation authorities.

Submission received from the Centre for Applied Physics, Dating and Diagnostics Department of Mathematics and Physics of the University of Salento (CEDAD)

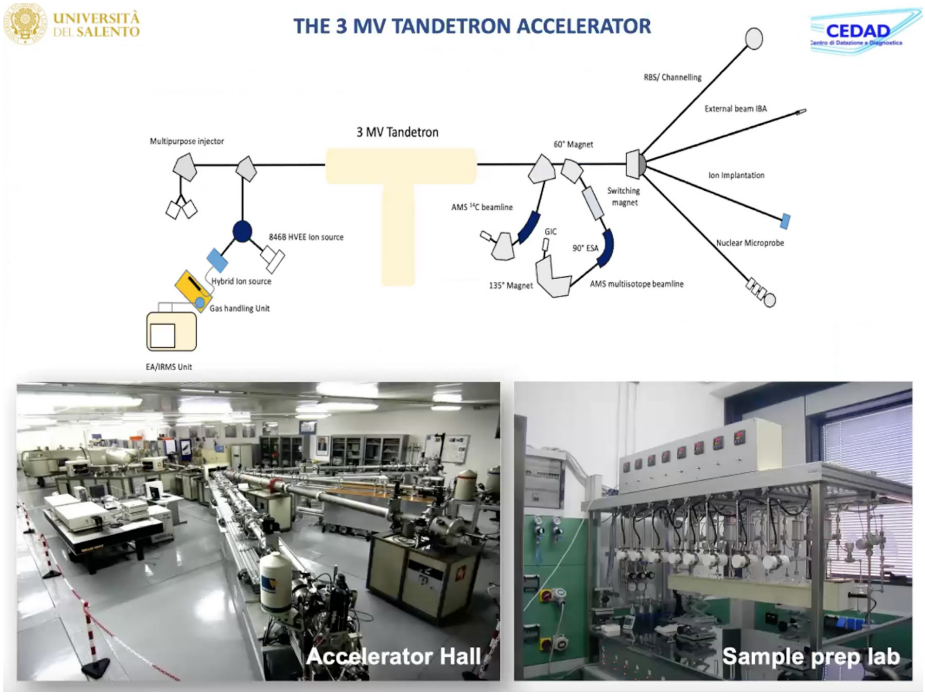
This submission can be used to show the application of Accelerator Mass Spectrometry for forensic analyses of food products. The use of this technology can provide results useful for forensic presentation in court and can support discovering breaches of the supply chain and fraudulent practices. The sample required in order to perform the analysis is small, facilitating the process, and once the sample is prepared, results are obtained quite quickly. The use of AMS techniques is well-established and the infrastructure to use them is available in most countries.

As seen in the case of submission 8, this technology also focuses on the composition of food itself and can mitigate some of the steps of the risk scenarios, in particular: repackaging operations and substitution of original products with counterfeit ones; the mislabelling of package to promote false claims related to the origin, process or composition of the product, as well as the lack of control over the product once it is packed, including the substitution of products with lower-quality or cheaper species.

Furthermore, it can be used as a tool to examine evidence and to trace the geographical origin of the product in order to determine if there was illicit infiltration in the supply chain or any other illegal activities were performed. It can also be used to identify if the product has been diluted or if there are adulterants in its composition.

Technology solutions falling within this technological approach target some of the steps of the criminal plan identified in the three risk scenarios related to food fraud. In particular, for what concerns **risk scenario 1**, the forensic analysis element is capable of unequivocally identifying the geographical origin of the products and its components. However, as clarified before, in the case of nuclear and other analytical techniques, these will come into play once an incident occurs or once a suspicion arises and cannot be used to prevent the criminal activity from happening. Consequently, these technologies may play a role in uncovering the following steps of the criminal plan:

- Control of the supply chain by using original packaging of the businesses controlled by the criminal group to market substandard and fraudulent products.
- Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.
- Use of low-quality milk or dairy products.



Source: CEDAD

By using Accelerator Mass Spectrometry to analyse products marketed by the criminal groups, it can be immediately detected that they are of low quality and that they do not originate from the correct geographical location. The use of adulterants, including possible toxic/poisonous substances, will also be revealed. Furthermore, by progressively analysing samples in the supply chain, it will also be able to trace back the source of the incident and present this evidence in court.

In the case of **risk scenario 2**, the technology may reduce risks linked to the following steps of the criminal plan:

- Control of the anti-counterfeiting solutions to market fraudulent products using original packaging bearing authentication technology.
- Procurement of low-quality materials from areas with high levels of pollution, marketing vegetables grown using illicit pesticides as well as low-quality and diluted tomato concentrate.
- Develop a fully-fledged supply chain for vegetables and dairy products.
- Building a parallel market for catering food supplies targeting small shops.

If suspicions arose of criminal operations, the technology can be used to confirm what the criminal group was marketing using the original packaging or what elements do not correspond to the original composition of the product, and this element can be brought in court as evidence. The considerations already made in the case of risk scenario 1 are also valid for mitigating these steps, since the technology is capable of recognizing the geographical origin of food products as well as their composition, including the presence of toxic ingredients and if they have been diluted.

For what concerns risk scenario 3, the technology can limit the following step:

- Selling fraudulent food as genuine via the e-supermarkets controlled by the criminal group.

The same considerations presented for the previous risk scenarios also apply in this scenario in relation to analysis that can be performed in the case of incidents or following investigations to determine the nature of products marketed by the criminal group.

Summary table for submission 8: possible application to limit risks highlighted by the scenarios

Scenario	Applicability of the solution
Scenario 1: *Infiltration of the dairy supply chain*	
Step 1 – Control of the distribution market by owning or controlling legitimate operators.	.
Step 2 – Control of the supply chain using the technology owned by the controlled legitimate operators.	The use of spectrometry would enable the identification of fraudulent, or low-quality food, and it can be used to determine the correct geographical location.
Step 3 – Copying local producers' packaging design and subsequent infiltration of these products into the legitimate supply chain.	As mentioned in the previous submissions, the adoption of this technology would allow for the identification of counterfeit products and determine if they do not originate from the correct geographical location. However, this technology cannot prevent infiltration, rather it can identify counterfeit products and their characteristics after it happens. The continuous use of this technology over time will create a dissuasive effect on criminals, but it cannot prevent criminal activities.

Step 4 – Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.	Adulterations and the presence of possible toxic/poisonous substances can be revealed by the technology.
Step 5 – Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.	The technology solution can be used to analyse the marketed products and determine if they are fraudulent, of low quality and whether they do not originate from the correct geographical location.
Scenario 2: *Parallel market for catering supplies*	
Step 1 – Control over legitimate businesses.	
Step 2 – Control of the anti-counterfeiting solutions used by the infiltrated businesses.	In case of proven or suspected criminal operations, the technology can be used to confirm what the criminal group was marketing using the original packaging, and the anti-counterfeiting features and this element can be brought in court as evidence.
Step 3 – Develop a fully-fledged supply chain for vegetables and dairy products.	Spectrometry can detect fraudulent, low-quality products and indicate if they do not originate from the correct geographical location. As previously clarified, the technology cannot prevent infiltration, but serves as a tool to identify counterfeit products after the security breach occurs. Criminal activity cannot be prevented unless their continuous use over time creates a dissuasive effect on criminals.
Step 4 – Use of low quality and diluted materials.	The technology is capable of recognizing the geographical origin of food products as well as their composition, including the presence of toxic ingredients and if they have been diluted.
Step 5 – Building a parallel market for catering food supplies targeting small shops.	The same considerations explained in step 3 apply to this stage.
Step 6 – Distortion of competition.	

Scenario 3: *E-commerce: criminal infiltration of online supermarket chains for home delivery of fake food*	
Step 1 – Control of legitimate e-operators.	
Step 2 – Selling fraudulent food as genuine through the controlled e-supermarkets.	The adoption of these technological tools can be used to analyse the marketed products and determine if they are fraudulent, of low quality and whether they do not originate from the correct geographical location.
Step 3 – Expansion of e-commerce market through the creation of a Super E-food app.	
Step 4 – Creation of dedicated social network groups/pages to sell fraudulent products to final customers.	

2.3.3 Iso-elemental fingerprinting techniques

Technology submission 9

The term seafood provenance refers to determining both the geographic origin and production method of seafood. Seafood provenance has become increasingly important to consumers, seafood industries and regulatory bodies. Methods such as DNA and fatty acid profiling, stable isotope analysis and elemental profiling using inductively coupled plasma mass spectrometry (ICP-MS) have been used to determine the origin of seafood as well as to distinguish between wild-caught and cultured seafood. Recently, bookkeeping methods such as blockchain or radio-frequency identification (RFID) have been added to trace the origins of seafood. However, each method has its advantages and disadvantages, with some methods excelling in determining the geographic origin and others better at distinguishing the production method.

The nuclear techniques used, including stable isotope analysis, ITRAX X-ray fluorescence, neutron activation analysis, and ion beam analysis technologies provide great precision in determining geographical locations of food.

The technology submission is based on iso-elemental fingerprint techniques, including stable isotope analysis and X-ray fluorescence (XRF) through the use of an Itrax scanner, to obtain the unique elemental and isotopic composition of seafood. The technology was tested on high valued seafood products such as Asian seabass and giant tiger prawns. These iso-elemental fingerprints were then used to create a provenance predicting model which could distinguish both the production methods and geographic origins of both species with greater than 80% accuracy. Following the success, a larger scale research project has been established to improve the prediction accuracy of the technology to distinguish between wild and farmed origin of seafood, including their geographical origins.

The iso-elemental fingerprint data is processed in a machine learning model where this information is analysed to find patterns in order to predict the provenance.

Furthermore, a portable method using handheld XRF to determine seafood provenance is being developed. It is expected that the portable method will be used to quickly screen seafood products, while complex samples will be analysed using the lab-based techniques to provide a higher accuracy. Regular screening points along the seafood supply chain using the handheld XRF technology in development will also ensure that any fraudulent produce is identified before it has a chance to be sold to consumers. This will provide consumers with the confidence that the product they are purchasing is legitimate, which in turn contributes to the market chain traceability. In addition to addressing seafood provenance, this technology provides the opportunity to make safety assessments for biosecurity purposes (i.e. if any bans are imposed on food products).

Submission received from the Australian Nuclear Science and Technology Organisation (ANSTO). Collaborators (University of New South Wales, Macquarie University, National Measurement Institute and Sydney Fish Market)

This submission allows us to discuss the possible use of iso-elemental fingerprint techniques to detect fraudulent activities and respond to some of the risks highlighted by the scenarios. Apart from laboratory analysis, this submission also includes the possibility to develop the use of portable methods to constantly check the supply chain and increase the chances that fraudulent food is identified before it reaches the consumer.

Interesting aspects of this submission include the wide use of iso-elemental fingerprints to determine the correct provenance of the food as well as its quality. Apart from fraudulent food detection, this could be an interesting method to ensure, for instance, that products labelled as Geographical Indications (GIs) are really produced in a specific area, respecting the established manufacturing processes. Producers and suppliers may also be able to use these iso-elemental fingerprints to brand the food, providing an option for the client to identify accurately labelled and high-quality products.

On the other hand, certain environmental factors can affect the stability of the isotopic and elemental signals. Using stable isotopes or the elemental profile alone tends to produce less reliable results when trying to predict provenance. However, using them together in mathematical models determines the geographic origin and production method of seafood (wild and farmed) with a high degree of accuracy (>80%). Therefore, using the multiple nuclear techniques can provide reliable and accurate predictions of seafood provenance.

In terms of the application of these technologies to the risk scenarios, this submission can identify frauds deriving from illicit repackaging operations and from the substitution of original products with counterfeit ones. It could also be used to identify the mislabelling of packages to promote false claims related to the origin, process or composition of the product. Furthermore, this technology can be used as a tool to examine evidence and to trace the geographical origin of the product in order to determine if there was an illicit infiltration in the supply chain or if any other illegal activities targeting the food were performed. It can also be used to identify if the product has adulterants in its composition.

In particular, for what concerns **risk scenario 1**, the forensic analysis element is capable of unequivocally identifying the geographical origin of the products as well as its production methods (wild or farmed). Nuclear and other analytical techniques only come into play once an incident occurs or once a suspicion arises. They cannot be used to prevent the criminal activity from happening, but they can be used to unequivocally identify the adulteration of a product. Consequently, these technologies may play a role in uncovering the following steps of the criminal plan:

- Control of the supply chain by using original packaging of the businesses controlled by the criminal group to market substandard and fraudulent products.
- Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.
- Use of low-quality solid dairy products.

X-ray fluorescence can be used to analyse the quality in relation to the presence of essential elements and origin of products. The analysis of specific elements in the composition of a product also enables the clear authentication of the goods. Furthermore, as previously explained, by progressively analysing samples in the supply chain, it can also trace back to the source of the incident and present this evidence in court.

In the case of risk scenario 2, the technology may reduce the following steps of the criminal plan:

- Control of the anti-counterfeiting solutions to market fraudulent products using original packaging bearing authentication technology.
- Procurement of low-quality materials from areas with high levels of pollution, marketing vegetables grown using illicit pesticides as well as low-quality and diluted tomato concentrate.
- Develop a database of elemental fingerprints fully-fledged along select nodes in the supply chain for vegetables and solid dairy products.

If suspicions arose of criminal operations, the technology can be used to confirm what the criminal group was marketing fraudulently using the original packaging or what elements do not correspond to the original composition of the product, and this element can be used in court as evidence. This can be done in the case where trace-back to the products origin (i.e. geographic location and production method) is needed. This is dependent on the final product in the packaging to be unprocessed (e.g. raw fillets, uncooked vegetables, etc), in order to determine provenance accurately. If it is only necessary to trace a product back to a producer, it is possible to do this with processed foods. However, the technology will only be able to trace the product back to the factory that produced it (dependent on having that factory's fingerprint in the database first).

The considerations already made in the case of risk scenario 1 are also valid for mitigating these steps of the criminal plan, since the technology is capable of recognizing the geographical origin of food products as well as their composition.

For what concerns risk scenario 3, the technology can limit the following step:

- Selling fraudulent food as genuine via the e-supermarkets controlled by the criminal group.

The same considerations presented for the previous risk scenarios also apply in this scenario in relation to analysis that can be performed in the case of incidents or following investigations to determine the nature of products marketed by the criminal group.

Summary table for submission 9: possible application to limit risks highlighted by the scenarios

Scenario	Applicability of the solution
Scenario 1: *Infiltration of the dairy supply chain*	
Step 1 – Control of the distribution market by owning or controlling legitimate operators.	
Step 2 – Control of the supply chain using the technology owned by the controlled legitimate operators.	X-ray fluorescence can be used to analyse the quality and origin of solid products, allowing the detection of counterfeit goods.

Step 3 – Copying local producers' packaging design and subsequent infiltration of these products into the legitimate supply chain.	The same considerations described for the previous submissions apply. The technology solution can detect if solid products are fraudulent, and if they do not originate from the correct geographical location. However, it cannot prevent infiltration, rather, after it happens it can provide accurate information about the analysed product or the fraudulent behaviour of criminals involved in food fraud. Its frequent use over time can create a dissuasive effect on criminals.
Step 4 – Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.	Adulterations of solid daily products can be revealed by the technology.
Step 5 – Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.	The features explained in step 3 also apply to this step.
Scenario 2: *Parallel market for catering supplies*	
Step 1 – Control over legitimate businesses.	
Step 2 – Control of the anti-counterfeiting solutions used by the infiltrated businesses.	In case of proven or suspected criminal operations, the technology can be used to confirm what the criminal group was marketing using the original packaging and the anti-counterfeiting features if we need to trace back to the products origin (i.e. geographic location and production method), depending on the final product in the packaging being unprocessed; or if we only need to trace it back to a producer, it is possible to do this with processed foods. However, the technology will only be able to trace the product back to the factory that produced it (dependent on having that factory's fingerprint in the database first).
Step 3 – Develop a fully-fledged supply chain for vegetables and dairy products.	The considerations analysed in risk scenario 1 also apply here. X-ray fluorescence can be used to analyse the quality and origin of solid products, allowing the detection of counterfeit goods, but cannot prevent the infiltration. Its continuous use over time might create a dissuasive effect on criminals.
Step 4 – Use of low quality and diluted materials.	The technology is capable of recognizing the geographical origin of solid food products as well as their composition, including the presence of toxic ingredients and if they have been adulterated.
Step 5 – Building a parallel market for catering food supplies targeting small shops.	The same considerations explained in step 3 apply to this step.
Step 6 – Distortion of competition.	

Scenario 3: *E-commerce: criminal infiltration of online supermarket chains for home delivery of fake food*	
Step 1 – Control of legitimate e-operators.	
Step 2 – Selling fraudulent food as genuine through the controlled e-supermarkets.	The technology will be able to analyse the marketed products and determine if they are fraudulent and if they do not originate from the correct geographical location.
Step 3 – Expansion of e-commerce market through the creation of a Super E-food app.	
Step 4 – Creation of dedicated social network groups/pages to sell fraudulent products to final customers.	

2.3.4 Using ion beam analytical techniques

Technology submission 10

In this area, one solution uses ion beam analytical techniques such as PIXE (Particle-Induced X-ray Emission), RBS (Rutherford Backscattering Spectrometry), Ion Microprobe and MeV- SIMS (Secondary Ion Mass Spectrometry with MeV ions) as tools to find markers belonging to all components of a products like, for example, wine bottles. Tandem-type accelerators provide swift protons and other ions to be used for different analytical applications. PIXE (Particle-Induced X-ray Emission) is based on the detection of characteristic X-rays stemming from the target atoms. In this way, all elements present in the sample can be quantified, leading to the identifications of particular element markers.
These markers will then be used to create the identity of an original product, leading to the possibility of identifying counterfeit ones. The analysis performed may allow for the identification of markers belonging to different materials which form the final product. The latter is seen as a whole set of elements composing it, including the product itself (organic material) and its packaging.
Following this, and in the specific example of wine bottles, the analysis to find markers includes the beverage itself, the glass of the bottle, the labels and the cork used to seal the bottle. PIXE employs energetic ions (of the order of a few MeV) provided by particle accelerators as primary probes of the material under study. The energetic ions collide with the atoms of the material giving rise to ionization and subsequent de-excitation of the target atoms, which could take place through the production of characteristic X-rays. These X-rays are then detected by suitable detectors. The data is then processed by nuclear modular electronics and stored in computers as X-ray spectra. These spectra are analysed by specialized computer software in order to obtain the desired information and differentiate original products from counterfeit ones in the case in which an incident occurred or if the need for this type of control arose.
Submission received by Ion Implantation Laboratory, Institute of Physics of the Federal University of Rio Grande do Sul.

The use of ion beam analytical techniques, as seen also in the previous submissions in this area, can support limiting certain risks highlighted by the scenarios. They are accurate and well-established techniques with multi-elemental capacity and reasonable sensitivity. By using PIXE (Particle-Induced X-ray Emission), for instance, the sensitivity is equal to 1 mg/kg (1 ppm). These techniques are non-destructive for the sample and can be used to analyse different kinds of materials.

As seen in the case of previous submissions, the use of these techniques comes into play when a possible breach of the supply chain has to be discovered and suspect, fraudulent products are analysed to determine their composition. Consequently, they can be used to identify repackaging operations and substitution of original products with counterfeit ones as well as the mislabelling of packages to promote false claims related to the origin, process or composition of the product. They can also be used to examine evidence of fraud in the food area and, by further analysing suspect, fraudulent products in the supply chain, to trace back the origin of the product to its source. Furthermore, they can be used to identify if the product has been diluted or if there are adulterants in its composition.

In particular, for what concerns risk scenario 1, the forensic analysis element is capable of unequivocally identifying the geographical origin of the products as well as their components. Consequently, these technologies may play a role in uncovering the following steps of the criminal plan:

- Control of the supply chain by using original packaging of the businesses controlled by the criminal group to market substandard and fraudulent products.
- Distribution of the falsified goods via the criminal group comprehensive and well-structured network, which includes wholesalers and supermarkets controlled by their frontmen.
- Use of low-quality milk or dairy products.

As explained in the previous submissions, using these analytical techniques would enable the identification of adulterants, and the origin and composition of products. Furthermore, by progressively analysing samples in the supply chain, it will also be able to trace back the source of the incident and present this evidence in court.

In the case of risk scenario 2, the technology may reduce the following steps:

- Control of the anti-counterfeiting solutions to market fraudulent products using original packaging bearing authentication technology.
- Procurement of low-quality materials from areas with high levels of pollution, marketing vegetables grown using illicit pesticides as well as low-quality and diluted tomato concentrate.
- Develop a fully-fledged supply chain for vegetables and dairy products.
- Building a parallel market for catering food supplies targeting small shops.

If suspicions arose of criminal operations, the technology can be used to confirm what the criminal group was marketing using the original packaging or what elements do not correspond to the original composition of the product, and this element can be brought in court as evidence.

The considerations already made in the case of risk scenario 1 are also valid for mitigating these steps, since the technology is capable of recognizing the geographical origin of food products as well as their composition, including the presence of toxic ingredients and if they have been diluted.

For what concerns risk scenario 3, the technology can limit the following step:

- Selling fraudulent food as genuine via the e-supermarkets controlled by the criminal group.

The same considerations presented for the previous risk scenarios also apply in this scenario in relation to analysis that can be performed in the case of incidents or following investigations to determine the nature of products marketed by the criminal group.

Summary table for submission 10: possible application to limit risks highlighted by the scenarios

Scenario	Applicability of the solution
Scenario 1: *Infiltration of the dairy supply chain*	
Step 1 – Control of the distribution market by owning or controlling legitimate operators.	
Step 2 – Control of the supply chain using the technology owned by the controlled legitimate operators.	PIXE (Particle-Induced X-ray Emission), RBS (Rutherford Backscattering Spectrometry), Ion Microprobe and MeV-SIMS (Secondary Ion Mass Spectrometry with MeV ions) are able to analyse products and determine if they are fraudulent, of low quality and whether they do not originate from the correct geographical location by comparing particular markers in both original and counterfeit products.
Step 3 – Copying local producers' packaging design and subsequent infiltration of these products into the legitimate supply chain.	As explained for the previous submissions, the technology can be used to detect counterfeit products since it can analyse the composition of food and can determine its origin. This, however, cannot prevent the infiltration. The continuous use of these technologies over time will create a dissuasive effect on criminals, but they can be used to unequivocally identify the adulteration of a product or the fraudulent behaviour of criminals involved in food fraud.
Step 4 – Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.	Adulterations and the presence of possible toxic/poisonous substances can be revealed by the technology
Step 5 – Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.	The same considerations explained in step 2 apply to this step.
Scenario 2: *Parallel market for catering supplies*	
Step 1 – Control over legitimate businesses.	
Step 2 – Control of the anti-counterfeiting solutions used by the infiltrated businesses.	In case of proven or suspected criminal operations, the technology can be used to confirm what the criminal group was marketing using the original packaging and the anti-counterfeiting features and this element can be brought in court as evidence.

Step 3 – Develop a fully-fledged supply chain for vegetables and dairy products.	As explained for the previous submissions, the technology will be able to analyse the marketed products and determine if they are counterfeit and whether they do not originate from the correct geographical location. However, it is relevant to highlight that this technology cannot prevent the infiltration, rather it works as a mechanism to identify counterfeit products and their characteristics after the security breach occurs. The continuous use over time will create a dissuasive effect on criminals.
Step 4 – Use of low quality and diluted materials.	The technology is capable of recognizing the geographical origin of food products as well as their composition, including the presence of toxic ingredients and if they have been diluted.
Step 5 – Building a parallel market for catering food supplies targeting small shops.	The same considerations explained in step 3 apply to this step.
Step 6 – Distortion of competition.	
Scenario 3: *E-commerce: criminal infiltration of online supermarket chains for home delivery of fake food*	
Step 1 – Control of legitimate e-operators.	
Step 2 – Selling fraudulent food as genuine through the controlled e-supermarkets.	The technology will be able to analyse the marketed products and determine if they are fraudulent, of low quality and whether they do not originate from the correct geographical location.
Step 3 – Expansion of e-commerce market through the creation of a Super E-food app.	
Step 4 – Creation of dedicated social network groups/ pages to sell fraudulent products to final customers.	

2.3.5 Fourier Transform InfraRed (FTIR) spectroscopy, Optical- Photothermal InfraRed (O-PTIR) spectroscopy and X-ray Fluorescence spectroscopy (XRF)

Technology submission 11

A different submission in this area proposes several solutions that enable screening for abnormalities in a given product and identify its geographical origin.

These solutions use several techniques, such as:

1) The Fourier Transform InfraRed (FTIR) spectroscopy, which measures the fundamental vibrations of covalently bound atoms in molecules and identifies the unique spectrum of a compound and may be

treated as a molecular fingerprint. This technique may be also applied to authenticate products and search for adulterants in food.

2) The O-PTIR (Optical-Photothermal InfraRed) spectroscopy, which works as a non-contact, far-field reflection mode and delivers high quality, spatially resolved FTIR transmission-like spectra below the diffraction limit of infrared wavelengths.

Both FTIR and O-PTIR can be applied to verify the provenance and authenticity of the food and to detect dilution or illegal additives. FTIR spectra may be shared among the actors of the supply chain from the manufacturer, through distributors, to the final user in order to check the preservation of quality. By using semi-portable devices, it is possible to set up intermediate checkpoints to avoid the insertion of illicit products within the supply chain.

3) X-ray fluorescence (XRF) spectroscopy, which is a well-known technique to analyse the multielemental content of different kinds of samples in a non-destructive manner.

X-ray fluorescence photons are collected when an ion/synchrotron radiation beam excites the inner shell electrons in the target atoms (PIXE: Proton Induced X-ray Emission; SRIXE: Synchrotron Induced X-ray Emission). As a result of the ejection of inner electrons, X-rays are emitted to fill created vacancies. The energies of X-rays are characteristic of the elements from which they originate, and their number is proportional to the mass of the corresponding element in the sample being analysed. XRF spectroscopy has a huge range of applications including chemistry, life science, medicine, earth science, cultural heritage, environmental science, material science and forensics. XRF is the only technique that can provide definitive data to quantify elements like iron, zinc, phosphorus and other trace elements.

The food materials may be screened for their geographic location by trace element profiling and concentration variations. Most importantly, they may be checked for potentially poisonous materials such as lead, nickel or arsenic.

Submission received from Singapore Synchrotron Light Source

As seen during previous chapters of this report, these techniques have a great potential of verifying if a breach of the food supply chain has happened by analysing the composition of the suspicious food itself. FTIR, O-PTIR and XRF are accurate analytical techniques which are well-established and only need small sample handling. Additionally, O-PTIR eliminates one of the longstanding limitations for IR microscopy, namely the inability to work on thick samples.

FTIR and O-PTIR spectra are searchable and interpretable in both commercial and institutional IR databases without mathematical modelling. This fact allows for very quick and independent analysis.

XRF and FTIR methods can be applied with portable or semi-portable devices, hence the increase of their usage in field analysis.

On the other hand, the use of these techniques usually necessitates highly qualified staff and some of the techniques have limitations in detection. In the case of FTIR, for instance, the detection limit is around 1% and if mixture is multicomponent, the separation of all ingredients can be complicated and usually requires the use of multivariate statistical methods. As was mentioned earlier, FTIR spectroscopy measures the fundamental vibrations of covalently bound atoms in molecules, hence each chemical compound has its own unique spectrum that may be treated as the molecular fingerprint.

In the case of XRF, the emitted X-rays may be attenuated or enhanced by material surrounding the sample of interest (matrix effects) and there is also a clear inability to measure radiation from all elements.

For what concerns the application to the risk scenarios, the considerations are similar to those that were presented for other submissions in this area. These technologies can be used to identify repackaging operations and substi-

tution of original products with counterfeit ones, as well as the mislabelling of packages to promote false claims related to the origin, process or composition of the product. They can be used as a tool to examine evidence and to trace back the origin of the product, as well as to identify if the product has been diluted or if there are adulterants in its composition.

In particular, for what concerns risk scenario 1, elemental analysis is capable of unequivocally identifying the geographical origin of the products as well as its components. Consequently, these technologies may play a role in uncovering the following steps of the criminal plan:

- Control of the supply chain by using original packaging of the businesses controlled by the criminal group to market substandard and fraudulent products.
- Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.
- Use of low-quality milk or dairy products.

The same considerations explained in the previous submissions also apply here. One of several of the technology options can be selected to perform the analysis, depending on the type of material that is being processed or the type of issues that are being identified. For example, FTIR and O-PTIR technologies may be applied to verify the provenance and authenticity of the food and to detect dilution or illegal additives. FTIR spectra may be shared among the actors of the supply chain from the manufacturer, through distributors, to the final user in order to check the preservation of quality; whereas XRF is the only technique that can provide definitive data to quantify the elements like iron, zinc, phosphorus and other trace elements. The food materials may be screened for their geographic location by trace element profiling and concentration variations. Most importantly, they may be checked for potentially poisonous materials such as lead, nickel or arsenic.

In the case of risk scenario 2, the technology may reduce the following steps:

- Control of the anti-counterfeiting solutions to market fraudulent products using original packaging bearing authentication technology.
- Procurement of law-quality materials from areas with high levels of pollution, marketing vegetables grown using illicit pesticides as well as low-quality and diluted tomato concentrate.
- Develop a fully-fledged supply chain for vegetables and dairy products.
- Building a parallel market for catering food supplies targeting small shops.

If suspicions of criminal operations arose, the technology can be used to confirm what the criminal group was marketing using the original packaging or what elements do not correspond to the original composition of the product, and this element can be brought in court as evidence.

The considerations already made in the case of risk scenario 1 are also valid for mitigating these steps, since the technology is capable of recognizing the geographical origin of food products as well as their composition, including the presence of toxic ingredients and if they have been diluted.

For what concerns risk scenario 3, the technology can limit the following step:

- Selling fraudulent food as genuine via the e-supermarkets controlled by the criminal group.

The same considerations presented for the previous risk scenarios also apply in this scenario in relation to analysis that can be performed in the case of incidents or following investigations to determine the nature of products marketed by the criminal group.

Summary table for submission 11: possible application to limit risks highlighted by the scenarios

Scenario	Applicability of the solution
Scenario 1: *Infiltration of the dairy supply chain*	
Step 1 – Control of the distribution market by owning or controlling legitimate operators.	
Step 2 – Control of the supply chain using the technology owned by the controlled legitimate operators.	FTIR, O-PTIR and XRF analyses can provide accurate information about the composition of the products and determine if they are counterfeit, of low quality and whether they do not originate from the correct geographical location.
Step 3 – Copying local producers' packaging design and subsequent infiltration of these products into the legitimate supply chain.	As previously described, the technology options can identify the composition and origin of food, although they cannot prevent infiltration. The solutions can only mitigate the risk if their continuous use over time creates a dissuasive effect on criminals, but they can be used to unequivocally detect the adulteration of a product or the fraudulent behaviour of criminals involved in food fraud.
Step 4 – Procurement of low-level milk or dairy products, their packaging with falsified labels imitating the design of legitimate and well-known local producers, and their insertion into the supply chain.	Adulterations and the presence of possible toxic/poisonous substances can be revealed by the technology.
Step 5 – Distribution of the falsified goods via the criminal group comprehensive and well- structured network, which includes wholesalers and supermarkets controlled by their frontmen.	The considerations explained in step 3 apply to this step.
Scenario 2: *Parallel market for catering supplies*	
Step 1 – Control over legitimate businesses.	
Step 2 – Control of the anti-counterfeiting solutions used by the infiltrated businesses	In case of proven or suspected criminal operations, the technology can be used to confirm what the criminal group was marketing using the original packaging, and the anti-counterfeiting features and this element can be brought in court as evidence.
Step 3 – Develop a fully-fledged supply chain for vegetables and dairy products	As explained in the analysis of risk scenario 1, the technology options can analyse the marketed products and determine if they are fraudulent, of low quality and whether they do not originate from the correct geographical location. However, they cannot prevent the infiltration, unless their continuous use over time creates a dissuasive effect on criminals.
Step 4 – Use of low quality and diluted materials.	The technology is capable of recognizing the geographical origin of food products as well as its composition, including the presence of toxic ingredients and if it has been diluted.

Step 5 – Building a parallel market for catering food supplies targeting small shops.	The same considerations described in step 3 apply to this step.
Step 6 – Distortion of competition.	
Scenario 3: *E-commerce: criminal infiltration of online supermarket chains for home delivery of fake food*	
Step 1 – Control of legitimate e-operators.	
Step 2 – Selling fraudulent food as genuine through the controlled e-supermarkets.	The technology will be able to analyse the marketed products and determine if they are fraudulent, of low quality and whether they do not originate from the correct geographical location.
Step 3 – Expansion of e-commerce market through the creation of a Super E-food app.	
Step 4 – Creation of dedicated social network groups/ pages to sell fraudulent products to final customers.	

2.4 Examples of technology targeting e-commerce fraud

Technology option for e-commerce 1

The technology solution uses artificial intelligence to detect fraudulent product reviews and third-party sellers. Fraudulent reviews are used by sellers of counterfeit goods to create a false public image of consumer trust and exploit the fact that online consumers frequently use existing reviews as a reference point to base their purchases on, making them an important factor to consider in order to increase sales and consumer trust. Through the use of big data analytics and artificial intelligence, this technology option can identify fraudulent reviews supporting the selling of counterfeit products online.

The solution consists in an online analyser bar where consumers can introduce the web address of a website in which the product they are interested in is being advertised. Another option is to install a browser extension in order to have a real-time analysis.

As a result of the analysis, the technology displays relevant information related to the product, including:

1) A review grade that compares the review displayed on the website or app with the one generated by the analyser,

2) Highlights on the product (quality, packaging, competitiveness), its overview (reliability, deception level, total number of reviews), details about the reviews, insights, and review count and price graphs. In addition to the online analyser bar and the browser extension, the technology also gives consumers the possibility of downloading an app to perform the same check on a smartphone.

This is a customer-centric solution that helps individuals to identify fraudulent products and providers through the detection of faults in the algorithms of the marketplace platforms, thus highlighting false reviews or suspicious low prices that can be the symptoms of counterfeit products and fraudulent sellers.

Technology developed by Fakespot

This submission highlights the possibility that consumers are unaware of possible fraudulent purchases. It therefore allows them to check the authenticity of the sellers, by providing a tool to identify fraudulent reviews in online market stores.

The tool works by conducting a real-time analysis. Both the browser extension and the online platform perform an analysis at the moment the customer wants to perform a purchase. The analysis takes from a few seconds to a minute, providing a quick feedback of the seller. The online platform displays a complete overview related to the product the potential buyer would like to purchase, including: a review grade that compares the review displayed on the website or app with the one generated by the analyser, the product's highlights (quality, packaging, competitiveness), its overview (reliability, deception level, total number of reviews), details about other reviews, insights, a review count and price graphs.

In view of being user-friendly, the technology solution displays the most relevant information found during the analysis to the user, while highlights enable the user to easily identify threats. Furthermore, through the analysis of consumer reviews, the system can identify suspicious activities and the information is used to recommend better alternatives to consumers. Its functioning is also quite simple, since it only requires that the customer copies and pastes the URL of the website where they are looking for a product to a search bar on the online platform or the app to start the analysis. The browser extension does the analysis automatically.

Finally, the solution can be downloaded and used for free.

This is an interesting approach which, however, is of course dependant on the analysis of customer reviews in comparison to other products advertised on the website, making the scope of analysis relatively small. The results from the analysis depend on the feedback of real customers. If they do not provide a negative feedback after their purchase, even if they identify issues, then their experience of the product will not be used in the analysis made by the solution. Even if the analysis of reviews and prices can provide useful insights, it may be difficult to identify if the provider is selling a counterfeit product or if there are other related issues. A characteristic that could help in this case is the highlighting of comments from real reviews that might mention the nature of the problem.

Notwithstanding this, the tool provides an interesting option at no cost to enable customers to perform a fast check on the product they intend to purchase online based on the engagement of customers with online marketplaces.

For **risk scenario 3,** this submission can partly support securing online markets, limiting the following risks deriving from the criminal plan:

- Selling fraudulent food as genuine via the control of well-known e-supermarkets and by copying the design, packaging and trademark of well-known producers.
- Creation of dedicated social network groups/pages to sell fraudulent products to final customers.

This technology solution is not centred on the supply chain in general, but on the commercialization of products in online markets. Considerations on the role of consumers apply in this case and are possibly even more relevant, since online purchases may involve a direct relationship and line of shipping from the seller to the purchaser. This requires that the consumer is fully aware of the verification method and how to interpret the analysis provided. The analysis of the product can alert the customer about certain characteristics of the seller or the product itself, which would prevent its purchase. False product reviews are used to manipulate the existing algorithms of the online-based markets in order to promote products and brands by making them appear genuine.

Summary table for e-commerce submission 1: possible application to limit risks highlighted by the scenario

Scenario	Applicability of the solution
Scenario 3: *E-commerce: criminal infiltration of online supermarket chains for home delivery of fake food*	
Step 1 – Control of legitimate e-operators.	
Step 2 – Selling fraudulent food as genuine through the controlled e-supermarkets.	Technologies, such as big data analytics and artificial intelligence may be used to monitor the creation of false reviews in online markets. However, if the website is fully owned by the criminal organization and does not accept feedback from customers, the solution might not work correctly.
Step 3 – Expansion of e-commerce market through the creation of a Super E-food app.	
Step 4 – Creation of dedicated social network groups/pages to sell fraudulent products to final customers.	In the case in which the collection of reviews also targets activities on social media, then this risk can be limited.

Technology option for e-commerce 2

Other technology solutions are focused on providing security measures to the businesses that use e-commerce to distribute goods. These options use big data analytics to systematically monitor search engines, social media, online marketplaces, instant messaging apps and web pages, mobile app stores, aggregators, domain names, contextual advertising, and in some cases, the deep web.

Machine learning is adopted to analyse and classify information, as well as to identify the connections between websites and users in order to have integral insights of the online sale of counterfeit products. These solutions also avail themselves of the additional support of experts to corroborate the results obtained to conduct a comprehensive investigation, which sometimes includes test purchases to obtain evidence.

In a nutshell, these technology options are based on three main processes:

1) Continuous online monitoring,

2) Detecting violations and online counterfeiting through the use of machine learning, providing an analysis of connections between sellers and websites to reveal more complex networks of groups or of individuals selling in different platforms,

3) Eliminating fraudulent content, which is partially automated due to certifications and agreements with social media networks. Otherwise, provision of legal support if needed.

In some cases, and also by liaising with competent law enforcement authorities, these technologies may enable a company to take down online content, to block websites, and even to detect the entire chain of counterfeit distribution with point-of-sale analysis and comprehensive investigations. The technology solutions include Cloud-based platforms that are able to display real-time analytics and insights through the reporting of key performance indicators (KPIs) and the most relevant results, such as the status of the infringements and the infringements' segmentation.

Technology developed by Group-IB, OpSec, and Smart Protection

These technologies are interesting since they allow the use of big data analytics and artificial intelligence to perform deep monitoring of e-commerce platforms, apps, social media activity, and other online elements that are used in the distribution of counterfeit goods. Real-time analysis is continuously performed using big data analytics, enabling an accurate assessment of the ongoing situation and giving the user time to make decisions to act against a possible threat. The combination of big data analytics and machine learning techniques facilitates the recognition of abnormal patterns and behaviours indicating fraudulent activity.

For this purpose, machine learning uses algorithms that absorb data, to later produce more precise models based on that information. If the solutions are using the right algorithms and information, it is possible to continuously train the machine learning model and learn from its outcomes by further analysing the data. These technology solutions offer platforms to facilitate the display of the most relevant information found during the analysis for the user. Graphs and highlights enable the user to easily identify threats. They can also be adapted to different industries and for diverse products or brands from the same company.

When cooperation is established with competent law enforcement authorities, these solutions can also lead to the elimination of the fraudulent content. The elimination can be partially automated in some cases; however, the solutions offer the possibility of providing users with the tools and legal assistance to remove the rest of the content.

Some issues may derive from the functioning of algorithms used for the detection of the counterfeit products offered via e-commerce means, since mistakes in classifications may occur and original products might be classified as counterfeits. However, the use of human intermediaries to corroborate the accuracy of the detection can minimize this issue. Finally, the degree of effectiveness of independent takedown and website blocking procedures remains to be seen.

For what concerns the application to the risk scenario, these technology options are focused on providing tools to enable business owners to perform a continuous monitoring of the products and the commercialization of counterfeit ones in online markets, and can reduce risks related to the following steps of the criminal plan:

- Selling fraudulent food as genuine via the control of well-known e-supermarkets and by copying the design, packaging and trademark of well-known producers.
- Expansion of e-commerce market through the creation of a Super E-food app.
- Creation of dedicated social network groups/pages to sell fraudulent products to final customers.

These technology solutions are not centred on the supply chain in general, but on the commercialization of products through online markets. Big data analytics and machine learning are used to monitor the different online platforms where products can be sold or advertised, since algorithms programmed through machine learning can identify fraudulent offerings. These tools also enable the identification of users or groups involved in fraudulent offerings in different platforms, facilitating the understanding of how groups operate online. If confirmed by experience, the fact that the online promotion of counterfeit products can be eliminated almost immediately is an advantage that targets the fast movements of counterfeit goods in the online markets.

Scenario	Applicability of the solution
Scenario 3	
Step 1 – Control of legitimate e-operators.	
Step 2 – Selling fraudulent food as genuine through the controlled e-supermarkets.	Through the constant monitoring of the different online platforms where products can be sold or advertised, algorithms programmed through machine learning can eliminate and identify fraudulent food.

Step 3 – Expansion of e-commerce market through the creation of a Super E-food app.	Big data analytics can be used to monitor apps, allowing the user to obtain an alert if an app is selling counterfeit goods.
Step 4 – Creation of dedicated social network groups/pages to sell fraudulent products to final customers.	Big data analytics can target social media as part of the constant monitoring of the e-commerce platforms. Groups and users selling fraudulent products can be eliminated or reported.

2.5 Conclusions

The agro-food mafia risk scenarios presented some of the threats that can affect the integrity of the supply chain. Thanks to research conducted by UNICRI and the submissions we received from technology experts; it has been possible to assess how technology solutions may contribute to increase the security of the supply chain of these products while limiting related criminal activities.

Existing technology solutions usually encompass one or several of these elements to protect the flow of products in the supply chain:

- **Authentication technology:** This option is defined by specific characteristics that allow the differentiation of a product to help the different stakeholders of the supply chain, which could possibly include consumers, to identify original products and, consequently, the presence of counterfeits. To define what an original product is, it is possible to refer to certain intrinsic features of the product itself or to apply specific technology on the product, which will provide for the distinction between original and counterfeit (a hologram or a code, for instance). The solutions can be overt (using the sensorial capability of the individual) or covert (that require a device or an additional tool to be revealed) or a combination of both.

- **Track and trace systems:** Frequently, authentication technology on the products is coupled with the implementation of track and trace systems that allow the **monitoring** of the authenticated goods throughout the different stages of the supply chain and secure the latter from infiltration of unauthorized products. This grants visibility to identify illicit activities related to the deviation of the products from the supply chain, including the use of expired or low-quality products that are repacked and relabelled with falsified dates, dosage and brand information. Traceability options can also use **space technologies** as a proof of origin as well as for monitoring purposes.

- **Blockchain technology:** This solution has been integrated to traceability systems. It can connect the different parties in the supply chain that have not established trusted relationships with each other, by ensuring transparency. Blockchain stores every transaction or exchange of data that occurs in the network, reducing the need for intermediaries by providing a means by which all the actors in the network may share access to the same information, including what is added to the data, by whom, and the date and time of the submission.[2]

- **Forensics**: A product resulting from the supply chain process can be seen as the culmination of certain **contingencies** (nodes in the supply chain) and **continuities** (production methods) intrinsic in its manufacture. Forensics can be used to analyse a product which has already reached the market to verify if it is counterfeit or not. This evidence can even be brought in **court** to support allegations of counterfeiting since it may also serve as a tool to trace back the origin of the incident and to compare other counterfeits to verify if they have the same origin. In the case of food fraud, the following techniques can be used: stable isotope

2 Accenture. (2019, January 15). Tracing the Supply Chain. Retrieved August 23, 2020, from https://www.accenture.com/_acnmedia/pdf-93/accenture-tracing-supply-chain-blockchain-study-pov.p

analysis, Accelerator Mass Spectrometry, PIXE (Particle-Induced X-ray Emission), RBS (Rutherford Backscattering Spectrometry), Ion Microprobe and MeV-SIMS (Secondary Ion Mass Spectrometry with MeV ions), Fourier Transform InfraRed (FTIR) spectroscopy, O-PTIR (Optical- Photothermal InfraRed) spectroscopy, XRF (X-ray Fluorescence) spectroscopy, using PIXE (Proton induced X-rays emission) and SRIXE, portable NIR or RAMAN spectrometers.

The submissions analysed in the report use different types of technology that are applied following various approaches. Technology is frequently combined to provide multiple levels of security and to achieve a combination of objectives. The submissions might use similar approaches to mitigate risks, however, they offer unique features that focus on the use of specific technology tools. In the case of food fraud, the submissions offered the following approaches:

- **Use of package-based authentication mechanisms that are combined with traceability systems.** They also combine the identification of the original product with a track and trace technology, in order to monitor goods throughout the supply chain. These systems are frequently secured with blockchain technology to protect the exchange of data between the different authorized stakeholders. This approach is taken by submission 3, which additionally proposes the use of data analytics in a platform to obtain relevant insights. Submission 1 provides the option of integrating track and trace technology and blockchain. Submission 2 also adopts this approach and incorporates a hidden code on the packaging and a smartphone app equipped with a specific algorithm for the digital decoding of the printed code, a web-based interface for the management of information connected with the production in the supply chain, and Information Communication Technology (ICT) communication infrastructure for product authentication. This approach is **package-dependent**; therefore, traceability begins at the first packaging point and is linked to the package, not the product. The content of the package is not directly linked to the authentication feature, which limits the protection against a possible manipulation of the content or a substitution of the product before the first packaging point. This element is relevant in those cases in which the criminal organizations control manufacturing companies

- **Use of package-based authentication mechanism to secure the various ingredients of food products,** combined with a traceability system. This approach provides for a solution that secures the composition of the food and of all its ingredients throughout the supply chain. Submission 6 uses tamper-proof labelling solutions to create the digital identity of the product, which is adopted to secure the detailed information about such product and its composition from the harvest point in a traceability mechanism that is protected by blockchain technology. In this way, the solution protects not only the final processed food, but also all its ingredients along the supply chain before they are processed into the final product. This is also a package-dependent solution, but criminals should control the entire supply chain of all ingredients to realize some steps of the criminal plan.

- **Use of a multilayer approach that links the content of a product to the other security measures can be adopted.** This approach adopts a combination of technologies to target the complex risks in an integral manner by using the unique identity of the product (by obtaining the specific composition and other characteristics to create a DNA fingerprint), a traceability system that connects the physical and digital identity of the product, blockchain technology to protect the data exchange and the mass balance equation, data analytics in a platform to have an overview of the supply chain and space technologies for proof of origin as well as for track and trace. In addition to the protection of the package, this approach adds securing the food itself together with end-to-end monitoring of the supply chain. The biometry of the product to create an inimitable identification reference of the product and the mass balance equation protection are essential to achieve this. Submission 4 provides this combination of technologies to protect the integrity of the supply chain. Submission 5 proposes a similar approach which, however, still has to fully develop and integrate the DNA analysis element in the actual technology portfolio. Cooperation with other stakeholders and technology providers may facilitate this integration.

- **Forensic and nuclear analytical techniques** have a different approach, since they do not focus on preventing infiltration, but can be used to identify counterfeit products and their characteristics **after the security breach occurs**. The technology is capable of recognizing the geographical origin of food products as well as their composition, including the presence of toxic ingredients and if they have been diluted. These technologies will come into play once an incident occurs or once a suspicion arises. In the case of portable devices

using these technologies, they are a very interesting element since their widespread use and diffusion may allow for the possibility to conduct frequent analysis of the products during processing in the supply chain. Their continuous use over time might create a dissuasive effect on criminals and they can be used to unequivocally identify the adulteration of a product or the fraudulent behaviour of criminals involved in food fraud. Submissions 8, 10 and 11 use this approach to analyse the products. Submission 7 presents the concept of using a portable device to make routine checks without the need of using an external laboratory and submission 9 is currently in the process of developing a portable device.

- Technology solutions for **e-commerce** centre on the commercialization of products in online markets, not on the entire supply chain. **Big data analytics and artificial intelligence** are used in this approach to analyse the large amount of data exchange in online transactions. Big data analytics can be used to systematically monitor search engines, social media, online marketplaces, customer reviews, instant messaging apps and web pages, mobile app stores, aggregators, domain names, contextual advertising, and in some cases, the deep web. Machine learning is adopted to analyse and classify information, as well as to identify the connections between websites and users in order to have integral insights of the online sale of counterfeit products. Technology option 1 and 2 adopt this approach to mitigate risks.

With specific reference to the risks that were highlighted by the risk scenarios, the following considerations can be made:

- Criminal organizations are able to **infiltrate the legitimate supply chain at various stages and by using complex techniques** that include the exploitation of technology itself, taking advantage of corruption opportunities, obtaining resources from other illicit activities, theft, shark loans, package manipulation and imitation, procurement of low-quality products, creation of distribution channels, among others. As a consequence, the solutions adopted to secure the supply chain should consider the use of a multilayer security approach, bringing together multiple technologies to support stakeholders and authorities. This element has been confirmed by the majority of the submissions that we received, where multilayer security was at the core of many of them.

- Some criminal activities highlighted by the scenarios cannot be limited by supply chain security technology. This has to be expected since the main purpose for which these technologies were developed is to protect the integrity of the supply chain and not to stop different kinds of criminal operations. This is the case, for instance, for the acquisition of legitimate businesses by criminal organizations or the gaining of control over their operations. The mitigation of these steps will necessarily require actions and strategies implemented by law enforcement agencies to better understand how crime operates and how to better **understand and monitor organized crime strategies** to prevent these criminal activities. It is for these reasons that some steps of the criminal plans in the risk scenarios were difficult to limit by supply chain technology solutions. This is the case, for instance, for some steps indicated in risk scenario 1, in particular: step 1) Control of the distribution market by owning or controlling legitimate operators, step 2) Control of the supply chain using the technology owned by the controlled legitimate operators and step 5) Distribution of the falsified goods via the criminal group through its comprehensive and well-structured network, which includes wholesalers and supermarkets controlled by its frontmen.

- Following on from the previous point, an integrated approach between different technology typologies and options is needed to **support at the same time investigators and law enforcement agencies** on the one side as well as **supply chain operators and consumers** on the other.

- **Supply chain technology producers are constantly looking for ways to innovate the modality through which products' integrity and security can be enhanced**. The analysis of the submissions we received testifies to this element. Concrete examples include the attempt to go beyond the authentication of the simple packaging to try and implement modalities through which the food itself and its composition can be authenticated and progressively checked along the supply chain. Along the same line, the creation of a series of redundant checks which include the monitoring and reconciliation of the mass balance of products moving between intermediary points represents an interesting attempt to create additional layers of security.

- This constant search for innovation can also be seen in attempts aimed at improving the primary authentication element itself: the code and the label containing it. **The submissions we collected allowed us to appreciate a wide array of technology options which could be used to improve the security of the label and of the code themselves**, including the possibility of integrating various security and authentication elements into the label.

- **Consumer education** is essential in order to implement authentication solutions. The authentication codes used by different providers are frequently easy to scan through the use of smartphone cameras, however, the consumer needs to be aware of the existence of the verification mechanism and of the steps that need to be taken to corroborate the authenticity of the products.

Nuclear analytical techniques:

- Forensic analysis through the use of **nuclear analytical techniques** comes at a different stage, when it is necessary to recognize if a breach of the supply chain happened. Even if these technologies cannot be used to prevent the criminal activity from happening, unless their continuous use over time creates a dissuasive effect on criminals, they play a very important role since they are capable of unequivocally identifying the **geographical origin** of the products as well as its **components or possible adulteration**.

- The analysis of specific elements in the composition of a product enables the clear authentication of the products. Furthermore, by progressively analysing samples in the supply chain, it will also be able to trace back the source of the incident and present this **evidence in court**.

- The development of **portable devices** will enable routine analysis, which will provide a highly beneficial tool that would eliminate the limitations that arise from the need to use an external laboratory to examine the samples.

E-commerce:

- Monitoring of online markets, social media and e-commerce operators should be improved in order to **assess the evolution of the problem, map applied responses and support law enforcement authorities** in sharing data on suspect violations. This applies in complex situations, including in the case in which the e-commerce operator itself fell in the hands of organized crime and the case in which organized crime acquires control of an enterprise operating in the physical world.

- **Cooperation** should also be enhanced between **online payment service providers and law enforcement authorities**, in particular to block money flows to illegitimate operators and/or recover money spent by consumers who are victims of fraudulent online practices.

- Regarding e-commerce, other platforms should be considered when providing security solutions, including **apps** and dedicated **social network groups and pages** created by the criminal group to promote and sell their products.

CHAPTER 3
Illicit trafficking of precious metals

The illicit trafficking of precious metals, including counterfeiting operations, is an issue that affects the socio-economic development of producing countries and of local communities. This form of illicit trade also showed the capacity to evolve and adapt to different scenarios, as demonstrated, for instance, by what happened recently during the COVID-19 outbreak. In view of exploiting profit opportunities created by the pandemic, criminals adopted sophisticated online marketing techniques for the sale of fake gold and silver, significantly increasing the number of websites selling these products. The aim was clearly to take advantage of the uncertainty caused by the pandemic and the vulnerability of the population during the quarantine and stay-at-home measures.[1]

Prior UNICRI research has shown that the crimes most closely associated with precious metals are illicit trafficking, corruption, product theft and illegal mining, which consists in extractive activities being carried out in violation of environmental, fiscal, statutory and labour law.[2]

Illegal mining and product theft are attractive activities for criminals because of the ease with which one can process precious metals, as they can be easily reworked and placed into the legitimate market. Moreover, several studies have found a link between illegal gold mining and serious abuses of human rights, including human trafficking and child labour.[3]

Illegal mining, in fact, is often conducted in remote, abandoned and/or ownerless mines or mines which have been placed under liquidation, where law enforcement capability is limited. When these mines are directly controlled by criminal groups, there is a high risk of human trafficking for forced labour, rape, murder and vigilantism. The United Nations (UN) Special Rapporteur on Contemporary Forms of Slavery reported that middlemen recruiting miners in least developed countries lure them in with advances of money, tools and transport service. Such treatment is then deducted from the salary, overestimating the goods provided and underestimating the quantity and quality of the gold handed over, thus preventing workers from leaving due to debt bondage.[4]

With respect to child labour, the International Labour Organization (ILO) estimates that approximately one million children aged five to 17 are still working in mines worldwide.[5] Children are commonly used to enter mine shafts too narrow for adults and/or are required to treat gold-bearing rocks with mercury – which is highly toxic to humans when they are exposed to it. Furthermore, illegal miners may also suffer from malnutrition as they lack adequate water and food supplies due to protracted periods underground in deep level mines.

Another prominent consequence of illegal mining is environmental degradation. The extraction of precious metals often results in deforestation, soil erosion, pollution of soil and water, while the dumping of processed gold bearing material is common to most illegal mining sites.[6]

1 Anti-Counterfeiting Educational Foundation (ACEF). (2020, April 30). Counterfeits Gone Viral: Online Sales of Fake Gold and Silver Cost Public Millions. Retrieved from https://acefonline.org/counterfeits-gone-viral-online-sales-of-fake-gold-and-silver-cost-public-millions/

2 See UNICRI, *Strengthening the Security and Integrity of the Precious Metals Supply Chain* (2016), available at: http://www.unicri.it/in_focus/on/Precious_Metals_Supply_Chain_Report

3 See Global Initiative against Transnational Organized Crime, *Organized Crime and Illegally Mined Gold in Latin America* (2016) available at:
https://globalinitiative.net/organized-crime-and-illegally-mined-gold-in-latin-america/
See also OECD, Due Diligence in Colombia's gold supply chain, overview, available at:
https://mneguidelines.oecd.org/Colombia-gold-supply-chain-overview.pdf

4 See OHCHR, Report of the Special Rapporteur on contemporary forms of slavery, including its causes and consequences, 8 July 2015, available at:
https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session30/documents/a_hrc_30_35_eng.docx

5 See ILO, International Programme on the Elimination of Child Labour, Mining and quarrying, available at: https://www.ilo.org/ipec/areas/Miningandquarrying/lang--en/index.htm

6 See Global Initiative against Transnational Organized Crime, Organized Crime and Illegally Mined Gold in Latin America and UNICRI, Strengthening the Security and Integrity of the Precious Metals Supply Chain.

Trafficking in precious metals is linked to illicit financial flows. Several fraudulent schemes are used to evade tax, launder money or fund other crimes. The incorrect valuation of precious metals on export or import documents, or the practice of trading precious metals as "low-value scrap" are typical examples. Misinvoicing of transactions involving precious metals can be used for laundering money, claiming tax incentives (VAT and tax fraud) or dodging national capital controls.

Finally, the trafficking of precious metal is connected to the theft of products containing Platinum Group Metals (PGMs) (such as catalytic converters, chemical catalysts and other applications containing PGMs). A high percentage of PGMs can be refined and reutilized nearly an unlimited number of times. The high technical recyclability of PGMs means that over 95% recovery can be achieved once PGM-containing scrap reaches a state-of-the-art refining facility[7] (e.g. 90% of the PGMs ever produced is still existing).

There have been many incidents involving the theft of automotive catalysts and other products that contain PGMs. Media reports show that thieves are ripping catalytic converters from cars at an alarming rate. One bag containing 1000kg of scrap spent automotive catalysts (a device used to reduce emissions from an internal combustion engine) can have a value of up to 50.000 USD while a repair could cost a victim thousands of dollars.

For example, in the United States, according to a report by the National Insurance Crime Bureau (NICB), the increase in these thefts is dramatic. In 2018, there were 1,298 catalytic converter thefts reported. In 2019, it was 3,389 reported thefts. In 2020, reported catalytic converter thefts jumped massively to 14,433, with December leading the way with 2,347 thefts, or roughly 16 percent of the yearly total – in just one month.[8]

Furthermore, in the UK, an investigation by *The Times* showed that almost 6,000 catalytic converters had been stolen from 2015 to 2019, of which 2,894 occurred in the first six months of 2019.[9]

This section of the report describes three different risk scenarios related to the illicit trafficking of precious metals, to show how organized crime can explore vulnerabilities in this area. The scenarios are dedicated respectively to the illicit trafficking of precious metal materials, illicit trafficking of counterfeited gold bars, and the infiltration of the legal industrial refining process. Subsequently, the report analyses possible technology solutions aimed at limiting risks highlighted by the scenarios.

3.1 Risk scenarios

Three risk scenarios have been elaborated on in the area of illicit trafficking of precious metals.

Risk scenario 1: Illicit Trafficking of Precious Metal Materials

A developing country is known for its large reserves of precious metals, such as gold and platinum group metals, and mining is the primary national industry. In close proximity to large-scale mining sites controlled by foreign multinational companies, the government has awarded gold mining concessions to small-scale local mining operations. The small-scale mining operations: 1) exploit marginal or small gold deposits; 2) are labour-intensive; and 3) have poor access to markets and support services. The national authorities recognize the role of the developing domestic, small-scale industry and are therefore subsidizing local companies.

However, operations in a specific region are under the control of organized crime groups, which have infiltrated the supply chain of extractive industries to profit from the illicit trade in precious metals. The leader of a prominent organized crime group has realized that engaging in the illicit trade in precious metals would provide a high return on investment with a lower level of risk than other illicit activities.

7 See Recycling the Platinum Group Metal. A European Perspective, available at https://www.researchgate.net/publication/233563592

8 National Insurance Crime Bureau, 15 April 2021, https://www.nicb.org/news/blog/catalytic-converter-thefts-skyrocket-across-nation

9 BBC News, 20 September 2019 https://www.bbc.co.uk/news/business-49767195

To achieve this goal, she/he implements the following business model:

Step 1. *Taking control of informal mines*: Armed members of the criminal group raid the mining sites of the region, forcibly recruiting the workers to continue the operations to the benefit of the criminal group.

Step 2. *Setting up an international smuggling ring*: Precious metals extracted from the sites are then stored in a warehouse close to the main national seaport, where members of the criminal group take care of marking, weighing and analysing the precious batches of metals to determine their economic value. The criminal group aims to export the precious metals to a neighbouring country, where another affiliated criminal group owns shares in a metal smelting and refinery plant.

Step 3. *Trade misinvoicing*: In order to evade tax duties and dodge Customs controls, the leader of the criminal group proposes a lucrative business to a scrap dealer, who is licensed to export copper and other material containing precious metal components, for use in computers and telephone equipment. In exchange for a commission, the dealer misrepresents the nature of the merchandise as scrap metal on trade documents, with a significant underestimation of its value, thus avoiding the clearance required for the exportation of precious metals. The falsified trade documents are shared with the criminal group operating in the neighbouring country, who, thanks to its participation in the smelting and refinery plant, is able to receive such products for professional reasons, without raising suspicions. The content and the value of the consignment is then reassessed, to determine its economic value. The plant is then able to sell the refined gold to goldsmiths and retailers.

Step 4. *Money laundering*: At this stage, an amount equivalent to the underreported value of the scrap metal is wired from the purchasing smelting and refinery company to the shipper, thus simulating a licit economic transaction. At the same time, the criminal group transfer the proceeds of the sale of the precious metals to foreign bank accounts attributed to other front companies controlled by the same criminal organization.

The exploitation of workers at the mines allowed the leader of the criminal group to arrange monthly consignments of unwrought precious metals to her/his affiliate plants in the neighbouring country. After the refining stage, the metal-bearing rocks yield over 5 kg of gold, which is worth 175,000 euros (35,000 euros per kg). Over a year, the illicit trade scheme based on the misrepresentation and under-invoicing of precious metals generates over 2,100,000 euros in illicit profits for the criminal group.

Risk scenario 2: Illicit Trafficking of Counterfeit Gold Bars

A country is known for its large reserves of precious metals, such as gold and platinum group metals, and mining is the primary national industry. The leader of an organized crime group, which controls the production of narcotics in the same remote areas where informal mines operate, is seeking opportunities to launder illicit profits and, at the same time, generate additional incomes. She/he realizes that the illicit trade in gold would provide a high return on investment, at a relatively lower level of risk.

Her/his criminal group implements the following criminal business model:

Step 1. *Acquisition of gold from illegal mining*: The criminal group uses illicit profits (mainly generated by illicit trafficking of narcotics) to buy gold.

Step 2. *Transform the gold into counterfeit gold bars*: The criminal group uses a corrupt bar producer to manufacture counterfeit gold bars. The bars are fraudulently stamped with a logo of poor quality of accredited refinery companies. The purity and form of the bars are below the standards set by LBMA.10

Step 3. *Smuggling to a neighbouring country*: The criminal group illegally smuggle the gold bars to another country. They use two different routes: by boat for large quantities or by air for small quantities. In Redland, the gold bars are collected by an associate of the criminal group, which owns a precious metal import company. Through illegal smuggling, the criminal group evades consumption tax (VAT).

10 The Independent Precious Metals Authority.

Step 4. *Selling of the bars*: The associate operating in the neighbouring country sells the gold bars though their distributors and receives payment including VAT. After a few transactions, the gold bars are exported, and the VAT is reclaimed.

Risk scenario 3: Infiltration of the Legal Industrial Refining Process

An organized crime group realizes that infiltrating the legal industrial refining process of precious metals would provide a high return on investment at a lower level of risk compared to other more "traditional" crime sectors.

The criminal group implements the following business model:

Step 1. *Illegal acquisition of catalysts and scrap metals*: The criminal group steals products containing PGMs (such as catalytic converters, chemical catalysts and others).

Step 2. *Exportation of the stolen material*: The criminal group does not have a licence to refine precious metals and scrap (which is requested by the regulatory framework of the country where the group operates). Therefore, criminals use a front import/export company to export the stolen products containing precious metals to another front company that operates in a different country. The latter is a well-established company and is owned/controlled by an affiliate of the main criminal group and is specialized in metal smelting and refining, including industrial platinum, palladium and rhodium.

Step 3. *Extraction of precious metals*: The front refinery company crushes and mixes the stolen (but legally exported) products with spent catalysts and other material containing precious metals. It then extracts the precious metals (rhodium, palladium and platinum).

Step 4. *Selling the precious metals*: The front refinery company legally sells the precious metals (rhodium, palladium and platinum) which have been melted and poured into various forms (buttons/bars), thereby concealing their origin.

3.2 Technology solutions to address the risk scenarios

The supply chain of precious metals has its own peculiarities and any activity aimed at securing it will have to take into account specific issues, such as the metals' sourcing, their purity, weight, and tampering, among others.

Supply chain security solutions in this field have been developed keeping these elements in consideration, in view of minimizing threats deriving from infiltration, counterfeiting and smuggling, also looking at the sourcing phase of the product. In this regard, for instance, some of the tools available to guarantee responsible sourcing include multilayer approaches that are based on track and trace systems to monitor precious metal provenance and their subsequent handling, transformation, distribution and sale. Frequently, track and trace systems are combined with other features such as blockchain technology and third-party based auditing and certification. In the case of metal purity, analytical techniques include magnetic tests, acid tests on stone, ultrasonic tests, testing electrical properties, X-ray fluorescence (XRF) and spectrography. These techniques are used by stakeholders to corroborate the quality of the products, since for end-users the cost of these techniques is quite high, making it hardly affordable.

As mentioned, one additional element to consider in the field of precious metal supply chain security is weighing. However, even if traditionally this has been a widely used method to avoid the commercialization of counterfeit metals, it is currently relatively simple to maintain a specific weight for metals and still use counterfeit products. One of the threats that is directly related to weighing is tampering. Tampering precious metals is done to artificially increase the product weight by the addition of less expensive materials through different methods. To minimize this risk, analytical techniques to combat purity concerns are used by stakeholders.

Finally, to improve security measures for the customer, new mobile apps are being designed to corroborate authenticity through the scanning of visible or invisible codes. The codes can be linked to a traceability system. This technology option is frequently combined with traditionally used serial numbers to facilitate the tracking of the product through the supply chain and with certificates to validate the authenticity and quality of the product.

Some of the current technology solutions to protect the supply chain of precious metals can be divided into authentication options, mainly based on visible and invisible marking, traceability systems, forensic analysis of the materials, customized apps for clients and data analytics that use artificial intelligence.

The authentication of bullions can be achieved through different methods or a combination of them. One of the traditional authentication mechanisms is the use of a stamp with a unique serial number. Serial numbers are usually marked along with other information such as characteristics, weight, manufacturer, and origin. This can be carried out by impact, dot peen marking, scribe, and laser marking. In general, marking techniques cannot imperially alter or modify the shape, size or weight of the ingot. These marks provide a unique identification based on the specific characteristics of the product, however, they can still be imitated or modified to present different information.

Marking has evolved to use more complex techniques that enhance the uniqueness of the authentication method and make it more difficult to imitate it. Some innovative techniques include the marking of scannable data matrix micro-codes, QR codes, laser micro-machining and diffractive optical element technology on embossing stamps, punching a random dispersion of diamond particles, laser markings with deterministic drawings or even registering fingerprints/unique microscopic features of minted or bullion products and linking this to the serial number[11]. The marks that are codified include scanning features to reveal further information about the product or its authenticity, which can be accessed by using smartphone cameras or validators.

In addition to marking, other special features can be added onto bullions and minted products. These features may require special revealing devices. Some examples include holograms, invisible inks, Ultraviolet, Infrared (UV, IR), optical variable inks, fluorescent inks, and moiré-based features, among others. Other authentication methods include the use of seals with these security features and tamper-proof NFC labels.[12]

Apart from authentication, track and trace technology can also be used and added for the purpose of improving the security of the supply chain. Once the authentication technology is in place, the track and trace component will work in a similar way to what has been described in Chapter 1 of this report, including possible enhancements deriving from the use of blockchain technology for increasing the security of the track and trace database.

Forensics technology also finds application in the area of precious metals. Usually, the identification process for precious metals applies a systematic approach that starts with chemistry to determine the main producing area. After this process, more detailed mineralogical techniques are used to further identify the specific product and the producer. Variations in processing the metals between different producers in the same mining area culminate in some differences in the products' textures and compositions, which can be identified with specialized techniques. These techniques include a combination of X-ray diffraction, automated scanning electron microscopy and electron microscopy. In order to corroborate the authenticity of precious metals one of the common techniques is the use of a non-destructive X-Ray Fluorescence (XRF) machine.[13] This technology and the use of an extensive library of certified reference materials enable the recognition of authentic material. In the case of platinum, for instance, the identification techniques vary depending on the differences in grade between primary platinum producers and those that have platinum group metals as a by-product and the differences in the precious metal extraction processes.

Another analytical technique is the LA-ICP-MS (Laser Ablation Inductively Coupled Plasma Mass Spectrometry), which enables highly sensitive elemental and isotopic analysis to be performed directly on solid samples. For example, LA-ICP-MS analysis of native gold shows that measurable amounts of many elements are present at detectable and highly variable levels in gold from different styles of lode mineralisation. This provides a wide range of elements to use as a geochemical fingerprint for gold. However, to date, very little LA-ICP-MS compositional data is available for gold with which to compare illicit material.[14]

11 For the latter, see, for instance, the work being done by AlpVision: https://alpvision.com/precious-metals-counterfeiting/

12 See for instance: https://www.globenewswire.com/news-release/2020/05/20/2036434/0/en/Identiv-and-MintID-Launch-the-World-s-First-NFC-Protected-IoT-Connected-Gold-and-Silver-Bullion.html

13 Dixon, Roger & Schouwstra, R.. (2017). The role of forensic geology in the illicit precious metals trade. Episodes. 40. 132-140. 10.18814/epiiugs/2017/v40i2/017015.

14 Dixon, Roger & Schouwstra, R.. (2017). The role of forensic geology in the illicit precious metals trade. Episodes. 40. 132-140. 10.18814/epiiugs/2017/v40i2/017015.

Elemental analysis and profiling can be used to distinguish between legal gold alloys and illegally processed gold, which represents gold stolen from mining operations, providing a legal mechanism for its seizure. Elemental analysis of seized gold is sufficient to discriminate between the various methods by which the metallic gold has been produced.[15]

Nonetheless, it is relevant to highlight that although chemical data can be used to discriminate between the world's Platinum Group Mineral deposits, these deposits are frequently exploited by different mining companies, resulting in overlaps in chemical and mineralogical characteristics that complicate the determination of the exact provenance.[16]

Finally, another relevant technological incorporation is the use of artificial intelligence. This technology, and specifically machine learning, has been developed to find and continuously identify, monitor and assess the direct, indirect and cumulative impacts of artisanal and small-scale gold mining. Machine learning can be defined as the use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyse and draw inferences from patterns in data.[17] Mapping and tracking with machine learning algorithms enables stakeholders to continuously analyse the situation in the mines and close surroundings and to gather the information in a database for future reference and decision-making processes.

Artificial intelligence can also be used as an important analytical tool in the supply chain. Machine learning, as well as Cognitive Computing, Deep Learning, and Natural Language Processing can be combined to create platforms that enable not only the analysis of the situation, but that can predict circumstances or trigger alerts if something outside the normal activity is happening. In a supply chain, these types of platforms can be used to identify patterns, anomalies, and to perform trend forecasting, and graph analyses. This system can detect if there is an infiltration in the supply chain, since it is able to recognize standards of what is normal.

This part of the report will now present possible solutions to the challenges posed by the three risk scenarios described in the previous section. It describes the main aspects of the technology submissions, their relevance to the risk scenarios and possible advantages and limitations. Advantages and limitations usually refer to the technology categories in general. However, in some cases, reference will be made to some of the specific submissions we received, and this will be done just in view of providing a specific example of technology application.

By analysing the above-mentioned submissions, we found a variety of different approaches that, especially when combined, could contribute to improve the control and the securing of the precious metal supply chain. As a way of example, some of the submissions we received focus more on securing the supply chain by marking the precious metal itself while others rely more on its forensic analysis, which can also ensure the correct provenance of the material. These two main approaches, each one showing specific advantages as well as possible shortcomings, are coupled by other technologies based on the use of Earth Observation to identify illicit mining operations and that could provide an added value for early discovery of possible illicit activities.

In general, the submissions showed that technology solutions have the capacity to provide improvements in the following areas:

- Lack of control over the distribution of the product and full monitoring and data exchange in the supply chain, which might give rise to major issues such as the establishment of national and international smuggling rings or the exportation of the stolen materials.
- Need to identify suspicious precious metal exports and imports (in-transit shipments) and to enable traceability and real-time monitoring of precious metals throughout the supply chain.
- Intentionally mismarking to hide the origin, components and quality of the products.

15 Dixon, Roger & Schouwstra, R.. (2017). The role of forensic geology in the illicit precious metals trade. Episodes. 40. 132-140. 10.18814/epiiugs/2017/v40i2/017015.

16 Dixon, Roger & Schouwstra, R.. (2017). The role of forensic geology in the illicit precious metals trade. Episodes. 40. 132-140. 10.18814/epiiugs/2017/v40i2/017015.

17 Lexico by Oxford. Machine Learning. https://www.lexico.com/definition/machine_learning

- The use of trade misinvoicing in order to evade tax duties and dodge Customs controls.
- Selling the products as original and legal, concealing their origin and the illegal processes that they went through during their manufacture.
- Need to identify counterfeit products.

For what concerns the interesting features of technologies applied in this field, supply chain security technology based on the marking of the precious metal allows for the following interesting elements:

Monitoring: Track and trace technology is used to monitor the product through the different processes in the supply chain, limiting diversion and infiltration possibilities. Traceability is integrated to the authentication solutions to provide an additional layer of security.

Codes are easily readable: Technologies enable the user to access the information about the specific product with a single scan by using a laser pointer or a small and fast 3d scanner.

Code can hardly be reproduced: The technology used for the coding of the precious metal is quite sophisticated and can hardly be reproduced, if at all possible.

Unique: Technologies offer a unique, unclonable mark for each metal object.

Adaptability: Technologies can be adapted to the kind of precious metals they have to mark and to the requirements of customers.

Technologies focused on the elemental analysis of the precious metals present the following interesting features:

Accuracy: Determination of the chemical composition of the material is done through methods that provide high accuracy results, such as by X-ray fluorescence spectroscopy and/or scanning electron microscopy with X-ray microanalysis.

Well-established techniques: the techniques are widely used and there is evidence supporting the results of the processes.

Large database: The sample database contains information about a large number of products and materials, providing a solid reference to compare the analysed materials to the existing samples.

Furthermore, both approaches are often linked with the blockchain in order to increase the security and transparency of related information included in databases. When the blockchain is used, there are additional interesting elements that should be mentioned, such as:

Immutability: The information about the product and its movement in the supply chain or about its chemical composition cannot be modified. This is achieved through the ability of a blockchain ledger to remain unchanged, unaltered and indelible.

Auditability and accountability: Accountability is verified as a part of timestamps established by the blockchain system. This system allows every stakeholder to confirm whether the service operates in the intended way. If the product fails the verification process, then the stakeholders have proof of malicious behaviour which could be used to hold the responsible accountable. In addition, a transaction can only be made when both the sender and receiver are authorised through the private and public key system.

Transparency: Blockchain technology allows stakeholders to monitor the supply chain with openness, communication, and accountability. The stakeholders included in the chain can access the information at any point to corroborate the status of the products and the processes. Recorded product and time/location data is stored for easy data access in the bridge-database but cannot be adulterated in any way because it is locked to the cryptographic hashing in the blockchain, and a change would immediately be visible.

Some possible limitations for these technologies in general include the need to properly train and/or educate the various actors of the supply chain as well as final customers on the use of the system and on how to perform checks, otherwise it will be difficult to obtain the intended results.

Furthermore, in many cases the technology is registration dependent. This means that the artefact of metal is only secure after being marked and registered in the database. The operations carried out before the marking process are not protected. In these cases, the link with Earth Observation technology aimed at spotting illegal mining operations can complement this element.

Finally, those technologies based only on forensic analysis come into play once the illegal activity has already taken place. They are extremely useful for identifying the criminal activity, but they cannot be used to prevent it.

This report will now focus on concrete examples which demonstrate how technology can respond to some of the risks highlighted by the scenarios.

3.2.1 Embossing codes into gold bars with blockchain and satellite integration

Technology submission 1

This submission focuses on the authentication and track and trace of gold bullion bars. Currently, most gold bullion bars include a serial number that is added at the time of manufacture. During the first shipment from the original manufacturer and onwards at every change of ownership in the supply chain, this serial number can be used as part of a blockchain authentication. Changes in ownership of the product and aggregation and de-aggregation of gold bars in larger shipments are recorded immutably in the blockchain. Cryptographic keys are exchanged, allowing the receiver to become the new owner of each item when authorised to do so by the sender. Each transaction is recorded as a new block. To ship or receive bars, a person must be authorised as the owner by the previous person in the chain and be in possession of the bar with the correct serial number.

As the blockchain only includes hashes of information, a bridge-database connected to the blockchain can be used in which the serial numbers and any other required traceability data about the gold bars can be recorded. Once this data has been uploaded to the blockchain it cannot be changed even if someone breaks into the database, because the related hash would no longer compute correctly and the blockchain would change. A trusted computing platform is used for secure interfacing with the internal systems of manufacturers.

The submission also stresses that, for location tracking, the recording of where the serial number data was entered on a computer is not enough. One solution to this would be to stamp scannable data matrix micro-codes onto each bar. The stamps can be made from hardened steel, each laser-written with a unique barcode. This technology has been developed and proven on other materials, including soft metals. Scanning is performed by using a small and fast 3D scanner or a 2D camera barcode scanner with the correct lighting. To upload data to the bridge-database and blockchain for a transaction, the embossed code on the actual gold bar must be scanned. The scanner can record time and location data from a satellite, and this can be hashed together with the serial number from the barcode to complete the change of ownership transaction, which is done in combination with the necessary cryptographic key.

For tracing or checking historical information with readable, non-hashed data, the bridge-database can be searched and checked. With the serial-number system, counterfeit gold bars could be made and swapped with real gold bars that have the same serial number stamped on them after breaking into a transport or storage facility. In principle the same could happen if the criminals could make a copy of the steel barcode stamp and duplicate it on counterfeit gold. Although they would not be able to introduce the stolen gold bar into the official supply chain because of the blockchain, it could be re-melted and used for other gold items. However, there are ways in which the counterfeit gold bar can be identified.

One option to authenticate the gold bars is to use hidden information in the embossed code by using laser micro-machining and diffractive optical element technology on embossing stamps. Different options are possible, and these security features can be covert whilst at the same time allowing the code to be read as a normal barcode. Authentication is done via a laser pointer or a small and fast 3D scanner.

Another option for authentication of the gold bars is to use a fast 3D scan that records micron-level information taken from regions of interest on the gold bar. The information is encrypted and recorded in the bridge-database. To check the authenticity of a gold bar, the latter is scanned in the regions defined for that specific bar and that are defined in the database. The encrypted result is checked against the original. The company has been developing this type of technology for the past five years for other industries.

Submission received from Nano4u

This submission allows us to discuss some interesting elements for the authentication and track and trace of gold bars. One of the most interesting features of this submission lies in the marking method used for the precious metal. Thanks to a technique already developed by the company, this technology option proposes to directly mark the gold bar through embossing. This feature would render the copying of codes extremely difficult if not impossible for criminals. Apart from this feature, the integration with blockchain and satellite technologies is an interesting element of this submission, which also renders the system applicable in those cases in which a traditional marking method is used on the gold bars.

In particular, in the case in which the embossed codes are working together with the blockchain based database, the advantage is that the data in the database originates from the actual gold bar itself. Recorded gold bar and time/location data cannot be adulterated in any way because it is locked to the cryptographic hashing in the blockchain, and a change would immediately be visible.

Source: Nano4U

Furthermore, blockchain technology allows for immediate alerts in case of detection of any issue or unprogrammed change. This alerts the stakeholders in the supply chain and in addition, the technology allows them to search for a product at any point in the chain to verify its status. If an attempt is made to change any entries in the bridge-da-

tabase resulting in a change in the blockchain, warning information flagging this issue can be set up to notify only those "who need to know" for security purposes, without alerting other actors in the supply chain that their actions have been discovered.

Finally, the integration with space technology allows for the possibility of using precise location and time data from satellite navigation and communications. This can be achieved by (a) locking this into data in a blockchain-based database for current and historical tracking and authentication purposes, (b) providing a unique cryptographic stamp for embossed codes that makes each code unique.

More specifically, the solution targets some of the issues identified in the scenarios related to illicit trafficking of precious metals. The technology solution offers a multi-layer security option to protect different areas involved in the manufacture and commercialization of precious metals. The submission proposes different options to authenticate the gold bars: 1) to use hidden information in the embossed code through laser micro-machining and diffractive optical element technology on embossing stamps, 2) to stamp scannable data matrix micro-codes onto each bar. The stamps can be made from hardened steel, each laser-written with a unique barcode, 3) to use a fast 3D scan that records micron-level information taken from regions of interest on the gold bar. The information is stored in the blockchain to protect traceability in the supply chain.

In particular, for what concerns **risk scenario 1** (illicit trafficking of precious metal materials), the described technology can support a risk reduction for several steps of the criminal business model, especially the ones related to the authentication of products:

- Setting up an international smuggling ring to export the precious metals.
- Trade misinvoicing in order to evade tax duties and dodge Customs controls.
- Money laundering.

In **risk scenario 1**, some of the steps are still difficult to limit, in particular step 1 "control of the mines and forcefully recruiting workers". The multilayer technology solution protects different aspects in the supply chain, however, if the criminal organization controls the entire supply chain and particularly the extraction of materials, it is not possible to identify the illicit activities behind the manufacture of the product. The submission offers customers an option to identify and verify products that have not gone through illicit processes.

For what concerns **risk scenario 2** (illicit trafficking of counterfeit gold bars) the same considerations presented for risk scenario 1 also apply. The combination of authentication through a unique mark that is combined with track and trace and a simple validation tool can limit the following steps of the criminal plan:

- Transformation of the gold into counterfeited gold bars by stamping a logo of poor quality of accredited refinery companies.
- Illegal smuggling, to evade consumption tax (VAT).

If the option to allow authentication by customers is developed, the technology could also limit the selling of counterfeit bars through their distributors.

With reference to step 2, "transformation of the gold into counterfeited gold bars by stamping a logo of poor quality of accredited refinery companies", the different authentication solutions provide a tool to create unique marks and codes that are able to encrypt specific information about the gold bar. The information is highly protected in the blockchain-based database, mitigating any risk related to the possible imitation of a mark or a code. The use of traceability systems not only provides an additional layer of security, but it also targets other issues presented in the scenarios, such as the distribution of the falsified goods, the use of clandestine sweatshops and production centres, and the lack of full monitoring and control of the production and distribution chains. The track and trace solutions enable the monitoring of the processes involved in the supply chain, granting visibility to identify illicit activities related to the deviation of the products from the supply chain. The capability of the solution of monitoring data and the adoption of blockchain technology create a platform where any anomalies in the process would be

pointed out immediately. Furthermore, the data introduced into the system would automatically be immutable and transparent for all the stakeholders, enabling auditability and accountability. The traceability is highly supported by satellite navigation and communication in order to obtain precise location and time data and to provide a unique cryptographic stamp for printed codes that makes each code unique. Space-related data are also used by this submission to track the origin and the location of products as they are packaged or repackaged.

As for step 3 "Illegal smuggling, to evade consumption tax (VAT)", the submission can be used to partly minimize the risk. The unique mark on the product and the traceability system to monitor it provide a security option to protect the authentication of the original materials that have a legitimate origin. However, if the criminal organization controls mines, it would be difficult to detect the illicit activities. In this regard, the technology solution offers an authentication mechanism that enables stakeholders and customers to corroborate the licit origin of the product and its authenticity.

Also, for risk scenario 2, the same steps identified for risk scenario 1 cannot be mitigated by the use of supply chain security technology. Step 1, "acquisition of gold from illegal mining by using illicit profits" cannot be prevented since the solution can only be applied once the material is available, regardless of its origin.

In the case of **risk scenario 3**, other technological resources should be used to mitigate the criminal plan, whose steps cannot be limited through supply chain security technology. The technology solution can only be applied after the materials are extracted and processed, therefore, the operations carried out before that stage are not protected. In the case of these steps, the submission proposed can only partly mitigate the risk, since the solution cannot avoid the illegal acquisition of catalyst and scrap metals by theft, yet it allows the identification of authentic products by providing a unique mark that can be easily scanned to verify its quality, whereas the track and trace system adds a security layer.

Summary table for submission 1: possible application to limit risks highlighted by the scenarios

Scenario	Applicability of the solution
Scenario 1: *Illicit trafficking of precious metal materials*	
Step 1 – Control of the mines and forcefully recruiting workers.	
Step 2 – Setting up an international smuggling ring to export the precious metals.	The unique mark on the product and the traceability system to monitor it provide a security option to protect the authentication of the original materials that have a licit origin, however, if the criminal organization controls mines, it would be difficult to detect the illicit activities.
Step 3 – Trade misinvoicing in order to evade tax duties and dodge Customs controls.	The supply chain is protected by blockchain technology. All transactions, including invoices are secured and cannot be changed without triggering an alert for all stakeholders with permission to access the platform.
Step 4 – Money laundering.	The same considerations described in step 2 apply and can also limit money laundering activities in the case in which the criminal group does not also control mines and the whole supply chain.

Scenario 2: *Illicit trafficking of counterfeited gold bars*	
Step 1 – Acquisition of gold from illegal mining by using illicit profits.	
Step 2 – Transformation of the gold into counterfeited gold bars by stamping a logo of poor quality of accredited refinery companies.	The unique identification mark created by either process provides an unclonable authentication mechanism that enables the tracking of the product and its easy verification through a laser pointer or a small and fast 3D scanner. In addition, the information in the codes is introduced into the blockchain-based database, which secures the information provided in the authentication method.
Step 3 – Illegal smuggling, to evade consumption tax (VAT).	The same considerations described in step 2 of scenario 1 apply to this step.
Step 4 – Selling the counterfeit bars through their distributors.	At this stage the technology does not allow the customers to check the authenticity. However, this option is being developed by the company.
Scenario 3: *Infiltration of the legal industrial refining process*	
Step 1 – Illegal acquisition of catalysts and scrap metals by stealing products containing precious metals.	
Step 2 – Exportation of the stolen material through front import and export companies.	
Step 3 – Extraction of precious metals in the front refinery.	
Step 4 – Legally selling the precious metals, which have been melted and poured into various forms.	

3.2.2 Unique marking through random chaotic process coupled with artificial intelligence

Technology submission 2

The submission is based on a system that provides an object with a unique unclonable mark that can be applied to a variety of products, not exclusively on precious metal artefacts, to secure their authenticity. The marks produced are not only unique, since they are the result of a random chaotic process, but also very difficult to reproduce, eliminating the criminal incentive to clone them. These two characteristics are critical to improve the security of the marks, since by working together, they guarantee that there are no two identical marks. The markings can be applied to precious metals by using two main technologies:

1) Punching a random dispersion of diamond particles to guarantee the incrustation of these particles on the metal. Since the diamond particles generate a random pattern, resulting from a chaotic process, and the punching will disseminate them in an unpredictable way, this physical process is practically impossible to reproduce;

2) Laser markings. In this case, the design of the laser beam path is deterministic, not random. However, the path itself is designed by a mathematical function so that the resultant pattern is unique. These marks are still impracticable to reproduce since the response of the metal during the laser marking, when the metal is in the melting phase, is unpredictable and determined by several uncontrollable and unobservable variables.

Thus, by either punching a random dispersion of diamond particles on the metal surface or by marking a precious metal artefact with a laser beam through a deterministic path in the melting phase of the metal, the system is able to provide the object with a unique mark. As for the validation of the uniqueness of these marks, the image of the mark is used to validate it. Depending on the security level, the system can have a database to store a photo of the mark, a minutiae vector produced by a known, yet private, algorithm or both the photo and the minutiae. Artificial intelligence is used to identify the patterns in the database and to link that information with georeferencing data and the track and trace system.

The technology option can validate the marks produced by using a digital, off-the-shelf microscope or by using a smartphone with a simple commercial macro lens. This validation process, simple and accessible to retailers and consumers, as well as to stakeholders in the supply chain, is one of the main advantages of the system. The consumer is able to check the product before the purchase, validating the quality and authenticity of the object by using a smartphone. Furthermore, the retailers themselves can provide simple digital microscopes to their customers in their shops and boutiques that allow them to check the marks. At the logical level, for the validation of the marks, the system is based on the processing of the image of the mark itself. The solution uses an algorithm to detect, rectify and reconstruct the dispersion of particles or the salient characteristics of the laser marking using deep learning algorithms and computer vision methodologies. In general, the algorithms used to perform the pattern matching are designed to perform verification (1-to-1) as well as identification (1-to-many).[18] Additional applications of the technology solution include the marking of gold bars, weapons, clocks and other objects made or composed of metals.

Submission received from INCM – Portuguese Mint and Official Printing Office

18 A 1:1 match refers to the situation where each case is matched with one and only one control, while in a 1:N match, each case is matched with up to N controls.

Technology submission 2

The submission is based on a system that provides an object with a unique unclonable mark that can be applied to a variety of products, not exclusively on precious metal artefacts, to secure their authenticity. The marks produced are not only unique, since they are the result of a random chaotic process, but also very difficult to reproduce, eliminating the criminal incentive to clone them. These two characteristics are critical to improve the security of the marks, since by working together, they guarantee that there are no two identical marks. The markings can be applied to precious metals by using two main technologies:

1) Punching a random dispersion of diamond particles to guarantee the incrustation of these particles on the metal. Since the diamond particles generate a random pattern, resulting from a chaotic process, and the punching will disseminate them in an unpredictable way, this physical process is practically impossible to reproduce;

2) Laser markings. In this case, the design of the laser beam path is deterministic, not random. However, the path itself is designed by a mathematical function so that the resultant pattern is unique. These marks are still impracticable to reproduce since the response of the metal during the laser marking, when the metal is in the melting phase, is unpredictable and determined by several uncontrollable and unobservable variables.

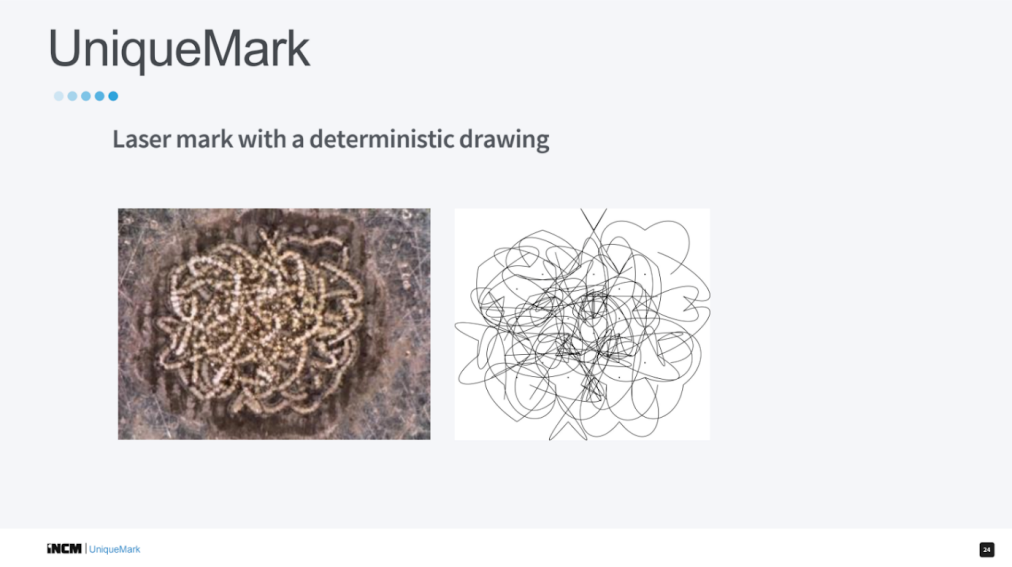
Thus, by either punching a random dispersion of diamond particles on the metal surface or by marking a precious metal artefact with a laser beam through a deterministic path in the melting phase of the metal, the system is able to provide the object with a unique mark. As for the validation of the uniqueness of these marks, the image of the mark is used to validate it. Depending on the security level, the system can have a database to store a photo of the mark, a minutiae vector produced by a known, yet private, algorithm or both the photo and the minutiae. Artificial intelligence is used to identify the patterns in the database and to link that information with georeferencing data and the track and trace system.

The technology option can validate the marks produced by using a digital, off-the-shelf microscope or by using a smartphone with a simple commercial macro lens. This validation process, simple and accessible to retailers and consumers, as well as to stakeholders in the supply chain, is one of the main advantages of the system. The consumer is able to check the product before the purchase, validating the quality and authenticity of the object by using a smartphone. Furthermore, the retailers themselves can provide simple digital microscopes to their customers in their shops and boutiques that allow them to check the marks. At the logical level, for the validation of the marks, the system is based on the processing of the image of the mark itself. The solution uses an algorithm to detect, rectify and reconstruct the dispersion of particles or the salient characteristics of the laser marking using deep learning algorithms and computer vision methodologies. In general, the algorithms used to perform the pattern matching are designed to perform verification (1-to-1) as well as identification (1-to-many).[19] Additional applications of the technology solution include the marking of gold bars, weapons, clocks and other objects made or composed of metals.

Submission received from INCM – Portuguese Mint and Official Printing Office

This submission allows us to present the integration of various technologies and approaches into a single solution, aimed at increasing the security of the supply chain of precious metals. This submission belongs to those technologies focused on the marking of the precious metal itself, however there are several elements which renders it very interesting. The marking methods themselves, which results in marks which are unique and very difficult to reproduce, eliminating the criminal incentive to clone them. The integration of artificial intelligence to recognize the patterns in the marks, validate the product and link the information to georeferencing data is also extremely interesting, since it has the potential to increase the security of the supply chain and the authentication of the precious metals by creating a series of redundant checks in the system.

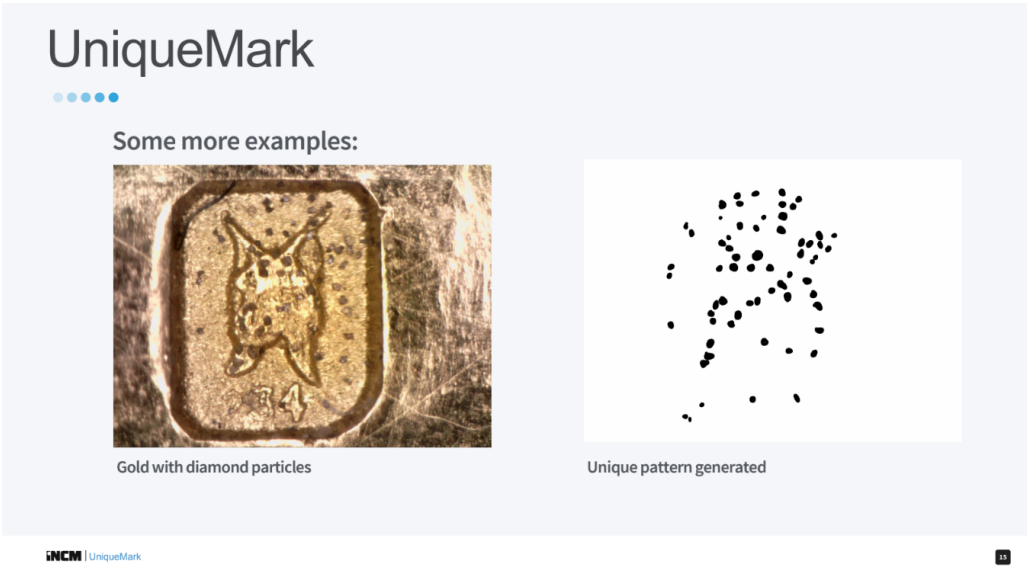
19 A 1:1 match refers to the situation where each case is matched with one and only one control, while in a 1:N match, each case is matched with up to N controls.



Source: INCM

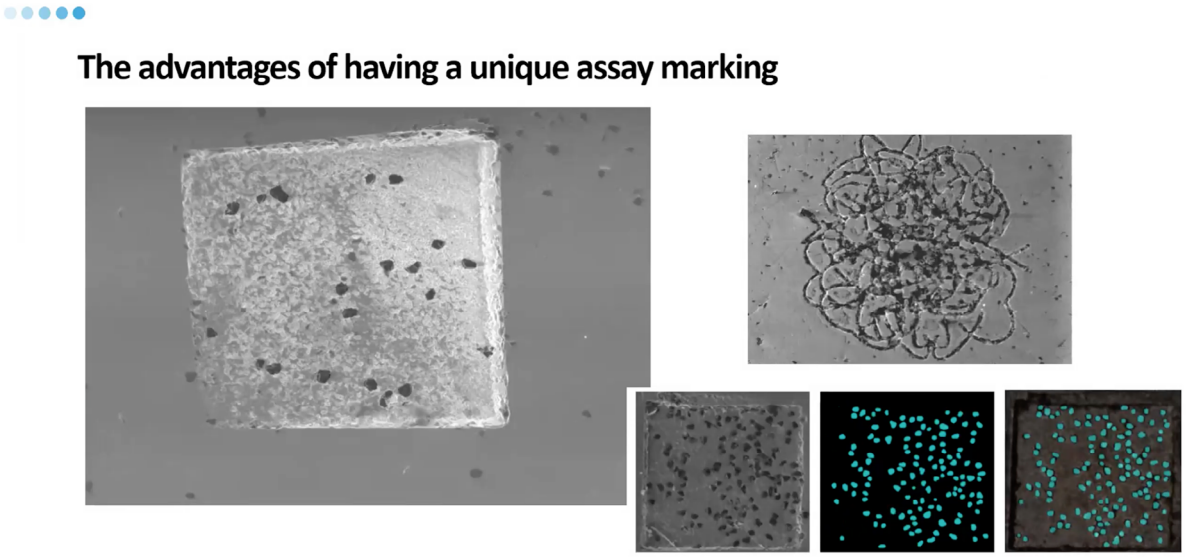
For what concerns the marking methods in particular, the solution offers a unique, unclonable mark for each metal object. In the case of the laser mark, the deterministic drawing is based on a mathematical description of the drawing to maximize uniqueness; and, although the drawing is deterministic, the reproduction of the same drawing in another mark will produce different distinguishable marks due to different behaviour of the supporting material.

Regarding puncturing with diamond particles, the dispersion is unique since it comes from uncontrollable and unclonable chaotic processes.

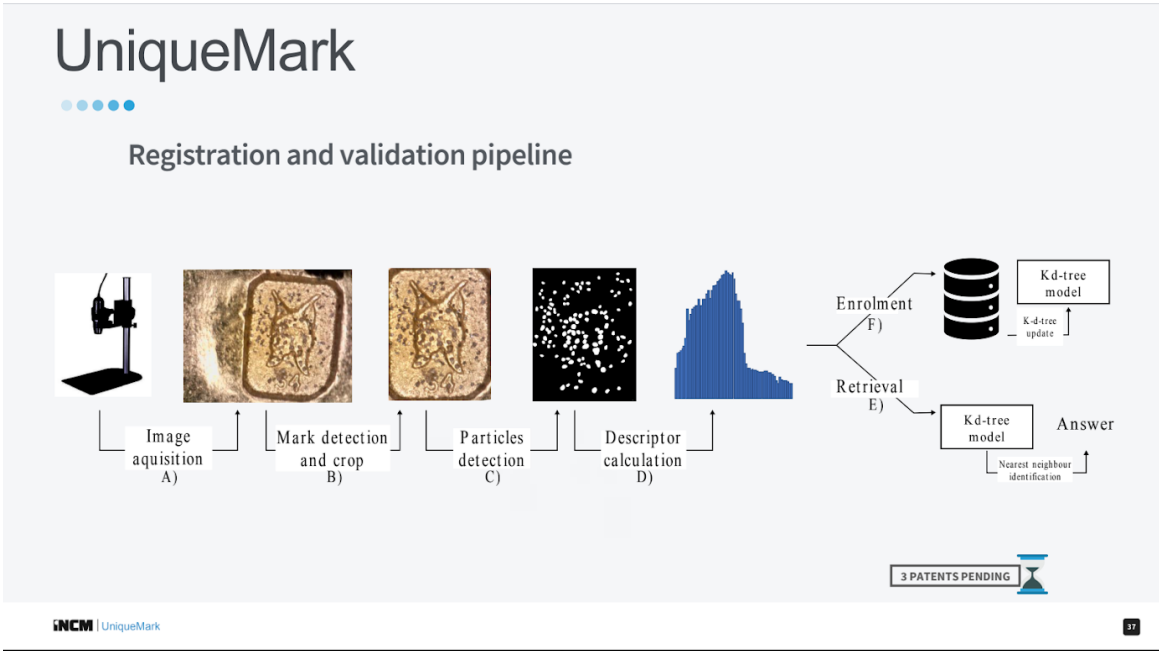


Source: INCM

In addition, a proprietary mathematical description of the drawing is studied to maximize the uniqueness of marks. In addition, a coding frame for the mark can be created to add a security level and an easy means of validation. During the punching process, particles can be engraved depending on different needs. Particles have an approximate diameter between 40 and 100 microns, while marks are approximately 1mm^2. Yet, this can be made with any dimension since the number of particles depend on the desired density.



Source: INCM



Source: INCM

For what concerns the response to the risk scenarios, the solution targets some of the issues identified in the risk scenarios related to illicit trafficking of precious metals. The technology solution offers a multi-layer security option to protect different areas involved in the manufacture and commercialization of precious metals. The authentication of the product by marking it with laser or by punching a random dispersion of diamond particles is used as a tool to control the quality and integrity of the product, whereas the possibility of integrating a track and trace system provides a useful mechanism to monitor the cycle of the product throughout the supply chain. Finally, the validation can be made by both stakeholders and customers by using a smartphone camera or a simple microscope.

In particular, for what concerns **risk scenario 1** (illicit trafficking of precious metal materials), the described technology can support a risk reduction in several steps of the criminal business model. The solution proposed provides elements to mitigate the risks presented in this scenario, especially the ones related to the authentication of products, preventing customers from acquiring products that are related to illicit activities or funding.

This can limit the following steps of the criminal plan:

- Setting up an international smuggling ring to export the precious metals.
- Trade misinvoicing in order to evade tax duties and dodge Customs controls.
- Money laundering.

As mentioned in the previous submission, in **risk scenario 1**, the risks related to control of the mines and forcefully recruiting workers cannot be mitigated. If the criminal organization controls the entire supply chain and particularly the extraction of materials, it is not possible to identify the illicit activities behind the manufacture of the product.

For what concerns **risk scenario 2** (illicit trafficking of counterfeit gold bars) the same considerations presented for risk scenario 1 also apply. The combination of authentication through a unique mark that is combined with track and trace and a simple validation tool, can limit the following steps of the criminal plan:

- Transformation of the gold into counterfeited gold bars by stamping a logo of poor quality of accredited refinery companies.
- Illegal smuggling, to evade consumption tax (VAT).
- Selling the counterfeit bars through their distributors.

With reference to step 2, "transformation of the gold into counterfeited gold bars by stamping a logo of poor quality of accredited refinery companies", and step 4 "selling the counterfeit bars through their distributors", the technology solution can be used to combat the risks through the use of a unique identification mark created by laser marking or punching a random dispersion of diamond particles to provide an unclonable authentication mechanism that enables the tracking of the product and its easy verification through a smartphone camera. A non-original logo would not pass this verification since it would need to be an exact match to the original one. This is extremely complicated because the melting process modifies the mark in a unique manner, making it harder to attempt to imitate it. Furthermore, customers can verify the authenticity of the product by scanning the code before buying. However, they must be aware that they have the option to do it in order to have an effective mechanism of validation.

As for step 3 "Illegal smuggling, to evade Value Added Tax (VAT)", the submission can be used to partly minimize the risk. The unique mark on the product and the traceability system to monitor it, can provide a security option to protect the authentication of the original materials that have a legitimate origin. However, if the criminal organization controls mines, it would be difficult to detect the illicit activities. In this regard, the technology solution offers an authentication mechanism that enables stakeholders and customers to corroborate the licit origin of the product and its authenticity.

Also, for risk scenario 2, the same steps identified for risk scenario 1 cannot be mitigated by the use of supply chain security technology. Step 1, "acquisition of gold from illegal mining by using illicit profits" cannot be prevented since the solution can only be applied once the material is available, regardless of its origin.

In the case of **risk scenario 3**, other technological resources should be used to mitigate the criminal plan, whose steps cannot currently be limited through supply chain security technology.

Summary table for submission 2: possible application to limit risks highlighted by the scenarios

Scenario	Applicability of the solution
Scenario 1: *Illicit trafficking of precious metal materials*	
Step 1 – Control of the mines and forcefully recruiting workers.	
Step 2 – Setting up an international smuggling ring to export the precious metals.	The unique mark on the product and the traceability system provide a security option to protect the authentication of the original materials that have a licit origin, however, if the criminal organization controls mines, it would be difficult to detect the illicit activities.
Step 3 – Trade misinvoicing in order to evade tax duties and dodge Customs controls.	For the same reasons explained in relation to step 2, if the criminal organization controls the mines, it would be difficult to detect the illicit activities.
Step 4 – Money laundering.	The considerations explained above apply to this step. Money laundering activities can be limited in the case in which the criminal group does not also control mines and the whole supply chain.
Scenario 2: *Illicit trafficking of counterfeited gold bars*	
Step 1 – Acquisition of gold from illegal mining by using illicit profits.	
Step 2 – Transformation of the gold into counterfeited gold bars by stamping a logo of poor quality of accredited refinery companies.	The unique identification mark created by either process provides an unclonable authentication mechanism that enables the tracking of the product and its easy verification through a smartphone camera. A non-original logo would not pass this verification. In addition, the melting process modifies the mark in a unique manner, making it harder to attempt to imitate it.
Step 3 – Illegal smuggling, to evade consumption tax (VAT).	For the same reasons explained in relation to scenario 1, if the criminal organization controls the mines, it would be difficult to detect the illicit activities.
Step 4 – Selling the counterfeit bars through their distributors.	Customers can verify the authenticity of the product by scanning the code before buying. They must be aware that they have the option to do so in order to have an effective mechanism of validation.

Scenario 3: *Infiltration of the legal industrial refining process*	
Step 1 – Illegal acquisition of catalysts and scrap metals by stealing products containing precious metals.	
Step 2 – Exportation of the stolen material through front import and export companies	
Step 3 – Extraction of precious metals in the front refinery.	
Step 4 – Legally selling the precious metals, which have been melted and poured into various forms.	

3.2.3 Integrating blockchain, big data analytics and artificial intelligence

Technology submission 3

This technology submission proposes a holistic solution by incorporating perspectives from a wide array of technologies, including blockchain, big data analytics and artificial intelligence. Thanks to its characteristics of immutability and auditability, technologies like blockchain can be an extremely effective means for complementing tracking and tracing technologies focused on provenance and the pipeline for precious metals. For all the advantages of security, immutability, anonymity, and shareability that are inherent to digital peer-to-peer ledgers, the information they contain is intended to be secured and transmitted. However, improvements could be made concerning the data analytics phase. This submission stresses the fact that, unlike traditional Relational Database Management Systems (RDBMS), which are constructed for the purpose of information storage and retrieval, the information stored in a blockchain is not inherently amenable to analysis. However, when combined with artificial intelligence, machine learning, and Nonlinear Dynamic Systems Analysis capabilities, these technologies have the ability to reveal patterns, disclose anomalies, and provide forecasting insights. In addition, other benefits include transparency, accountability, and security for supply chain management.

1) The submission presents a holistic solution that is based on:
2) The optimal mix of technologies.
3) The delivery through systems that augment human capabilities, and that people will actually use.
4) The possibility of financially benefitting stakeholders, who are seen as partners by the solution.
5) The possibility of improving the likelihood of success in significantly curtailing the illicit trafficking of precious metals.

The technology solution uses the following combination of technology:

1) Registering unique identification. Precious metals can be registered in a blockchain platform through the coding of ore shipments, by capturing records created during the refinement processes, and through auditable seals adhered to shipping containers. Blockchain records can likewise be constructed to reflect everything from unique chemical signatures to the identification of the personnel involved in every phase of the supply chain, from production to final distribution.

2) Blockchain to track any valuable information, including origin and distribution. Smart contract is used to secure transactions between stakeholders without any intervention, which is fully integrated with an artificial intelligence platform.

3) An artificial intelligence, machine learning, Cognitive Computing, Deep Learning, Natural Language Processing platform that enables pattern identification in the whole supply chain, anomaly detection, trend forecasting, and graph analyses.

Submission received from ProtectedBy.AI

The key element of this submission can be found in the integration of various technologies which makes it possible to build a complete system to register and trace objects from their origin, while enabling stakeholders to access information about every person, process and policy that contributed to that product's production in real time.

For what concerns identification, this submission focuses on a unique identification for the material generated through the coding of ore shipments, by capturing records created during the refinement processes, and through auditable seals adhered to shipping containers.

Integration with blockchain technology makes it possible to construct blockchain records in order to reflect a series of different data, from unique chemical signatures to the identification of the personnel involved in every phase of the supply chain.

On the other hand, integration with an artificial intelligence-based platform was designed to detect patterns, trends and anomalies during the processes in the supply chain. The use of artificial intelligence makes it possible to:

1) Create insights for optimization of the system.

2) Automatically alert stakeholders about potential dangers.

3) Detect anomalies such as waste, fraud, and theft.

4) Analyse possible outcomes by gathering trends-related information.

This technology also provides a tool to view patterns with a graph data topological analysis.

More specifically, the solution targets some of the issues identified in the risk scenarios related to illicit trafficking of precious metals. The technology solution offers a multi-layer security option to protect different areas involved in the manufacture and commercialization of precious metals. The blockchain-protected platform provides a tool that has relevant intrinsic characteristics such as immutability, auditability, transparency and accountability. This technology solution protects the information that is introduced in the database, securing the transactions involved in the different processes in the supply chain.

In particular, for what concerns **risk scenario 1** (illicit trafficking of precious metal materials), the described technology can support a risk reduction for several steps of the criminal business model. The solution proposed provides elements to mitigate the risks presented in this scenario, especially the ones related to illicit transactions.

This can limit the following steps of the criminal plan:

- Setting up an international smuggling ring to export the precious metals.
- Trade misinvoicing in order to evade tax duties and dodge Customs controls.
- Money laundering.

The same considerations explained in the previous submissions regarding **risk scenario 1** apply to this submission. The risks related to control of the mines and forcefully recruiting workers cannot be mitigated, and if the criminal organization controls the entire supply chain, it is not possible to identify the illicit activities. The submission offers customers an option to identify and verify products that have not gone through illicit processes.

For what concerns **risk scenario 2** (illicit trafficking of counterfeit gold bars) the same considerations presented for risk scenario 1 also apply. The use of a blockchain-protected track and trace tool can partly limit the following steps of the criminal plan:

- Illegal smuggling, to evade consumption tax (VAT).
- Selling the counterfeit bars through their distributors.

As for step 3 "Illegal smuggling, to evade consumption tax (VAT)" and step 4 "Selling the counterfeit bars through their distributors", the submission can be used to partly minimize the risk since it provides a tool to secure the transactions that are recorded in the blockchain, however, if the criminal organization controls mines and the supply chain, it would be difficult to detect the illicit activities. In this manner, the technology solution offers a traceability mechanism that enables stakeholders to corroborate the licit origin of the product and its authenticity.

As explained for the previous submissions, for risk scenario 2, step 1, "acquisition of gold from illegal mining by using illicit profits" and step 2 "Transformation of the gold into counterfeited gold bars by stamping a logo of poor quality of accredited refinery companies" cannot be prevented since the solution can only be applied once the material is available and registered.

Also, in the case of **risk scenario 3**, other technological resources should be used to mitigate the criminal plan, whose steps cannot be currently limited through supply chain security technology.

Summary table for submission 3: possible application to limit risks highlighted by the scenarios

Scenario	Applicability of the solution
Scenario 1: *Illicit trafficking of precious metal materials*	
Step 1 – Control of the mines and forcefully recruiting workers.	
Step 2 – Setting up an international smuggling ring to export the precious metals.	The traceability system protected by blockchain technology provides a security option to protect the materials since the intrinsic characteristics of the blockchain provide immutability, auditability, transparency and accountability. However, if the criminal organization controls mines, it would be difficult to detect illicit activities. The technology solution offers a traceability mechanism that enables stakeholders to corroborate the licit origin of the product and its authenticity as long as it was registered from the beginning of its production. The solution only protects the products if they are registered in the database.

Step 3 – Trade misinvoicing in order to evade tax duties and dodge Customs controls.	The supply chain is protected by blockchain technology. All transactions, including invoices are secured and cannot be changed without triggering an alert for all stakeholders with permission to access the platform.
Step 4 – Money laundering.	The previous considerations apply to this step and the use of technology can also limit money laundering activities in the case in which the criminal group does not also control mines and the whole supply chain.
Scenario 2: *Illicit trafficking of counterfeited gold bars*	
Step 1 – Acquisition of gold from illegal mining by using illicit profits.	
Step 2 – Transformation of the gold into counterfeited gold bars by stamping a logo of poor quality of accredited refinery companies.	
Step 3 – Illegal smuggling, to evade consumption tax (VAT).	The explanation given in step 2 of the risk scenario 1 apply to this step and the technology can limit this risk if the criminal organization does not control the entire supply chain, including mines.
Step 4 – Selling the counterfeit bars through their distributors.	The previous considerations also apply to this step.
Scenario 3: *Infiltration of the legal industrial refining process*	
Step 1 – Illegal acquisition of catalysts and scrap metals by stealing products containing precious metals.	
Step 2 – Exportation of the stolen material through front import and export companies.	
Step 3 – Extraction of precious metals in the front refinery.	
Step 4 – Legally selling the precious metals, which have been melted and poured into various forms.	

3.2.4 Chemical Forensic Bureau for the identification of mining and metallurgical products and blockchain-based digital metal tokens

Technology submission 4

The submission proposes two different technology solutions.

The first technology solution is based on the use of a complex procedure for the identification of mining and metallurgical products developed by Nornickel's Chemical forensics bureau (CFB). It focuses on the use of analytical equipment, skilled experts, a database of products and materials, and an expert IT system. These techniques have been used in public-private partnerships to cooperate with law enforcement authorities. The Complex Procedure for Identification of Mining and Metallurgical Operations Products contains a descriptive part including decision-making algorithms and six analytical protocols:

1) Determination of the chemical composition of the material by X-ray fluorescence spectroscopy and/or scanning electron microscopy with X-ray microanalysis.

2) Chemical digestion of materials for subsequent ICP-OES and ICP-MS analysis.

3) Determination of the chemical composition by ICP-OES.

4) Determination of the chemical composition by ICP-MS.

5) Determination of the phase composition by XRD.

6) Investigation of chemical composition of the particles using scanning electron microscopy in conjunction with X-ray microprobe analysis.

CFB is a unique research-and-production unit carrying out forensic examinations and special forensic studies following requests from law-enforcement authorities as well as special forensic studies requested by security units of subsidiary refining hubs and industrial facilities. The sample database used contains more than 500 products from different companies, more than 4350 ores and minerals and 3050 metal alloys. The sample database is used to store and identify the elemental composition of the substance, its visual appearance, phase composition of the substance, and the elemental composition of the particles. The expert IT system Genesys is used to find the information about the product and to identify unknown substances.

Further validation of the Complex Procedure for Identification of Mining and Metallurgical Operations Products stipulates the following stages: 1) verifying compliance of documents with Eurochem requirements, 2) testing operational viability of the methodology at CFB, and 3) cross-laboratory comparative tests. The validation of the methodology contributes to the enhancement of analytical procedures, automating decision-making in the expert IT system and to broader target use cases, expanding the database with products of other miners and processors. Through this process, the methodology becomes universal and can be adopted by all producers and fabricators to counteract illicit international trafficking of precious and non-ferrous metals.

The second technology solution is based on the digitalization of precious metal sales contracts using blockchain technology. This offers an option where tokens are backed by commodities and can be settled physically or financially. The transactions are done via a digital platform based on modified Hyperledger Fabric blockchain technology. There are industrial tokens for industrial consumers and investment tokens for traders and commodity investors. Some of the benefits that this platform provides include unique opportunities to manage value chain and supply risks, responsible sourcing, possible blockchain verification of ESG, mitigating risks of illicit trafficking and criminal operations during multiple transactions, and protection from organized crime activities (money laundering, counterfeiting precious metals, among others).

The platform provides unique opportunities to protect the supply chain including mitigating risks of illicit trafficking and criminal operations during multiple transactions with precious metals (gold, silver, platinum and palladium). The platform enables safer and quicker transactions with minimal security and safety risks, since only verified users are permitted to make transactions. Transparency as well as verification of users and the origin of metals protect the platform from operations conducted by organized crime.

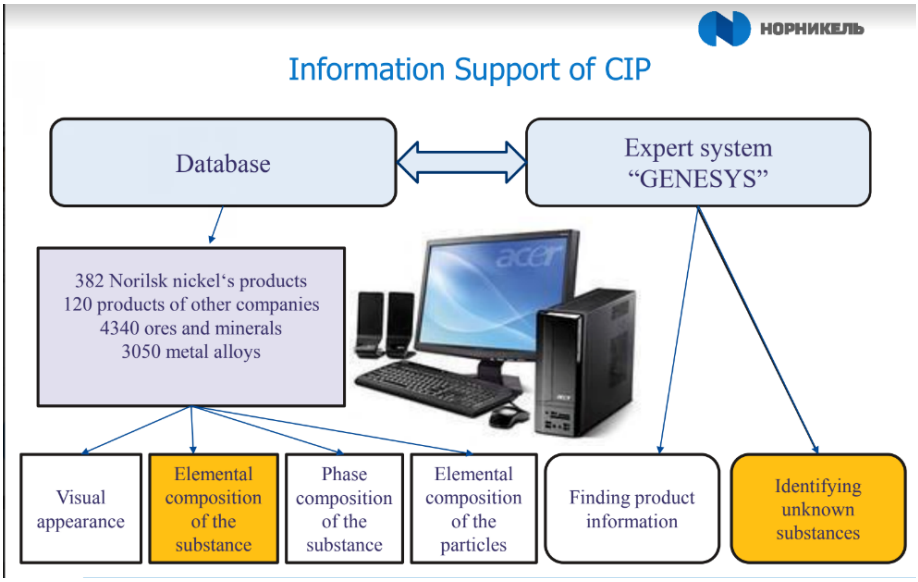
Submission received from Nornickel

This submission provides the opportunity to discuss the potential benefits for the security of the precious metals supply chain created by forensic analysis technology and by the digitalization of precious metal sales contracts using blockchain technology.

Especially in relation to the first element of this submission, this technology solution is also based on the need to collectively mobilize all actors operating in the precious metals' arena, from private companies to law enforcement agencies. This is a key element which necessitates closer cooperation between public and private sectors to detect and investigate crimes related to the illicit trafficking of precious metals. In particular, the CFB is conducting analysis following requests originating from law enforcers, as well as exchanging information and conducting training for Custom service officers.

However, this submission also presents the use of a different kind of approach, which relies on a blockchain-based digitalization of metal sales contracts.

The digitalization of metal sales contracts using blockchain technology makes it possible to secure this kind of contract and limit related criminal activities along the supply chain. It can be expected that activities, such as money laundering during the different processes in the supply chain, the use of illegal production methods, and the creation of clandestine manufacturing facilities, could be limited by the use of this blockchain platform.



Source: Nornickel

More specifically, for what concerns the risk scenarios, the solution targets some of the issues identified in the risk scenarios related to illicit trafficking of precious metals. The submission offers two main separate options to protect different areas involved in the manufacture and commercialization of precious metals. The blockchain platform provides a tool that has relevant intrinsic characteristics such as immutability, auditability, transparency and accountability. This technology solution protects the information that is introduced in the database, securing the transactions of the final products. Whereas the use of chemical-forensics bureau tools can be performed to corroborate the composition and origin of the products (ore, concentrate, minerals, metal alloys, etc.) at different technological process stages.

In particular, for what concerns **risk scenario 1** (illicit trafficking of precious metal materials), the described technology can support a risk reduction for several steps of the criminal business model. The solution proposed provides elements to mitigate the risks presented in this scenario, especially the ones related to illicit transactions.

This can limit the following steps of the criminal plan:

- Setting up an international smuggling ring to export the precious metals.
- Trade misinvoicing in order to evade tax duties and dodge Customs controls.
- Money laundering.

In **risk scenario 1**, some of the steps are still difficult to limit, in particular step 1) "taking control of the mines and forcefully recruiting workers". The solutions cannot prevent the control of mines by criminal organizations, however, if transactions are made through the platform, then the licit origin of the metals has to be proven.

For what concerns **risk scenario 2** (illicit trafficking of counterfeit gold bars) the same considerations presented for risk scenario 1 also apply. The use of a blockchain-protected platform can partly limit the following steps of the criminal plan:

- Illegal smuggling, to evade consumption tax (VAT).
- Transformation of the gold into counterfeited gold bars by stamping a logo of poor quality of accredited refinery companies.

As for step 3 "Illegal smuggling, to evade consumption tax (VAT)", the submission can be used to partly minimize the risk since it provides a tool to secure the transactions that are recorded in the blockchain and strict requirements are requested to use the platform. In this manner, the technology solution offers a platform that enables stakeholders to corroborate the licit origin of the product and its authenticity.

Also, for risk scenario 2, the same steps identified for risk scenario 1 cannot be prevented by the use of supply chain security technology. Step 1, "Acquisition of gold from illegal mining by using illicit profits" and step 4 "Selling the counterfeit bars through their distributors" cannot be prevented since these activities are made outside the scope of the platform.

As explained for the previous submissions, the threats presented in **risk scenario 3** (infiltration of the legal industrial refining process) cannot be currently limited through supply chain security technology. The operations carried out before the registration in the platform or the corroboration of the chemical compositions of metals are not protected. As previously mentioned, the use of these techniques can allow the identification of illegal activities or any irregularities in the final product but cannot prevent criminal activities that are outside this scope.

Summary table for submission 4: possible application to limit risks highlighted by the scenarios

Scenario	Applicability of the solution
Scenario 1: *Illicit trafficking of precious metal materials*	
Step 1 – Control of the mines and forcefully recruiting workers.	
Step 2 – Setting up an international smuggling ring to export the precious metals.	The solution would not prevent the creation of an international smuggling ring, however, the blockchain platform would protect all the transactions which are made with metals that have a licit origin, increasing the security of the licit supply chain and of licit trade of precious metals. In addition, cooperation with law enforcement authorities and the use of the CFB can help to corroborate the origin of precious metals.
Step 3 – Trade misinvoicing in order to evade tax duties and dodge Customs controls.	The transactions are protected by the blockchain-based platform. All transactions, including invoices, are secured and cannot be changed without triggering an alert for all stakeholders who have permission to access the platform. However, it is important to consider that only the transactions made through the platform would be protected.
Step 4 – Money laundering.	The considerations described above also apply to this step and money laundering operations can be limited in the case in which the criminal group does not control the entire supply chain, including mines.
Scenario 2: *Illicit trafficking of counterfeited gold bars*	
Step 1 – Acquisition of gold from illegal mining by using illicit profits.	
Step 2 – Transformation of the gold into counterfeited gold bars by stamping a logo of poor quality of accredited refinery companies.	
Step 3 – Illegal smuggling, to evade consumption tax (VAT).	The solution would not prevent illegal smuggling, however, the blockchain platform would protect all the transactions which are made with metals and that have a licit origin. In addition, cooperation with law enforcement authorities and the use of the CFB can help to corroborate the origin of precious metals.
Step 4 – Selling the counterfeit bars through their distributors.	

Scenario 3: *Infiltration of the legal industrial refining process*	
Step 1 – Illegal acquisition of catalysts and scrap metals by stealing products containing precious metals.	
Step 2 – Exportation of the stolen material through front import and export companies.	
Step 3 – Extraction of precious metals in the front refinery.	
Step 4 – Legally selling the precious metals, which have been melted and poured into various forms.	

3.2.5 Using Earth Observation to identify illicit mining operations

Technology submission 5

This submission deals directly with potential issues surrounding artisanal and small-scale mining (ASM), including artisanal and small-scale gold mining (ASGM). One characteristic of ASM is that it is often informal and un(der)regulated,[20] as well as that it is primarily located in developing and low-middle income countries, where resource constraints may hamper monitoring and, consequently, regulatory compliance. Another challenge is the scarcity of data on the scale and impacts of ASM.

This submission proposes a technological solution designed to help public authorities and stakeholders to effectively and continuously identify, monitor and assess the direct, indirect and cumulative impacts of ASM over large geographic regions. This result is achieved by automating the detection of ASM sites through the application of machine learning and Computer Vision algorithms to satellite imagery. The Deep Learning architecture used is called U-Net, a form of a Convolutional Neural Network for fast and precise segmentation of images. A Convolutional Neural Network (ConvNet/CNN) is a Deep Learning algorithm which can take in a submission image, assign importance (learnable weights and biases) to various aspects or objects in the image and differentiate them from each other.[21] The model is available as a Python library. The solution uses AI algorithms to analyse satellite images from the European satellite Sentinel-2 of the European Space Agency (ESA) from the Copernicus program and from Planet, a commercial provider of satellite images. Other submission data sources can be built into the model to enhance functionality and widen indicators monitored. The program automatically identifies artisanal and small-scale mine sites and can help to monitor change over time using time-lapse series.

20 In many countries, 70 to 80 percent of small-scale miners are informal. Retrieved from https://www.iisd.org/system/files/publications/igf-asm-global-trends.pdf

21 Saha, S. (2018, December 15). A Comprehensive Guide to Convolutional Neural Networks-the ELI5 way. Retrieved from https://towardsdatascience.com/a-comprehensive-guide-to-convolutional-neural-networks-the-eli5-way-3bd2b1164a53

The technological solution to target these challenges maps and tracks ASM systems over time based on satellite data submission update frequencies. This permits periodic updates of ASM activity within an area of interest (AoI) and allows for automatic change detection over time. Outputs from the product can be produced in a Geographic Information System (GIS) format that the client is already using and can therefore be easily embedded into existing monitoring solutions. In addition, service features include a client due diligence and onboarding process, user license agreements, including safeguarding against irresponsible usage, and a best practice usage guide, focused on how to make the most of the solution to optimize product value for consumers.

The ASM mapping and change detection system can also include optional additional features, such as an ASM monitoring/baseline data. This optional feature enables access to several components, including:

1) Enhanced automatic change alerts e.g. rapid growth, forest cover loss, proxies for illicit investment etc.

2) Tailored user interface such as a web-based platform.

3) Detailed characterisation of mining operations e.g. levels of mechanisation, population, forest impact, use of chemical submissions etc.

4) Impact attribution modelling (defining cause and scale of impact – ASM vs. other drivers).

5) "Ground-truthing" to improve algorithm and build functionality (required for many of the "bolt on" options).

6) Mapping of ASM operations to legal and regulatory requirements to determine compliance.

7) Historical analysis of trends in ASM activity to inform ASM management planning

8) Monitoring and evaluation of ASM management activities to inform continuous improvement.

Submission received from ASMSpotter

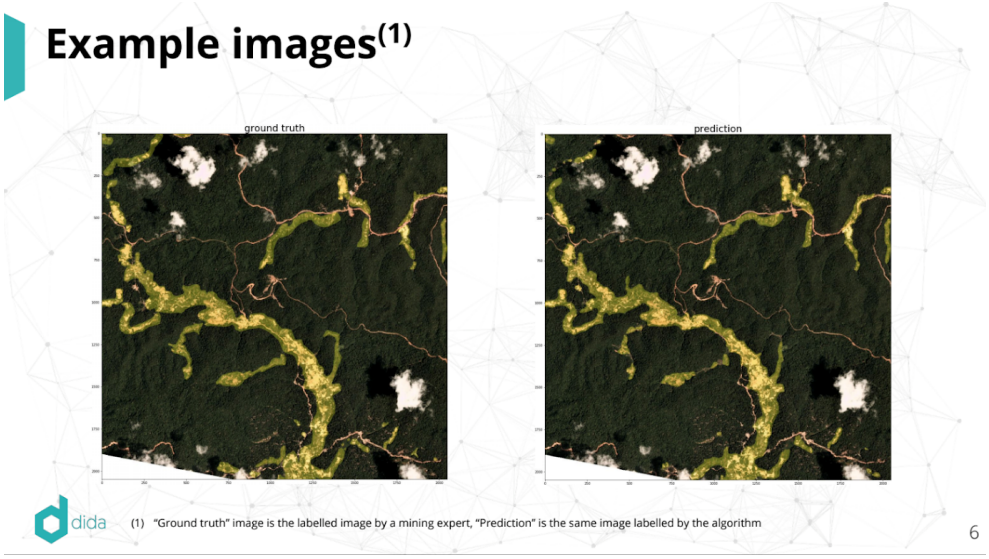
This submission provides the opportunity to discuss how Earth Observation technology can support the fight against illegal mining operations of small scale. As seen for previous submissions related to the fight against illicit trafficking of precious metals, the integration of different technologies creates a series of benefits. In particular, through the use of Deep Learning and artificial intelligence for the analysis of satellite images, the technology is capable of identifying illicit mining operations as well as their evolution over time. In this way, the technology responds to problems related to lack of monitoring and data exchange in the supply chain that could enable the identification of illicit activities.

In particular, the technology helps public authorities and industry to effectively and continuously identify and monitor ASM over large geographic regions by automating the detection of ASM sites through the application of machine learning and Computer Vision algorithms to satellite imagery. It provides a tool to gather baseline data on the evolution of the sector, including risk profiles of operations. Such data is an essential ingredient to inform effective, evidence-based policy making to regulate and support the development of the sector. ASM activity can also change rapidly making it difficult to keep up to date and respond to the latest challenges effectively. To target this issue, this submission provides an early alert mechanism to warn of rapid growth or "rush" situations and other concerning indicators such as mechanization.

It can further be integrated into Key Biodiversity Area conservation activities, as well as responsible production and sourcing efforts to inform site identification, ASM engagement, impact assessment and risk management approaches. The technology submission affirms that ASM operations can be automatically detected – to 80-95% pixel accuracy – based on training of an AI algorithm with more than 10,000 satellite images. One of the challenges identified is that it is impossible to quantify the scale, volume and value of ASM mined minerals, especially in areas

with only nominal state control. The technology makes it possible to quantify the scale and production of mining activities in given areas, as well as identify and classify mining operations, proxies for illicit activity, population, production, spatial impact, and mining types.

Illegal investment in ASM is another major concern that is difficult to resolve once established. The solution can be programmed to predict issues such as illegal investment by using proxies for investment (mechanization, rate of growth of observable impact, type of operations etc.).
It is also difficult to model "attribution" of environmental impact due to multiple land uses and cumulative impacts. The technology described by this submission can provide an analysis of time-lapse series data outputs to establish models for understanding drivers of cumulative impacts on the environment e.g. heavy metal sedimentation in waterways. The solution also uses a bespoke algorithm to sort images on an ongoing basis ensuring (1) no recurring fees for manual interpretation of satellite images and (2) near "live" updates, which target issues such as the fact that remote sensing monitoring is costly and slow to update.



Source: ASMSpotter

The submission also provides an early alert mechanism for regulatory non-compliance, e.g. through overlay of data with cadastral information, and the technology solution could also be used as a tool to facilitate the evaluation of the evolution and trends of the sector to better inform appropriate policy and programme design. In addition, it is frequently hard to identify trends in ASM activity that can inform how we engage with ASM miners and communities. In this case, the solution can be applied retroactively using publicly available data to map evolution of ASM over time, enabling the analysis of trends to inform strategic response to ASM management.

For what concerns its application to the risk scenarios, the solution targets some of the issues identified in the risk scenarios related to illicit trafficking of precious metals. The technology solution helps public authorities (and industry) to effectively and continuously identify, monitor and assess the direct, indirect and cumulative impacts of artisanal and small-scale mining (ASM) over large geographic regions, by automating the detection of ASM sites through the application of machine learning and Computer Vision algorithms to satellite imagery. The tool can therefore be used to inform monitoring and enforcement efforts of mineral host countries, as well as provide the baseline data necessary to contribute to improved policy and programmatic design, thereby contributing over time to improved formalization outcomes, narrowing the spaces in which criminal activities can thrive. In this regard, the data obtained through this technology solution is used to support the implementation of additional tools to target additional threats analysed in the scenarios.

In particular, for what concerns **risk scenario 1** (illicit trafficking of precious metal materials), the described technology can partially support a risk reduction for several steps of the criminal business model. The solution proposed provides elements to mitigate some of the risks presented in this scenario, especially the ones related to effectively and continuously identifying, monitoring and assessing the direct, indirect and cumulative impacts of artisanal and small-scale mining (ASM).

This can limit the following steps of the criminal plan:

- Control of the mines and forcefully recruiting workers.
- Setting up an international smuggling ring to export the precious metals.

In the case of step 1 "Control of the mines and forcefully recruiting workers", satellites and machine learning are used to identify mining activity using earth observation with significant degrees of automation and with high degrees of accuracy. Furthermore, manual tagging of satellite outputs permits the building of algorithms to automatically identify complex patterns that replicate in Earth Observation satellite images when mining activity is occurring. Large territories can be monitored automatically to identify new activities, changes in activities, or patterns. For example, the speed of growth combined with proxies for establishing demographic shifts, physical infrastructure surrounding the mine, sedimentation in nearby water bodies and others, overlaid with cadastral information ought to allow stakeholders to determine the likelihood that what is being seen is the result of unregulated activity. The results can be used by authorities to design action plans and policy in order to combat criminal groups that are taking control of the mines.

The abovementioned can also have repercussions on limiting step 2 "Setting up an international smuggling ring to export precious metals", since the successful identification of illicit mining operations would render it more difficult for criminals to do so.

In risk scenario 1, some of the steps are still difficult to limit, in particular the trade misinvoicing in order to evade tax duties and dodge Customs controls and money laundering. The technology solution enables the automatic monitoring of large territories to identify new activities or changes in activities. Even if through deeper analysis, ground truthing and refined algorithms, it could be possible to identify patterns, this technology does not focus on the subsequent processes of the supply chain. Nevertheless, proof of origin claims can be checked against actual mining activity in a given area, which can give an indication of current production and productive capacity and thereby be an indicator of erroneous origin claims.

For what concerns **risk scenario 2** (illicit trafficking of counterfeit gold bars) the monitoring of the territory can partly limit the following step of the criminal plan:

- Acquisition of gold from illegal mining by using illicit profits.

The technology solution can partially limit the risks related to the acquisition of gold from illegal mining since it provides information about the location and state of the mines. Specifically, the technology solution can help to determine potential wrongful claims of origin, which could be an indicator of illicit origin of the mineral through the Financial Action Task Force (FATF), which, for example, identifies any spike or decline in reported gold production at a site as being a potential indicator of illicit or criminal activity. Regular monitoring of the site characteristics from space, including through spatial impact, mechanization, and impact of indirect human activity, can be used as proxies, in combination with the known geological potential of an area, to assess whether such shifts in volumes are suspicious.

It is also possible to identify non-registered mine operations in the proximity of registered operations – these operations might seek to channel production through legal operations as a way of "laundering" the outputs. Growth in these activities alongside a corresponding rise in reported legal production provide clues as to the origin and volume plus value. The technology could serve to identify likely origins of potential inbound leakage of material, giving a perspective of likely productive outputs of a site against what is being declared by the system.

With respect to the rest of the steps in this scenario, the tool cannot limit them free-standing.

For what concerns **risk scenario 3** (infiltration of the legal industrial refining process), other technological resources should be used to mitigate this criminal plan, whose steps cannot be limited through satellite monitoring.

Summary table for submission 5: possible application to limit risks highlighted by the scenarios

Scenario	Applicability of the solution
Scenario 1: *Illicit trafficking of precious metal materials*	
Step 1 – Control of the mines and forcefully recruiting workers.	The use of satellites and machine learning are adopted to identify mining activity using Earth Observation and support the identification of unregulated operations.
Step 2 – Setting up an international smuggling ring to export the precious metals.	The tool helps public authorities (and industry) to effectively and continuously identify, monitor and assess the direct, indirect and cumulative impacts of artisanal and small-scale gold mining (ASGM) over large geographic regions. The information obtained by using this technology solution can be used by authorities to design action plans and policy in order to combat criminal groups that are taking control of the mines; however, it does not prevent the illicit activities from taking place.
Step 3 – Trade misinvoicing in order to evade tax duties and dodge Customs controls.	
Step 4 – Money laundering.	
Scenario 2: *Illicit trafficking of counterfeited gold bars*	
Step 1 – Acquisition of gold from illegal mining by using illicit profits.	The solution can support the identification of potential wrongful claims of origin, non-registered mine operations in the proximity of registered operations and their likely origins of potential inbound leakage of material, by giving a perspective of likely productive outputs of a site against what is being declared by the system.
Step 2 – Transformation of the gold into counterfeited gold bars by stamping a logo of poor quality of accredited refinery companies.	
Step 3 – Illegal smuggling, to evade consumption tax (VAT).	
Step 4 – Selling the counterfeit bars through their distributors.	

Scenario 3: *Infiltration of the legal industrial refining process*	
Step 1 – Illegal acquisition of catalysts and scrap metals by stealing products containing precious metals.	
Step 2 – Exportation of the stolen material through front import and export companies.	
Step 3 – Extraction of precious metals in the front refinery.	
Step 4 – Legally selling the precious metals, which have been melted and poured into various forms.	

3.3 Conclusions

The illicit trafficking of precious metals risk scenarios presented some of the threats that can affect the integrity of the supply chain. Thanks to research conducted by UNICRI and to the submissions we received from technology experts, it has been possible to assess how technology solutions may contribute to increasing the security of the supply chain of these products while limiting related criminal activities.

Existing technology solutions usually encompass one or several of these elements to protect the flow of products in the supply chain:

- **Authentication technology**: The authentication of precious metals is frequently achieved through marking. Serial numbers and, more recently, codes that contain unique information about the product are usually marked along with other information such as characteristics, weight, manufacturer, and origin. This is usually carried out by impact, dot peen marking, scribe, and laser marking. In general, marking techniques cannot imperially alter or modify the shape, size or weight of the ingot. **Marking** has evolved to use more **complex techniques that enhance the uniqueness of the authentication method** and make it more difficult to imitate it.

- **Track and trace systems**: They are characterized by the application of an identifier to the product or to a batch of products, which is then used to track its movements throughout the different stages of the supply chain. The adoption of these technology solutions is linked to the use of a back-end database in which each movement of goods along the supply-chain is recorded. Traceability options can also use space technologies as a proof of origin as well as for monitoring purposes and can be added to the authentication options. They can also alert different stakeholders when the products are no longer in the supply chain. It is essential to consider the **addition of strong authentication features** which are difficult to be copied and allow for the attribution of a unique and strong secure identifier to each product, rendering counterfeiting operations much more difficult.

- **Blockchain technology**: Can connect the different parties in the supply chain that have not established trusted relationships with each other, by ensuring transparency. Blockchain stores every transaction or exchange of data that occurs in the network, reducing the need for intermediaries by providing a means by which all the actors in the network may share access to the same information, including what is added to the data, by whom, and the date and time of the submission.[22]

- **Forensics**: If suspicion related to the authenticity of the product arises, forensic techniques can be adopted to analyse the composition of the metals, their quality and origin. Usually, the identification process for precious metals starts with chemistry to determine the main producing area. After this process, more detailed mineralogical techniques are used to further identify the specific product and the producer. Variations in processing the metals between different producers in the same mining area culminate in some differences in the products' textures and compositions, which can be identified with specialized techniques, such as X-ray fluorescence spectroscopy, scanning electron microscopy with X-ray microanalysis, and Laser Ablation Inductively Coupled Plasma Mass Spectrometry.

- **Artificial intelligence:** AI tools have been developed to find and continuously identify, monitor and assess the direct, indirect and cumulative impacts of mining. Mapping and tracking with machine learning algorithms enable stakeholders to continuously analyse the situation in the mines and close surroundings and to gather the information in a database for future reference and decision-making processes. AI can also be used as an important analytical tool in the supply chain. Machine learning, as well as Cognitive Computing, Deep Learning, Natural Language Processing can be combined to create platforms that enable the analysis of information and that can predict circumstances or trigger alerts. Platforms can also be used to identify patterns, anomalies, and to perform trend forecasting, and graph analyses.

The submissions analysed in the report use different types of technology that are applied following various approaches. Technology is frequently combined to provide multiple levels of security and to achieve a combination of objectives. The submissions might use similar approaches to mitigate risks, however, they offer unique features that focus on the use of specific technology tools. In the case of illicit trafficking of precious metals, the submissions offered the following distinctive approaches:

- **Creation of a unique unclonable mark to authenticate and validate the original products**, as proposed by submission 2. Different techniques are adopted to create the unique mark that is engraved on the product, such as laser marking and punching a random dispersion of diamond particles. The marking and/or the patterns created by the marking process can be recorded in a database, in view of obtaining integration with a traceability system. In this case, artificial intelligence is used to identify the patterns created by the marking process in the database and to link that information with georeferencing data in view of deploying the track and trace system. The artefact of metal is only secure after being marked and registered in the database. The operations carried out before the marking process are not protected.

- **Implementation of multi-layered technology solutions**. Submissions 1 and 3 adopt this perspective to offer solutions based on a unique identification mark that is linked to a track and trace system. The additional use of blockchain technology protects the information exchange between the different authorized stakeholders by providing immutability, transparency and accountability. As clarified in relation to the previous approach, the product is only secure after being marked and registered in the database. The operations carried out before the marking process are not protected. submission 3 also uses big data analytics and artificial intelligence to provide relevant insights and predictions related to the different processes in the supply chain.

- **Use of forensic techniques for the identification of mining and metallurgical products**. This solution can be used if suspicion related to the authenticity of the product arises since and, in this case, it will be possible to analyse the composition of the metals, their quality and origin. Submission 4 uses this approach to propose chemical-forensics bureau (CFB) tools to implement a procedure for the identification of mining and metallurgical products by using analytical equipment, skilled experts, a database of products and ma-

22 Accenture. (2019, January 15). Tracing the Supply Chain. Retrieved August 23, 2020, from https://www.accenture.com/_acnmedia/pdf-93/accenture-tracing-supply-chain-blockchain-study-pov.p

terials, and an expert IT system. These tools are designed to analyse possible counterfeit products; however, they were not developed to prevent infiltration in the supply chain. They are frequently used to support the work of law enforcement authorities.

- **Focus on specific parts of the supply chain**. Automating the detection of artisanal and small-scale gold mining (ASGM) with machine learning and Computer Vision algorithms using satellite imagery is proposed as a solution to provide accurate and relevant information for public authorities and stakeholders to identify, monitor and assess the direct, indirect and cumulative impacts of ASGM over large geographic regions. This approach, used by submission 5, provides tools to monitor and detect any unusual activities in the mines, however, it was not created to secure the entire supply chain.

- **Focus on a specific process of the supply chain.** Submission 4 provides an example of this approach, proposing the creation of digital metal tokens of Platinum Group Metals (PGM) trading combined with the use of blockchain technology to trade in a protected digital platform. This enables mitigation of risks related to illicit trafficking and criminal operations during multiple transactions with precious metals (gold, silver, platinum and palladium). Transparency as well as verification of users and the origin of metals protect the platform from operations conducted by organized crime.

With specific reference to the risks that were highlighted by the risk scenarios, the following considerations can be made:

- **Supply chain technology producers are constantly looking for ways to innovate the modality through which products' integrity and security can be enhanced**. The analysis of the submissions we received testifies to this element. Concrete examples include the use of multilayer solutions that combine several authentication features and that use techniques to ensure the uniqueness of the mark and identification, while adopting further protection mechanisms such as track and trace systems, artificial intelligence, and blockchain technology to protect transactions.

- **Innovative marking techniques** include scannable data matrix micro-codes and QR codes, laser micro-machining and diffractive optical element technology on embossing stamps, punching a random dispersion of diamond particles, laser markings with deterministic drawings or even registering unique microscopic features of minted or bullion products and linking this to the serial number.

- Marking can be combined with other **security features** that may require special revealing devices. Some examples include holograms, invisible inks (UV, IR), optical variable inks, fluorescent inks, and moiré-based features, among others. Other **authentication methods** include the use of seals with these security features and tamper-proof NFC labels.

- The analysis of the submissions received demonstrated that technology is being adopted to **target other highly relevant vulnerabilities**, such as extraction processes in the mines through machine learning, the identification of metals through complex forensic examinations and the trade of precious metals through the use of blockchain-based platforms for transactions. This comprehensive view enables the protection of diverse areas of the supply chain from the increasingly sophisticated criminal operations.

- To improve **security measures for the customer**, new mobile apps are being designed to corroborate the authenticity through the scanning of visible or invisible codes. The codes can be linked to the traceability system. This technology option is frequently combined with traditionally used serial numbers and authentication mechanisms to facilitate the tracking of the product through the supply chain and certificates to validate authenticity and quality of the product.

- **Artificial intelligence** has been adapted to provide analytical tools that help stakeholders to identify trends and issues in diverse stages of the supply chain. Machine learning is based on the use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyse and draw inferences from patterns in data. AI tools process a large amount of data and provide **relevant insights to facilitate decision-making processes and to identify threats** in the supply chain.

- Criminal organizations are able to **infiltrate the legitimate supply chain at various stages and by using complex techniques** that include taking control of informal mines, acquiring precious metals from illegal

mining by using illicit profits (mainly generated by illicit trafficking of narcotics), or the illegal acquisition of catalysts and scrap metals, establishment of national and international smuggling rings, creation of clandestine manufacturing facilities to transform the materials or refineries to extract precious metals from stolen or illegally acquired products, mismarking to hide the origin, components and quality of the products, trade misinvoicing in order to evade tax duties and dodge Customs controls, selling the products as original and legal and money laundering. As a consequence, the solutions adopted to secure the supply chain should consider the use of a **multilayer security approach**, bringing together multiple technologies to **support stakeholders and authorities**. This element has been confirmed by the majority of the submissions that we received, where multilayer security was at the core of many of them.

- Some criminal activities highlighted by the scenarios cannot be limited by supply chain security technology. This has to be expected since the main purpose for which these technologies were developed is to protect the integrity of the supply chain and not to stop different kinds of criminal operations. The mitigation of these risks will necessarily require actions and strategies implemented by law enforcement agencies to better **understand how crime operates and how to monitor organized crime strategies to prevent these criminal activities.** It is for these reasons that some steps of the criminal plans in the risk scenarios were difficult to limit by supply chain technology solutions. This is the case, for instance, for some of the steps indicated in risk scenario 1, in particular, the control of the mines and in risk scenario 2, forcefully recruiting workers or the acquisition of gold from illegal mining by using illicit profits. It also includes all the steps described in risk scenario 3, infiltration of the legal industrial refining process.

- Following on from the previous point, an integrated approach between different technology typologies and options is needed to **support at the same time investigators and law enforcement agencies** on the one side, as well as **supply chain operators and consumers** on the other.

- This constant search for innovation can also be seen in attempts aimed at improving the marking process as the primary authentication element itself. **The submissions collected proposed an array of solutions to improve the uniqueness of the marks, the authentication processes and the inclusion of several technologies** that are linked to the mark, such as the use of blockchain protected traceability systems.

- **Consumer education** is essential in order to implement authentication solutions. The authentication codes used by different providers are frequently easy to scan through the use of smartphone cameras, however, the consumer needs to be aware of the existence of the verification mechanism and of the steps that need to be taken to corroborate the authenticity of the products.

- **Forensic techniques** like the Chemical Forensic Bureau for the identification of mining and metallurgical products are decisive tools to support the work of **law-enforcement authorities** and stakeholders since they provide a **cooperation mechanism** to obtain accurate results regarding the origin and composition of metals.

- **Forensic analysis** comes at a different stage, when it is necessary to recognize if a breach of the supply chain happened. Even if these technologies cannot be used to prevent the criminal activity from happening, unless their continuous use over time creates a dissuasive effect on criminals, they play a very important role since they are capable of identifying the **nature and origin** of the products as well as their **components** and authenticity**.**

- The analysis of specific elements in the composition of a product enables its clear authentication. More complete sample databases are constructed as the analyses are performed. Furthermore, by progressively analysing samples in the supply chain, it will also be able to trace back the source of the incident and present this **evidence in court**.

- As demonstrated by the submissions received, security in the supply chain is being adapted to include **digital platforms**. The digitalization of metal sales contracts using blockchain technology can mitigate the risks of possible criminal operations during multiple transactions and can improve protection from organized crime activities such as money laundering and counterfeiting precious metals, among others.

- Using Earth Observation to identify illicit mining operations can be crucial to create better **strategies and policies** to target these illegal activities. Cooperation between different stakeholders and law-enforcement authorities can be facilitated by the data analysis obtained through the implementation of these tools. **Regulatory compliance** can also be monitored and protected with this technology.

CHAPTER 4
Illegal, Unreported and Unregulated (IUU) fishing

Irregular, Unreported and Unregulated (IUU) fishing refers to fishing practices that violate relevant laws or take place beyond the reach of fisheries laws and regulations.

IUU fishing has emerged as a lucrative business run by organized criminal networks, which make systematic efforts in this low-risk, high-return illegal activity, in a context of overfishing and diminishing stocks.

Illegal fishing describes fishing which is conducted in waters under the jurisdiction of a State and in violation of laws and regulations of that State, as well as those of fishing vessels' flag states.

Unreported fishing refers to the practice of not reporting details of catches or deliberately misreporting catches to the relevant national authority, in contravention of national laws and regulations.

In particular, unregulated fishing refers to fishing conducted by vessels without nationality, or fishing conducted against the regulations of Regional Fisheries Management Organizations (RFMO), i.e. the international organizations formed by countries with fishing interests in an area. Unregulated fishing can occur in ocean areas which are outside the control of any RFMO and in the high seas, which are more difficult to monitor.

IUU fishers seek to circumnavigate regulatory regimes by fishing in areas beyond state jurisdictions, or increasingly in areas under the jurisdiction of States with weak governance.
IUU catches are then laundered through the legitimate fish supply chain. This leads to deceptive marketing practices with respect to the geographical origin of the product, through mislabelling, species substitution and falsification of documentation, thus endangering the health of the consumers. These practices lead to the over-exploitation of fish stocks and threaten the food security of developing countries.

While the main driver of IUU fishing is profit-making, several factors contributed to the rise of the phenomenon, including the globalization of the fish chain, which has provided and increasing number of opportunities for fraudulent activities; the low risk of detection of species substitution by food control authorities; and the prevalence of paper-based traceability programmes, which can be easily forged, instead of DNA-based fish identification methods.

According to the United Nations Food and Agriculture Organization, IUU fisheries' turnover can be estimated between 10 billion USD and 23 billion USD per annum, representing between 11 million and 26 million tonnes of illegally obtained fish.[1]

4.1 Risk scenario

One risk scenario has been elaborated in the area of IUU fishing.

Risk Scenario

An emerging and unscrupulous company is operating in one of the leading countries for what concerns fishing and aquaculture harvests. The company is active in the domestic market of highly priced species, including prawns, salmon and tuna. However, there is also suspicion around their potential use of illegal fishing practices, and, with international fish demand expected to grow steadily for a number of years, the company is trying to consolidate its position and boost its exports abroad.

1 http://www.fao.org/3/a-i6069e.pdf

To achieve this goal, their representatives decide to strengthen their ties with a different company operating the main national container port. The fishing company is attracted by this business opportunity but is unaware that the port operator is under the influence of the leader of a criminal group operating in the country.

The criminal group has a deep-rooted presence in the social and economic fabric of the country and is capable of hampering or favouring the implementation of business initiatives related to the port, through fuel bunkering and pilot services. Through racketeering and corruption of freight forwarders, criminals interfere in the selection of manpower and in the attribution of contracted works in the harbour.

Willing to engage in the fishing business, the leader of the criminal group implements the following criminal plan:

Step 1. Money laundering and entering the fish market through cooperation with the fishing company: the leader of the criminal group, acting through her/his cargo port operator front company, proposes the investment of 8 million euros to the fishing company, to participate in the purchase of new fishing gear and the upgrade of the fishing fleet, in exchange for 10% of the fishing company's annual profits for three years. The fishing company is unaware that the 8 million euros derive from illicit operations managed by the criminal group, who wants to launder illicit proceeds through them. Hiding behind complex corporate ownership structures, involving multiple front companies in different countries, the fishing company and the port cargo operator join forces to purchase three new boats and a refrigerator vessel to store the catches at sea.

Step 2. Using illegal fishing methods: while largely relying on a workforce employed in irregular work conditions, the fleet deploys illegal fishing methods, taking their boats near protected areas to maximize their catches. To evade law enforcement scrutiny and defuse suspicion in the event of an inspection, vessel masters are instructed to falsify catch records and keep an empty logbook to be filled in case of incoming inspection. The illegal fishers are also able to remain out at sea for longer than their competitors, as they are able to transfer their catch onto their refrigerator vessel, which is exempted from catch documentation because it does not fish. The fleet is also able to unload their catch at the harbour thanks to the cooperation of the cargo port operator controlled by the criminal group, where lax controls and corrupt forward agents ensure that clearance procedures are finalized without delay.

Step 3. Infiltrating the supply chain: the fishing company's processing facilities and aquaculture plants are involved in mixing illegal catches with legal ones and infiltrating them into the licit fish supply chain. The fishing company also exploits the difficulty in identifying species once they have been filleted and flavoured, and fraudulently places pangasius on the market, presenting it to buyers as a more expensive, white-fleshed species.

Step 4. Packaging mislabelling to fool consumers and buyers: the fishing company plants consistently mislabelled packaging, fraudulently claiming that they use sustainable fishing methods, whereas in reality they use entangling nets and even explosives, which substantially degrade the health of the country's marine ecosystem.

Other forbidden practices: the fishing company also transfers illegally caught undersized tuna to its aquaculture facilities. The fish are kept here until they reach the legal marketable size. Upon leaving the plant, the tuna complies with legal requirements and are sold to unsuspecting retailers. The fishing company also employs food additives such as water-binding agents to deceptively increase the weight of products and carbon monoxide to enhance their visual quality.

Cooperation with the cargo company controlled by the criminal group allows the fishing company to dramatically increase its share in seafood products on the domestic market and to strengthen exportation to foreign countries, with annual profits doubling from 25 million to 50 million euros. At the same time, this opportunistic alliance enables the criminal group to launder 8 million euros in illicit proceeds, while receiving almost twice the amount over three years.

Such mutual benefits come at a price. IUU fishing practices give the fishing company an unfair comparative advantage over their legitimate competitors and has the effect of rapidly depleting the fish stocks of the country, damaging its marine ecosystem.

4.2 Technology solutions to address the risk scenario

The negative consequences of Irregular, Unreported and Unregulated (IUU) fishing are extensive, impacting environmental issues such as marine biodiversity, over-exploitation of fish stocks and long-term sustainability, to labour issues involving human rights abuses and food security for communities. The existing technology options have been developed to combat these threats with multilayer security approaches that support the work of both stakeholders in the supply chain and national and international authorities. The technology solutions are focused on providing more accurate tools for the authentication of the products, including the identification of relevant characteristics such as their origin and the use of substances; as well as on monitoring the activity of vessels and reporting of information. New solutions also attempt to provide customers with mechanisms to verify the origin and quality of the products, improving transparency from the source to the final stage. The technology options complement strict regulations and labelling protocols, serving as tools to improve the management of information and coordination between the different stakeholders.

In the case of fishing, products' authentication can be achieved through different methods. For instance, radio-frequency identification (RFID) tag systems have been used to capture relevant information about the product, such as the fishing time, position, biological data as species name, sex, body length and weight. In addition to the function of tag and code systems, authentication solutions have frequently been designed to be integrated to traceability systems in order to strengthen the security from the fishing stage to the packaging and distribution of the products. An example in this regard, for instance, can be found in the combination of RFID and QR codes that has been proposed to capture information throughout the supply chain in New Zealand in cooperation with World Wide Fund for Nature (WWF).[2] In this case, a RFID tag has to be affixed when the fish comes on board the vessel to follow it and register information automatically at various devices positioned on the vessel, at the dock, and in the processing facility. Once the product is processed and partitioned out into various products in the processing facility, it will receive a QR code (or potentially in the future a near field communication NFC device) that will track the product past the retailer.[3] The code that is used to track the product along the supply chain can also contain unique information about each product by using processes such as polymerase chain reaction (PCR) to obtain data related to the DNA of the sample.

As presented in the introduction to this report, track and trace systems are used to monitor the products along the different stages of the supply chain. In the case of fishing, integrated satellite imaging and tracking is essential to understand the movement and fishing practices employed by vessels. Some technologies have been created to obtain accurate information even when vessels are not actively transmitting a signal. Passive vessel detection technologies such as Synthetic Aperture Radar (SAR), Visual Imaging Infrared Radiometer Suite (VIIRS), combined with other required active transmitting systems such as Automated Identification Systems (AIS) and Vessel Monitoring Systems (VMS) are being used to achieve this.[4] Furthermore, global night-time satellite images can be used to monitor and identify IUU fishing activities such as intrusions into restricted or no-fishing zones.[5]

Some changes are also being made in electronic monitoring to detect irregularities on board of the vessels, making it more effective through the use of WiFi and satellite data transmission and the implementation of artificial intelligence (AI) analysis.[6] Electronic monitoring can supplement the work of observers and at-sea monitors through the

2 "Tracking fish from vessel to the supermarket, the Blockchain Supply Chain Traceability Project " by WWF-New Zealand, WWF-Australia, and WWF-Fiji, ConsenSys,TraSeable, and Sea Quest Fiji Ltd.

3 World Wide Fund for Nature (WWF). (n.d.). New Blockchain Project has potential to revolutionise the seafood industry. Retrieved from https://www.wwf.org.nz/what_we_do/marine/blockchain_tuna_project/

4 Synthetic Aperture Radar (SAR) is a type of active data collection where a sensor produces its own energy and then records the amount of that energy reflected back after interacting with the Earth; the Visible Infrared Imaging Radiometer Suite (VIIRS) instrument collects visible and infrared imagery and global observations of land, atmosphere, cryosphere and oceans; Automatic Identification System (AIS) is an automated tracking system that displays other vessels in the vicinity; and the Vessel Monitoring System (VMS) is a satellite-based monitoring system which at regular intervals provides data to the fisheries authorities on the location, course and speed of vessels.

5 Geronimo, Rollan C.; Franklin, Erik C.; Brainard, Russell E.; Elvidge, Christopher D.; Santos, Mudjekeewis D.; Venegas, Roberto; Mora, Camilo. 2018. "Mapping Fishing Activities and Suitable Fishing Grounds Using Nighttime Satellite Images and Maximum Entropy Modelling" Remote Sens. 10, no. 10: 1604. https://doi.org/10.3390/rs10101604

6 World Wide Fund for Nature (WWF). (2020, December). How Data and Technology Can Help Address Corruption in IUU fishing. Retrieved from https://www.worldwildlife.org/pages/tnrc-blog-how-data-and-technology-can-help-address-corruption-in-iuu-fishing

use of data reporting and collecting technologies that include electronic reporting of the trip data such as catch, landings, and purchase data and electronic monitoring equipment like cameras and sensors that capture information on fishing location, catch, and discards.

In addition to the traceability technology options, improvements have been made to facilitate their implementation and efficiency. In 2020, the Global Dialogue on Seafood Traceability (GDST) presented the Standards and Guidelines for Interoperable Seafood Traceability Systems, v1.0 (GDST 1.0), an initiative to provide basic technical standards to enable interoperability across the different seafood traceability platforms.[7] The standards seek to make global seafood traceability more reliable and affordable.

Forensic-related technology, focused on the biological and chemical properties of a product, also have a role to play in this context. Authentication of fish can only be performed by a limited variety of methods due to the nature of the product. This is partially caused due to the wide biological diversity of fish and seafood products, the removal of external features during processing steps, as well as the close phylogenetical relationships among them which render the morphological identification almost impossible.[8] In this area, some of the options to verify the authenticity, provenance and traceability in the seafood and fish industries include the use of polymerase chain reaction–restriction fragment length polymorphisms (PCR-RFLPs) to create a DNA barcoding for identification of fish species and the application of vibrational spectroscopy (near- and mid-infrared, Raman) combined with chemometric methods to identify, detect, and classify the products. These procedures provide highly useful tools for law enforcement since they can give accurate information about the specific product, allowing the simple detection of mislabelled or fraudulent fish products.

For example, PCR-RFLP is a method which is often regarded as less time-consuming and more cost-effective than DNA sequencing, which requires equipment that is usually readily available in most molecular laboratories and has proven its utility in species identification.[9] Molecular authentication is useful in order to identify species from tissue samples in the absence of morphological characters used to distinguish between legal and illegal products, to relocate animals for their natural populations, and to mark and track DNA profiles.[10] Other techniques that have been used to detect illegally substituted and mislabelled products include chemometrics and spectroscopy.[11] Mid- (MIR), near-infrared (NIR) and Raman spectroscopy are molecular/vibrational spectroscopy techniques that are used to evaluate and study the interactions of electromagnetic waves. The vibrational responses provide information about the chemical composition of the sample.[12] In addition, nuclear analytical techniques including stable isotope analysis, ITRAX X-ray fluorescence, neutron activation analysis, ion beam analysis and synchrotron technologies provide great precision in determining geographical locations of food. Biochemical tracking can be obtained to identify the exact origin of the product, providing a similar or supplementing option to genetic tools.

Finally, artificial intelligence (AI) can be used in analytics tools to improve the insights obtained from data gathering. Its use was usually mentioned as a relevant addition to electronic monitoring; however, it can be adopted to other processes. Existing solutions use algorithms that can improve the quality and speed of information related to fishing activities. An AI-powered platform can track data points from Automatic Information System (AIS) including vessel activity, vessel size and engine power, the type of fishing being carried out and the type of gear used.[13] AI

7 Global Dialogue on Seafood Traceability. (n.d.). GDST 1.0 Standards and Materials. Retrieved from https://traceability-dialogue.org/gdst-1-0-materials/

8 Phylogenetic relationship refers to the relative times in the past that species shared common ancestors.
Power, Aoife; Cozzolino, Daniel. 2020. "How Fishy Is Your Fish? Authentication, Provenance and Traceability in Fish and Seafood by Means of Vibrational Spectroscopy" Appl. Sci. 10, no. 12: 4150. https://doi.org/10.3390/app10124150

9 Torres, Rodrigo & Feitosa, Rafael & Carvalho, Daniel & Freitas, Matheus & Hostim-Silva, Mauricio & Ferreira, Beatrice. (2013). DNA barcoding approaches for fishing authentication of exploited grouper species including the endangered and legally protected goliath grouper Epinephelus itajara. Scientia Marina. https://doi.org/10.3989/scimar.03805.29A.

10 Torres, Rodrigo & Feitosa, Rafael & Carvalho, Daniel & Freitas, Matheus & Hostim-Silva, Mauricio & Ferreira, Beatrice. (2013). DNA barcoding approaches for fishing authentication of exploited grouper species including the endangered and legally protected goliath grouper Epinephelus itajara. Scientia Marina. https://doi.org/10.3989/scimar.03805.29A.

11 Chemometrics may be defined as the combination of algebra, mathematics and statistical analysis techniques to analyse and process data, which for multivariate analysis for processing large datasets derived from food analysis, particularly instrumental analysis.
Power, Aoife; Cozzolino, Daniel. 2020. "How Fishy Is Your Fish? Authentication, Provenance and Traceability in Fish and Seafood by Means of Vibrational Spectroscopy" Appl. Sci. 10, no. 12: 4150. https://doi.org/10.3390/app10124150

12 Ibid.

13 Global Fishing Watch. (n.d.). How our vessel tracking map works. Retrieved from https://globalfishingwatch.org/map-and-data/technology/

can train algorithms to detect fishing-related patterns to detect how close ships get to transhipment vessels, and whether they turn off their AIS when they do, resulting in the possibility to map IUU fishing hotspots. The platform can also access the Vessel Monitoring System, a satellite-based monitoring system that provides information to the fisheries authorities about the location, course and speed of vessels. This technology can be adopted to identify other issues, such as slave labour, through the use of algorithms that flag suspicious behaviours like the amount of times nets were set in a day or the number of days the vessels have spent without landing.[14]

This part of the report will now present possible solutions to the challenges posed by the risk scenario described in the previous section. It describes the main aspects of the technology submissions, their relevance to the risk scenario and possible advantages and limitations. Advantages and limitations usually refer to the technology categories in general. However, in some cases, reference will be made to some of the specific submissions we received, and this will be done just in view of providing a specific example of technology application.

By analysing the above-mentioned submissions, it is clear that there are different technological approaches that can be used, very often mixing supply chain security technology with forensic analysis of the species, artificial intelligence to improve data analysis, blockchain technology to render the set of data inserted in a database immutable, and also space technology to monitor the movement of vessels and then of the tracked and traced product. The starting point of the track and trace is also a very interesting element to consider, and some options are trying to implement authentication and track and trace features starting as early as the vessels.

In general, the submissions showed that technology solutions have the capacity to provide improvements to limit risks identified in the following areas:

- Use of illegal fishing methods and techniques to operate processing facilities and aquaculture plants which are involved in mixing illegal catches into the licit fish supply chain.
- Packaging mislabelling to fool consumers and buyers, including false declarations over the origin of catches.
- Lack of full monitoring and data exchange in the supply chain, which might enable the spread of other forbidden practices.
- Employment of food additives such as water-binding agents to deceptively increase the weight of products and carbon monoxide to enhance their visual quality.

They also respond to some of the needs highlighted by the risk scenario, in particular:

- The need to implement a comprehensive traceability system from vessel to supermarket.
- The lack of digitized processes and a need to update or replace paper-based traceability programmes which are prone to falsification.

Those technologies which also include a forensic component, may also address the following element:

- Lack of comprehensive data related to genetic traceability markers.
- Need to identify new genetic traceability markers (isotopic analysis) to support and supplement the use of DNA sequencing and render their application.

14 Global Fishing Watch. (2020, December 21). Satellites can reveal risk of forced labor in the world's fishing fleet. Retrieved from https://globalfishingwatch.org/press-release/forced_labor_risk_fishing/

For what concerns the interesting features of the technologies applied in this field, supply chain security technology allows for the following interesting elements:

- *Customization*: Codes and labels can be widely modified to create unique and personalized options, showing great adaptability to products and surfaces. Customized codes, tags and labels can be harder to imitate since they are not widely available for a large range of products. The codes can be shaped into different icons, depending on the product. The labels can be fully customized to fit the needs of the producer.
- *Codes are easily readable*: Codes with encrypted information can be machine-readable by smartphones and ubiquitous devices. In some options, validation is easy and fast and can be made offline.
- *Non-reproductible*: Codes can hardly be reproduced without knowing the cryptographic key, this is essential to: authenticate the original product, monitor its movement along the supply chain and prevent infiltration of non-authenticated and non-original products.
- *Unique*: Codes, labels and tags create an identity for every object or product. They contain a unique sequence of codes and information that provides specific information about the individual product.
- *Large data storage*: Available codes and tags can encode large amounts of information.

The use of blockchain and artificial intelligence adds the following interesting features:

- *Immutability*: The information about the product that is registered in the blockchain-based platform cannot be modified. This is achieved through the ability of a blockchain ledger to remain unchanged, unaltered and indelible.
- *Auditability and accountability*: Accountability is verified as a part of timestamps established by the blockchain system in the platform. This system allows every stakeholder to confirm whether the service operates in the intended way. If the product fails the verification process, then the stakeholders have proof of malicious behaviour which could be used to hold the responsible stakeholder accountable. In addition, a transaction can only be made when both the sender and receiver are authorised through the private and public key system.
- *Transparency*: The blockchain technology used in the digital platform allows stakeholders to monitor the supply chain with openness, communication, and accountability. The stakeholders included in the chain can access the information at any point to corroborate the status of the products and the processes. Recorded product and time/location data is stored for easy data access in the database but cannot be adulterated in any way because it is locked to the cryptographic hashing in the blockchain, and a change would immediately be visible.

Finally, those technologies which are based on, or which make use of, forensic analysis, also offer the following interesting features:

- *Unique*: Geographical and environmental conditions ultimately control the elemental and isotopic makeup of a product. Nuclear techniques can determine the intrinsic isotopic and elemental fingerprints in the samples, with greater detail and accuracy than conventional methods (i.e., morphological traits, fatty acid analysis, DNA profiling etc.). Other identification techniques include polymerase chain reaction (PCR) and biometrics.
- *Non-imitable*: Isotopic signatures are very difficult to mimic. Biomarkers are compounds that have a biological specificity in the sense that they are produced only by a limited group of organisms.
- *Accuracy*: The methodology is highly sensitive, accurate and has been validated by a wide scientific literature. The use of this technology in other areas provides corroboration of the usefulness and accuracy of the method.

Some limitations can also be identified, and they may relate essentially to the intrinsic characteristic of isotopic analysis or of other nuclear and forensic analytical techniques. In particular:

- *Environmental factors*: There are environmental factors that can affect the stability of the isotopic and elemental signals. Using stable isotopes or the elemental profile alone tends to produce less reliable results when trying to predict provenance. However, using them together in mathematical models determines the geographic origin and production method of seafood (wild and farmed) with a high degree of accuracy (>80%). Therefore, using multiple nuclear techniques can provide reliable and accurate predictions of seafood provenance.

- *Time consuming*: Sample preparation may be time consuming with multiple steps. In those cases, results are therefore produced with a significant time difference with respect to the moment in which the seafood has entered the market. This element could be avoided by the development of portable analytical methods, which would allow for a rapid in-situ analysis where supply-chain actors could rapidly screen samples and determine which samples require further investigation using, in that case, more accurate and time-consuming lab-based analyses.

- *Space*: The size of a laboratory is large, therefore, in order to apply these analytical techniques, it is necessary to have considerable space to build related facilities. However, this limitation would be eliminated if a portable device is developed.

- *Highly qualified staff*: To implement these analysis, highly qualified engineers are needed, and they need to have the technical knowledge to operate the equipment in the laboratory.

4.2.1 Applying track and trace technology starting from the vessel

Technology submission 1

The submission proposes the adoption of two main technology options that are fully integrated to help secure the fishing supply chain:

Digital end-to-end blockchain traceability platform that directly operates in the vessels.
A machine-readable code that provides an authentication mechanism for stakeholders and consumers.

The platform is used to trade fish catches directly from the vessel to the final buyer by using a complete digital approach. The technology is installed inside the vessels to obtain the information about the product directly from the fishers. Artificial intelligence is employed to realize the fish identification and classification as soon as it is caught, automating the process. Fishers have an automatic weighing scale which works together with an app operated via their mobile phones. As soon as the information about the fish is uploaded in the app, consumers can access it through the marketplace by using the app itself, allowing fishers to sell their products immediately from the vessel. After this process is carried out in the vessel, a quality control on the landing facility is performed by a team of experts that receives the fish and evaluates the freshness level, species identification, size, and the compliance with rules. A mobile application that analyses the fish according to European standards is used in order to objectively evaluate the freshness of the product. After this validation, a smart contract in the blockchain is closed and the products move to the packaging and distribution partners.

At this stage, the lots of products receive a QR code with the information about the specific lot, adding product authentication to the package to create an additional security layer. In addition, the submission offers two other options that could be implemented to start the traceability in the vessel, specifically:

1) pre-printing the QR codes that go in the vessels and that are associated with the catch when the blockchain entry is created

2) whenever the QR code is created and printed (on sea or land) it can be created with information retrieved from the blockchain, linked to the catch – Batch Number.

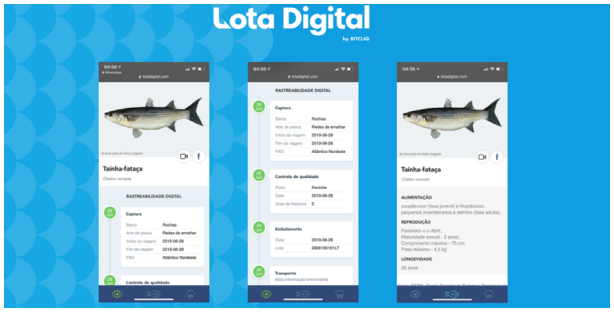
A complete system to code information in a unique identifier is used, providing several levels of security at the physical and the digital levels. The code is completely configurable and adaptable to any document, stamp or product. This option offers a machine-readable security information system for a variety of products that is readable by smartphones which allows auditors and authorities to use the solution in the field to validate the code and the consumer to validate authenticity anywhere. Different access privileges to information can also be set up, responding to different needs in terms of security levels (private, public, and encrypted). The solution is based on the printing of stamps, seals or labels that are attached to the products and that are tamper evident.

The authentication component of this technology merges different elements to authenticate the product, namely a machine-readable 2D barcode (using symmetric and asymmetric cryptography), security holograms and glitter inks with unique patterns. The objective of the solution is to code information in a unique identifier that combines several layers of security measures by combining the physical characteristics of the product with a digital identity that is stored in a code that is fully customizable and adaptable to any product. The code can be hidden in the aesthetics of the design and has high capacity to store a great amount of information. In a nutshell, the complete authentication solution can be divided into different security layers: 1) the printed-graphic code, 2) holographic Optical Variable Devices (OVD), and the 3) glitter inks; all which have a unique and irreproducible pattern.

Through the code, the consumer can access information about the product (vessel, day of capture, fishing method), including data related to quality control (port, freshness, date), packaging (date and lot), transportation, some information about the species (general characteristics and image), and recipes.

Submission received from INCM and BITCLIQ

This submission give us the opportunity to describe possible advantages created by the application of authentication and track and trace technology starting as early as the vessel. Some interesting elements include the recording of catches, including their species, number and weight, as soon as the fish is caught via an app operated by the fishermen and connected with a database.



Source: INCM, BITCLIQ

Information included in this database is immediately accessible by potential buyers in the port and will then be verified by independent authorities once the catches are unloaded. This redundancy ensures an additional control in relation to what is declared by the fishermen, in view of trying to identify possible misdeclarations or fraud on their part.

Source: INCM, BITCLIQ

Information is recorded on a blockchain at this stage. Traceability using blockchain technology is used to monitor the product through the different processes from the vessel to the port, limiting diversion and infiltration possibilities. Traceability is complemented by the authentication system to provide an additional layer of security. The app provides information that is taken directly from the traceability system, such as the origin and time and place stamp.

Artificial intelligence is also used to identify and classify the fish as soon as it is caught and registered by using the app. This also automatically uploads the product to the online marketplace, facilitating the transactions between fishers and customers without the intervention of third parties.

Once the product is sold, a new step in the process starts and each sold product is given a unique code which will then ensure its traceability and authentication along further steps of the supply chain. In this case, a code contains data about the product (vessel, day of capture, fishing method), including data related to quality control (port, freshness, date), packaging (date and lot), transportation, some information about the species (general characteristics and image).

These codes are tamper evident and are available using multiple security options, 1) the printed-graphic code, 2) the holographic OVD, and the 3) glitter inks, that are combined to provide different layers of security. These options have tamper-evident mechanisms that facilitate the identification of any issue with the product, including easy spotting of manipulation attempts and/or infiltration of non-original products into the supply chain. The app would recognize if the product was manipulated, generating a red cross when scanning the code. Identification of the product along the supply chain can be done using non-intrusive methods and without opening the package through the use of scanners or special readers.

The technology is still package-dependent for the part that goes from the port onwards and the blockchain technology is only used in the digital platform from the catching process to the quality control performed in the port. The cycle of the product during packaging and distribution uses the QR code and the authentication system and can be included in the blockchain if the QR codes are pre-printed and applied in the vessels. Whenever the QR code is created and printed (on sea or land), it can be created with information retrieved from the blockchain, linked to the catch – ACV/Batch Number.

The technology solution proposed by the submission can be used to mitigate most of the risks presented in the risk scenario. The combination of a digital, end-to-end blockchain traceability platform that directly operates in the vessels and machine-readable code that provides an authentication mechanism for stakeholders and consumers creates a multilayer security solution that targets different vulnerabilities in the supply chain. These technologies may play a role in limiting the following steps of the criminal plan:

- Using illegal fishing methods.
- Infiltrating the supply chain.
- Packaging mislabelling to fool consumers and buyers.
- Other forbidden practices.

In particular, for what concerns step 2 "use of illegal fishing methods", the digital platform registers the catching method used for each fish and this should avoid the use of illegal fishing. The limitation, in this regard, lies in the fact that the registration relies on the honesty of the fishermen, since they are the ones who will use the app at sea through their smartphones. However, it has to be added that the complementary check performed at the sea docks' facilities by independent authorities can limit the risk of illicit behaviour by the fishermen.

In relation to step 3 "infiltration into the supply chain", the boat-to-buyer seafood e-marketplace platform uses digital traceability to directly secure the fish caught through the integration of blockchain. This enables the customer to have transparent information about the product they are acquiring without the intervention of other parties. The fish that is caught in the vessel is almost immediately registered, which serves as a tool to mitigate the risk of any infiltration in this part of the supply chain. Later, the validation performed in the port corroborates the information about the products before sending them to the packing and distribution stages. The information about each fish is then encrypted in an authentication code that can be scanned by using the camera of a smartphone, allowing the customer to verify the authenticity of the product and to access information about the product (vessel, day of capture, fishing method), including data related to quality control (port, freshness, date), packaging (date and lot), transportation, some information about the species (general characteristics and image), and recipes. The code can be linked to the traceability system that started with the initial registration of the product in the vessel. The submission proposes two different options to achieve this, mainly by, 1) pre-printing the QR codes that go in the vessels and that are associated with the catch when the blockchain entry is created or, 2) whenever the QR code is created and printed (on sea or land) it can be created with information retrieved from the blockchain, linked to the catch – ACV/Batch Number.

The use of a unique code with security and tamper-evident features can also limit step 4 "packaging mislabelling". Specific features are used to increase the security of the code, such as glitter inks, while the identity of each product is created by using a unique tamper-evident code merging a graphic and a physical component. Furthermore, the graphic and the physical part of the code can also cross-validate for increased security. The product can then be followed along the supply chain thanks to the app.

For what concerns step 5 "use of other forbidden practices", this submission relies on the good use of the digital platform which is already implemented at the vessel level to record the catches and their fishing method, location and quantity. Furthermore, the digital platform is integrated with blockchain and artificial intelligence, providing additional security and control features. In particular, AI is used to perform the fish identification and classification as soon as it is caught, automating the process. The use of blockchain technology during the first stages of the supply chain and the authentication system that is used after packaging the product limits the actions of organized crime.

In the case of step 6 "use of food additives", as indicated, the technology is package dependent once the product reaches the port. The solution targets the packaging and not the food itself, its ingredients or its unique chemical composition. Consequently, criminals capable of infiltrating companies working at the production level can package fraudulent goods using original packaging. If the QR codes are added with integration of data from the vessel to the final distribution, this step could also be limited, since the blockchain traceability that starts as soon as the fish is caught would be continuous and not stop at the port to then restart once the product is processed and ready to follow the other phases of the supply chain.

Summary table for submission 1: possible application to limit risks highlighted by the scenario

Scenario	Applicability of the solution
Scenario 1: Infiltrating the fishing legitimate supply chain	
Step 1 – Money laundering and entering the fish market.	
Step 2 – Using illegal fishing methods.	The digital platform registers the catching method used for each fish. However, this relies on the honesty of the fishers, since they are the ones who will use the app at sea through their smartphones. The complementary check performed at the sea docks' facilities can limit the risk of illicit behaviour by the fishermen.
Step 3 – Infiltrating the supply chain.	The digital platform backed by blockchain technology and the authentication system provided by the unique code create a multilayer solution that protects different stages in the supply chain. However, the information is protected by the blockchain when the digital platform is used. After the validation is performed at the port, the smart contract is closed, and an infiltration might be harder to detect even with the following authentication. However, the submission also proposes adding the QR code that is linked to the blockchain from the vessel, protecting the products from the catch.
Step 4 – Packaging mislabelling to fool consumers and buyers.	Risk is reduced thanks to the use of non-replicable codes that are recognizable both visually and via the use of specific tools and by using track and trace technology to secure the supply chain. The flow of products along the supply chain can be checked using an app, giving consumers the possibility of performing an offline check. Fish are registered directly to the app from the moment in which they were caught.
Step 5 – Other forbidden practices.	The risk is mitigated due to the use of the digital platform that is installed inside the vessels to obtain the information about the product directly from the fishers. Artificial intelligence is employed to make the fish identification and classification as soon as it is caught, automating the process. The use of blockchain technology during the first stages of the supply chain and the authentication system that is used after packaging the product limits the actions of organized crime.
Step 6 – Use of food additives such as water-binding agents.	

4.2.2 Using forensic technology

Technology submission 2

One of the starting points of this submission lies in the importance of seafood provenance. The term seafood provenance refers to determining both the geographic origin and production method of seafood. Seafood provenance has become increasingly important to consumers, seafood industries and regulatory bodies. Methods such as DNA and fatty acid profiling, stable isotope analysis and elemental profiling using inductively coupled plasma mass spectrometry (ICP-MS) have been used to determine the origin of seafood as well as to distinguish between wild-caught and cultured seafood. Recently, bookkeeping methods such as blockchain or radio-frequency identification (RFID) have been added to trace the origins of seafood. However, each method has its advantages and disadvantages, with some methods excelling in determining the geographic origin and others better at distinguishing the production method.

The nuclear techniques used, including stable isotope analysis, ITRAX X-ray fluorescence, neutron activation analysis, and ion beam analysis technologies, provide great precision in determining geographical locations of food.

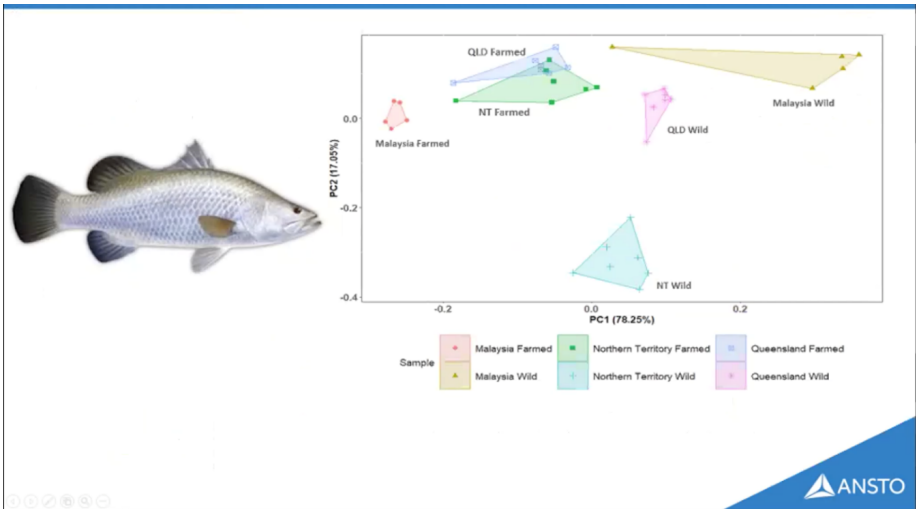
This technology option is based on iso-elemental fingerprint techniques, including stable isotope analysis and X-ray fluorescence (XRF) through an Itrax scanner, to obtain the unique elemental and isotopic composition of seafood. The technology was tested on high valued seafood products such as Asian seabass and giant tiger prawns. These iso-elemental fingerprints were then used to create a provenance predicting model which could distinguish both the production methods and geographic origins of both species with greater than 80% accuracy. Following the success of this test, a larger scale research was established to improve the prediction accuracy of the technology to distinguish between wild and farmed origin of seafood, including their geographical origins.

The iso-elemental fingerprint data is processed in a machine learning model where this information is analysed to find patterns in order to predict the provenance.

Furthermore, a portable method using handheld XRF to determine seafood provenance is being developed. It is expected that the portable method will be used to quickly screen seafood products, while complex samples will be analysed using the lab-based techniques to provide a higher accuracy. The regular screening of points along the seafood supply chain using the handheld XRF technology, currently in development, will also ensure that any fraudulent catch is identified before it has a chance to be sold to consumers. This will provide consumers with the confidence that the product they are purchasing is legitimate, which in turn contributes to the market chain traceability. In addition to addressing seafood provenance, this technology provides the opportunity to make safety assessments for biosecurity purposes (i.e. if any bans are imposed on food products).

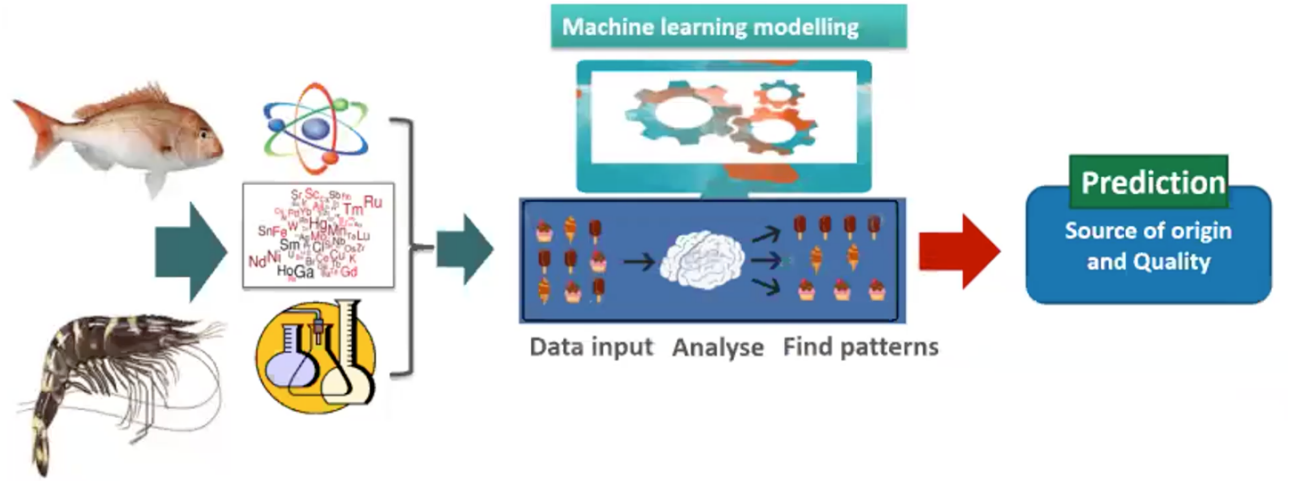
Submission received from the Australian Nuclear Science and Technology Organisation (ANSTO). Collaborators (University of New South Wales, Macquarie University, National Measurement Institute and Sydney Fish Market)

This submission is useful to discuss the potential benefits of the use of forensic analytical techniques against criminal and fraudulent practices in the IUU fishing area. This submission highlights the importance of using technology as a tool to establish a validated provenance of the catches. Seafood species assimilate isotopic and elemental signatures from their environment in which they live and grow. If these intrinsic fingerprints are determined accurately by forensic analysis, they can be subsequently used to develop scientifically validated provenance tools based on repositories of information.



Source: ANSTO

There is also a potential link to supply chain security technology that can be added to the forensic component, since the technology also offers actors of the supply chain the opportunity to assess food safety and quality characteristics based on elements present in the food.



Source: ANSTO

Producers and suppliers may be able to use the iso-elemental fingerprints to brand their food, providing an option for the client to identify accurately labelled and high-quality, products through field testing. Of course, specific tools to allow for field testing possibilities will have to be developed.

In the case in which field testing is not developed, then this technology will probably come into play once an incident occurs or once a suspicion arises on the nature or legality of catches and fish products. Iso-elemental fingerprinting techniques, including stable isotope analysis and X-ray fluorescence (XRF) through Itrax cannot be used to prevent the criminal activity from happening (unless their continuous use over time creates a dissuasive effect on criminals), but they can be used to unequivocally identify the adulteration of a product or the fraudulent behaviour of criminals involved in food fraud. Consequently, these technologies may play a role in limiting the following steps of the criminal plan:

- Using illegal fishing methods.
- Infiltrating the supply chain.
- Packaging mislabelling to fool consumers and buyers.

In particular, for what concerns step 2 "using illegal fishing methods", the iso-elemental fingerprinting techniques provide the unique elemental and isotopic composition of seafood, which can then be used to create a provenance predicting model which could distinguish both the production methods and geographic origins. This feature can be extremely interesting for establishing the correct origin of catches, ensuring that they do not come from protected areas and limiting fraudulent practices based on fish substitution.

In relation to step 3 "infiltration into the supply chain" and step 4 "packaging mislabelling", through forensic analysis, the technology is able to identify counterfeit and fraudulent products as well as their characteristics after a breach in the supply chain occurs. This will also highlight any mislabelling claiming different composition or origin of the fish, as well as the use of substances that modify the characteristics of the fish. If a field-testing tool were developed, then a screening of the characteristics of the fish would quickly be performed in the field and could also be used to prevent the infiltration of fraudulent fish into the supply chain. On the contrary, in the case in which the field-testing tool is not available, the analysis would respond to breaches and could also be used to identify their source.

Summary table for submission 2: possible application to limit risks highlighted by the scenario

Scenario	Applicability of the solution
Scenario 1: Infiltrating the fishing legitimate supply chain	
Step 1 – Money laundering and entering the fish market.	
Step 2 – Using illegal fishing methods.	The iso-elemental fingerprint techniques provide the unique elemental and isotopic composition of seafood, which can then be used to create a provenance predicting model which could distinguish both the production methods and geographic origins
Step 3 – Infiltrating the supply chain.	The technology will be able to analyse the marketed products and determine if they are fraudulent and whether they do not originate from the correct geographical location. However, it is relevant to highlight that this technology cannot prevent infiltration, rather it works as a mechanism to identify counterfeit products and their characteristics after the security breach occurs. Criminal activity cannot be prevented unless their continuous use over time creates a dissuasive effect on criminals, but they can be used to unequivocally identify the adulteration of a product or the fraudulent behaviour of criminals involved in food fraud.
Step 4 – Packaging mislabelling to fool consumers and buyers.	The same considerations listed above also apply to this risk step.
Step 5 – Other forbidden practices.	
Step 6 – Use of food additives such as water-binding agents.	

4.2.3 Integrating forensic and supply chain security technology

Technology submission 3

The submission proposes a technology solution that integrates several layers of security in order to obtain a higher degree of overall security. For instance, relevant security measures that should be applied include the management of quotas, the need for vessels to be equipped with automatic identification systems, the introduction of electronic logbooks, the issuance of catch certificates, the labelling of fish trays and the traceability of fish by processing and distribution actors. This submission also stresses the fact that, although each of these measures contributes to increasing control of the supply chain, one of the challenges that prevents competent authorities from achieving significant reductions in IUU fishing is that these solutions only have an effect within their limited scope. Without the ability to integrate different solutions, it would be possible, for instance, to obtain a catch certificate for a vessel that fraudulently declares the fishing area, thereby reducing the relevance of any downstream controls to effectively reduce IUU fishing.

To achieve an integral solution, this approach suggests the implementation of an identification and authentication system with supporting technologies enabling a secure track and trace system. The initial

identification of the raw materials is key for this approach, as it captures and records the fundamental characteristics of the products. This includes the true DNA of the species (genomics through polymerase chain reaction (PCR)), as well as the "environmental DNA", i.e. the conditions in which the product is grown. These data are then stored in a blockchain which creates strong and irrefutable references for continuous or ulterior use and checks. The first "DNA" capture is further enriched with a secure marking (active or passive) of the packaging and the immutable digital storage in the blockchain of the associated transaction and process data. Data analytics and artificial intelligence algorithms are also integrated and can provide additional means of predicting and checking the overall mass flow reconciliation balance along the supply chain, in view of checking if the mass flow of products from origin to destination triggers any alert in terms of quantities, weight or routes.

This process can be integrated into a Centralized Fishing Data Management System (FDMS) based on a Traceability as a Service platform, which includes an ecosystem of trust-enabling technologies and can easily integrate strategic technology from external providers. The FDMS solutions objective is to help governments prevent, mitigate and combat emerging and future risks posed by counterfeiting and criminal infiltration into the legal economy of the fishing supply chain. The FDMS collects, transforms and aggregates data from various fishing control systems as well as from Earth Observation and satellite communication systems, including:

- Vessel registration data from maritime authorities;
- Vessel tracking data based on classic Automatic Identification Systems (AIS) such as the vessel draught data, as an indication of the fish payload;
- Improved vessel route and position prediction using deep learning on S-AIS data;
- Vessel recognition and object tracking based on deep learning over high-resolution images from vertically integrated satellite solutions;
- Fishing electronic recording and reporting system (ERS), including integration with catch certificate databases and quota management databases;
- Data on economic operators licensed by the competent health and safety authority;
- Chain of Custody certificates issued by sustainable seafood organizations;
- Data from systems used to track and trace fish trays unloaded at the port;
- Automatic fishing species recognition using advanced image processing (e.g. fishmeal products);
- Molecular methods to support the identification of species, the place of capture and the origin (wild or farming).

The FDMS can also be integrated with Customs Management Systems where import and export declarations are filed, also extending controls to cross-border trade. Although it will be capable of integrating data covering the complete lifecycle of the fishing industry, the FDMS will also be capable of operating when only some of the data is available from external systems. By applying advanced data analytics, the FDMS will be capable of detecting data inconsistencies, and to identify anomalies and possible fraud patterns of IUU fishing, generating automatic alerts to competent authorities.

Submission received from SICPA

This submission presents the possibility of utilizing several layers of security using a variety of approaches and technologies which, when combined, can ensure a high degree of security of the fish supply chain, starting from the catches on the vessels.

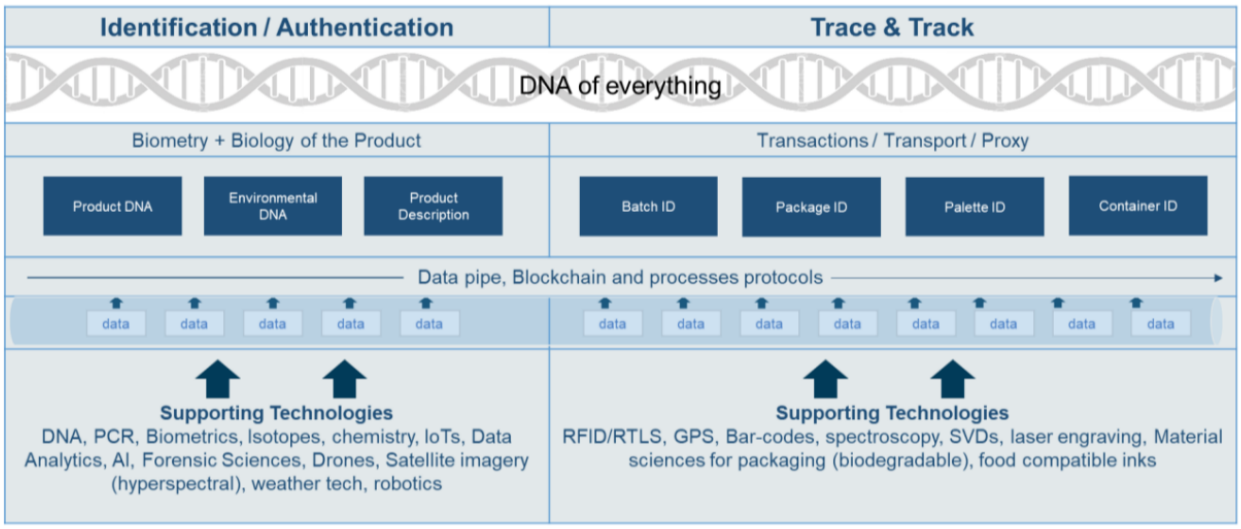


Figure: The numerical and physical "DNA" of an agrifood product.

Source: SICPA

The key approach is that all the layers of security respond to a specific security need, but they need to be integrated and be able to work together if the response to criminal activities needs to be as effective as possible. It is for this reason that forensic analysis revealing the DNA composition of each fish is used for the registration of catches at the vessel level and is then used to create the unique ID of the product, which will allow for the subsequent track and trace of the fish products along the supply chain. The ID, including information on the DNA properties, can be checked at subsequent intermediate checkpoints, as well as in case of need. However, in order to be checked, the DNA element will need the use of on-field testing devices capable of performing DNA analysis. Processes, permissions and checks, as well as corresponding data, are stored in a blockchain and are available to be verified at any point.

This premise is integrated into a wider management system which is probably at the heart of the submission, the FDMS which, as it can be read in the description, integrates several additional layers of securities and enables collection and sharing of information with law enforcement authorities, including on vessels' positioning thanks to satellite technology integration and on catches' analysis and recording performed at the vessel level. Such integration into a single platform of solutions for maritime monitoring offers coverage of open water areas that is probably not currently possible with the traditional land monitoring solutions, enabling improved detection of vessels and marine life monitoring. As space data is used for continuous and ulterior controls along the supply chain, data and processes are certified and timestamped in a blockchain to avoid falsification. Compressed spatial images with their embedded unforgeable signatures and localisations through quantum derived technologies will be used in the near future. In addition, the FDMS collects, transforms and aggregates data from various fishing control systems.

Data analytics and artificial intelligence algorithms provide additional means of predicting and checking the overall mass-flow balance of fish along the supply chain, reconciling estimated quantities to be delivered at the various checkpoints with the quantities actually received. This reconciliation mechanism can help uncovering illegitimate insertions into the supply chain or diversions of products from their intended course. In addition, by applying advanced data analytics, the FDMS will be capable of detecting data inconsistencies, identifying anomalies and possible fraud patterns of IUU fishing and generating automatic alerts to the competent authorities.

The technology solution proposed by the submission can be used to mitigate most of the steps of the criminal plan presented in the risk scenario. The combination of an identification and authentication system with supporting technologies enabling a secure track and trace and the development of a centralized Fishing Data Management System (FDMS) protected by blockchain can be used to protect different processes in the supply chain. The connection with information shared by authorities and Customs Management Systems provides a valuable cooperation tool to detect illicit activity. Consequently, this technology may play a role in limiting the following steps of the criminal plan:

- Using illegal fishing methods.
- Infiltrating the supply chain.
- Packaging mislabelling to fool consumers and buyers.
- Other forbidden practices.
- Use of food additives such as water-binding agents.

For what concerns step 2 "use of illegal fishing methods", the use of the different layers of security enables the protection of the multiple stages of the supply chain, with exception of mitigating the risk of money laundering since this process would take place in an area outside the scope of the solution. The identification, record, DNA capture, tracking and tracing of the catches starts at the vessel, whose position is constantly monitored and compared with the declared route thanks to satellite integration. This can avoid fishing in forbidden areas as well as the use of unauthorized fishing methods. Furthermore, the constant communication established by the FDMS with port and Customs authorities ensures the constant information of responsible authorities.

These security characteristics also have a direct application in relation to step 3 "infiltrating the supply chain" and step 4 "packaging mislabelling". The encrypted information containing the DNA profiles of the catches provides a clear description of the specific products, exponentially complicating the imitation of the authentication solution. The physical authentication mechanism is immediately connected to the second layer of protection by linking the product to the track and trace system. This way, the unique identifier is providing a secure mechanism to easily recognize the product, while at the same time the information is protected with blockchain technology during the monitoring through the traceability solution to combat the lack of control over the product quality once it is packed. It has to be noted that, in the case in which the DNA component of the ID has to be verified, a DNA analysis will be needed and could be performed through on-field testing and/or dedicated laboratory facilities. Space assets for geolocalization along the supply chain and for mass balance of trade flow reconciliation are also an integral part of the solution, both to ensure the quality and origin of the product and to monitor its movements. The blockchain technology also protects the data exchange that is made through the monitoring.

Step 5 of the criminal plan "use of other forbidden practices", can be limited by the integrated approach, in particular 1) the use of biometry to create the identity of the product and its subsequent monitoring along the supply chain, 2) the data analysis of flow mass balance of products, and 3) the use of space technology to add additional time-stamped controls on the origin and quality of products and of their ingredients as well as to support the mass balance calculations. The combination of these elements will make it difficult to insert products into the supply chain for which no record exists, that do not correspond to the established DNA profile, that have not been followed by the satellite-integrated features of the technology, and that do not respect the mass-balance reconciliation of products' flow. The addition, the Centralized Fishing Data Management System (FDMS) based on a Traceability as a Service platform for the unique authentication of the products, creates a comprehensive solution that can protect the product and its processing and distribution.

Finally, for what concerns step 6 "use of food additives", the incorporation of the DNA into the ID of the product, as well as all the previously described features performed by the FDMS, can limit this step of the criminal plan.

Summary table for submission 3: possible application to limit risks highlighted by the scenario

Scenario	Applicability of the solution
Scenario 1: Infiltrating the fishing legitimate supply chain	
Step 1 – Money laundering and entering the fish market.	
Step 2 – Using illegal fishing methods.	This submission adds layers of security if compared to more traditional approaches, such as: 1) use of biometry to create the identity of the product and its subsequent monitoring along the supply chain, 2) data analysis of flow mass balance of products, and 3) use of space technology to add additional time-stamped controls on the origin and quality of products and of their ingredients, as well as to support the mass balance calculations. In addition, the Centralized Fishing Data Management System FDMS collects, transforms and aggregates data from various fishing control systems as well as from Earth Observation and satellite communication systems, including specific information about vessels and Chain of Custody certificates issued by sustainable seafood organizations. Any attempt of using illegal fishing methods would be detected by using this solution.
Step 3 – Infiltrating the supply chain.	The integration of the various layers of security would limit this step, including: the DNA ID inclusion into the coding of the product, the verification of the catches at the vessel level and starting their coding and track and trace from that point, integration with satellites to verify the movement of products along the supply chain, and the mass balance reconciliation mechanism.
Step 4 – Packaging mislabelling to fool consumers and buyers.	For the same reasons as the previous step, the strong product ID and the way in which it is monitored throughout the supply chain will make it extremely difficult, if not impossible, to insert fraudulent products by simply imitating the original packaging. The mass balance calculations and the link with space technology provide additional layers of security.
Step 5 – Other forbidden practices.	The same considerations presented in step 2 also apply here.
Step 6 – Use of food additives such as water-binding agents.	The use of the biography and biometry of the product for creating its unique ID, along with space technology and mass balance reconciliation, will greatly reduce the risk of using food additives to deceptively increase the weight of products and carbon monoxide to enhance their visual quality.

4.3 Conclusions

The Irregular, Unreported and Unregulated (IUU) fishing risk scenarios presented some of the threats that can affect the integrity of the supply chain. Thanks to research conducted by UNICRI and to the submissions we received from technology experts, it has been possible to assess how technology solutions may contribute to increasing the security of the supply chain of these products, while limiting related criminal activities.

Existing technology solutions usually encompass one or several of these elements to protect the flow of products in the supply chain:

- **Authentication technology**: It is focused on providing more accurate tools for the authentication of the products, including the identification of relevant characteristics such as their origin and the use of substances. **Radio-frequency identification (RFID)** tags can be used to capture relevant information about the

product, **such as the fishing time, position, biological data like species name, sex, and body length and weight**. The code that is used to track the product along the supply chain can also contain unique information about each product by using processes such as polymerase chain reaction (PCR) to obtain data related to the **DNA** of the sample. In the case of fishing, it is relevant to authenticate the product from the vessel to the different processes after fish goes through processing facilities and is partitioned.

- **Track and trace systems**: The authentication solutions have frequently been designed to be integrated into traceability systems. Different technologies, such as **RFID and QR codes** can be used to capture information throughout the supply chain. Tags can be affixed when the fish comes on board the vessel to follow it and register information automatically at various devices positioned on the vessel, at the dock, and in the processing facility. Once the product is partitioned out into various products, it can receive a QR code (or, potentially in the future, a near field communication (NFC) device) that will track the product past the retailer. In addition, integrated satellite imaging and tracking is essential to understand the **movement and fishing practices employed by vessels**. Some technologies have been created to obtain accurate information even when vessels are not actively transmitting a signal. Some changes are also being made in electronic monitoring to detect irregularities on board of the vessels, making it more effective through the use of **Wi-Fi and satellite data transmission** and the implementation of **artificial intelligence** (AI) analysis.

- **Blockchain technology**: Can connect the different parties in the supply chain that have not established trusted relationships with each other, by ensuring transparency. Blockchain stores every transaction or exchange of data that occurs in the network, reducing the need for intermediaries by providing a means by which all the actors in the network may share access to the same information, including what is added to the data, by whom, and the date and time of the submission.[15]

- **Forensics**: Authentication and provenance of fish can also be achieved through forensic analysis. In this area, some of the options to verify the **authenticity, provenance and traceability** in the seafood and fish industries include the use of polymerase chain reaction–restriction fragment length polymorphisms (PCR-RFLPs) to create a **DNA barcoding** for identification of fish species and the application of vibrational spectroscopy (near- and mid-infrared, Raman) combined with chemometric methods to identify, detect, classify the products. These procedures provide highly useful tools for law enforcement since they can give accurate information about the specific product, allowing the simple detection of mislabelled or fraudulent fish products. In addition, **nuclear techniques** including stable isotope analysis, ITRAX X-ray fluorescence, neutron activation analysis, ion beam analysis and synchrotron technologies provide great precision in determining geographical locations of food. **Biochemical tracking** can be obtained to identify the exact origin of the product, providing a similar to or supplementing option to genetic tools.

- **Artificial intelligence**: Artificial intelligence can be used in analytics tools to improve the **insights obtained from data gathering** by applying algorithms that can improve the quality and speed of information related to fishing activities. An AI-powered platform can track data points from Automatic Information System (AIS) including vessel activity, vessel size and engine power, the type of fishing being carried out and the type of gear used. AI can train algorithms to **detect fishing-related patterns** to detect how close ships get to transhipment vessels, and whether they turn off their AIS when they do, and map IUU fishing hotspots can be detected. This technology can be adopted to identify other issues, such as slave labour, through the use of **algorithms that flag suspicious behaviours** like the amount of times nets were set in a day or the number of days the vessels have spent without landing.

The submissions analysed in the report use different types of technology that are applied following various approaches. Technology is frequently combined to provide multiple levels of security and to achieve a combination of objectives. The submissions might use similar approaches to mitigate risks, however, they offer unique features that focus on the use of specific technology tools. In the case of IUU fishing, the submissions offered the following distinctive approaches:

- **Use of a multilayer security approach that combines food classification at the vessel level, track and trace, and authentication of the product**. Submission 1 uses a system that starts with fish identification and classification from the vessel by providing fishers with an app to directly register the catch, enabling

15 Accenture. (2019, January 15). Tracing the Supply Chain. Retrieved August 23, 2020, from https://www.accenture.com/_acnmedia/pdf-93/accenture-tracing-supply-chain-blockchain-study-pov.p

the tracking of the product. The solution is based on the printing of labels that are attached to the products, are tamper evident and that can be scanned by customers to verify authenticity. The app designed for customers allows them to obtain information about the product they acquired and to corroborate its authenticity. This provides layers of security centred on the packaging of the fish, making it package dependent.

- **Use of a multilayered security approach that integrates different technologies, including a unique identification that is linked to a digital identity, traceability system and blockchain technology to protect the exchange of information**. This approach is proposed by submission 3, which uses an identification method by obtaining the DNA of the species, as well as the "environmental DNA", and linking that information to a Centralized Fishing Data Management System (FDMS) based on a Traceability as a Service platform to monitor along the supply chain. The use of the DNA for the identification of the fish renders this approach non-dependent on packaging authentication alone. Data analytics are then used to detect data inconsistencies, and to identify anomalies and possible fraud patterns of IUU fishing, generating automatic alerts to the competent authorities. In addition, a mass balance equation is used to protect the movement of products through the analysis of volumetric balance between departure and arrival points, which can be protected by fingerprints or in-product tracers and in parallel. The data from departure to arrival point could be authenticated, recorded and secured in a blockchain.

- **Forensic techniques** represent a different approach to combat threats. The iso-elemental fingerprint techniques provide the unique elemental and isotopic composition of seafood, which can then be used to create a provenance predicting model which could distinguish both the production methods and geographic origins. This technology cannot prevent infiltration, rather it works as a mechanism to identify counterfeit products and their characteristics after the security breach occurs. If a portable field-testing tool will be developed, then the analysis of the characteristics of the fish will be quickly performed in the field and can also be used to prevent the infiltration of fraudulent fish into the supply chain. Submission 2 uses this approach.

With specific reference to the risks that were highlighted by the risk scenario, the following considerations can be made:

- The risk scenario analysed how threats that involve multiple layers of actors and interactions can be found during diverse processes in the supply chain. **Criminal organizations are able to infiltrate the legitimate supply chain at various stages and by using complex techniques** that include the initial infiltration into the fish market through money laundering, the use of illegal fishing methods and techniques to operate processing facilities and aquaculture plants which are involved in mixing illegal catches into the licit fish supply chain, packaging mislabelling to fool consumers and buyers, including false declaration over the origin of catches, employment of food additives such as water-binding agents to deceptively increase the weight of products and carbon monoxide to enhance their visual quality, and falsification of elements in paper-based traceability programmes.

- Existing technology options have been developed to combat these threats with **multilayer security approaches that support the work of both stakeholders in the supply chain and national and international authorities**. The technology solutions are focused on providing **more accurate tools** for the authentication of the products, including the identification of relevant characteristics such as provenance, composition of the product and the use of substances; as well as for monitoring the activity of vessels and reporting of information.

- Technology solutions can be adopted to mitigate important risks related to the lack of **full monitoring and data exchange** in the supply chain, which might enable the spread of other forbidden practices, the absence of **digitized processes** and a need to update or replace paper-based traceability programmes which are prone to falsification, and the unavailability of **comprehensive data** related to genetic traceability markers.

- Some criminal activities highlighted by the scenarios cannot be limited by supply chain security technology. This has to be expected since the main purpose for which these technologies were developed is to protect the integrity of the supply chain and not to stop different kinds of criminal operations. **The mitigation of these risks will necessarily require actions and strategies implemented by law enforcement**

agencies to better understand how crime operates and how to monitor organized crime strategies to prevent these criminal activities. It is for these reasons that some steps of the criminal plan in the risk scenario were difficult to limit by supply chain technology solutions. This is the case, for instance, of step 1 related to money laundering and entering the fish market and step 6 regarding the use of food additives such as water-binding agents.

- Following on from the previous point, an integrated approach between different technology typologies and options is needed to **support at the same time investigators and law enforcement agencies** on the one side, as well as **supply chain operators and consumers** on the other.

- **Supply chain technology producers are constantly looking for ways to innovate the modality through which products' integrity and security can be enhanced**. The analysis of the submissions we received testifies to this. Concrete examples include the attempt to go beyond the authentication of the simple packaging to try and implement modalities through which the fish itself and its composition can be authenticated and progressively checked along the supply chain. Authentication is achieved through the end-to-end cooperation between fishers that secure the products from the vessels to the intervention of other stakeholders in further processes. Along the same line, the creation of a series of redundant checks which include the monitoring and reconciliation of the mass balance of products moving between intermediary points represents an interesting attempt to create additional layers of security.

- The challenges related to package dependency are being addressed by incorporating the unique characteristics of the product in the authentication mechanisms. This includes the incorporation of the true DNA of the species (genomics through polymerase chain reaction PCR), as well as the "environmental DNA" (the conditions in which the product is grown).

- The technology options **complement strict regulations and labelling protocols**, serving as tools to improve the management of information and coordination between the different stakeholders.

- In addition to the traceability technology options, improvements have been made to facilitate their implementation and efficiency. An example of this was the Standards and Guidelines for Interoperable Seafood Traceability Systems, v1.0 (GDST 1.0), an initiative to provide basic technical standards to **enable interoperability** across the different seafood traceability platforms presented by the Global Dialogue on Seafood Traceability (GDST) in 2020.

- The incorporation of **blockchain technology** in the digitization of processes and the traceability systems protect the exchange of data between authorized stakeholders and guarantee immutability, transparency and accountability.

- New solutions also attempt to provide customers with mechanisms to verify the origin and quality of the products, improving transparency from the source to the final stage. **Consumer education** is essential in order to implement authentication solutions. The authentication codes used by different providers are frequently easy to scan through the use of smartphone cameras, however, the consumer needs to be aware of the existence of the verification mechanism and of the steps that need to be taken to corroborate the authenticity of the products.

- **Forensic technology** is focused on identifying and protecting seafood provenance. Unique information related to the specific product, such as the **geographic location, production method and composition of the fish**, can be obtained using iso-elemental fingerprint techniques, including stable isotope analysis and X-ray fluorescence (XRF) through Itrax scanner, to obtain the unique elemental and isotopic composition of seafood. The iso-elemental fingerprint data can be processed in **artificial intelligence tools**, including machine learning models where this information is analysed to find patterns in order to predict the source of origin and quality.

- The development of **portable devices** (using XRF technology) for forensic examination can minimize the existing limitations of laboratory-based analyses. The portable method would provide a high enough accuracy for quickly screening seafood products on a regular basis. The **regular screening** of various points along the seafood supply chain using handheld devices would help ensure that any fraudulent catch is identified before it has a chance to be sold to consumers. This would provide consumers with the confidence that the product they are purchasing is legitimate, which in turn contributes to the market chain traceability.

CHAPTER 5
Trafficking in counterfeit and substandard pesticides

The infiltration of organized crime into the legal economy targets numerous product markets. The agrochemical sector is no exception, due to the booming market demand for these products.

Prior UNICRI research, conducted in consultation with law enforcement agencies, rights holders from the agrochemicals industry and international organizations, has identified that illicit pesticides trafficking is carried out by organized criminal networks, which exploit international shipping routes to disseminate five product categories, i.e. expired, counterfeit, mislabelled and unauthorized pesticides imports, as well as refilled product containers.[1]

Obsolete pesticides are chemicals that have been banned due to their harmful health or environmental effects, degradation, or subsequent re-formulation of product standard specifications. They may originate from excess in supplies of stored goods and changes in the regulations governing international trade in agrochemicals. Most national laws require producers to manage stocks of obsolete pesticides, although efforts to identify, collect and properly dispose of them have not resulted in total elimination. In developing countries, technical, institutional and financial constraints may hinder compliance with safe management and disposal schemes for obsolete pesticides, thus favouring the infiltration of organized crime into the supply chain.

Counterfeit pesticides are manufactured products whose origin or contents are deliberately misrepresented to exploit the reputation of well-known agrochemical companies. Criminals may adopt a similar modus operandi; Mislabelling – consisting in rebranding generic versions of flagship products with the distinctive labels of legitimate right holders.

On the other hand, unauthorized pesticide imports consist in the trade of registered or non-registered agrochemicals, conducted without a license from the competent plant protection authority, or through the falsification of shipping documents. However, in reality these products do not comply with quality specifications and they may ultimately draw law-abiding companies out of the market.

Finally, the use of re-filled or non-compliant containers is a criminal practice of illicit pesticide suppliers and distributors, as well as uninformed traders seeking to capitalize on bulk purchases. While this is a relatively small component of the illicit trade, which mainly affects least developed countries, the potential harm emanating from the ingestion of pesticide residues is a serious public health threat.

The potential health and safety consequences for unsuspecting consumers has prompted the international community to increase vigilance against pesticides fraud. In 2015, Europol launched the first Operation Silver Axe, resulting in the seizure of 600 tonnes of counterfeit and substandard agrochemicals at major European seaports, over a three-year period. During Operation Silver Axe III, for instance, the Hungarian and Slovak Customs intercepted a suspicious consignment of 20,400 kg of pesticides (thiamethoxam 350 g/l) on its way from China to Hungary via Ukraine. The shipment containing unmarked packaging (no indication of producer, country of origin, trade name) was successfully seized at Szolnok by Hungarian customs officers (National Tax and Customs Administration of Hungary – NTCA). The value of the shipment exceeded 240,000 USD. The retail value of the genuine pesticide would have exceeded 1 million USD. The latest edition of the Silver Axe operation, which took place between 13 January and 25 April 2020 and involved 32 countries, confirmed the extent of the problem and the involvement of criminal organizations in this form of illicit trade. According to Europol, the operation led to the seizure of 1,346 tonnes of illegal pesticides. This quantity could be enough to spray 207,000 km2, or more than all the farmland in Germany which accounts for nearly half the country, almost 75% of farmland in France or more than 150% of the farmland of Romania.[2]

1 See UNICRI, Illicit Pesticides, Organized Crime and Supply Chain Integrity, 2016, available at: http://www.unicri.it/in_focus/files/The_problem_of_illicit_pesticides_low_res1.pdf

2 https://www.europol.europa.eu/newsroom/news/record-number-of-1-346-tonnes-of-illegal-pesticides-taken-market-in-2020-global-operation-silver-axe

From a broader perspective, the prevalence of counterfeit and substandard agrochemical compounds creates inherent pesticide risks through the introduction of mislabelled, unregulated, and unidentified substances, which affect workers, consumers, crops and broader ecosystems. Ultimately, exposure to illicit pesticides may result in the loss of harvest and a serious degradation of soil, which will become unproductive for several years.

5.1 Risk scenario

One risk scenario has been elaborated in the area of illicit trafficking of counterfeit and substandard pesticides.

Risk Scenario: Infiltration into the Agrochemicals' Supply Chain

The agricultural sector of a country is well-developed but requires a lot of pesticide use for effective crop production. The country itself is experiencing a wave of foreign investments as a result of its recent opening up to international trade. The agrochemical industry provides a key contribution to the national agricultural production. However, the legal and regulatory framework has not kept pace with the most advanced international standards on chemicals management and the production of several highly hazardous pesticides remains legal in the country.

Always on the lookout for high profits at low risk, the ringleader of a domestic organized crime group has strong interests in the distribution of counterfeit goods, which are a low priority for national authorities and law enforcement agencies. In a bid to differentiate the group's investments, the leader of the criminal group wants to start operating in the chemical sector, especially in the pesticides area, and implements the following criminal business model:

Step 1. Acquiring control over legitimate companies: Thanks to the reinvestment of its illicit profits into the legal economy, the criminal group has taken over a chemical manufacturing plant in the country's coastal area, where major industrial development projects are taking off. The leader of the criminal group entrusts the business to frontmen with no criminal record and exploits the company's expertise and customer base to meet the growing domestic and foreign demand for plant protection products.

Step 2. Production of illicit pesticides: The criminal group takes advantage of the country's outdated agrochemicals management regulatory framework (or of the fact that the law is not enforced) to produce sub-standard products, using cheaper active ingredients and other chemicals, not in line with the registered dossiers. These products are intended for sale in least developed countries. The criminal group also copies the container design and trademarks of well-known international companies, replacing the authentic products with low-cost and hazardous ones.

Step 3. Infiltrating the market: Unencumbered by high research costs, associated to the development of innovative and safer active ingredients, and disregarding the potential risks related to the manufacturing and distribution of agrochemicals, the criminal group is able to offer its products at highly competitive prices, which draw the attention of hundreds of unsuspecting farmers. Some of its counterfeit pesticides are exported as ready-packed and mislabelled products. Other products are misrepresented in invoices as solvents or emulsifiers, and shipped as active ingredients or in bulk consignment, rather than as packaged goods, significantly reducing the risk of raising the attention of law enforcement authorities.

In the space of a year, the criminal group has been able to place 1000 tonnes of counterfeit and substandard pesticides on the market, reaping over 5 million euros in illicit profits. The criminal group has thus infringed the intellectual property rights of major legitimate agrochemicals producers, while disrupting fair competition and reducing fiscal revenues.

In the same period, the sale of banned substandard pesticides has had the most destructive consequences on the targeted least developed countries, where leakages and the inadequate storage and disposal of toxic ingredients have contaminated their cattle, waterways and the wider food chain. Tonnes of crops have wasted away on the sprayed land and soil fertility will not be restored for over three years.

5.2 Technology solutions to address the risk scenario

The increased complexity of supply chains has also impacted the manufacture and distribution of pesticides, hindering regulatory efforts and the detection of counterfeit products. Trafficking in counterfeit and substandard pesticides can negatively affect different areas, especially enhancing issues related to environmental degradation and human health risks. Pesticides are substances that are used to kill, repel, or control certain forms of plant or animal life that are considered to be pests and that are frequently potentially toxic to other organisms, including humans. Pesticides can contaminate due to spill-over at different stages of production, transportation and storage, provoking further surface and groundwater contamination from leaching, runoff or spray drift, soil contamination and lower soil fertility due to the decline of beneficial soil microorganisms, air contamination from spray drift, and negative effects on non-target organisms.[3]

In addition, exposure to pesticides can be harmful for human health, mainly for farmers and consumers. Particular components of agrochemicals (fertilizers and pesticides) can also be used to manufacture explosive devices.[4] Furthermore, the impact on the economy has also been documented. The European Union Intellectual Property Office (EUIPO) estimated in 2017 that when both direct and indirect effects are considered, counterfeiting of pesticides causes approximately 2.8 billion euros of lost sales to the European Union economy, which leads to annual employment losses of about 11,700 jobs and a loss of 238 million euros in government revenue from taxes and social security contributions.[5]

The trafficking of counterfeit pesticides is frequently carried out through different methods, including mislabelling and repacking, avoiding high risk custom borders and exploiting international shipping routes to disseminate five product categories (expired, counterfeit, mislabelled, unauthorized pesticides imports, and product containers), forging documents to distribute the products, and by using re-filled or non-compliant containers. Technology solutions play a relevant role in the mitigation of these threats, alongside effective formal and informal social control mechanisms in regulatory, production and supply chain networks such as the awareness and engagement of authorities and stakeholders, international harmonization and regulatory oversight, supply chain protection and defence activities, enhanced investigation and interdiction capacities, control of financial flows and incentives and end-user and consumer awareness.[6]

One of the solutions used to secure pesticides along the supply chain is the adoption of authentication mechanisms by stakeholders, which consist of overt, covert and forensic security features. Additional techniques, such as tamper-evident packaging (TEP), can be added to increase the protection of the authentication method. TEP is triggered by any attempt of removal or manipulation and provides customers and stakeholders with a tool to identify if a product has been tampered with and is not safe to use or consume.

Security hologram seals and labels, tamper-evident security film, low-cost transponder tags, and light sensitive ink designs have been proposed as authentication mechanisms for pesticides.7 Other authentication solutions use a combination of tools to verify authenticity, for example, employing unique holographic fingerprint tags, that are instantly verifiable by using a smartphone. They enable automatic recognition, geo-location, and immediate reporting of any tampering.[8]

3 Frezal, C., Garsous, G. (2020, May 15). OECD Joint Working Party on Trade and Environment, New digital technologies to tackle trade in illegal pesticides. Retrieved from http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=COM/TAD/ENV/JWPTE(2020)8/FINAL&docLanguage=En

4 UNICRI (2016). Illicit Pesticides, Organized Crime and Supply Chain Integrity. Retrieved from http://www.unicri.it/sites/default/files/2019-11/Illicit%20pesticides%2C%20organized%20crime%20and%20supply%20chain%20integrity.pdf

5 Wajsman, N., C. Arias Burgos and C. Davies (2017,February), The Economic Cost of IPR Infringement in the Pesticides Sector, European Union Intellectual Property Office (EUIPO) ,https://euipo.europa.eu/ohimportal/en/web/observatory/ipr-infringement-pesticides-sector

6 UNICRI (2016). Illicit Pesticides, Organized Crime and Supply Chain Integrity. Retrieved from http://www.unicri.it/sites/default/files/2019-11/Illicit%20pesticides%2C%20organized%20crime%20and%20supply%20chain%20integrity.pdf

7 Jeena, C. S. (2017, December 17). Identify fake pesticides with authenticated solutions. Retrieved from https://krishijagran.com/featured/identify-fake-pesticides-with-authenticated-solutions/

8 Authentic Vision. (2019, August 14). Authentication for Agro-Chemicals. Retrieved from https://www.authenticvision.com/getting-at-the-root-cause-authentication-for-agro-chemicals/

Additional features have been combined with authentication solutions for pesticides, including Information and Communication Technology (ICT) models. In Greece, a database platform was developed aiming to highlight the legitimacy of pesticide registration, the hazards of pesticides, the dangers of pesticides to humans' health and finally the dangers of pesticides on the environment and ecosystem. It facilitates the communication with the regulatory authority.[9]

Other options include the implementation of mobile-based solutions that assist with the authentication of the agro-submissions products. In Tanzania, the use of an Agro-submissions Products Verification System (APVS) has been analysed to authenticate the genuineness of agricultural submissions through the mobile phones of agro-stakeholders, by scratching a secret code which is affixed with the agro-submission package and then sending the code to a verification server (VS) via SMS.[10] Similar solutions have been used in Kenya and Uganda. Along similar lines, a mobile application that scans text and image has been proposed to obtain specific information such as batch number, product registration number, name of the product, manufacturer and registrant of the product, and the production and expiry dates of the particular product. At the same time, this captures the longitude and latitude of the requester in the background, creating a map with red markers to identify threat areas.[11]

Authentication mechanisms like labels, codes and RFID are frequently integrated into traceability systems.

Approaches for corroborating the authenticity of a product include the use of specific techniques for forensic investigations. The Fourier Transform InfraRed (FTIR) spectroscopy is a method used to examine samples, both to detect the presence of target compounds and to measure their quantities (quantification). It can serve as a relevant analytical instrument in a forensic investigation. In the case of pesticides, a portable FTIR spectrometer can be used to rapidly analyse pesticides before distribution, before mixing, and/or before application to crops.[12] Spectra can be searched against a commercially available pesticides library, and the identity of the sample pesticide is determined in less than one minute and with a minimum sample preparation. A portable device enables the analysis of counterfeit pesticides in different stages of the supply chain, where they are manufactured, shipped, received, stored and sold.[13] Other techniques include the use of Optical Photothermal Infrared Spectroscopy (O-PTIR) to analyse the samples of the products.

This part of the report will now present possible solutions to the challenges posed by the risk scenario described in the previous section. It describes the main aspects of the technology submissions, their relevance to the risk scenario and possible advantages and limitations. Advantages and limitations usually refer to the technology categories in general. However, in some cases, reference will be made to some of the specific submissions we received, and this will be done solely in view of providing a specific example of technology application.

By analysing the above-mentioned submissions, it is clear that there are different technological approaches that can be used, including supply chain security technology enriched with analytical tools to better identify potential breaches in given markets, forensic analysis with on-field capabilities, and also approaches mixing the two elements. Artificial intelligence tools to improve data analysis, as well as blockchain technology to render sets of data inserted in a database immutable, are also used. In some cases, the integration with space technology is also proposed in view of certifying the place of origin of agrochemicals and then monitoring their movement along the supply chain. The starting point of the track and trace is also a very interesting element to consider, and some options try to implement authentication and track and trace features which include the chemical properties of the product into the unique ID that will be used for authentication and track and trace purposes.

9 Vassiliadou, S., Mpoutakidis, D., &; Karikas, M. (2011, September). Application of Relational Database in Listing Pesticides used in Greece according to their Hazards in Human Health and the Environment. Retrieved from http://ceur-ws.org/Vol-1152/paper41.pdf

10 Shao, D., &; Edward, S. (2014). Combating Fake Agro-Submissions Products in Tanzania using Mobile Phones. International Journal of Computer Applications, 97(17), 21-25. doi:10.5120/17099-7681

11 Ngirwa, C. C., &; Ally, M. (2018). An ICT Based Solution for Pesticides Authenticity Verification: A Case of Tanzania. Journal of Information Systems Engineering & Management, 3(4). doi:https://doi.org/10.20897/jisem/3938

12 Richard, S., &; Rein, A. (2013, June 11). Pesticide Authentication by Portable FTIR Spectroscopy. Retrieved from https://www.agilent.com/cs/library/applications/5991-2531EN.pdf

13 Richard, S., & Rein, A. (2013, June 11). Pesticide Authentication by Portable FTIR Spectroscopy. Retrieved from https://www.agilent.com/cs/library/applications/5991-2531EN.pdf

In general, the submissions showed that technology solutions have the capacity to provide improvements in the following areas:

- Lack of control over the product once it is packed through mislabelling, copy of design and trademarks, and substitution of contents.
- Lack of intermediate technology checkpoints to avoid the insertion of illicit products within the supply chain.
- Lack of full monitoring and data exchange in the supply chain, including the possibility of the final users verifying the authenticity of agrochemicals at the time of purchase.

Those technologies which also incorporate the chemical composition of the product as part of the authentication and supply chain solution, usually offer mechanisms to calculate deviations from the intended mass-flow of products between points of departure and of destination. These calculations may in fact trigger alerts for diversion, counterfeiting or other fraudulent and illicit activities. In these cases, the technologies may also provide improvements to limit risks in the following areas:

- Exploitation of international shipping routes to disseminate expired, counterfeit, mislabelled and unauthorized pesticide imports, as well as refilled product containers.
- Importation of unauthorized pesticides that do not comply with quality specifications through the falsification of shipping documents or trade without a license.
- Use of re-filled or non-compliant containers that might pose a serious public health threat.

Interesting features of supply chain-based solutions proposed in this field include:

- *Clear identification*: Authentication solutions can be produced allowing identification by customers. The encoded characteristics of the product can be decoded through a scanner, providing stakeholders with a mechanism to differentiate original from counterfeit goods.
- *Monitoring*: Track and trace technology is used to monitor the product through the different processes in the supply chain, limiting diversion and infiltration possibilities. Traceability can be integrated with authentication solutions to provide an additional layer of security.
- *Non-reproducible*: Codes can hardly be reproduced without knowing the cryptographic key, this is essential to: authenticate the original product, monitor its movement along the supply chain and prevent infiltration of non-authenticated and non-original products.
- *Unique*: Codes, labels and tags create an identity for every object or product. The solutions can be customized to provide a unique authentication mechanism, moreover, they also contain a unique sequence of codes and information that provide specific information about the product.
- *Large data storage*: Available codes and tags can encode large amounts of information.
- *Adaptability*: Authentication and track and trace can be adapted to different products and industries. The technology option also offers the possibility of adapting it to existing systems. The use of this solution is not limited to this industry, since it can be used in a wide range of products.

Furthermore, in the case in which blockchain technology is used for storing ID and track and trace data of products, the following interesting features can be identified:

- *Immutability*: The information about the product and its movement in the supply chain cannot be modified. This is achieved through the ability of a blockchain ledger to remain unchanged, unaltered and indelible. Introducing falsified products in the authorized distribution chain will not be possible because each trans-

action is locked in the blockchain through cryptographic key authorisation. The supplier must have an authorised key and be connected cryptographically to the receiver.

- *Search options and flagging of issues*: Blockchain technology in the system makes it possible to set-up immediate alerts in case of any issue or unprogrammed change. This warns the stakeholders in the supply chain and in addition, the technology allows them to search for a product at any point on the chain to verify its status.

- *Auditability and accountability*: Accountability is verified as a part of timestamps established by the blockchain system. This system allows every stakeholder to confirm whether the service operates in the intended way. If the product fails the verification process, then the stakeholders have proof of malicious behaviour which could be used to hold the responsible stakeholder accountable. In addition, a transaction can only be made when both the sender and receiver are authorised through the private and public key system.

- *Transparency*: Blockchain technology allows stakeholders to monitor the supply chain with openness, communication, and accountability. The stakeholders included in the chain can access the information at any point to corroborate the status of the products and the processes. Recorded product and time/location data is stored for easy data access in the database but cannot be adulterated in any way because it is locked in the blockchain and a change would immediately be visible.

In addition, those technologies which also offer satellite-integration, present the following interesting features:

- *Satellite integration*: In addition to providing multilayer security to the supply chain as a space technology, satellites have other advantages such as large-scale coverage, various spectrometers that can be used for identification, time series, connection with ground data, working on land and sea, communication and collection of large data sets.

- *Embedded security*: As space data is used for continuous and ulterior controls along the supply chain, data and processes are certified and timestamped in a blockchain to avoid falsification. Compressed spatial images with their embedded unforgeable signatures and localisations through quantum-derived technologies will be used in the near future.

- *Volume measurement*: There is a measurable set of volumes of substances that enter a complex supply chain or a subset of it. The change in the volume measurement would trigger an alert.

Some of these technologies are still package-dependent, the traceability begins at the first packaging point and is linked to the package, not to the product. However, as it will be better explained in the following sections, there are attempts to overcome this limitation in some of the submissions we received. Furthermore, multilayer security and integration of different systems and technologies may result in a certain complexity. Achieving interoperability between the different systems can be a challenge. However, once the initial interoperability is achieved, it becomes an advantage since it allows the integration of the different systems. Finally, the flow of data with all these features requires personnel who are able to interpret the information that is received. Most options include tools that facilitate the interpretation of results through graphs and data simplification, yet in order to have a full analysis of all the information received, it is necessary to have specialized individuals.

For what concerns forensic-based technologies, these solutions come into play once the breach of the supply chain already occurred or when there is a suspicion of illicit activity. In these cases, they have an important role to play to confirm whether a product is genuine or not. Attempts are also underway to create portable on-field analysers that could also complement some of the supply chain-based solutions in this field, since they could allow for a rapid check of the chemical properties of the products contained in each ID.

Interesting features of these technologies include:

- *Fast*: Usually the measurement time is relatively low, down to a few minutes.

- *Accuracy*: The methodology is highly sensitive, accurate and has been validated by a wide scientific literature. The use of the technology in other areas provides corroboration of the usefulness and accuracy of the method.

- *Routine applications*: It is possible to make routine applications with the semi-portable devices if needed.
- *Well-established techniques*: the techniques are widely used and there is evidence supporting the results of the processes. Moreover, the infrastructure to use the techniques is available in most countries.
- *Multi-elemental capability*: The solution allows multi-molecular analysis.
- *Portability*: Some methods can be used in portable or semi-portable devices (FTIR), facilitating the analysis of the goods.
- *Simple detection*: Information on the elements present in the sample has a limit of detection as low as a few parts per million. Sample preparation protocols are relatively simple for most cases, thus demanding little sample handling.
- *Encompassing*: Different kinds of materials like liquids and solids can be analysed by a single technique, thus enhancing the credibility of the analysis. There is an option to identify pure compounds and mixtures (with the use of multivariate statistical techniques).

On the other hand, these technologies usually need a full laboratory to be properly implemented and space could be an issue in this case, since the laboratory would have to be built, if it does not already exist. The development of portable devices could overcome this problem in the future. Other possible limitations of these technologies include:

- *Highly qualified staff*: Highly qualified engineers are needed, and they need to have the technical knowledge to operate the accelerator and other equipment in the laboratory.
- *Identical chemical markers*: Some products have identical chemical markers, even if their origin is different. This could complicate the identification of the authentic product from a cheaper version if they both share chemical markers.
- *Time-consuming in some cases*: Sample preparation can be complex and time-consuming.
- *Maintenance*: The results of some methods depend on the state of the instruments and their maintenance.

5.2.1 Using nuclear analytical techniques

Technology submission 1

This submission is based on the analysis of the chemical composition of the product and proposes several solutions that enable screening for abnormalities.

These solutions use several techniques, such as:

1) The Fourier Transform InfraRed (FTIR) spectroscopy measures the fundamental vibrations of co-valently bound atoms in molecules and identifies the unique spectrum of a compound. It may be treated as a molecular fingerprint. An Attenuated Total Reflection (ATR) accessory is a tool used when the sample is neither transparent nor reflective for IR. When there is intimate contact between the sample and ATR crystal and the conditions for refractive indices and incident angle are met, the sample absorbs internally reflected electromagnetic radiation through the interaction with the evanescent wave.

2) The Optical-Photothermal InfraRed (O-PTIR) spectroscopy works as a non-contact, far-field reflection mode and delivers high quality spatially resolved FTIR transmission-like spectra below the diffraction limit of infrared wavelengths. The IR diffraction limit is overcome by combining a pulsed tuneable laser with a proprietary optical technique measuring photothermal response of the sample in a fast, easy to use manner.

Both technologies may be applied to verify the content of the pesticides and to detect dilution or inadequate additives. FTIR spectra may be shared among the stakeholders of the supply chain from the manufacturer, through distributors to final users in order to check the authenticity of agrochemicals. By using semi-portable devices, it is possible to set up intermediate checkpoints to avoid the insertion of illicit products within the supply chain.

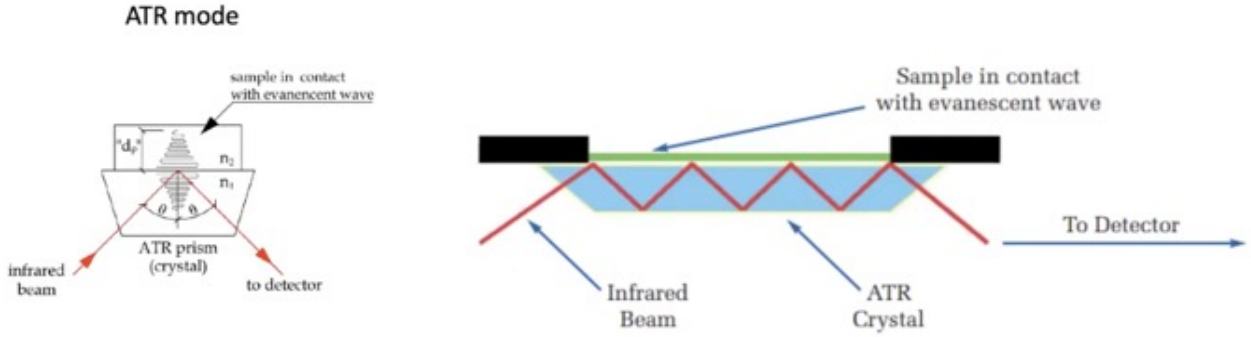
Submission received from Singapore Synchrotron Light Source

The submission describes different technology options to offer diverse solutions to the issues identified, specifically, the adoption of Fourier Transform InfraRed (FTIR) spectroscopy and Optical-Photothermal InfraRed (O-PTIR) spectroscopy. Each technology tool has its own advantages and disadvantages, demonstrating the versatility of the options. Technology solutions falling within this technological approach target some of the issues identified in the risk scenario related to trafficking in counterfeit and substandard pesticides.

This submission allows us to describe the contribution that forensic based technologies, and in particular nuclear analytical techniques, may make to the identification of counterfeit, fraudulent or illegal agrochemicals, which were inserted into the supply chain. As mentioned in the introduction, these technologies usually come into play once the supply chain has been infiltrated or when there is a suspicion of infiltration. They are not used to prevent the breach or infiltration. However, as it can be seen from this submission, research and development activities are also aimed at developing portable devices capable of on-field testing. A widespread use of these devices could support checks along the supply chain at intermediate distribution phases, making it possible to identify illegal products before they reach the final customer.

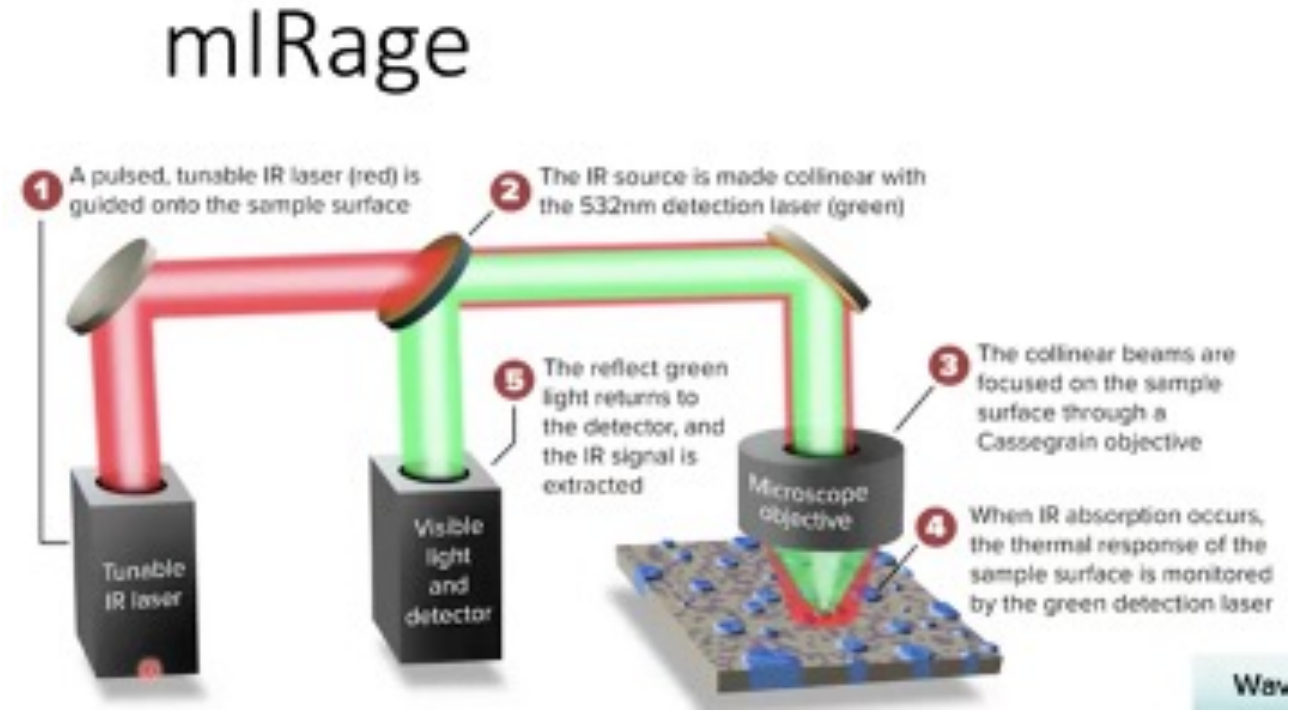
The portable devices could bridge a gap between the information included in the unique IDs and the possibility of actually conducting rapid on field testing to verify them. We propose the incorporation of the chemical composition of the product into its unique ID for authentication purposes by linking to some of the submissions that we will discuss in the next paragraphs.

In this specific submission, the validation is performed using Fourier Transform InfraRed (FTIR) and Optical-Photothermal InfraRed (O-PTIR) spectroscopy. Collected FTIR and O-PTIR spectra are also searchable and interpretable in both commercial and institutional IR databases without the need for mathematical modelling. The particles analysed by the O-PTIR method can be even smaller than 1 µm (in diameter) and the resulting spectra are of high quality. This represents an advantage in relation to the use of classical FTIR spectroscopy. The sample could be further analysed by other analytical methods for confirmation purposes.



Source: Singapore Synchrotron Light Source

O-PTIR spectroscopy also eliminates one of the longstanding limitations for IR microscopy, namely the inability to work on thick samples.



Source: Singapore Synchrotron Light Source

From the above, it derives that these technologies can support responding to the lack of control over the product once it is packed through mislabelling, copy of design and trademarks, and substitution of contents. They can identify if pesticides have been produced using sub-standard products, cheaper active ingredients and other chemicals, not in line with the registered dossiers. Along the same lines, they can also identify cases in which pesticides contain diluted, inert, banned or improperly identified agents. In the case in which a widespread use of on-field testing devices will be registered, these technologies can also overcome the lack of intermediate technology checkpoints validating the composition of the product, in view of avoiding the insertion of illicit products within the supply chain.

However, the technology in general is still quite expensive. The costs related to the equipment after the initial investment, such as maintenance (every one or two years) and replacement of parts, can be significantly high. Replacement of certain parts can elevate costs. In the case of FTIR, ATR crystals can be scratched or broken over time leading to the need for costly replacement in addition to the cost of the equipment and the spectra database.

Furthermore, some of the techniques have limitations in detection. In the case of FTIR, the detection limit is around 1% and if the mixture is multicomponent, separation of all ingredients can be complicated and usually requires the use of multivariate statistical analysis. As was mentioned earlier, FTIR spectroscopy measures the fundamental vibrations of covalently bound atoms in molecules, hence each chemical compound has its own unique spectrum that may be treated as a molecular fingerprint.

For what concerns the risk scenario, the use of spectroscopy is capable of unequivocally identifying the content of the pesticides and to detect dilution or inadequate additives. As already mentioned, it is important to highlight that these technologies cannot prevent infiltration of the supply chain, rather they work as a mechanism to identify counterfeit products and their characteristics after a security breach occurs. Criminal activity cannot be prevented unless their continuous use over time is able to create a dissuasive effect on criminals. Having said that, it is important to reiterate that a widespread use of on-field testing devices may also result in the application of these technologies for preventive purposes, checking suspicious products along the supply chain to prevent reaching the final customer. These technologies may play a role in limiting the following steps of the criminal plan:

- Production of illicit pesticides.
- Infiltrating the market.

By analysing the products marketed by the criminal group with the proposed technologies, it will be immediately visible that they are of low quality or counterfeit. Adulterations can also be revealed. Furthermore, by progressively analysing samples in the supply chain, it will also be able to trace back the source of the incident and present this evidence in court. One of several of the technology options can be selected to perform the analysis, depending on the type of material that is being processed or the type of issues that are being identified. For example, FTIR and O-PTIR technologies may be applied to verify the authenticity of the food and to detect dilution or illegal additives. FTIR spectra may be shared among the stakeholders of the supply chain from the manufacturer, through distributors, to final users in order to check the authenticity of agrochemicals. The use of semi-portable devices enables the creation of intermediate checkpoints to avoid the insertion of illicit products within the supply chain.

Summary table for submission 1: possible application to limit risks highlighted by the scenario

Scenario	**Applicability of the solution**
Scenario 1: Infiltration into the agrochemicals' supply chain	
Step 1 – Acquiring control over legitimate companies.	
Step 2 – Production of illicit pesticides.	The technology can be used to analyse the marketed products and determine if they are fraudulent, of low quality, or if there is anything abnormal in their composition.
Step 3 – Infiltrating the market.	The technology will be able to analyse the marketed products and determine if they are fraudulent or if they use sub-standard products.

5.2.2 Multilayer security example 1

Technology submission 2

This submission incorporates several security layers for the creation of the digital identity of the product and for controlling its movements along the supply chain. The overall process can be divided in different stages:

1) Creating a unique identity of the product using its chemical properties and initiating physical traceability,
2) Transferring the identity into a secure database (digital identity) and initiating digital traceability,
3) Monitoring the life of the product along the supply chain and
4) Providing data analytics.

The starting point of this technology commences with the linking of the physical journey of a product to the digital journey, to guarantee integrity and auditability and to fight against fraud or diversion. This submission proposes initiating physical traceability by recording the chemical properties of the product. This initial identification is essential, as it captures and records the fundamental characteristics of the product.

This element provides for a unique and innovative identification of the product at its very first point of authentication, creating its unique chemical signature. This first signature capture identifies and contains the chemical components of the product and is further enriched with secure marking (active or passive) of the packaging. This marking also includes the signature of the product, which provides its description and credentials, including its components.

The information allows for the creation and management of "physical reference" databases, which are integral parts of this proposed solution. These databases are used to secure the aforementioned complex identity. The data is then inserted into an immutable digital storage. This is a crucial step since the signature information of the product then has to be connected to a platform of integrity that will enable the tracking through the supply chain.

To begin the digital traceability, the product identity is stored in an immutable manner using blockchain technology to achieve a controlled monitoring of the various processes along the supply chain. Product packages will also be marked using information on the signature identity of the product. Where possible, in-product marking can be used. The product signature can be checked at any point of the chain with specific tools in case of need.

In this regard, it has to be noted that the company developed its own tools to perform rapid signature field testing, making it possible to verify that the chemical composition of the product matches the recorded signature. For this purpose, the company developed a Portable Authentication Device (PAD) encompassing a Fourier Transform Near-Infrared (FT-NIR) spectrometer. Spectrometers are used to identify and characterize chemicals and compounds in a test sample. These devices are based on the characteristic absorption spectra determined by the chemical bonds in organic materials, which can be used to identify organic compounds, the same method fingerprints are used for identification. FT-NIR provides a useful complement to, or replacement of, the screening method before laborious chemistry tests and chromatographic methods. FT-NIR is non-destructive, needs little or no sample preparation, as well as being fast, safe and dependable as it doesn't need dangerous chemicals.

The PAD SICPA FT-NIR spectrometer can be used to detect on site at import points or at points of sales the non-conformal pesticides products. The PAD in its present form cannot determine whether the deviation from the genuine signature is due to counterfeiting, adulteration, or quality related problem. However, coupled with the rest of the technology included in this submission, it complements the proposed approach. This gives to field inspectors a useful screening tool to rapidly check if the biography information included in the identification and traceability code matches the detected spectral signature without the need to perform a lab test.

Storage in a blockchain ensures immutability and auditability. Data is used to control processes and perform mass balance calculations to detect fraud, diversion and malfunction during the movements of the product along the supply chain. This feature compares data related to the volume of traded goods at their point of origin with volume of the same goods at their point of destination. Variations in volume that cannot be justified by possible losses happening in the normal course of trade, will trigger an alarm and can represent signals of smuggling, diversion or counterfeiting operations. Data analytics and artificial intelligence algorithms provide additional means of predicting and checking the overall balance along the supply chain.

This submission also links product identification and traceability with space technologies to improve the control of the supply chain. The idea is to use them for proof of origin as well as for track and trace, by generating data that, when added to those directly obtained from the products, can guarantee an increased level of assurance on the quality of the products and the integrity of their transactions along the supply chain. Furthermore, satellite integration can also be used for improving the aforementioned mass balance calculations and reconciliations on trade volumes.

In particular, this submission foresees three main applications for space technologies:

Use for proof of origin and mass balance verification: images from drones and satellites can be used to link products to their place of origin. They make it possible to calculate production volumes and to anticipate and facilitate reconciliation.

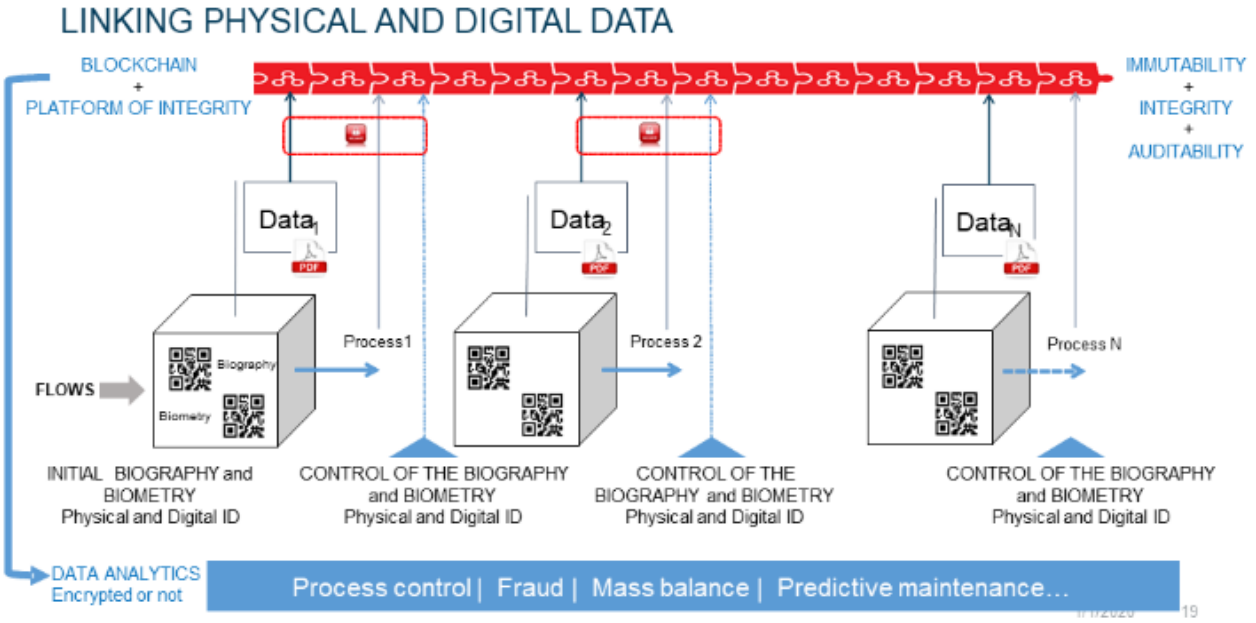
Use for ensuring product quality: products' quality assessed using specific imaging technologies including hyperspectral cameras related to the origin and components of the product.

Use for monitoring and communication: spatial monitoring of land can also be used to detect criminal operations. Together with proof of origin, it can provide additional data to check mass balance along the supply chain.

This submission stresses the fact that secure communication and data exchanges between drones, satellites and ground IoTs are key for supply chain auditability. Therefore, it is also important to secure images, transmissions and positioning of devices (IoTs and software).

Space data can be used for continuous and ulterior controls along the supply chain and, consequently, data and processes will also be certified and timestamped in a blockchain to improve security and avoid falsification. According to the submission, in the near future compressed spatial images with their embedded unforgeable signatures and localisations through quantum-derived technologies will be used for this purpose. By using space technologies, the quality of the product can be assessed through specific imaging technologies, including hyperspectral cameras.

Submission received from SICPA



Source: SICPA

The submission targets many issues identified in the risk scenario related to trafficking in counterfeit and substandard pesticides and is useful to present how multilayer security can work in practice and be used to prevent a series of criminal activities related to infiltration into the supply chain.

The starting point, and first layer of security, is the creation of the unique identification of the product by using its chemical composition, which also becomes its signature. When scanning or reading this type of code, the information obtained will also include the product signature and, in case of suspicion or in the case in which intermediate checkpoints are established, the actual composition of the product can be checked with respect to the information contained in the code. To this aim, this submission proposes the use of a FT-NIR spectrometer developed by the company, which would make it possible to conduct rapid field testing to verify the product signature.

Once the physical ID of the product has been created, its digital counterpart is created and stored in a blockchain-based database, which incorporates the security features typical of the blockchain, like immutability and transparency. This is the second layer of security while the next levels are represented by satellite integration and mass balance reconciliation of products' flow. Satellite integration allows for the geolocalization of products along the supply chain, while the origin and movement of products is time stamped into the blockchain, verifying that the intended origin, destination and routes are respected. This type of control also allows for mass balance reconciliation, since discrepancy on products' flow between origin and destination of products, as well as between intermediary points, may trigger an alert if not justified.

When fully implemented in all its parts, multilayer security of this kind can limit several steps of the criminal plan described in the scenario. It would be difficult for criminals to exploit international shipping routes to disseminate expired, counterfeit, mislabelled and unauthorized pesticide imports, as well as to refill product containers, because of the way in which the system constantly checks several characteristics of the tracked and traced products, including origin and movements corroborated by space technology, mass balance verification and the use of a unique ID also containing the signature of the product that can be checked at various points of the supply chain through the FT-NIR spectrometer. This approach could also overcome the lack of control over the product once it is packed, through mislabelling, copying of design and trademarks, and substitution of contents.

Importation of unauthorized pesticides that do not comply with quality specifications through the falsification of shipping documents or trade without a license can also be identified thanks to the multilayer security approach, as can the use of re-filled containers with non-compliant agrochemicals that might pose a serious public health threat. The same can be said for the production and distribution of illicit pesticides by using sub-standard products, cheaper active ingredients and other chemicals as well as for the distribution of agrochemicals containing diluted, inert, banned or improperly identified agents. In all these cases, the use of the product's signature within its unique ID would make it possible to spot unauthorized pesticides or ingredients if checks are performed on the chemical composition of the agrochemical.

With regard to the risk scenario, the technology solution may play a role in limiting the following steps of the criminal plan:

- Production of illicit pesticides.
- Infiltrating the market.

The use of biometric elements of pesticides in the traceability system in the supply chain (including chemical and physical properties for the production of its ID) creates a certain barrier to these illegal activities, because the systems will not recognize any correspondence with the identity of the fraudulent pesticides in the case of checking, given that its signature is radically different, and an infiltration would trigger an alert in the system. The infiltration of illicit pesticides into the supply chain would also be detected by an alert due to the mass balance equation protection and the use of blockchain, which is also achieved thanks to the use of space assets.

From what is described above, both steps 2 and 3 of the criminal plan can be limited by the application of this multilayer security approach. These elements also renders it more difficult if not impossible for criminals to use the same technology as producers, because alerts will necessarily be triggered at one of the stages if fraudulent products are inserted in the supply chain, even before their first packaging, since they do not respect the signature of the original product. Furthermore, the described use of space technology and of mass balance calculations will trigger alerts in the system. The infiltration of illicit pesticides into the supply chain would be quickly detected.

In the case in which:

- independent repositories for the chemical composition of agrochemicals were established, including the composition of all products which are authorized to be marketed in given markets, and
- the signature ID was created also using information contained in these repositories

The solution could be applied, even in the case in which organized crime controlled the full supply chain, since random checks performed by relevant authorities with on-field testing tools would discover a discrepancy b*etween the chemical composition of the product and what is included in the ID*[14].

The solution can of course limit risk in the case in which criminals try to infiltrate the legitimate supply chain at certain points. It cannot be applied in the case in which the whole trade is realized through illicit channels.

Summary table for submission 2: possible application to limit risks highlighted by the scenario

Scenario	*Applicability of the solution*
Scenario 1: Infiltration into the agrochemicals' supply chain	
Step 1 – Acquiring control over legitimate companies.	
Step 2 – Production of illicit pesticides.	*This submission adds layers of security if compared to more traditional approaches, such as: 1) use of biometry to create the identity of the product and its subsequent monitoring along the supply chain, 2) field identification through the FT-NIR spectrometer, 3) data analysis of flow mass balance of products, with the support of blockchain technology and 4) use of space technology to add additional time-stamped controls on the origin and quality of products and of their components, as well as to support the mass balance calculations.*
Step 3 – Infiltrating the market.	*As previously described, the technology solution can protect the supply chain from the infiltration of counterfeit products. However, the solution would mitigate the risk only if the criminal supply chain attempts to infiltrate the legitimate one at a certain stage.*

5.2.3 Multilayer security example 2

Technology submission 3

As seen in submission 2, this submission also focuses on multilayer security linked to the use of blockchain. The proposed technology solution comprises a blockchain with a bridge-database, combined with accurate time and position data from satellite navigation, and an option to digitally encrypt data from a product-level signature at origin to verify against printed packaging codes, using cryptographic keys. The blockchain can be public or private, or a combination of both, depending on the user groups involved. A trusted computing platform is used to securely interface to the internal systems of manufacturers. The different processes offered by this technology solution can be divided into:

1) Product fingerprint: The unique identification of the product (characteristics or chemical fingerprint) is obtained and linked to the traceability system. It can be read by using a smartphone or through a fast µ-level-3D scan if the digital fingerprint is on the product. Currently, the use of a chemical fingerprint is a proposal that can be adopted in this technology option if a partnership is created with other providers that have developed the technology or if it is later developed by the company.

2) Primary packaging: The initial digital fingerprint is linked to the primary packaging using cryptography to create a code. This code is verifiable by scanning it with a smartphone. An interesting feature developed by this submission is the possibility to embed the code directly into the primary packag-

14 This is probably an area where this approach could be feasible given that products in circulation have certain determined characteristics while it could be more complicated for a more complex market like the one of food products, since creating a repository like the one described here would be extremely difficult in practice.

ing, so as to avoid any possibility to remove it. The company already developed this technology and applied it in different markets.

3) Further packaging: If the product needs further packaging, the process can be repeated. The code on the new package is linked to the other different codes used, starting with the product-linked code. All barcodes are uploaded to the blockchain.

4) Blockchain tracking: Blockchain is used to protect the product fingerprint and the rest of the cryptographically secured codes that were used for packaging. The data is logged in a "bridge-database" between the data collection and the blockchain. This enables visibility in the changes of ownership, aggregation and disaggregation from the product-level encoding.

5) Integration with space technology: The submission also proposes the integration with satellite technology to verify the origin and movement of goods along the supply chain. Verification of products' flow quantities is also realized thanks to the use of both satellite integration and progressive timestamps into the blockchain.

Changes in ownership of the product and aggregation and de-aggregation of containers in larger shipments are recorded immutably in the blockchain. Cryptographic keys are exchanged, allowing the receiver to become the new owner of each item when authorised to do so by the sender. Each transaction is recorded as a new block. The scanned barcodes include location and time stamping which allows tracking of the location of the product at each change of ownership or transaction point. The scanned data is logged in a "bridge-database" as it is collected – before the hashed transaction data is saved in the blockchain. This allows data to be stored for later reference and easy checking, but groups of data are uploaded in a "hashed" form into the blockchain so that no changes to the data can be made.

An additional function uses a balance ratio between submission and output that is recorded on the blockchain. For example, if the amount of pesticide and containers coming in was monitored (geographical satellite data would strengthen this), it should match a particular amount of packaged pesticide output. If the same output is happening but with less authorised submission, this suggests an issue. This would require legitimate suppliers to log their shipments to the blockchain.

Sharing of relevant data is facilitated by search functions available in the bridge-database. Only authorised users have access to data. If anyone breaks into the database, no data can be changed, because it would change the blockchain. Such a change can be flagged in different ways depending on security needs, as it may not be desirable to alert everyone in the chain when such an issue occurs.

To transfer ownership of the product to the next supply chain point or end user, the sender must have both the authorised relationship with the next owner (via exchange of cryptographic keys) and a correct barcode to scan, which is traceable through the bridge-database linked to the immutable blockchain. Hence fake containers with fake or copied barcodes cannot be used.

The recorded product and time/location data is stored for easy data access in the bridge-database but cannot be adulterated in any way. This allows location tracking at every uploaded data point. Hence the history of movement of the products can be tracked. For what concerns the security of the database, only authorized users have access to it and any change of data can be flagged in different ways depending on security needs.

In the case of trafficking of pesticides, some relevant points should be highlighted:

1) Changes of ownership in the product and aggregation/de-aggregation of containers in shipments are immutably recorded.

2) Scanned barcodes include location and time stamping (via satellite), tracking at each transaction point.

3) Submission and output balance ratios can be helpful in order to identify an infiltration.

4) Hash-trees perfectly protect levels of information access.

5) Search functions and controlled flagging of issues.

6) Trusted computing platforms for supplier data integration.

Submission received from Nano4u.

As mentioned, multilayer security is also at the core of this submission. The key feature is the creation of the unique ID of the product by using the chemical signature of the agrochemical. It has to be noted that, at the current stage, this is a feature that the company is proposing but is not actually available. However, it could be achieved by partnering with providers offering this type of analytical tools. The chemical signature will become one element of the unique ID, which will show this information if scanned or checked. In this case, checks can also be performed via a smartphone app. As seen in the case of the other submission based on a similar approach, field testing devices will be needed if checks are also to be performed on the chemical composition of the products at intermediary check points in the supply chain or in case of suspicious illicit activities.

Once created, the unique ID is stored in the blockchain, with advantages in terms of immutability and transparency, and is printed on the packaging. There are some interesting features in this regard, both in terms of the code printing on the packaging and in terms of subsequent packaging phases. For what concerns the printing of the code, the company developed a method through which the code can be printed directly on the primary package of the product by engraving the code on the package itself. For example, the code can be engraved on the bag or initial package of the product instead of using a label or printed code over the surface of the bag or initial package. This renders the code non-removable and adds a layer of security if compared to traditional labels. For what concerns the second element, a relation can be established by the code on the primary packaging and all the other codes belonging to further packaging of the product. This information is also stored in the blockchain.

The use of satellite integration also allows for constant verification related to intended origin and destination of the product and its movements along the supply chain, while the information about the total weight of parcels or packages received and sent at each node is critical for adding another layer of security, since the change in the volume measurement would trigger an alert.

These characteristics allow this approach to limit several steps of the criminal plan, especially if and when the possibility of obtaining the chemical signature of the product and incorporating it into its unique ID is developed and fully integrated. This element, together with the further codes directly embedded on the different layers of packages and stored in the blockchain, can protect the authentication mechanism of the pesticide. The use of traceability systems relying on space assets not only provides an additional layer of security, but it also targets the lack of full monitoring and control of the production and distribution chains. The track and trace solutions enable the monitoring of the processes involved in the supply chain, granting visibility to identify illicit activities related to the deviation of the products from the supply chain. This can also be achieved thanks to the analysis of information about the change in the total weight of parcels or packages and by the fact that unjustified changes in the volume measurements would trigger an alert. In this regard, the adoption of blockchain technology creates a platform where any anomalies in the process would be pointed out immediately. Furthermore, the data introduced into the system would automatically be immutable and transparent for all the stakeholders, enabling auditability and accountability. The traceability is highly supported by satellite navigation and communication in order to obtain precise location and time data and to provide a unique cryptographic stamp for printed codes that makes each code unique. Space-related data are also used by this submission to track the origin and the location of products as they are packaged or repackaged.

As for other multilayer security approaches, for this submission, achieving interoperability between the different systems can also be a challenge. However, once the initial interoperability is achieved, it becomes an advantage since it allows the company to integrate the different systems being used. Along the same lines, the complex flow of data created by this technological approach would require personnel able to interpret the information that is received. Even in the case in which tools will be used to facilitate the interpretation of results through graphs and

data simplification, in order to have a full analysis of all the information received it may be necessary to have specialized individuals. Finally, if the optional capture of the chemical signature is not developed, the technology will be package dependent and will not be able to control the inner quality of the product.

For what concerns the risk scenario, the technology solution provides a multilayer security option that protects the product through the use of an identification code that is tracked through a blockchain-protected traceability system. If the option of adding chemical properties to the unique code is developed, then the authentication could be more secure. In many cases the replication of these codes, even if possible in theory, would involve a great investment from organized criminals, limiting their business case. In the case in which the optional element of the submission is developed/integrated, even if the code is imitated, by attempting to scan it, it would be clear that it is not an original product since it would probably not show the information related to the characteristics of the product. The traceability system and blockchain technology would protect the information and integrity of the product throughout the supply chain. Consequently, these technologies may play a role in uncovering the following step of the criminal plan:

- Infiltrating the market.

Apart from the security of the code, the fact that it is embedded directly on the primary and secondary packaging increases the security of the supply chain, since it would not be possible for criminals to remove the code, while obtaining technology to perform this process would not be easy and could limit the business case of the criminal operation. Furthermore, the implementation of the blockchain protects information shared by stakeholders as well as the data coming from the traceability system. It also enables visibility in the changes in ownership, and aggregation and disaggregation from the product-level encoding. Analysis realized thanks to the data stored in the blockchain would also make it possible to recognize any anomaly in the volume of products distributed along the supply chain. The infiltration of illicit pesticides into the supply chain would be detected by an alert, since the volume calculations would trigger an alert if there was any change in the quantity of products that were being processed.

In the case in which the optional integration of the chemical signature into the unique ID is developed, then this submission could also limit step 2 of the criminal plan "production of illicit pesticides".

Summary table for submission 3: possible application to limit risks highlighted by the scenario

Scenario	**Applicability of the solution**
Scenario 1: Illicit infiltration into the agrochemicals' supply chain	
Step 1 – Acquiring control over legitimate companies.	
Step 2 – Production of illicit pesticides.	This risk could be highly mitigated by the development or integration of an option using the chemical properties of the product in the code that is linked to the traceability system. Furthermore, the described use of space technology and of submission and output product calculations at all nodes could be a useful element to mitigate this risk.
Step 3 – Infiltrating the market.	Risk is reduced thanks to the use of non-replicable codes that are recognizable both visually and via the use of specific tools and by using a track and trace system and blockchain technology to secure the supply chain. The identity of each product is created by using a unique non-removable code. In this case, if the optional component is developed or integrated, the code would also include encrypted information about the characteristics of the specific product, creating a unique identification that is linked to the blockchain-protected traceability system. If the infiltration is attempted, alerts due to the change in volume would be triggered. In addition, the counterfeit products would not be scannable.

5.2.4 Linking non-reproductible QR codes with Business Intelligence

Technology submission 4

The submission proposes a technology solution that focuses on applying a secure, serialized QR code in which a copy detection pattern, or secure graphic, is integrated to authenticate the product. This option enables a simple integration of the solution into the existing packaging production, which can be used by all parties in the supply chain and is able to capture key events in the supply chain (movement of goods, transfer of ownership, among others) while being verifiable with a smartphone. The secure, serialized QR codes are managed by a connected product cloud platform. This enables several features, allowing alerts, messaging, authenticity and verification in one format. In addition, printing or copying the copy detection pattern in the QR code causes an irreversible information loss, which ensures that counterfeits are detected when scanning the product with a smartphone.

The serialization of the QR codes included in the system gives any product, object, or sample a unique digital identity, and specific supply chain data can be associated at a unit level. The high number of scans in turn provides increased visibility on product flow in different markets and can support the early detection of counterfeit hotspots. Alerts can also be set for key markers and problematic product distribution areas. The integration of loyalty programmes through the scanning of the codes serves as an additional incentive for customers to use the technology as often as possible.

For what concerns data aggregation and binding, typically different labels are used to associate unique codes to products, cases, pallets and shipping containers. This binding makes it possible to track products geographically and activate functions such as off-market alerts, black-listing, or target-specific messaging for consumers' engagement. The solution is connected to a Business Intelligence (BI) dashboard to obtain insights and predictive analytics about the products in the supply chain that serves as a real time tool for managing and analysing data generated in the system by scans. The codes are designed to also be easily scanned and authenticated using a smartphone camera.

Digital files of secure QR codes are provided to the printer by the manufacturer. Consequently, the system could be applied to cases concerning, for example, a criminal organization attempting to take a high-resolution scan of the packaging and QR code to print it on the counterfeit product packaging. In this case, in fact, the app would give a "counterfeit" alert if this code is scanned, due to the natural differences created by re-printing the secure graphic.

In the case in which a counterfeit code is scanned, the solution:

1) Sends an email and alert to a messaging app.

2) Reviews the scan to confirm the issue.

3) Blacklists confirmed counterfeit codes.

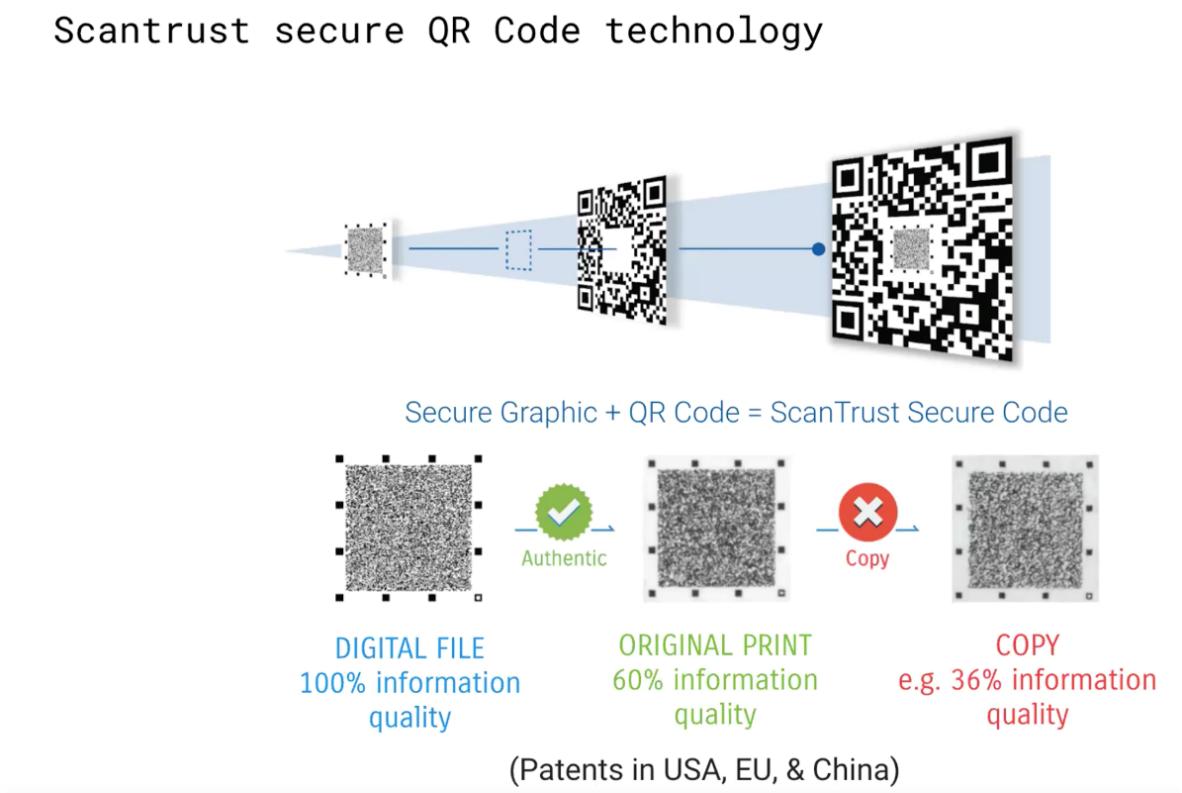
4) Performs deeper analysis, considering scan location, user app ID, and other scans from the same code to gain insights about counterfeit operations.

In this way, counterfeits can be identified and blacklisted before they hit the market when counterfeiters attempt to "test" their copies by scanning them.

Additional features can be added to increase security, for example, a Hyperledger Sawtooth blockchain to the track and trace system. The codes containing unique information about the product, as well as supply chain traceability events, are added as transactions to the blockchain, providing other characteristics such as immutability, transparency and accountability in the exchange and management of data in the supply chain.

Submission received from Scantrust.

This submission focuses on enhancing the security of the agrochemicals' supply chain by combining a complex secure code with a Business Intelligence (BI) system which enables accurate monitoring along the supply chain, including issuing alerts in the case in which illicit operations are registered.



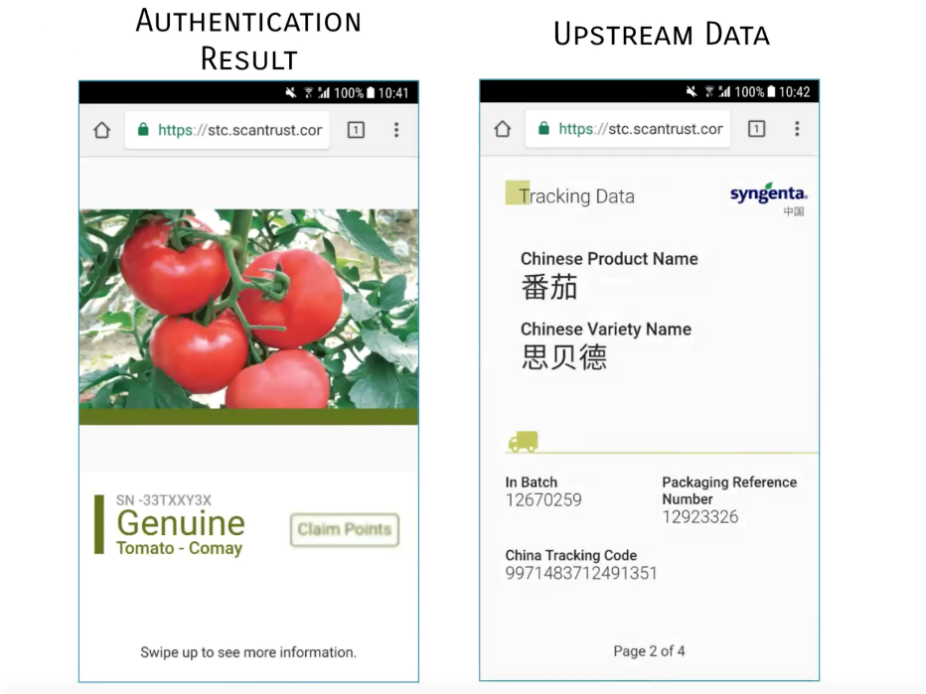
Source: Scantrust

For what concerns the structure of the code in itself, it is interesting to analyse how the security of the code is achieved, by combining the serialized QR code with a copy detection pattern, or secure graphic element. The secure graphic, which is a few millimetres large, is placed in the centre of the QR code and does not affect its scannability. Every time the code is printed and copied, it loses information irreversibly through naturally occurring effects of dot gain and ink smearing. This allows the detection of counterfeits with a smartphone camera scan, as the secure graphic element will contain less information than that in original prints. In this manner, counterfeiters cannot rely on the copying of labels to market fake products as originals to infiltrate the supply chain.

One advantage deriving from this approach is, for instance, that subsequent printing of the original code by illegitimate operators will lead to a loss of accuracy in the printed code itself, which will lead to non-recognition and non-validation during one of the subsequent scans along the supply chain. In this way, counterfeiters cannot rely on the copying of labels to market fake products as originals and infiltrate the supply chain.

Another other interesting element of this submission lies in the role played by the BI dashboard, which provides useful insights about the different processes in the supply chain and the cycle of products in it. Thanks to the combination of the secure code and the functions provided by the BI dashboard, the system is able to capture key events in the supply chain (movement of goods, transfer of ownership) allowing verifiability of the codes for the customers and stakeholders by using a smartphone. The secure QR code in combination with the BI dashboard also makes it possible to send alerts, have messaging features, and verify authenticity and movements of goods. The QR codes can also provide data at the unit-level, concerning the number of scans of a single code. This may trigger an alert in the case in which a high number of scans are registered for a single code, since it may indicate that the same code is used on multiple products. These kinds of analysis may provide an increased visibility of the situation in different markets and possibly allow for the detection of counterfeit hotspots.

Finally, the implementation of loyalty programmes through the scanning of the codes may increase the motivation of customers to continue to authenticate products. On the other hand, in order to be effective, the client needs to be aware of the security measures applied to the product and how to scan the code or tag to obtain the information. If the consumer has no information about the mechanism and on how to use the app correctly, then it might not serve its objective.



Source: Scantrust

The practical application of this technology can respond to different issues highlighted by the risk scenario. In particular, it could improve the control over the product once it is packaged, preventing mislabelling, copy of design and trademarks. At the same time, the technology can enable an improved monitoring of data exchanges in the supply chain, including in relation to the final users, which can verify the authenticity of agrochemicals prior to the time of purchase. Finally, given the fact that codes cannot be copied without incurring a loss in print quality which would lead to failed authentication, the system can also be used against the insertion of illicit products within the supply chain.

For what concerns the risk scenario, the technology solution provides a multilayer security option that protects the product through the use of an identification code that is tracked through a blockchain-protected traceability system, which enables the mitigation of threats in the supply chain. An infiltration would be detected through the scanning of the copied code. Consequently, this technology may play a role in uncovering the following step of the criminal plan:

- Infiltrating the market.

The infiltration of illicit pesticides into the supply chain would be detected by an alert triggered by the scanning of a counterfeit product. The continuous scanning of the products by consumers or users (and promoted by the adoption of loyalty programmes) can be used to identify how and where organized crime operates. Blockchain technology can be used to protect the data exchange and integrity through the different processes in the supply chain with its integration in the traceability system.

For what concerns step 2 of the criminal plan "production of illicit pesticides", the technology does not focus on the chemical properties of the product so it cannot detect the use of illicit substances. However, if the production activity also includes the replica of existing codes, this technology could limit this specific step, since its copied codes would fail verification at any following stage in the supply chain.

Summary table for submission 4: possible application to limit risks highlighted by the scenario

Scenario	Applicability of the solution
Scenario 1: *Illicit infiltration into the agrochemicals' supply chain*	
Step 1 – Acquiring control over legitimate companies.	
Step 2 – Production of illicit pesticides.	The use of a unique QR code on the package of the pesticide and the use of a blockchain-protected traceability system can prevent illicit production activities which include the replication of original authentication and track and trace codes.
Step 3 – Infiltrating the market.	The adoption of this technology solution can mitigate the risk of counterfeit pesticide infiltration in the supply chain. The secure QR serialized code that is combined with a secure graphic to authenticate the product and the use of a blockchain-protected traceability system provide a solution that combines several layers of security. If the code is scanned with a smartphone, the app would detect that the pesticide is counterfeit.

5.2.5 Focus on labels

Technology submission 5

The submission proposes a technology solution that combines tamper protection and authentication features with a traceability system to link a unique code to a specific product throughout the supply chain. Blockchain technology is used to secure authentication data, such as product information and tracking data from tampering related transactions. Blockchain technology can be seen as the digital tamper evidence. Data based on codes (IDs) protected with the technology are secured by a network of decentralised nodes. Currently, this technology is considered to be counterfeit-proof. Data analytics provide insights regarding the flow of goods and infringements of the supply chain.

This submission emphasises that, to protect a product on a physical level, effective tamper protection is one of the core challenges. This is valid, for instance, when using a variable code on the packaging to enable verification of the product: without appropriate tamper protection, the code can quite easily be transferred to a counterfeit product, compromising the effectiveness of the verification system. Security seals allow end users to check if a product has been tampered with. By using a VOID effect, a previously invisible symbol or text appears irreversibly when the seal is removed, making the latter non-reusable and non-transferrable. The patterns displayed by the VOID effect can be fully customized, using for example a lock symbol or language, in line with the security sealing label design and shape. These seals can be in different colours and shapes and can be highly translucent to leave text and barcodes underneath readable.

Security seals, including a VOID effect, allow end consumers to identify if a packaging has been tampered with. In the case of plastic screw caps, the possibility to use a seal on them is challenging, considering their small contact area to apply a seal. A dry-peel VOID, as a 2-layer construction for plastic screw caps, has been used in the pesticides market for many years. If a cap is unscrewed, the jagged design of the perforation points out that the product has been opened. Further integration of codes and security print makes the product even more secure against counterfeiting and allows all stakeholders within the supply chain to authenticate the product.

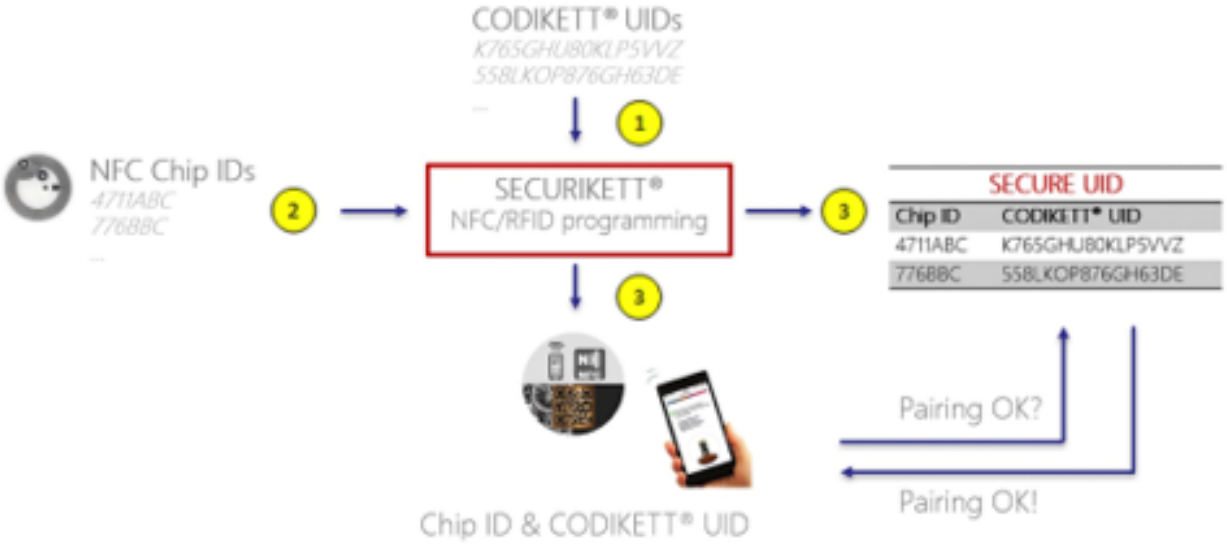
In the case of labels, they have a 2-layer construction and when a label is tampered with by peeling, a VOID effect appears. When an attempt is made to remove the label, a VOID effect is triggered between the two layers. The bottom layer of the label remains on the returnable packaging. If criminals try to reverse the manipulation attempt, the end consumer can see this through the VOID effect, as well as from the triggered perforation.

In addition to the physical product security, a security seal can be equipped with a serialised ID and a related traceability function. That means that each label has its own ID and can be managed and tracked individually. The technology proposed to enable this feature includes characteristics such as issuing secure codes, online authentication of each code, personalisation at item level, creating response pages driven by algorithms, geotracking with full track and trace for the entire supply chain and global distribution chain, management of packaging aggregation, and consumer engagement. IDs are often printed in the form of QR codes since consumers are used to scanning QR codes. Scanning such a QR code with a generic barcode reader app will lead to an authentication of the packaging and a tailored landing page showing the digital twin of this code/package/product. Individual and dynamic content is created by algorithms in view of also avoiding any tampering with the digital response. Every package and every delivery can be monitored in real-time throughout the supply chain. In addition, comprehensive data analytics help to understand the flow of goods and possible infringements of the supply chain.

The technology submission can also be used with RFID (NFC) technology, which is based on smart labels, consisting of physical tamper evidence (VOID), the same unique ID for printed codes and the programming of individual chip content for improved product security. Depending on the product and packaging, a digital tamper evidence feature can be added to the smart labels: a built-in tamper loop indicates the opening of a product (can, bottle, case, box). A comprehensive option in the case of labels is the All-in-One label, consisting of a secure ID, RFID (NFC) and RFID (UHF), all in one. The same ID is used for the printed code, the NFC chip and the UHF chip to provide full traceability throughout the entire supply chain, up to the consumer.

Submission received from Securikett

The submission offers different options to mitigate the threats presented in the risk scenario. Authentication is achieved through the implementation of unique codes and inks that are linked to the product. The codes are protected by tamper proof mechanisms that would indicate if the integrity of the product was compromised. At the same time, the codes can be linked to a digital traceability system that is protected by blockchain technology to monitor the product. The information exchange during these processes is immutable and transparent for stakeholders. Data analytics provide useful insights about the product in the supply chain and are capable of identifying possible infringements.



Source: Securikett

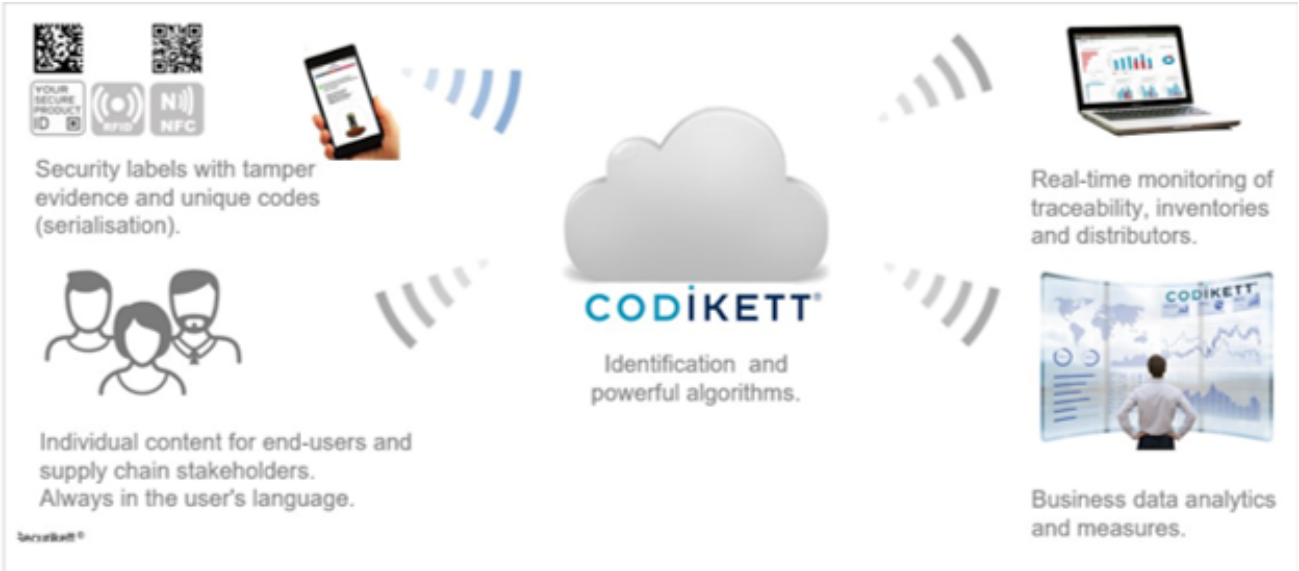
One of the key elements of this submission is the link between a label reuniting different functions with a fully-fledged traceability system using blockchain. For what concerns the label, it has anti-tampering and identification functions performed through different options, including customizable VOID tapes, dry-peel VOID as a 2-layer

construction for reusable packages, QR code or human readable code, RFID (NFC) technology, and an All-in-One label, consisting of secure ID, RFID (NFC) and RFID (UHF).

A specific design of VOID labels can also be applied on caps, in view of identifying if a bottle has been opened and its contents replaced.

Source: Securikett

Geotracking possibilities are also applicable to create a product which integrates several interesting features. This feature enables the identification of the current, physical location by obtaining GPS data from smartphones or other GPS-enabled devices. This characteristic is combined with a full track and trace for the entire supply chain and global distribution chain to protect the movement of the product. The database used for the track and trace is blockchain based.



Source: Securikett

Furthermore, the All-in-One label can include additional authentication features, such as fluorescent inks that can be added to enable brand owners or authorities to check if a product is from its legal origin or not. Finally, this technology is also ready for interoperability.

Of course, since it is focused on labels, this solution is package dependent.

For what concerns the risk scenario, the technology solution uses the different options to create a unique and tamper proof identification mechanism that can be tracked throughout the supply chain to protect the packages containing pesticides.

Consequently, these technologies may play a role in uncovering the following steps of the criminal plan:

- Infiltrating the market.
- Production of illicit pesticides.

The risk of infiltration of illicit pesticides into the supply chain is mitigated by protecting the packaged products with the use of unique and tamper-evident codes and inks that provide a specific identity to each pesticide. The infiltrated products would not have an authentication mechanism, and even if the criminal organization attempts to copy the design, the app will not read the code on the counterfeit product. The app indicates in a clear manner if the product is original or if it was opened at some point, which is highly relevant for customers. In addition, the products are monitored in the different stages of the supply chain with the track and trace system. Tracking the product and adopting blockchain technology to monitor the transactions enable the protection of the original pesticides and facilitate the identification of any counterfeit product since the platform would detect any anomaly in the processes. This is a package-level solution, therefore, the content (chemical composition and other characteristics of the pesticide) of the product would not be linked to authentication or track and trace.

Summary table for submission 5: possible application to limit risks highlighted by the scenario

Scenario	**Applicability of the solution**
Scenario 1: *Illicit infiltration into the agrochemicals' supply chain*	
Step 1 – Acquiring control over legitimate companies.	
Step 2 – Production of illicit pesticides.	The solution is designed to mitigate the risks of a possible infiltration into the legitimate supply chain; however, counterfeit pesticides cannot be identified by their composition and the technology comes into play at the first packaging point. The technology submission provides options to authenticate the package of original pesticides by using different labels, tags and VOID effects and a secure traceability system to protect the transactions made during the cycle of the product in the supply chain.
Step 3 – Infiltrating the market.	If the technology solution is implemented, the risks related to the infiltration of counterfeit pesticides can be mitigated. The use of a unique identification code that is tamper proof and its connection to a blockchain-protected traceability system provide a multilayer security mechanism that would detect the infiltration of counterfeit products that do not have the authentication features. The information transactions related to the movement of products in the different stages in the supply chain would be immutable since they would be in the blockchain.

5.3 Conclusions

The risk scenarios dedicated to the trafficking in counterfeit and substandard pesticides presented some of the threats that can affect the integrity of the supply chain. Thanks to research conducted by UNICRI and to the submissions we received from technology experts, it has been possible to assess how technology solutions may contribute to increasing the security of the supply chain of these products, while limiting related criminal activities.

Existing technology solutions usually encompass one or several of these elements to protect the flow of products in the supply chain:

- **Authentication technology**: Usually consists of overt, covert and forensic security features. Tamper-evident packaging (TEP) can be added as a tool to identify if a product has been tampered with and is not safe to use or consume. Authentication mechanisms can include security hologram seals and labels, tamper-evident security film, low-cost transponder tags, and light sensitive ink designs or use a combination of tools, like unique holographic fingerprint tags that are instantly verifiable by using a smartphone. Additional features have been combined with authentication solutions for pesticides, including Information and Communication Technology (ICT) models and the implementation of mobile-based solutions that contribute to the authentication of products.

- **Track and trace systems**: Authentication mechanisms like labels, codes and RFID are frequently integrated into traceability systems. Traceability allows the monitoring of the original pesticides throughout the different stages of the supply chain and protects them from infiltration of unauthorized products. This grants visibility to identify illicit activities related to the deviation of the products from the supply chain, including the dissemination of expired, counterfeit, mislabelled and unauthorized pesticide imports, as well as refilled product containers. Traceability options can also use space technologies as a proof of origin as well as for monitoring purposes.

- **Blockchain technology**: It has been integrated to traceability systems. It can connect the different parties in the supply chain that have not established trusted relationships with each other, by ensuring transparency. Blockchain stores every transaction or exchange of data that occurs in the network, reducing the need for intermediaries by providing a means by which all the actors in the network may share access to the same information, including what is added to the data, by whom, and the date and time of the submission.15

- **Forensics**: Approaches to corroborate the authenticity of a product include the use of specific techniques for forensic investigations. The Fourier Transform InfraRed (FTIR) spectroscopy is a method used to examine samples, both to detect the presence of target compounds and to measure their quantities. In the case of pesticides, a portable FTIR spectrometer can be used to rapidly analyse pesticides before distribution, before mixing, and/or before application to crops. A portable device enables the analysis of counterfeit pesticides in different stages of the supply chain, where they are manufactured, shipped, received, stored and sold. Other techniques include the use of Optical Photothermal Infrared Spectroscopy (O-PTIR) to analyse the samples of the products.

The submissions analysed in the report use different types of technology that are applied following various approaches. Technology is frequently combined to provide multiple levels of security and to achieve a combination of objectives. The submissions might use similar approaches to mitigate risks, however, they offer unique features that focus on the use of specific technology tools. In the case of trafficking in counterfeit and substandard pesticides, the submissions offered the following distinctive approaches:

- **Combination of a strong authentication mechanism that can be scanned with the additional implementation of data analytics solutions to obtain useful insights**. The creation of a unique code that acts as an identifier and as the authentication method enables customers and stakeholders to verify if the product is original or if it was manipulated. All this can be done by using a smartphone camera. In addition, the use of data analytics provides insights and predictive analytics about the products in the supply chain and serves

15 Accenture. (2019, January 15). Tracing the Supply Chain. Retrieved August 23, 2020, from https://www.accenture.com/_acnmedia/pdf-93/accenture-tracing-supply-chain-blockchain-study-pov.p

as a real time tool for managing and analysing data. The technology solutions are designed to secure the product once it is packed, making it package-dependant. However, the content of the package is not linked to the authentication. Submission 4 adopts this approach and incentivizes the use of the scanning feature by implementing a loyalty programme for customers. Submission 5 uses a similar approach and incorporates blockchain technology to the traceability system that is proposed.

- **Multilayer approach that links the content of a product to other security measures**. This approach adopts a combination of technologies to target the complex risks in an integral manner by using the unique identity of the product (by obtaining the specific composition and other characteristics to create a signature fingerprint), a traceability system that connects the physical and digital identity of the product, blockchain technology to protect the data exchange and the mass balance equation, data analytics in a platform to give an overview of the supply chain and space technologies for proof of origin as well as for track and trace. This approach is not only based on the protection of the package, but also on securing the product itself in addition to the package and the end-to-end monitoring of the supply chain. The biometry of the product to create an inimitable identification reference and the mass balance equation protection are essential to achieve this. Submission 2 provides this combination of technologies to protect the integrity of the supply chain. Submission 3 has a similar approach but still has to integrate the signature analysis technology in its portfolio of solutions. This could also be done in the future by partnering with different actors that already have these technological means.

- **Forensic and nuclear analytical techniques** have a different approach, since they do not focus on preventing infiltration but can be used to identify counterfeit products and their characteristics after the security breach occurs. Submission 1 adopts this approach to verify the content of the pesticides and to detect dilution or inadequate additives. By using semi-portable devices, it is possible to set up intermediate checkpoints to avoid the insertion of illicit products within the supply chain. Spectroscopy can be used to clearly identify toxic substances that are banned, such as camphechlor and aldrin.

With specific reference to the risks that were highlighted by the risk scenario, the following considerations can be made:

- **The trafficking in counterfeit pesticides is frequently carried out through different methods**, including mislabelling and repacking, avoiding high risk Customs borders, exploiting international shipping routes to disseminate illicit products,16 forging documents related to products' distribution, and using re-filled or non-compliant containers. As a consequence, the solutions adopted to **secure the supply chain should consider the use of a multilayer security approach**, bringing together multiple technologies to support stakeholders and authorities. This element has been confirmed by the majority of the submissions that we received, where multilayer security was at the core of many of them.

- Technology solutions play a relevant role in the mitigation of these threats, alongside **effective formal and informal control mechanisms in regulatory, production and supply chain networks** such as awareness and engagement of authorities and stakeholders, international harmonization and regulatory oversight, supply chain protection and defence activities, enhanced investigation and interdiction capacities, control of financial flows and incentives, and end-user and consumer awareness.

- The incorporation of **blockchain technology** in the digitization of processes and the traceability systems protects the exchange of data between authorized stakeholders and guarantees immutability, transparency and accountability.

- **Supply chain technology producers are constantly looking for ways to innovate the modality through which products' integrity and security can be enhanced**. The analysis of the submissions we received testifies to this element. Concrete examples include the use of multilayer solutions that combine several authentication features and that use techniques to ensure the uniqueness of the product, while adopting further protection mechanisms such as track and trace systems, forensic techniques and blockchain technology to protect transactions.

16 At least five product categories fall within this notion in the case of illicit agrochemicals: expired, counterfeit, mislabelled, unauthorized pesticide imports, and product containers.

- The challenges related to package dependency are being addressed by incorporating the unique characteristics of the product in the authentication mechanisms. This includes creating a unique identity of the product using its **biometry and biography** and then initiating physical traceability by transferring the physical identity into a secure database to create the digital identity of each product. Technologies also offer mechanisms to calculate deviations from the intended mass-flow of products between points of departure and of destination, providing improvements to limit risks in the exploitation of international shipping routes, importation of unauthorized pesticides through the falsification of shipping documents, conducting trade without a license, and the use of re-filled or non-compliant containers that might pose a serious public health threat.

- The submissions we received also showed that technology solutions have the capacity to provide improvements in order to combat the **lack of control over the product** once it is packed through mislabelling and copying of design and trademarks. They can also protect against the substitution of contents and respond to the need of establishing **intermediate technology checkpoints** to avoid the insertion of illicit products within the supply chain. Along the same lines, technology can also give final users the possibility of verifying the authenticity of agrochemicals at the time of purchase, responding at the same time to the need for **full monitoring of the supply chain and of related data exchange**.

- This constant search for innovation can also be seen in attempts aimed at improving the authentication elements. Authentication solutions that are based on **labels and codes incorporate innovative characteristics** to improve their protection, scannability, and uniqueness. Customizable VOID effects, the use of a secure ID, RFID (NFC) and RFID (UHF) in one label, and a secure, serialized QR code that is combined with a secure graphic are some examples of technology available in this regard.

- Some criminal activities highlighted by the scenario cannot be limited by supply chain security technology. This has to be expected since the main purpose for which these technologies were developed is to protect the integrity of the supply chain and not to stop different kinds of criminal operations. The mitigation of these risks will necessarily **require actions and strategies implemented by law enforcement agencies to better understand how crime operates and how to monitor organized crime strategies to prevent these criminal activities**. It is for these reasons that some steps of the criminal plan in the risk scenario were difficult to limit by supply chain technology solutions. This is the case, for instance, of step 1 "acquiring control over legitimate companies".

- Following the previous point, an integrated approach between different technology typologies and options is needed to **support at the same time investigators and law enforcement agencies** on the one side, as well as **supply chain operators and consumers** on the other.

- **Consumer education** is also essential in order to implement authentication solutions which give consumers or final customers the possibility of verifying the authenticity of the products they buy. The authentication codes used by different providers are frequently easy to scan through the use of smartphone cameras, however, consumers and final customers need to be aware of the existence of the verification mechanism itself and of the steps that need to be taken to corroborate the authenticity of the products. The use of loyalty programmes could constitute an incentive to use these authentication mechanisms and raise awareness on their importance and use.

- Forensic analysis, and in particular **nuclear analytical techniques**, can help to identify counterfeit, fraudulent or illegal agrochemicals which were inserted into the legitimate supply chain. The analysis of specific elements in the composition of a product enables the clear authentication of the products. These technologies usually come into play once the supply chain has been infiltrated or when there is a suspicion of infiltration.

- Rapid **on-field portable testers** are being developed and are becoming more widespread and they could allow for a wider use of on-field testing, rendering these checks easier to be performed, and significantly improving the security of the supply chain.

CHAPTER 6
Fuel fraud

Oil remains one of the most essential resources to the world economy. Yet the hydrocarbons supply chain is vulnerable to the actions of organized criminal groups, which operate a black market of fuel theft and fraud. Illegal activities may target the production, transportation and processing, as well as the refining and distribution phases of oil products.

The Atlantic Council estimates that fuel theft and fraud deprive governments and legitimate oil companies of billions of dollars per year.[1] Organized criminal groups have adopted several strategies to evade fiscal duties and profit from the sale of excisable goods at lower prices than their licit equivalents. The main areas of excise fraud include the smuggling of authentic goods, the manufacturing of counterfeits and the diversion of authentic products to a destination market without paying excise duty.[2]

The fuel/oil sector is particularly vulnerable to criminal activities, which affect the entire supply chain and vary according to the geographic context. In importing countries, fuel fraud is driven by disparities in tax rates applied in domestic Jurisdictions.[3] It may take the form of purchasing fuel in a State with relatively low tariffs and VATs and selling it in a neighbouring country with higher rates or misrepresenting a type of fuel taxed at a lower rate as a fuel taxed at a higher rate. It also gives rise to 'cocktailing', or chemically altering fuels so that they mimic hydrocarbon products assessed for lower tariffs or VATs, and then selling them as higher-taxed fuels.

The economic costs of hydrocarbon fraud are considerable and wide-ranging. In September 2018, EUROPOL coordinated an operation involving 23 EU Member States against organized crime groups involved in fuel fraud. To avoid paying VAT and excise duties, criminals have produced a mixture mainly made up of gasoil and additives, thus altering the final physical features of the product. The operation resulted in the arrest of 25 people, and the seizure of over 2.2 million kg of illicit fuel, and the confiscation of assets worth over 3,000,000 euros.[4]

6.1 Risk scenarios

Two risk scenarios have been elaborated in the area of fuel fraud.

Risk Scenario 1: Infiltration into the Supply Chain

Two decades ago, vast oil reserves were discovered in a given country. They were estimated to account for around 5% of the known oil reserves worldwide. A secessionist political movement is registering a growing consensus in the area where the reserves are located, aiming at making it independent from the national Government and only giving access to revenues from the oil extraction to the residents of that particular area.

1 Further information on the Atlantic Council report "Downstream oil theft. Global Modalities, Trends and Remedies" is available at: https://www.atlanticcouncil.org/images/publications/Downstream_Oil_Theft_web_0327.pdf

2 See EUROPOL, Serious and Organised Crime Threat Assessment (SOCTA) 2017, available at: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organisedcrime-threat-assessment-2017

3 See Atlantic Council, Downstream oil theft. Global Modalities, Trends and Remedies, available at: https://www.atlanticcouncil.org/images/publications/Downstream_Oil_Theft_web_0327.pdf

4 Further information is available at: https://www.europol.europa.eu/newsroom/news/end-of-road-for-fuel-fraudsters-eu-law-enforcement-seize-22-million-kg-of-illicit-fuel

From the geographical point of view, the country shares one of its borders with another country which, in turn neighbours with a customs union (free trade area) composed of 10 Member States. The customs union has set up a computerized system for monitoring the movement of excise goods under duty suspension in circulation in the territory of its Member States. It records, in real-time, the movement of alcohol, tobacco and energy products for which excise duties have yet to be paid. It is a crucial tool for information exchange and cooperation between the Member States of the customs union.

A transnational criminal organization, the "Black Gold Ring" (BGR), aims to take advantage of any fraud opportunity that is presented to them in the domain of oil thefts and refined fuel adulteration. In order to profit from the current business opportunities of the newly discovered oil reserves, they implement the following criminal business plan:

Step 1. Political and economic infiltration: the "Black Gold Ring" secretly infiltrates the secessionist movement operating in the area and corrupts key players in the oil business (from parastatals to multinational corporations and even ship captains) in an effort to steal oil while it is being lifted from bunkering facilities into ships.

Step 2. Infiltration into the legitimate supply chain: The head of the criminal group organizes the infiltration into the legitimate supply chain of the crude oil that has been stolen from the country, with the help of an oil trading company exploring and exploiting an offshore block in the neighbouring country. The block declares four times its actual production in order to launder the stolen oil, which is entering the neighbouring country using tankers from the country where the new oil reserves were discovered. The laundered production is then sold on to refineries established in the territory of the neighbouring country. The criminal group is consequently able to collect profits from this sale and distributes these profits to the chain of intermediaries who made the first part of the deal possible. It is necessary to use a number of operations and transactions to bring the illicit crude oil into the legitimate market in order to avoid triggering the suspicion of the public authorities. The criminal group relies on a series of mechanisms, ranging from opaque trading using ghost companies, to false documentation and invoicing, off-the-books transactions, tax evasion and money laundering.

Step 3. Infiltrating/controlling refineries: The criminal group infiltrates one of the refineries in the territory of the neighbouring country. As a result, it sells regular fuel as well as cheap fuel as part of its production, with the aim of selling it in the illicit market of the neighbouring customs union. Any discrepancy in price between neighbouring countries serves as an invitation to smuggling operations, so cross border crime is a recurring theme.

Step 4. Organizing a "cheap fuel trade": The criminal group organizes a cheap fuel illegal trade, which has the potential to cause damage to vehicles' engines – as the product is not compliant with the relevant customs union's standards. The cheap fuel also poses a risk to consumer health and safety due to excessive emissions. To avoid the fuel being subject to excise regimes once on the market (to avoid paying VAT nor excise duty), the criminals produce a mixture composed mainly of gasoil and other added compounds to modify the final physical features of the product. As a result, the final product, which is sold illegally on the black market, is particularly attractive as it is sold at a lower price than the authentic product and it enables the criminals to make huge profits. The criminal modus operandi (routes, types of products and economic operators involved in the fraud) also utilize the illegal unloading premises and supply chains of the other products (base oils, additives, etc.) of the infiltrated refinery located in the neighbouring country.

Step 5. Infiltration into public procurement: The criminal group undertakes another fraud scheme. The country where the reserves were discovered does not have refineries on its soil and it subsidises refined fuel importation. The head of the criminal group wants to take advantage of this situation and organizes the infiltration into the public procurement process of imported refined fuel. Thanks to corrupt government officials, he uses fuel deriving from refineries he had infiltrated in the neighbouring country and sells it, sharing the misappropriation of the granted subsidies with his accomplices.

Risk Scenario 2: Fuel Laundering and Mixing

A country is engaged in large-scale oil exploration activities off their national coastlines. The country applies a low excise rate on fuel products and has a "no-excise" policy on fuel intended for agricultural and urban development, which is marked with chemical dyes. However, corruption is rampant and turning a blind eye to economic crimes in exchange for a bribe is a widespread practice.

A neighbouring country, on the other hand, is led by a climate-conscious government, committed to a transition to sustainable energy sources. To that end, the government has increased excise duties on road fuel, creating a substantial price difference between the two countries. The move has resulted in higher costs for domestic industries and households, prompting discontent over its negative consequences for the national industry and consumers. Many motorists living in border areas have already started to refuel their tanks where it is cheaper.

Always on the lookout for high profits at a low risk, the ringleader of a criminal group in the country where large-scale oil exportation activities are taking place understood the potential high profits generated from black market sales of oil products. Anticipating a growing demand from the neighbouring country due to its environmental policies, she/he starts operating in the fuel sector, and implements the following criminal plan:

Step 1. Smuggling: The criminal group bribes truck drivers working at State refineries to bring out fuel in small tankers. The criminal group then relies on lorry drivers and the owners of fishing vessels, interested in earning extra money, to smuggle fuel for illicit sale into the neighbouring country by land and sea.

Step 2. Fuel laundering: At the same time, the head of the criminal group sets up makeshift fuel laundering plants in the several warehouses of the front businesses run by the criminal group. Posing as managers of construction and agro-food companies, her/his associates bribe representatives in the relevant country who award licenses to participate in the national scheme for the supply of excise-free fuel. At this stage, criminals perform a chemical treatment on the rebated fuel to remove dyes and covert markers and give it the appearance of legitimate road fuel.

Step 3. Mixing and distribution of adulterated fuel: In the same facilities, the associates of the criminal group use kerosene and lubricant oils to 'extend' the diesel used as road fuel. They also add methanol to petrol for similar effect. To ensure full control of the distribution chain and maximize illicit profits, the criminal group threatens several owners of fuel pumps located in border areas to sell their business to its straw-men, who then supply adulterated fuel to thousands of unsuspecting customers from both countries.

In the space of year, the criminal group has smuggled over 2,000,000 litres of petrol and gasoil into the neighbouring country by land and sea. As both road fuels sell for 1.5 euros, the criminal group stands to gain over 3,000,000 euros.

In the same period, the fuel laundering plants have treated and passed off 1,000,000 litres of rebated gasoil as road fuel. As the country applies a 0.25 euros duty per litre of petrol and gasoil, the criminal group has carried out an excise fraud valued at 250,000 euros. Such fuel, conveyed to the stations controlled by the criminal group, was sold to domestic and foreign motorists for one euro per litre, reaping 1,000,000 euros in illicit profits.

The criminal group has thus caused a drop in fiscal revenues, in both countries, and has obtained a new channel for funding its illicit activities. Furthermore, the adulterated fuel damaged hundreds of car engines, and the industrial waste of the laundering process was illicitly disposed of in the country's river basins, resulting in serious environmental degradation.

6.2 Technology solutions to address the risk scenarios

Fuel fraud negatively affects several issues that range from loss of revenues for stakeholders in the supply chain and government to adverse effects in the environment and human health due to the use of unregulated substances in adulteration. For consumers, other problems might arise from the use of counterfeit products, including the damage of their vehicles. The complexity of the challenge increases when additional factors are considered, for example, considering that governments often subsidize domestic fuels used in industry, the existence of fuels of a similar grade that are sold at different prices within the same country can lead to adulteration, blending and dilution. In addition, the differences in taxation between countries enhance criminal activities like smuggling and theft. Finally, with governments increasingly mandating the adoption of renewable energy sources, the wider use of biofuels has added a further level of complexity.

In some cases, governments develop fuel marking programmes to combat these issues. Marking fuel with different techniques to achieve diverse objectives, for example, detection of smuggling and adulteration, the recovery of lost revenues and increased revenues without the need of additional taxation, forensic evidence for the prosecution of criminals, and increased confidence among domestic fuel consumers as well as domestic and foreign investors.[5] However, additional considerations should be taken into account when implementing a fuel marking programme, such as the certification of operations to international process integrity standards like those of the International Organization for Standardization, the use of other technology solutions to further mitigate threats in the supply chain and the design of a testing system to corroborate the authenticity of fuel.[6]

Fuel protection programmes help secure supply chains by marking all branded fuel with covert markers to detect dilution, substitution or quality issues caused by equipment malfunction or human error. This guarantees that fuel quality and volume between the terminals and retail sites remain consistent to reduce unauthorized fuels in the market and eliminate unfair competition. Illicit trade in refined fuels can be substantially reduced with the right fuel marking programme combined with supported enforcement policies. Fuel Marking Programmes consist of sound technology (markers, analysers, information systems) that have been proven in implementations around the world. Moreover, they have repeatedly demonstrated efficacy at reducing illicit behaviour and delivering a high return on investment. A critical success factor is for testing to be visible with enforcement ramifications that would be applied to offenders.

As listed above, there are new threats to the fuel supply chain integrity, through the use of so called "designer fuels" which are imported, or produced locally, that are hydrocarbon mixes which mimic fuels but do not perform as such in combustion engines. These products not only harm the engine and the environment, but also contribute to the loss of legitimate government revenue. Major advances have recently been made in developing systems, both laboratory and field-based, to properly identify and control the introduction of these new and damaging designer fuels into the supply chain.

a) Authentication by marking

An important authentication solution is based on marking legally imported or produced and tax-paid fuel. Fuel markers are chemical compounds that are frequently added to a wide variety of petroleum products, including gasoline, diesel fuel, jet fuel, kerosene, and gas oil, among others, to guarantee product integrity, protect against counterfeiting, adulteration, and tax fraud. The compounds used must be miscible, impart no colour and be resistant to simple removal.[7] The technique has been evolving since the 1950's, when branded fuel suppliers began to use colorants as a mean to indicate fuel type, grade, or brand in the downstream petroleum industry. The evolution of markers can be observed in the use of more proprietary compounds designed and developed for fuel marking; moreover, machine-readable features that give unambiguous results were developed to minimize the possible errors caused by a human visual assessment.[8]

There are different types of markers that can be used, and they can range from coloured dyes to specialized covert markers with particular detection methodologies. Overt dyes are visibly coloured and are typically more economical but can be easily imitated or laundered. On the other hand, covert markers are invisible. There are several types of covert markers with specific characteristics, which include recognition, optical, and molecular markers. Recognition markers are captured by custom-matched antibodies and are then detected by a reader or test kit, and the detection can be in the field (qualitative) or laboratory (quantitative). Optical markers use covert organic chemicals that emit a detectable fluorescent light when excited and are visible only with a highly sensitive field detection device that provides near-instantaneous results. Finally, molecular markers exploit the unique mass spectrum of chemical entities, enabling lab-based qualitative and quantitative analysis using forensic lab devices such as gas chromatography mass spectrometer (GC-MS).

5 Soud, D. (2020, May). Downstream Oil Theft: Countermeasures and Good Practices. Retrieved from https://www.atlanticcouncil.org/wp-content/uploads/2020/05/AC_OilTheft-Final-1.pdf

6 Soud, D. (2020, May). Downstream Oil Theft: Countermeasures and Good Practices. Retrieved from https://www.atlanticcouncil.org/wp-content/uploads/2020/05/AC_OilTheft-Final-1.pdf

7 Verbanic, C.J. (2007). Fuel markers Create unique fingerprint. 13. 8, 10-12.

8 Conroy, J. (n.d.). Technology progression in fuel marking. Retrieved from https://authentix.com/technology-progression-in-fuel-marking/

Fuel markers of any kind can be qualitative, where they only indicate the presence of a marked product or in the case of molecular markers, quantitative, where they point out the presence of a product and its precise concentration, therefore, the degree in which the fuel has been diluted or adulterated.[9] Fuel markers that blend in a covert manner with the fuel at very low concentrations provide the highest level of security for the entire supply chain, and even at that level of concentration, their presence or absence in fuel can be detected with easy-to-use analysers.[10] Another relevant distinctive feature is that though solvent dyes, fluorescent markers, and even near-infrared fluorescent (NIRF) markers can all be chemically removed or "laundered" out of the fuel they mark, covert molecular markers are effectively impossible to remove, or even to detect without specialized equipment.[11]

Some advanced fuel markers carry a unique signature that can be detected only by proprietary readers and can be traced back to a specific point of origin. Fuel marking programmes have been developed to mitigate the risks of fuel fraud and in the case the fraud occurs, they can be used to identify the site within the supply chain where the fraud was committed, increasing accountability, the threat of smuggling of illegal fuels across borders, and helps to identify illegal traders. Fuel makers in fuel integrity programmes can be adopted to target diverse objectives, at a government level, a country can implement a "national marker" programme where the "chemical tax stamp" indicates that all taxes have been fully paid on fuels.[12] Another case where markers are used is to protect the use of subsidized petroleum products in the market.

b) Field detection analysis

Fuel marking programmes can also include field detection analysis of the products, which is performed by portable and proprietary devices that allow for frequent testing. Marking and analysing technologies can work as a multilayer integrated solution to mitigate risks related to fuel fraud. In this manner, counterfeit fuel can be detected in different stages of the supply chain after the markers are added. Additional data-driven management platforms that work with artificial intelligence can be adopted to obtain deeper insights related to vulnerable points. The portability of devices can also allow the immediate connection of test results to encrypted, cloud-based storage systems.

Field detection can be carried out through the use of different methodologies and analytical techniques like spectrometer systems. When fuel is laundered via chemical processing, heating or absorbent materials, a spectrometer can be used to detect the residual dye. Furthermore, the increased sensitivity of the analytical technique enables the use of lower concentrations of markers, reducing cost of implementing fuel markers and the likelihood of detection by criminals.[13] The fuel marking detection system can be customized to sense a diverse absorbing, fluorescent, Raman or SERS-active dyes and markers, or to include concurrent detection through multiple optical methods.[14]

c) Track and trace technology

Supervisory Control and Data Acquisition (SCADA) has been adopted in the industry to enhance security in the supply chain, including monitoring and the use of different sensors that can detect leaks, taps, or vibrations arising from activity in fuel storage as well as in the vicinity of pipelines. The use of targeted aerial surveillance can serve as a support tool to maintain visibility on high-risk areas and as a deterrent to theft.[15] In this case, unmanned aerial vehicles (UAVs) or drones are an increasingly a cost-effective option.

9 Soud, D. (2020, May). Downstream Oil Theft: Countermeasures and Good Practices. Retrieved from https://www.atlanticcouncil.org/wp-content/uploads/2020/05/AC_OilTheft-Final-1.pdf

10 Asian Development Bank (ADB). (2015). Fuel-Marking programmes: Helping governments raise revenue, combat smuggling, and improve the environment. Retrieved from https://www.adb.org/publications/fuel-marking-programs

11 Soud, D. (2020, May). Downstream Oil Theft: Countermeasures and Good Practices. Retrieved from https://www.atlanticcouncil.org/wp-content/uploads/2020/05/AC_OilTheft-Final-1.pdf

12 Conroy, J. (n.d.). Technology progression in fuel marking. Retrieved from https://authentix.com/technology-progression-in-fuel-marking/

13 General Microtechnology &; Photonics. (n.d.). Authentication & Anti-counterfeit. Retrieved from https://www.gmp.ch/pdf/Authentication_spectroscopy.pdf

14 General Microtechnology &; Photonics. (n.d.). Authentication & Anti-counterfeit. Retrieved from https://www.gmp.ch/pdf/Authentication_spectroscopy.pdf

15 Soud, D. (2020, May). Downstream Oil Theft: Countermeasures and Good Practices. Retrieved from https://www.atlanticcouncil.org/wp-content/uploads/2020/05/AC_OilTheft-Final-1.pdf

This part of the report will now present possible solutions to the challenges posed by the risk scenarios described in the previous section. It describes the main aspects of the technology submissions, their relevance to the risk scenarios and possible advantages and limitations. Advantages and limitations usually refer to the technology categories in general. However, in some cases, reference will be made to some of the specific submissions we received, and this will be done solely in view of providing a specific example of technology application.

By analysing the above-mentioned submissions, it is clear that one of the key elements in this area is the use of markers for the fuel products, which can allow for authentication of the product and for its traceability. However, the way in which the technology can be applied in practice differs from one submission to the other. In the case of traceability, integration with blockchain technology is also foreseen, mainly in view of rendering the data inserted in the blockchain-based database immutable to increase security. Analytical tools are also used, to provide data analysis that allows users to obtain a full picture of the supply chain situation, while raising alerts in case of potential issues.

In general, the submissions showed that technology solutions have the capacity to provide improvements in the following areas:

- Manufacturing of counterfeits or 'cocktailing', chemically altering fuels so that they mimic hydrocarbon products assessed for lower tariffs.
- Diversion of authentic products to a destination market without paying excise duty by purchasing fuel in a State with relatively low tariffs and VATs and selling it in a neighbouring country with higher rates or misrepresenting a type of fuel taxed at a lower rate as a fuel taxed at a higher rate.
- Lack of intermediate technology checkpoint to avoid the insertion of illicit products within the supply chain.
- Smuggling of authentic goods and/or organizing a "cheap fuel trade" that is not compliant with the relevant customs standards and that poses a risk to consumer health and safety due to excessive emissions.

Interesting features of supply chain-based solutions proposed in this field include:

- Marking: Fuel marking based on different options and markers in view of making it possible to authenticate the product and subsequently track and trace it.
- Mobile field inspections: Technologies offer the possibility to have on-field portable inspection devices which greatly support the authentication work with rapid results.
- Insights: Analytical tools are used by these technologies to obtain insights on the status of the supply chain and raise alerts in case of need. These tools are based on different options and approaches.
- Multi-layer: Fuel Marking Programmes consist of sound technology (markers, analysers, information systems) that have been proven in implementations around the world. Moreover, they have repeatedly demonstrated efficacy at reducing illicit behaviour.
- Multiple detection: The technology enables sample analysis to detect compositional matching, material identification, adulteration and property prediction.

The integration with blockchain technology, also allows for the following interesting features:

- Immutability: The information about the product and its movement in the supply chain cannot be modified. This is achieved through the ability of a blockchain ledger to remain unchanged, unaltered and indelible.
- Auditability and accountability: Accountability is verified as a part of timestamps established by the blockchain system. This system allows every stakeholder to confirm whether the service operates in the intended way. If the product fails the verification process, then the stakeholders have proof of malicious behaviour which could be used to hold the responsible accountable.

- Transparency: Blockchain technology allows stakeholders to monitor the supply chain with openness, communication, and accountability. The stakeholders included in the chain can access the information at any point to corroborate the status of the products and the processes.

6.2.1 Fuel Marking Programmes and use of a Field Sample Manager

Technology submission 1

This submission aims at enabling regulators to monitor and enforce key quality measures in the downstream refined fuels industry, thus preventing illegal practices such as adulteration, tax evasion (back dripping of untaxed transit fuels into the local market), and unfair trading practices, while ensuring the delivery of high-quality fuel products to all consumers. The use of markers is an integral component of this solution, since their use also enables stakeholders to combat adulteration, dilution and smuggling in gas, diesel, crude, lubricants and liquefied petroleum gas. The use of markers can also distinguish between road fuel and subsidized fuel. The road and subsidized fuel products may be exactly the same from a chemical composition perspective. A fuel marker can be used as a "tax stamp" or "fingerprint" to authenticate the low tax fuel and validate (qualitatively or quantitatively) if it has been used as an adulterant into the regular taxed fuel.

The fuel markers can be overt or covert. Overt markers such as coloured dyes can be visually authenticated in the fuel. Overt dyes can be used to mark subsidized fuel and its presence can signal an adulterant in the road fuels. Coloured dyes are typically more economical but are more susceptible to imitation, replication or laundering. Covert markers, on the other hand, are dosed into the fuel at low rates and are invisible. Proprietary devices and methods of detection are utilized to detect the markers and determine if any adulteration has occurred. Several different types of covert markers can be used, including:

- - Recognition markers: they are captured by custom-matched antibodies and are then detected by a reader or test kit. Detection can be in the field (qualitative) or laboratory (quantitative). Industry accepted and commercially proven, these markers provide a substantial barrier to entry and use low marking levels.
- - Optical markers: they use covert organic chemicals that emit a detectable fluorescent light when excited and are visible only with a highly sensitive field detection device that provides near-instantaneous results.
- - Molecular markers: they exploit the unique mass spectrum of chemical entities, enabling lab-based qualitative and quantitative analysis using forensic lab devices such as gas chromatography mass spectrometer (GC-MS).

This submission also presents several options for fuel analysers, which include:

Portable Field Analyser: A portable field analyser which is designed to detect non-launderable and environmentally safe markers. This is a self-contained portable device which is also easy to use for on-field inspections. Results are instantly stored in a secure, cloud-based database.

Field Test Kit: Called Lateral Flow Device (LFD), it is a simple field test designed to give terminal operators and station owners quick results in the field to indicate if the fuel is meeting specifications.

Fuel Quality Analyzer: The fuel quality monitoring solution is designed to increase the speed of commerce and decision-making by reducing the time and cost of fuel quality testing and inspection. The solution uses field-based equipment and sophisticated chemometric modelling to provide near instant quality testing and a more robust, rapid, efficient and affordable alternative to traditional testing programmes.

Forensic Lab-Based Analyzer: This system isolates the different components of fuel, and quantitatively measures the forensic marker. This forensic Gas Chromatography-Mass Spectrometry lab-based fuel marker analyser allows governments and oil companies to confidently take action against those committing fuel manipulation and fraud.

The fuel quality monitoring solution can be used to reduce the time and cost of fuel quality testing and inspection. This option uses mobile, field-based equipment and sophisticated chemometric machine learning to provide near instant quality testing results and a more rapid and efficient alternative to traditional testing programmes. As more samples are processed, the system has machine learning capabilities to perform comparative logging of conformity lab results to field sample results, thereby increasing the accuracy of the field results to be near lab quality over an implementation period. In this regard, the fuel quality monitoring can provide relevant information, such as:

Compositional Matching: The material's relational composition and its change at different measurement locations in the same supply chain, which also confirms if the material's profile matches a known or predicted profile based on the product type and supply source.

Material Identification: It indicates if the sample includes unleaded low-octane or high-octane gasoline as well as diesel.

Adulteration: It can be used to prove if the fuel is adulterated, identifying the adulterant that was added, the level of contamination or the percentage of the adulterant with respect to the total sample.

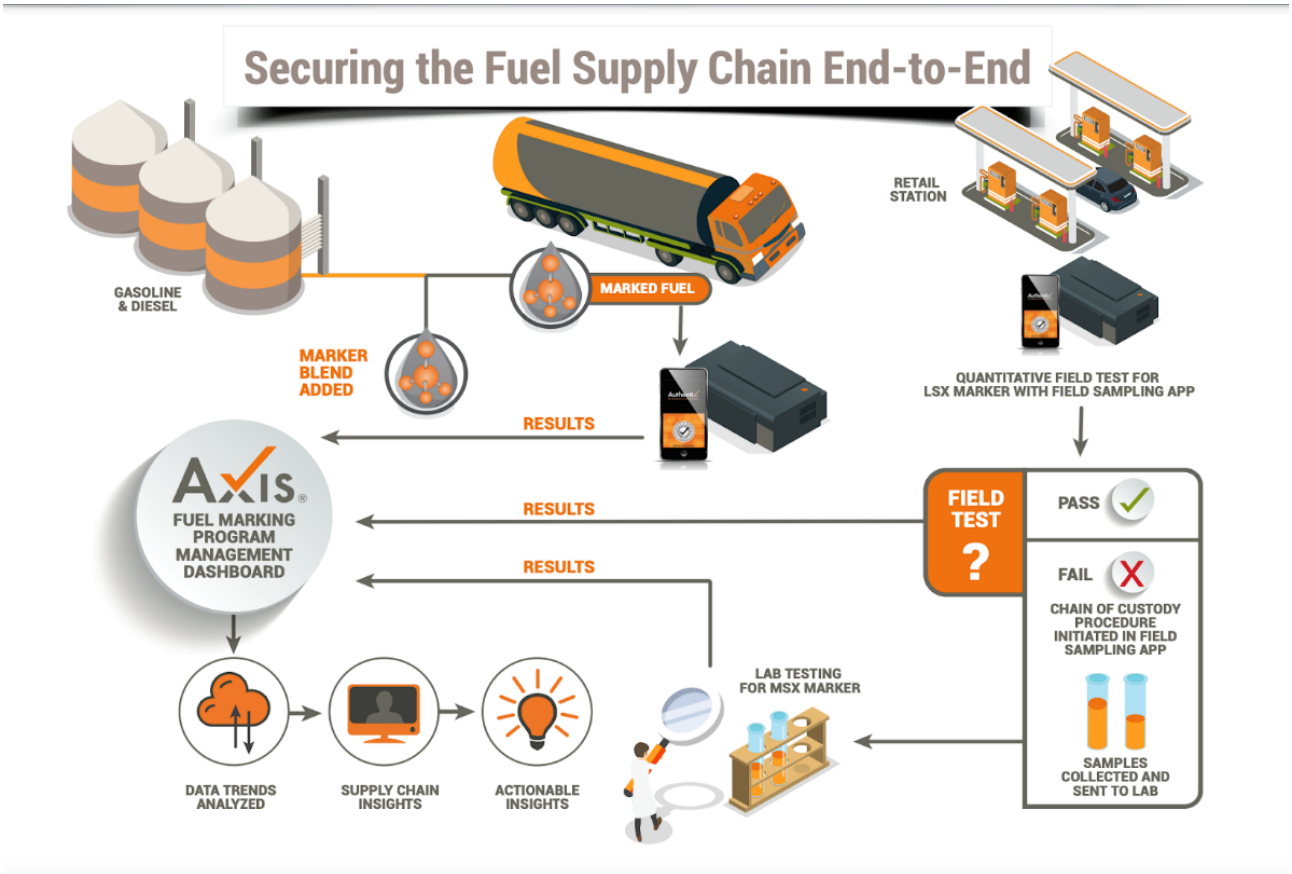
Property Prediction: Through analysis such as octane rating and sulphur content, it can determine if the fuel at a retail location matches the proper terminal location source.

The solution also has the capacity to integrate variable sample data results into a cloud-based information system, giving the user a single window for complete visibility into supply chain quality integrity and programme performance. Moreover, the technical solutions utilize GPS navigation and/or coordinates for logging sampling and testing of petroleum products throughout the supply chain. The adoption of traceability systems (such as IoT Sensors that can be deployed throughout the supply and distribution chain to track and trace petroleum products and monitor and report in (near) real-time) enables the tracking of in-transit products (equipping trucks with GPS locks and security seals at loading points). Additionally, Volume/Inventory Sensors for monitoring fuels in the bulk storage tanks report volume fluctuation activity in an integrated solution, which also includes points of sale data as well as data obtained from loading facilities.

An additional feature that can be added is blockchain technology, which can serve as an effective solution for detecting the falsification of paper-based transport documents for fuel. A blockchain could be used to carry the complete audit trail in the various production processes. For example, the specifications, batch, and quality control results for fuels and additives can be recorded as they are produced according to accredited suppliers' quality management systems. While a ledger provides a record of a series of steps or transactions involving digital data, the generation of data such as test results, certifications, or volumes of a product shipped between parties is also done in a way to ensure the data produced is authentic. As in other supply chain solutions, the key is to design the protocol by which the physical to digital transformation of data is robust to avoid accepting falsified data.

Submission received from Authentix.

This submission allows us to discuss the use of fuel markers as an integral component of a wider supply chain solution. The use of fuel markers is integrated into a fully-fledged system which also foresees the use of on-field analysers for rapid testing, several additional analysis methods to ascertain if fraudulent fuel has been inserted at a certain stage of the supply chain and to determine its exact composition. As seen in the description, the system is designed to target and identify different kinds of frauds and can be further enriched with the use of GPS tracking, volume sensors and blockchain technology to provide more control options on the one side while ensuring that information is safely stored in an immutable way.



Source: Authentix

For what concerns the fuel marking, it is based on secure molecular markers that are used to provide authentication. The system isolates the different components of fuel, and quantitatively measures the forensic marker. The advanced marking technology is environmentally friendly and difficult to compromise and tailored to protect all fuel types sold at the retail level. Rapid on-field checking is possible, and the solution uses mobile, field-based equipment and sophisticated chemometric machine learning to provide near instant quality testing and a more rapid, efficient and affordable alternative to traditional testing programmes. The submission affirms that samples can be taken from virtually any field location including import vessels, refineries, barges, terminals, depots and retail sites and then tested using the portable solution.

The data and results obtained from testing and analysis are integrated into a Field Sample Manager and subsequently into a cloud-based information system, which has the ability to capture variable data points from multiple sources and enables a holistic, single window for complete supply chain visibility and insights.

Source: Authentix

Traditional traceability technology is coupled with the use of IoT sensors, a cloud infrastructure and low-cost enterprise-grade software with machine-learning algorithms and data analysis capabilities. IoT Sensors can be deployed throughout the supply and distribution chain to track and trace petroleum products and monitor and report in (near) real-time (e.g. equipping trucks with GPS locks and security seals at loading points, volume/inventory sensors for monitoring fuels in the bulk storage tanks, single installation and maintenance of retail tank sensors with ability to report volume fluctuation activity integrated, Point of Sale data, and loading data).

The combination of all these elements results in the possibility to limit several risks highlighted by the two risk scenarios. Fuel can be marked with different techniques, especially covert markers (recognition markers, optical markers, and molecular markers), adopting authentication techniques that work on a product level and that are non-launderable. As described before, the unique marking is also highly effective in distinguishing between road fuel and subsidized fuel. The road and subsidized fuel products may be exactly the same from a chemical composition perspective. A fuel marker can be used as a "tax stamp" or "fingerprint" to authenticate the low tax fuel and validate (qualitatively or quantitatively) if it has been used as an adulterant into the regular taxed fuel. This enables stakeholders and authorities to verify the authenticity of the product. Additionally, the field inspections performed by portable devices provide a simple and fast tool to detect the infiltration of counterfeit fuel in the supply chain. Moreover, if traceability options are adopted, the movement of products can be monitored along the different stages in the supply chain. The integration of blockchain technology in data exchange and transactions in the physical world would protect the movements of the products in a digital platform that is transparent, immutable, and that provides accountability.

This can also directly impact the capacity that criminals may have to manufacture and distribute counterfeit fuel by 'cocktailing', chemically altering fuels so that they mimic hydrocarbon products assessed for lower tariffs. Diversion of authentic products to a destination market without paying excise duties will also be difficult since the chemical markers can allow for the recognition of specific types of fuels for specific markets or purposes and the same can be said for misrepresenting a type of fuel taxed at a lower rate as a fuel taxed at a higher rate. Along the same lines, the smuggling of authentic fuel and/or the setting-up of a "cheap fuel trade" that is not compliant with the relevant customs standards would be difficult considering the possibilities provided by the technology, which also responds to the need to have intermediate checkpoints to avoid the insertion of illicit products within the supply chain.

More concretely, we will now focus on the different stages of the criminal plan in the two risk scenarios. For what concerns risk scenario 1, the technology solution provides relevant tools to protect fuel and to detect infiltration of counterfeit products in the supply chain with the use of covert markers for authentication and field analysis with portable devices. Consequently, these technologies may play a role in uncovering the following steps of the criminal plan:

- Infiltrating/controlling refineries.
- Organizing a "cheap fuel trade".

The technology proposed by the submission focuses on the integration of covert marking as a secure authentication tool that protects fuel itself. Molecular fuel markers can be non-launderable, compatible with any fuel types (diesel, kerosene, gasoline, LPG, lubricants and crude). Moreover, these covert markers are stable at extreme temperatures -10C to 40C, have a shelf life exceeding one year, and have no impact on car engines or emissions, which act as a reliable mechanism to protect original products. The markers can be checked during field analysis with the portable devices which would detect "cheap fuel" or any other added substances that have been infiltrated to the supply chain. The mix of substances carried out in controlled refineries and their later distribution would be detected if they infiltrated the supply chain. If the additional features of blockchain-protected traceability and data exchange are added, then the infiltration can be immediately detected. However, it is important to consider that if the criminal organization controls the entire supply chain, then the only manner in which the counterfeit product can be detected is by performing the forensic analysis.

In the case of risk scenario 2, the authentication mechanism and the field analysis of fuel also play a relevant role in mitigating the risks presented in this scenario, especially in relation to the following steps of the criminal plan:

- Smuggling
- Fuel laundering.
- Mixing and distribution of adulterated fuel.

The molecular fuel markers have characteristics that combat laundering and adulteration, in particular:

- They cannot be laundered: Molecular fuel markers must be unique and cannot be imitated or purchased on the open market. Proprietary markers are confidential and virtually impossible to reverse engineer. If a solution utilizes patented markers, the composition of the markers is accessible to anyone who wishes to detect or replicate them. Tests can be conducted to demonstrate the robustness of the marker against laundering techniques such as heat treatment, clay, charcoal, acid wash, among others.
- Compatibility: Molecular fuel markers are able to be dosed at very low concentrations (parts per billion), remain stable in the fuel and have no impact on the chemical and physical properties of the petroleum products.
- Stability: Markers undergo testing to confirm long term stability in fuels. This typically involves testing at extreme temperatures between -10C to 40C.
- Shelf Life: Markers support a shelf life exceeding 1 year.
- No Impact on Engines/Emissions: Fuel markers exclusively composed of carbon, hydrogen, oxygen and nitrogen (CHON) – in exceedingly low concentrations (ppb), which are naturally occurring elements in refined fuel. These markers allow marked fuels to retain their performance specifications, emissions characteristics and environmental compliance. Markers are also compliant with the Stockholm Convention and international environmental laws. Fuel markers do not contain halogens, metals, metalloids or Persistent Organic Pollutants (POPs).

The nature of the markers and the fact that they cannot be laundered protects against this step of the criminal plan. In addition, the technology is used to ensure the authenticity of the product, protecting against mixing and/or adulteration, while the different types of field analyses act as reliable detection tools to recognize an infiltration of fraudulent fuel as soon as possible and stop its distribution. Smuggling could also be limited in the case in which the country in which the fuel has to be sold has a fuel control programme in place, since routine checks would identify that the imported fuel does not respect the established characteristics and does not have markers.

Summary table for submission 1: possible application to limit risks highlighted by the scenario

Scenario	**Applicability of the solution**
Scenario 1: Infiltration into the supply chain	
Step 1 – Political and economic infiltration.	
Step 2 – Infiltration into the legitimate supply chain.	In the case in which a marking method could be applied to crude oil.
Step 3 – Infiltrating /controlling refineries.	The technology solution offers diverse tools for analysis to corroborate the authenticity of fuel. The field-based equipment and chemometric machine learning can be used to obtain instant quality testing results, enabling the identification of lower quality fuel. Testing could be performed in almost any context. If the Fuel Marking Programmes (markers, analysers, information systems) are applied, authentic fuel can be protected from the infiltration of counterfeit products. If additional technology solutions, such as blockchain-protected platforms and traceability systems are used, then the risks are highly mitigated.

Step 4 – Organizing a "cheap fuel trade".	As described above, the use of covert markers is a tool to detect dilution, substitution or quality issues. The low-quality fuel that is infiltrated can be detected during the field inspections. Original fuel can also be protected with the adoption of IoT Sensors in the track and trace system to monitor the different stages of the product in the supply chain. Blockchain technology would protect the data exchange.
Step 5 – Infiltration into public procurement.	
Scenario 2: *Fuel laundering and mixing*	
Step 1 – Smuggling.	If the receiving country has a fuel control programme in place, this step of the criminal plan can also be limited since routine checks will identify the smuggled fuel.
Step 2 – Fuel laundering.	Markers can be designed to resist laundering techniques such as heat treatment, clay, charcoal, acid wash, among others. In addition, field testing can be used to identify if there has been an infiltration of lower quality fuel or that is not compliant to regulations and laws.
Step 3 – Mixing and distribution of adulterated fuel.	As previously described, the combination between markers for authentication and the use of field inspections for testing provide a tool to protect original fuel and detect counterfeit products. Data trends can also be analysed to have comprehensive insights of possible issues.

6.2.2 The Fuel Integrity Programme

Technology submission 2

The submission proposes the implementation of a Fuel Integrity Programme (FIP) intended as a turnkey solution to fight all aspects of fuel fraud. The FIP is a package of integrated services assuring the quality and traceability of the fuel products as they move through the supply chain using a marking technology. The FIP is composed of three main activities:

The marking of the fuel.
The inspection to determine the level of the marker in the products in the field and the collection of all data pertaining to these two processes.
The subsequent reporting.

The strategy proposed consists of adding a covert molecular marker to the taxed fuels so that they can be monitored and traced. Various technologies can be used for fuel marking; therefore, the most appropriate and optimized marker and detection equipment can be chosen to help the specific country achieve its policy and strategic objectives. The markers are invisible molecular markers, injected at very low concentration rates (few ppm), cannot be copied, laundered, removed or altered, they are compatible with any types of fuels, stable at extreme temperatures with long shelf-life and have no impact on car engines nor on emissions.

The solution proposes services which are fully coordinated and controlled to ensure their execution. Experts will deal with the marker logistics, security, stock management and transportation. Resources will be deployed for marking the fuels, collecting samples for inspection and testing management, the issuance of test reports and data analysis to provide intelligence and risk information about illegal activity.

The inspection process provides a quantitative determination of marker concentration in fuels that starts at 5% adulteration. Mobile field inspection units are usually installed in utility vehicles allowing for the performance of controls anytime anywhere. Fuel test results are available in a few minutes and transmitted in

real-time to the central database. Fuel test results are court admissible. No additive, no chemical reagent, no physical manipulation is necessary, guaranteeing normalization of the sampling. Fuel test results are protected, automatically transmitted and videotaped guaranteeing the sampling and test integrity. They can be performed through an on-field portable fuel analyser that can also precisely measure quality indicators (e.g. presence in the sample of Lead/Sulphur/Manganese).

Thanks to the network of experts that is set-up by this approach, checks can be conducted at designated sites to verify if taxed fuels have been diluted. In addition, the fuels can be tested at mines or other industrial sites where the possibility of fuel fraud exists, and the test results can be produced in a few minutes. The test detects, with a high level of accuracy, the levels of dilution or adulteration or simply the presence of the marker; this provides the authorities with evidence to support enforcement actions or legal prosecution.

Track and trace technology is also used along the supply chain, allowing for data analytics possibilities to perform mass balance calculations to detect frauds or diversion.

This submission also stresses the need to use technology in view of creating trust in the overall hydrocarbon ecosystem. This can be achieved by providing a system that can deliver trust in data for rapid and independent verification in real-time, secure communication between actors and stakeholders (human, systems or connected devices), trust in the business processes and in the identity of the actors (immutable records and process integrity) and functionalities developed for supply chains such as track and trace, event provenance and automated business processes.

Measures can be also put in place to protect the mass balance equation for any oil and fuel supply chain. Mass balance equation refers to volumetric balance of product moving between departure and arrival points. There is a measurable set of volumes (Ve) of substances (crude oil, refined oil, lubricants) that enter a complex supply chain or a subset of it. Most of the time, governments must reconcile the volumes to calculate excise tax or other tax incomes. They rely on data (De, Dx) recorded along the supply chain. Problems occur when the final volumes exiting (Vx) differ from the initial ones (Ve) after adjustment for expected losses (L1). Smuggling, counterfeiting, diversion and other manipulations affect the fuel volumes and can result in unexpected losses (L2).

$Ve = Vx + Lx$
$Lx = L1 + L2$

Reconciliation would become easier and more efficient if the volumes measured (V) could be protected by chemical fingerprints or in-product tracers and if, in parallel, data (D) from departure to arrival points could be authenticated, recorded and secured in a blockchain.

In addition, space technologies can be used for proof of origin as well as for track and trace.

There are 3 main applications for the fuel supply chain:

Proof of origin and mass balance: Images from drones and satellites can be used to link products to their place of origin. They make it possible to calculate production volumes, to anticipate and facilitate reconciliation, that is, check whether the quantity of products in circulation is bigger/smaller than the effective and verified original quantity.

Quality: Products' quality can be assessed using specific imaging technologies including hyperspectral cameras.

Monitoring and communication: Spatial monitoring of land areas or vessels at sea has been used for a while, in some cases to detect criminal operations. Together with proof of origin, it provides additional data to check mass balance along the supply chain. Secure communication and data exchanges between drones, satellites and ground IoTs are key for supply chain auditability.

As space data is used for continuous and ulterior controls along the supply chain, data and processes must be certified and timestamped in a blockchain to avoid falsification. Compressed spatial images with their embedded unforgeable signatures and localisations through quantum derived technologies represent the next generation of solutions to be used in this regard.

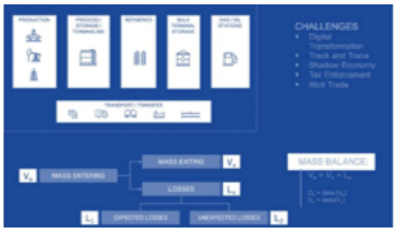
Submission received from SICPA.

This submission also focuses on the possibility to provide a fully-fledged solution which responds to a variety of issues concerning the control of the fuel supply chain. The core of the approach is the integration of various technologies to monitor the fuel, including markers to authenticate it, rapid on-field test analysis to verify its authenticity and to identify possible adulterations, data insights including mass balance verification related to the flow of goods moving from departure to destination to detect possible frauds, and the support of space technology and of blockchain. The combination of these elements forms the Fuel Integrity Programme (FIP), which, as seen in the description of the submission, provides a series of services and solutions to ensure the integrity of the fuel supply chain.

More specifically, the FIP is composed of three main activities; the marking of the fuel, the inspection to determine the level of the marker in the products in the field and the collection of all data pertaining to these two processes and the subsequent reporting. The markers used by this submission are invisible molecular markers, injected at very low concentration rates (few ppm), which cannot be copied, laundered, removed or altered. They are compatible with any types of fuels, are stable at extreme temperatures with long shelf-life and have no impact on car engines nor on emissions. The covert molecular marker will also be used for track and trace purposes, since its composition will be integrated in the information contained in the digital identity of the fuel which is transported and consequently tracked and traced. Verification between the information indicated in the digital identity of the product and the result of field analysis can quickly support identifying an illicit behaviour related to fuel smuggling, fraud or diversion.

In this regard, the mobile field inspection units are important to conduct rapid on-field checks and are usually installed in utility vehicles allowing for the performance of controls anytime anywhere. Fuel test results are available in a few minutes and transmitted in real-time to a central database. For the analysis, no additive, chemical reagent or physical manipulation is necessary, in view of guaranteeing the normalization of the sampling. Fuel test results are protected, automatically transmitted and videotaped guaranteeing the sampling and test integrity. Fuel test results can also be admissible in court in case of a trial as forensic evidence of illicit behaviour.

Data is stored in a blockchain-based database and the integration with space technologies allows for the possibility to improve the control of products along the supply chain and identify possible breaches. One of the ways in which this is achieved is, for instance, through the use of mass balance verification. Within this context, space technologies can be used for proof of origin as well as for track and trace purposes. They can be used as tools to create fully-fledged auditable supply chains. Images from drones and satellites can be used to link products to their place of origin. They make it possible to calculate production volumes, to anticipate and facilitate reconciliation, check whether the quantity of products in circulation is bigger/smaller than the effective and verified original quantity.



Source: SICPA

The use of a FIP could limit several risks highlighted by the two risk scenarios, since criminals would find it difficult, for instance, to chemically alter fuels so that they mimic hydrocarbons products assessed for lower tariffs. The practice of "cocktailing" would be identified by the technology along the supply chain as soon as a field test is performed. Along the same lines, diversion of fuel intended for different markets or different uses would be identified thanks to the different markers carried by the fuel on the basis of its destination or purpose, including in the case of fuel which is taxed at lower or higher rates. The FIP would also create a barrier towards the organization of a "cheap fuel trade" that is not compliant with the relevant customs standards of a given country and the system provides extensive monitoring possibilities for the legitimate supply chain of fuel, including at its intermediary points. For what concerns the specific application to the risk scenarios, in risk scenario 1, the technology solution can be used to detect the use of other substances in fuel and the alteration of its composition through the field inspections. The covert molecular marker and the use of a unique identity linked to the composition of fuel to trace the product

along the supply chain provide a useful tool to protect fuel, coupled with rapid on-field testing possibilities and the additional features provided by mass balance verification. Consequently, these technologies may play a role in limiting risks related to the following steps of the criminal plan:

- Organizing a "cheap fuel trade".
- Infiltrating /controlling refineries.

The infiltration of counterfeit fuel into the supply chain would be detected by an alert due to the mass balance equation protection and the use of blockchain. The systems will not recognize any correspondence with the identity of the fraudulent fuel given that its marker would not be recognized, and an infiltration would trigger an alert in the system. This is particularly relevant when the criminals produce a mixture composed mainly of gasoil and other added compounds to sell the product at lower prices in the "cheap fuel trade". The field inspection that is carried out to verify the authenticity of the product would be used to detect counterfeit fuel. Furthermore, in the case in which markers could be applied also to crude oil, the system could also prevent the smuggling of this product.

For risk scenario 2, the technology solution proposed can be used in the same manner to detect and avoid the infiltration of fraudulent fuel in the supply chain, especially in relation to the following steps of the criminal plan:

- Smuggling
- Fuel laundering.
- Mixing and distribution of adulterated fuel.

As previously mentioned, the application of the Fuel Integrity Programme (FIP) with its covert molecular marker and field inspections, and the adoption of the comprehensive analytical system formed by the use of blockchain technology and mass balance verification through space technology, can mitigate the risks of counterfeit fuel infiltration in the supply chain. In particular, the use of covert molecular markers adds an authentication mechanism that can resist a chemical treatment on the rebated fuel to remove dyes and covert markers while field inspections that can be performed to check the quality of the fuel and identify if fuel was laundered, adulterated or if it does not respect standards. In addition, infiltration into the supply chain can be detected with the use of the mass balance calculations and the integration with space technology adds additional time-stamped controls on the origin and quality of products, supporting the mass balance calculations themselves. For instance, in the case of step 1 of the criminal plan "smuggling", if the country of destination has a FIP in place, then the smuggled fuel could be identified when passing through checkpoints or during routine on-field inspections.

Summary table for submission 2: possible application to limit risks highlighted by the scenario

Scenario	**Applicability of the solution**
Scenario 1: Infiltration into the supply chain	
Step 1 – Political and economic infiltration.	
Step 2 – Infiltration into the legitimate supply chain.	In the case in which markers could be applied to crude oil, then the technology could also limit this step of the criminal plan.
Step 3 – Infiltrating /controlling refineries.	The solution can be used to detect when the criminal organization mixes cheap fuel in the sale of regular fuel since the composition of the legitimate fuel is linked as a biometric mark to create the identity of the product in the traceability system.

Step 4 – Organizing a "cheap fuel trade".	The technology solution can be used to detect the mixture composed mainly of gasoil and other added compounds that modify the final physical features of the product. The marking process in the Fuel Integrity Programmes (FIP) protects the composition of fuel and secures it in the traceability system. The use of the solution adds layers of security if compared to more traditional approaches, as the data analysis of flow mass balance of products, with the support of blockchain technology and the use of space technology to add additional time-stamped controls on the origin and quality of products and of their components as well as to support the mass balance calculations. Furthermore, the use of rapid portable on-field testing would make it possible to check the illicit fuel in case of infiltration.
Step 5 – Infiltration into public procurement.	
Scenario 2: Fuel laundering and mixing	
Step 1 – Smuggling.	The various elements of the technology would allow the identification of illicit fuel in the country of destination, provided that the latter has a Fuel Integrity Programme in place.
Step 2 – Fuel laundering.	As previously described, the technology solution can protect the supply chain from the infiltration of counterfeit products. The use of invisible molecular markers, injected at very low concentration rates (few ppm), cannot be copied, laundered, removed or altered, and are compatible with any types of fuels. Marking can later be checked through field inspection.
Step 3 – Mixing and distribution of adulterated fuel.	The technology solution can be used to detect adulterants and other added compounds that modify the final physical features of the product. The marking process in the Fuel Integrity Programmes (FIP) protects the composition of fuel and secures it in the traceability system. In addition, security is increased through data analysis of flow mass balance of products, with the support of blockchain technology and the use of space technology to add additional time-stamped controls on the origin and quality of products and of their components as well as to support the mass balance calculations.

6.2.3 Focus on documents' security

Technology submission 3

The submission provides a technology solution to mitigate risks related to the falsification of paper-based transport documents for mineral oils by using blockchain and secure immutable registries, including barcodes if used on containers for shipments. The paperwork used during the supply chain usually includes barcodes which are scanned each time that there is a change of ownership or location of the product, or when it is aggregated or de-aggregated from a batch of containers. Changes in ownership of the product and aggregation and de-aggregation of containers in larger shipments are recorded immutably in the blockchain. Cryptographic keys are exchanged, allowing the receiver to become the new owner of each item when authorised to do so by the sender. Each transaction is recorded as a new block.

A falsified or duplicated code that is introduced on false paperwork will not function in the blockchain because every code is linked to the previous supplier (holding an authorised cryptographic key) and to the next authorised owner after keys have been exchanged.

For tracing or checking historical information, a bridge-database can be used where the original unencrypted data resides. The bridge-database is in between the original scans and the blockchain and its contents are hashed in groups into the blockchain so that they become immutable. A trusted computing platform is used for secure interfacing to Enterprise Resource Planning (ERP) systems and other internal systems of manufacturers.

The location and time stamping can be used in different ways, e.g. to cryptographically sign codes so that they cannot be faked or to simply make a code unique by encrypting the time and location with the other data.

An additional blockchain function uses a balance ratio between submission and output that is recorded on the blockchain. This would require legitimate suppliers to log their shipments to the blockchain. If the amount of fuel and containers coming in was monitored (geographical satellite data would strengthen this), it should match a particular amount of packaged fuel output. If the same output is happening but with less authorised submission, this suggests an issue. The bridge database and blockchain solution with a trusted computing platform allows for a full and safe integration of ERP and other existing enterprise tracking and tracing software.

To transfer ownership of the product to the next supply chain point or end user, the sender must have both the authorised relationship with the next owner (via exchange of cryptographic keys) and a correct barcode to scan, which is traceable through the bridge-database linked to the immutable blockchain. Hence fake containers with fake or copied barcodes cannot be used.

Data from the bridge-database can be hashed together in different ways which provides higher information security for companies (e.g. there is no way anyone can see how many original data transactions they are making). If an attempt is made to change any entries in the bridge-database resulting in a change in the blockchain, warning information flagging this issue can be set up to first only notify those who need to know for security purposes, without alerting those earlier in the supply chain that their actions have been discovered.

The precise location and time data from satellite navigation and communications can be used (a) by locking this into data in a database and blockchain for current and historical tracking and authentication purposes, (b) to provide a unique cryptographic stamp for printed codes that makes each code unique. With advanced systems, the position data is many times more accurate than before, allowing such data to be highly reliable and even function around tall buildings. Without this space-related data, it would not be possible to track the origin and the location of products as they are packaged or repackaged.

Submission received from Nano4u.

This submission focuses on ensuring that documents related to fuel transactions, including barcodes affixed on containers, are original and properly secured and transmitted. It does not have a way to authenticate the fuel itself and it may have a more limited immediate risk reduction effect for some of the most relevant steps of the criminal plan identified by the two risk scenarios. For this reason, we did not insert a summary table at the end of the description. However, it is nonetheless interesting because it can work as an additional element improving the security of the supply chain by verifying that fuel transactions are authorized at any point of the supply chain by verifying related documents and containers. It is a similar approach used in the case of many other product categories where the focus of the protection is on the packaging and not on the product which is contained by the package.

The technology solution is based on a bridge-database that protects the data exchange related to ownership or location of the product container and related documentation between the different stakeholders in the supply chain. The solution uses blockchain to provide immutability, transparency and accountability. When a product is aggregated or de-aggregated from a batch of containers, the barcodes of the paperwork that is related to the movement of products in the supply chain is added to the blockchain. Each of the exchanges is recorded as a new block, linking every transaction and avoiding a falsification of the code. The barcode can be used to monitor the products since it contains information about them as well as location and time information from satellites. The infiltration of illicit products would be alerted during one of the documents' checkpoints because fake barcodes would not have cryptographically signed codes or would not have codes at all. Another feature which can contribute to securing the

supply chain is based on the need from legitimate suppliers to log their shipments to the blockchain. In this way, it would be possible to calculate the balance ratio between submission and output and record it on the blockchain. Therefore, if the amount of fuel and containers coming in was monitored it should match a particular amount of packaged fuel output, otherwise, if the output differs, this suggests an issue.

For what concerns the two risk scenarios, the technology solution would use this combination of elements to protect the movement of fuel containers along the different stages of the supply chain through the monitoring of barcodes and related paperwork (also authenticated via barcodes) and this approach may play a role in contributing to the securing of the supply chain from smuggling and unauthorized activities. However, if the criminal group directly infiltrated refineries (as in the case of the two risk scenarios) and is operating as a legitimate company, it will be difficult to spot the fraudulent fuel along the supply chain in the case in which there is no analysis of the fuel itself.

6.3 Conclusions

The fuel fraud risk scenarios presented some of the threats that can affect the integrity of the supply chain in this area. Thanks to research conducted by UNICRI and to the submissions we received from technology experts, it has been possible to assess how technology solutions may contribute to increase the security of the supply chain of these products, while limiting related criminal activities.

Existing technology solutions usually encompass one or several of these elements to protect the flow of products through the supply chain:

- **Authentication technology**: It is mainly based on using fuel markers to identify legally imported and tax-paid fuel, however there are new field-based and quite portable technologies entering the market capable of controlling illicit behaviour where traditional fuel marking is impractical. Fuel markers are chemical compounds that are frequently added to a wide variety of petroleum products to guarantee product integrity, protect against counterfeiting, adulteration, and tax fraud. There are different types of markers that can be used, and they can range from coloured dyes to specialized covert markers with particular detection methodologies. **Fuel markers** that blend in a covert manner with the fuel at very low concentrations provide the highest level of security for the entire supply chain, and even at that level of concentration, their presence or absence in fuel can be detected with easy-to-use analysers. Some advanced fuel markers carry a unique signature that can be detected only by proprietary readers and can be traced back to a specific point of origin. Fuel marking programmes have been developed to mitigate the risks of fuel fraud and in the case in which the fraud occurs, they can be used to identify the site within the supply chain where the fraud was committed, increasing accountability, limiting the threat of smuggling of illegal fuels across borders, and helping to identify illegal traders.

- **Field detection analysis**: Fuel marking programmes can also include field detection analysis of fuels, which is performed by portable devices to provide quick and frequent testing tools. Marking and analysing technologies can work as a multilayer integrated solution to mitigate risks related to fuel fraud. The **portability of devices** can also allow for the immediate connection of test results to encrypted, cloud-based storage systems. Field detection can be carried out through the use of different methodologies and analytical techniques like spectrometer systems. In the case in which fuel is laundered via chemical processing, heating or absorbent materials, a spectrometer can be used to detect the residual dye. Furthermore, the increased sensitivity of analytical techniques enables the use of lower concentrations of markers, reducing cost of implementing fuel markers and the likelihood of detection by criminals.

- **Track and trace systems**: They are characterized by the application of an identifier to the product or to a batch of products, which is then used to track movements throughout the different stages of the supply chain. Traceability options can also use **space technologies** as a proof of origin as well as for monitoring purposes and can be added to the authentication options. Supervisory Control and Data Acquisition (SCADA) has been adopted in the industry to enhance security in the supply chain, including **monitoring** and

the use of different sensors that can detect leaks, taps, or vibrations arising from activity in the vicinity of pipelines. The use of targeted aerial surveillance can serve as a support tool to maintain visibility on high-risk areas and as a deterrent to theft. In this case, unmanned aerial vehicles (UAVs) or drones are an increasingly cost-effective option.

- **Blockchain technology**: It has been integrated to traceability systems. It can connect the different parties in the supply chain that have not established trusted relationships with each other, by ensuring transparency. Blockchain stores every transaction or exchange of data that occurs in the network, reducing the need for intermediaries by providing a means by which all the actors in the network may share access to the same information, including what is added to the data, by whom, and the date and time of the submission.[16]

The submissions analysed in the report use different types of technology that are applied following various approaches. Technology is frequently combined to provide multiple levels of security and to achieve a combination of objectives. The submissions might use similar approaches to mitigate risks, however, they offer unique features that focus on the use of specific technology tools. In the case of fuel fraud, the submissions offered the following distinctive approaches:

- **Use of an integral approach to mitigate diverse risks**. This approach is adopted through the implementation of fuel marking programmes, field analyses and traceability systems protected by blockchain. Molecular fuel markers are integrated into a fully-fledged system which also foresees the use of on-field analysers for rapid testing. The markers can be checked during field analysis with the portable devices which would detect fraudulent fuel or any other added substances that have infiltrated the supply chain. Additional features such as GPS tracking, volume sensors and blockchain technology can provide more control options, while ensuring that information is safely stored in an immutable way. Submission 1 and 2 use this approach to mitigate the complex risks presented in the scenarios. Each submission uses different fuel markers, which have a unique composition, but due to the nature of the solution, must remain undisclosed.

- **Ensuring that documents related to fuel transactions, including barcodes affixed on containers, are original and properly secured and transmitted**. This different approach is presented by submission 3. The solution does not authenticate the fuel itself, limiting the immediate risk reduction effect for some of the most relevant steps of the criminal plan identified by the two risk scenarios. The technology solution is based on a bridge-database that protects the data exchange related to ownership or location of the product container and related documentation between the different stakeholders in the supply chain. Blockchain is used to provide immutability, transparency and accountability. When a product is aggregated or de-aggregated from a batch of containers, the barcodes of the paperwork that is related to the movement of products in the supply chain is added to the blockchain.

With specific reference to the risks that were highlighted by the risk scenarios, the following considerations can be made:

- The risk scenario presented some of the threats that involve multiple actors and interactions within various processes related to the fuel supply chain. **Criminal organizations are able to infiltrate the legitimate supply chain at various stages and by using complex techniques** that include: 1) the manufacturing of counterfeits or chemically altered fuels that mimic hydrocarbon products assessed for lower tariffs, 2) acquiring control over refineries and using illegal unloading premises, 3) diverting authentic products to a destination market without paying excise duties (often achieved by purchasing fuel in a State with relatively low tariffs and VATs and selling it in a neighbouring country with higher rates), 4) opaque trading using ghost companies, 5) using false documentation and invoicing, off-the-books transactions, tax evasion and money laundering, and 6) smuggling of authentic goods and/or organizing a "cheap fuel trade" that is not compliant with relevant customs standards and that poses a risk to consumer health and safety due to excessive emissions.

16 Accenture. (2019, January 15). Tracing the Supply Chain. Retrieved August 23, 2020, from https://www.accenture.com/_acnmedia/pdf-93/accenture-tracing-supply-chain-blockchain-study-pov.p

- Existing technology options have been developed to combat these threats with **multilayer security approaches that support the work of stakeholders in the supply chain and of national and international authorities**. In the case of fuel fraud, the implementation of fuel marking programmes provides a comprehensive tool that enables the secure authentication of fuel through marking and unique identification that can serve as a starting point for traceability systems. The field analysis performed with portable devices helps authorities and stakeholders detect counterfeit fuel, whereas the protection of data exchange is ensured with the use of blockchain technology. Government authorities and supply chain stakeholders benefit from the implementation of these technologies.

- **Supply chain technology producers are constantly looking for ways to innovate the modality through which products' integrity and security can be enhanced**. The analysis of the submissions we received testifies to this. Concrete examples include the integration of a unique identity of the product using its biometric composition which is in addition to the physical traceability in the fuel integrity programmes, mass balance equation, the development of portable devices to perform field analysis, and the protection of data exchange through the use of blockchain-protected systems.

- **Portable devices enable routine field analysis**. Relevant information can be obtained from their adoption, including compositional matching, material identification, possible adulteration, and they can be used for predictive analysis. They eliminate the need for taking a sample to the laboratory for the initial analysis, facilitating the constant verification of fuel and eliminating limitations related to the use of laboratories for examination.

- The use of an end-to-end multilayer approach can also be observed in the integration with **artificial intelligence** platforms. Data received from traceability systems that use IoT sensors can be processed in a cloud infrastructure and using low-cost software with **machine-learning algorithms** and **data analysis** capabilities. In this way, data analytics can provide useful insights to detect issues and to obtain a constant overview of the processes happening in the supply chain.

- The incorporation of **blockchain technology** for processes that were previously paper based as well as in traceability systems, protects the exchange of data between authorized stakeholders and guarantees immutability, transparency and accountability. In the case of the fuel supply chain, this integration can ensure that documents related to transactions, including barcodes affixed on containers, are original and properly secured and transmitted

- Existing **fuel markers have security features that can provide a high level of protection**. They cannot be laundered and contain proprietary markers that are confidential and virtually impossible to reverse engineer, they are able to be dosed at very low concentrations (parts per billion), remain stable in the fuel and have no impact on the chemical and physical properties of the petroleum products, they support a shelf life exceeding 1 year, and allow marked fuels to retain their performance specifications, emissions characteristics and environmental compliance. Markers are also compliant with the Stockholm Convention and international environmental laws.

- Some criminal activities highlighted by the scenarios cannot be limited by supply chain security technology. This has to be expected since the main purpose for which these technologies were developed is to protect the integrity of the supply chain and not to stop different kinds of criminal operations. The mitigation of these risks will necessarily **require actions and strategies implemented by law enforcement agencies to better understand how crime operates and how to monitor organized crime strategies to prevent these criminal activities**. It is for these reasons that some steps of the criminal plans in the risk scenarios were difficult to limit by supply chain technology solutions. This is the case, for instance, of step 1 "Political and economic infiltration" and step 5 "Infiltration into public procurement" of risk scenario 1.

- Following the previous point, an integrated approach between different technology typologies and options is needed to **support at the same time investigators and law enforcement agencies** on the one side, as well as **supply chain operators and consumers** on the other.

Annex 1
List of participants to SIRIO meetings on supply chain security

Organizations, Research Institutes, Universities and Industry

Advanced Track and Trace
Alitheon
Anglo American Platinum
Ashton Potter
Australian Nuclear Science and Technology Organisation – ANSTO
Authentix
BASF
Center of Applied Physics, Dating and Diagnostics of the University of Salento – CEDAD
Central Investigative Unit on food fraud - Italian Ministry of Agriculture
Community Plant Variety Office of the European Union – CPVO
Croplife
Dida
European Space Agency - ESA
Europol
Focos Food
Food and Agriculture Organization of the United Nations - FAO
German Federal Office of Consumer Protection and Food Safety - BVL
German Federal Police Office – BKA
Impala Platinum
Indicam
Institute of Physics of the Federal University of Rio Grande do Sul
International Atomic Energy Agency – IAEA
International Platinum Association - IPA
International Seeds Federation – ISF
Interpol
IPMI SECAM
Italian Carabinieri
Johnson Matthey
Malca
Materion
MKS Switzerland
Nano4U
Norilsk Nickel
Northam Zondereinde
Pierre Viaud Consulting
Portuguese Mint and Official Printing Office – INCM
Protected by AI
Royal Bafokeng Platinum
Scantrust
Securikett
Sibanie Stillwater
SICPA
Singapore Synchrotron Light Source
South African Police Services
Tecnoalimenti
UN Environment
Umicore
World Intellectual Property Organization

Independent experts
Christian De Vartaavan
Peter Bishop
Robert Schouwstra
Simon Dyson