15.12.21

A Collaborative Approach to Targeting Illicit Trade in Cross-border e-Commerce

WISE PERSON GROUP-CHALLENGES FACING THE CUSTOMS UNION

Dear Member of the Wise Person Group

Tobacco Europe AISBL[1] represents the common views of major European–based tobacco and nicotine products manufacturers such as British American Tobacco (BAT), Imperial Brands (IMB), and Japan Tobacco International (JTI).

We appreciate the work that Wise Person Group are doing with respect to challenges facing the customs union.

We would like to contribute to this work by proposing clarifications on certain issues which may cause concern for our members, if they are not appropriately addressed, and call for an increased collaboration between the private and public sector (EU customs and law enforcement authorities). This would:

- Achieve a more coherent and stronger Customs Union.
- Address the challenges brought about by the growth in e-commerce and the fight against criminal networks and fraud.
- Establish policies and solutions that are both effective in addressing illicit trade as well as safeguarding the EU citizens' interests and the economic competitiveness of EU businesses.

The annex paper attached presents several near-term solutions that follow the guiding principles of a collaborative mindset across jurisdictions and organisational siloes, common standards, interoperability between systems, a data-driven culture, and flexibility to learn and adapt. Solutions brought forward include the use of Inspection Feedback Loops, AI-Augmented Inspections, Social Network Analyses and Self-Assessments, Multiple-Source Data Integrations, and Data-Led Financial Crime Investigatory Capabilities.

These solutions consider the balance between compliance and trade facilitation. Through an increased collaboration with technology and trade experts from the private sector, authorities can drive coordination and trust across the trade ecosystem and create an environment that fosters industry innovation.

Our recommendations on the key topics are provided below:

1. An assessment of the impact of a decrease of the customs duty 'de Minimis' threshold: e-commerce created new distribution channels for illicit and counterfeit trade goods. A decrease of the customs duty 'de Minimis threshold' can contribute to the reduction of the illicit trade supply chains.

2. The 'wise persons' group should continue to monitor new technologies and make these known across the group. As experts in being able to determine these technologies their remit needs to evaluate new technologies that can support the EU in controlling the safety and security risks associated with e-commerce. These technologies may include blockchain and artificial intelligence (AI) solutions.

[1] https://www.tobacco-europe.eu/

Tobacco Europe AISBL
Avenue de Cortenbergh 120 - 1000 Brussels
EU Transparency Register: 1496873833-97
Registered number: 089 438 919

We would welcome the opportunity to meet at your convenience so that we can outline in more detail our recommendations. Should you need any additional information or clarification in the meantime, please do not hesitate to contact us.

We hope that the content provided in this submission contributes to the ongoing work of the Wise Persons Group, and we look forward further opportunities to comment and engage to support secure and efficient cross border trade.

Kind Regards,

On behalf of Tobacco Europe,

Nathalie Darge, Director

Tobacco Europe AISBL
Avenue de Cortenbergh 120 - 1000 Brussels
EU Transparency Register: 1496873833-97
Registered number: 089 438 919

1. The Challenges of Cross-Border E-Commerce

1.1. The Growth of E-Commerce in Europe

Global Retail e-commerce has grown significantly over the past years as consumers increasingly choose to shop online for the greater choice and value for money. E-commerce has created new opportunities for the global economy, creating new consumption behaviours, jobs, and methods of trade.

In the wake of the COVID-19 pandemic, consumers' reliance on e-commerce has surged following the global lockdown measures. Particularly in Europe, cross-border e-commerce has doubled in value between 2019 and 2021 from €108 billion to over €220 billion[1]. EU companies generate around 20% of their revenues from e-commerce and European cross-border transactions are predicted to grow at twice the rate of domestic e-commerce[2]. The Accenture Growth Analytics engine estimates a five-year growth rate of over 110% for all Consumer Packaged Goods (CPG) sold online in the EU from 2019 to 2024. The fastest growing CPG categories are *packaged food, soft drinks,* and excisable goods such as *tobacco*, with compound annual growth rates of 19.4%, 19.2% and 18.4%, respectively.

The changing trade environment due to the rapid expansion of cross-border e-commerce is impacting all EU Member States and a more inclusive, proactive and innovative collaboration between the public and private sectors is required to overcome the various challenges that go along with it.

1.2. Supply Chain Challenges in The Cross-Border Trade of CPGs

The proliferation of CPGs via e-commerce, coupled with the lockdown measures introduced by the EU Member States, have led to serious supply chain challenges. As EU customs authorities and national postal operators still rely on labour-intensive manual clearance of packages[3], they have been struggling to cope with the increasing frequency of shipments and temporary unavailability of staff. The current, largely manual, real-time clearing process is both inefficient and prone to human error, which makes it impossible for customs authorities to check every single consignment.

In addition, newly added complexities in regulations, such as the prioritisation of essential goods (i.e., COVID-19 vaccines and personal protective equipment (PPE)) over non-essential goods (such as CPGs), have put added pressure on EU customs authorities and postal operators. This is compounded by an inadequate integration between electronic customs declaration systems and postal services, which leads to significant delays and inefficiencies, effectively turning them into bottlenecks for cross-border trade.

The small, low-value consignments delivered by post or express courier are the most difficult for customs to monitor as the declarations currently rely on the sender to fill in the correct information. Poor quality of information, inaccurate data (due to misdeclarations) and the lack of adequate monitoring technologies in place have made the CPG trade, and particularly the trade in excisable goods, a target for fraud, counterfeiting and illicit trade.

Private entities, such as express couriers, have also been a target for fraud. According to the OECD, law enforcement agencies have indicated a significant growth in the use of both postal and courier streams by criminal networks as a delivery method for illicit trade[4]. A lack of information sharing with customs authorities leads criminal networks to exploit these weaknesses and use express couriers to move counterfeit goods.

1.3. Challenges for Excisable Goods Companies and Governments

Companies trading in goods with high excise duties, such as tobacco, vapour products, nicotine pouches, alcohol and energy, are a major target for illicit trade. Illicit trade can come from both the smuggling of products across

borders without the payment of taxes (contraband) and the illegal manufacturing of such products, often with illegally produced trademarks (counterfeit). The anti-competitive practices posed by the influx of contrabands and counterfeits (whether produced domestically or smuggled) lead to losses of excise, VAT, and import tax revenues for EU Member States as well as losses in profits for businesses.

EU authorities and the industry have been taking steps to collaboratively address this challenge. In 2010 for instance, EU law enforcement agencies have coupled their efforts with policies and technologies provided by the tobacco industry to reduce the number of cigarettes illegally entering the EU [5].

However, the reduction of smuggled cigarettes across EU borders was replaced by a growth in the illegal manufacturing of counterfeit cigarettes, possibly manufactured within the EU itself. In many cases consumers are tricked into buying identical looking but non-genuine products online. The KPMG 2020 Stella Report[6] has shown an 87% increase in counterfeit cigarette consumption in the EU between 2019 and 2020. Counterfeits now represent 30.1% of illicit consumption in the EU. This trend is thought to have been exacerbated by the COVID-19 pandemic, which reduced the opportunity for consumers to cross borders and buy cheaper products, therefore increasing demand for illegal locally manufactured cigarettes and those sent in smaller packages.

The Royal United Services Institute (RUSI) has revealed that criminal networks are increasingly adopting a low-volume, high-frequency approach to smuggling counterfeits, thereby minimising financial losses incurred in the event of a seizure[7]. As these products were not subject to the same (if any) level of quality or regulatory scrutiny during their manufacturing process, they pose significant health and safety threats to consumers. In addition, it puts EU businesses at a competitive disadvantage with a loss of market share and revenues, and makes governments lose out on custom duties and tax revenues.

The industry has experienced several instances whereby counterfeits have hampered its e-commerce operations for its Next Generation Products (i.e., NGP – vapour products and nicotine pouches) in the EU market. For instance, Italian customs officers have confiscated two illegal shipments of e-liquids in April 2021, posted from the UK[9]. These counterfeit devices, which involve inhalation, have not undergone the same rigorous quality control procedures as their genuine counterparts and pose serious health and safety hazards to unaware consumers. Unregulated and illegal e-liquids seized at borders often contain high traces of heavy metals, such as aluminium and lead, that exceed the legal limits.

Citizens expect under the EU's General Product Safety Directive (GPSD) that the products they purchase in the EU, including via e-commerce, meet all statutory safety requirements under national or European law. The circulation of these illicit products pose a reputational risk to both EU customs authorities and businesses. In many EU markets, the illicit trade in excisable goods account for over 20% of the market, effectively causing a significant loss of both company and tax revenues alike.

2. Existing E-Commerce Risk Management Plans and Initiatives

Several measures are currently in place to support risk management in e-commerce and the trade in excisable goods.

2.1. WCO SAFE Framework for E-Commerce

The *World Customs Organisation Security and Facilitation in a global Environment (WCO SAFE) Framework for e-commerce* is an instrument comprised of technical customs aimed at securing (without impending) international e-commerce by means of global standards, guidelines and recommendations[10].

The SAFE Framework advocates for a close collaboration between governments and e-commerce stakeholders (including customers and businesses) to develop fair and innovative solutions to the challenges of e-commerce.

As e-commerce is both data-driven and data rich, the SAFE Framework puts importance on the use of timely and accurate information to allow early risk assessments and rapid clearance of transactions with a minimum need for physical interventions.

As stated above, poor quality of information and inaccurate data have made excisable goods companies, customs authorities, and express couriers alike vulnerable to fraud and counterfeiting. To tackle this, the WCO SAFE Framework encourages the use of electronic interfaces between these stakeholders with harmonised messaging standards to facilitate pre-arrival and pre-loading (security) risk assessments. It also encourages governments to be proactive and forward-thinking by cooperating closely with the private sector to implement transformative technologies that help face emerging e-commerce challenges.

The SAFE Framework is not a binding instrument, but a model for customs administrations around the world to follow on a voluntary basis. One of the biggest challenges of mutual recognition is the need for interested countries to develop equivalent measures. WCO members who agree to implement the framework must ensure their measures are aligned with their trading partners[11].

2.2. US CBP Section 321 Data Pilot & Entry Type 86 Test

As part of its overall e-commerce strategy, the US Customs and Border Protection (CBP) set up the *Section 321 Data Pilot* in 2019[12]. The goal of this pilot is to improve the CBP's ability to identify and target high-risk e-commerce shipments, including for narcotics, counter-proliferation, and health and safety risks. It tests whether the transmission of additional advance data (i.e., beyond the data currently required for air, ocean, rail and road shipments), will enable more effective and efficient targeted screenings. The participants include e-commerce supply chain actors (Amazon, eBay, FedEx, DHL and UPS), technology firms (PreClear) and logistics providers (XB Fulfillment and BoxC Logistics). The CBP has extended the pilot to mid-2023.

In addition, the CBP also set up the *Entry Type 86 Test* in 2019 to test a new entry process for shipments. The test allows customs authorities and self-filers (owner or purchaser of low-value shipments) to electronically submit *de minimis* entries with a limited dataset through the Automated Broker Interface. This new entry type would provide greater visibility into low-value shipments and enhance import safety and security.

These two pilot initiatives have led to valuable lessons learned on how to cooperate with and formalise data sharing processes with multiple stakeholders. As of August 2021, the CBP has received data on 206 million transactions under the Section 321 Data Pilot and on 397 million transactions under the Entry Type 86 Test. These initiatives have led to more consistent enforcement processes for low-risk shipments, a reduced CBP workload thanks to the data sharing (e.g., from 6-day clearances to same-day clearances), fewer CBP holds and improved security[13].

2.3. EU Customs Risk Management Framework and Customs Action Plan

The *EU Customs Risk Management Framework (CRMF)*[14] was set up by the European Commission and Member States to establish the criteria for EU customs authorities to target illicit cross-border transactions. It proposes a harmonised application of customs controls by means of common risk criteria and standards, designated Priority Control Areas that are subject to reinforced customs checks, and a systematic exchange of risk information between customs authorities through a customs risk management system (CRMS). It also proposes a close customs-trade partnership through the use of Authorised Economic Operators (AEO). This concept aims to facilitate legitimate trade for economic operators, in exchange for their compliance with the customs legislation and transparent record keeping.

The European Commission also launched a *Customs Action Plan* to promote the implementation of the CRMF across the EU. It proposes several steps to improve the use of data and to promote compliance and cooperation

between the EU and partner countries' customs authorities. One of the key initiatives of the Action Plan is to establish a central *Analytics Hub* to ensure greater availability and use of data for customs purposes. The Analytics Hub will be built progressively[15]:

- End of 2021: use the data already available in the EU Customs surveillance database to support a uniform implementation of Union tariffs.
- End of 2023: expand the dataset to include data from COPIS (counterfeit goods seizures), AFIS (anti-fraud), and VAT payments.
- End of 2024: enable analytics on pre-loading and pre-arrival data provided by maritime, road and air carriers and logistics providers.

Another key initiative of the Action Plan is to *strengthen obligations on payment service providers and e-commerce platforms*. The goal is to have integrated data sharing between tax authorities and customs authorities by 2024, particularly on data that payment services providers (such as PayPal and Amazon Pay) will be obliged to share. This will be complemented with new customs reporting requirements.

2.4. EU Import Control System (ICS2)

Closely linked to the Commission's Customs Action Plan is the implementation of an *Import Control System (ICS2)*, a customs pre-arrival security and safety programme that aims to establish an integrated EU approach to reinforce customs risk management under the CRMF[16]. The ICS2 is expected to be completed by 2024 and will form the first line of protection of the EU internal market with its risk-based customs controls and data collected on all goods that will enter the EU.

The ICS2 implements a policy of multiple filing. While only carriers were required to provide an Entry Summary Declaration (ENS) in the past, the ENS is now mandatory for all postal operators and express couriers. This enrichment of the ENS dataset will help raise data quality and accuracy and provide essential information to customs authorities quicker. The ICS2 functionalities are rolled out over three release dates, whereby the first one took place in March 2021 (i.e., integration of the pre-loading datasets provided by postal and express courier operators).

2.5. EU Excise Movement and Control System (EMCS)

In 2010, the European Commission (DG TAXUD) set up the *Excise Movement and Control System (EMCS),* a computerised system for monitoring the trade in excisable goods for which the excise duties are yet to be paid. The system simplifies procedures for traders by collecting real-time information on the movement of these goods via electronic Administrative Documents (eAD), enhancing communications between the consignor, consignee, and customs authorities, and thereby creating a paperless administration[17].

2.6. EU Regulation on Electronic Freight Transport Information (eFTI)

Freight transport in the EU has increased by around 25% over the last 20 years and is expected to increase by 50% by 2050. A key challenge here are the current fragmented IT solutions in use and the resulting lack of adoption of electronic forms due to their incompatibility. Public authorities, transport operators and businesses still largely exchange information in paper format, which leads to poor quality of information and inaccurate data.

In 2018, the Commission proposed the *EU Regulation on electronic Freight Transport Information (eFTI)* to create a uniform EU legal framework with common datasets and procedures to process freight transport information[19]. The regulation would thereby oblige Member State authorities to accept electronic transport information to

facilitate the exchange and analysis of data. After a series of amendments, the Council and Parliament reached a provisional agreement on the proposal. The regulation will enter into force in August 2024.

2.7. EU customs duty 'De Minimis' threshold

De minimis shipment value rules have been set in place by EU to exempt consignments below a certain value threshold from custom duties and taxes. As such, customs duties are not due for e-commerce shipments imported from outside the EU of which the value does not exceed 150 euros.

The goal of this measure was to reduce the number of cross-border consignment inspections by authorities. However, with the growth of cross-border e-commerce, the growing number of low value consignments has put this practice into question as people started exploiting the de minimis regulation by under-declaring the value of goods.

We acknowledge that e-commerce has given new distribution channels for legitimate trade. However, the counterfeiters have also successfully exploited these channels- i.e. illicit trade goods are dispatched in small parcels with a value below the customs duty 'de minimis' threshold. There is little risk of detection for illicit goods, since the quantities of goods shipped in small parcels are intermingled with legitimately traded items. Therefore, the illicit trade implications should be considered before increasing the 'de Minimis duty threshold'.

In order to tackle this problem, we believe that a lower customs duty 'de Minimis' threshold can facilitate more targeted customs audits through better customs risk management.

2.8. Our Perspective on the Existing Plans and Initiatives

While these plans and initiatives have helped EU Member States improve their awareness and give the right priority to risk management in e-commerce and the trade in excisable goods, there is still a need to further strengthen national customs authorities' actual implementation of risk management activities.

Member States can enable more profound risk analyses by improving their data collection and analysis practices and collaborating more closely with the different public and private sector stakeholders in this ecosystem. According to a recent Public Service Workforce Survey conducted by Accenture (covering over 5000 respondents across five countries, including Germany) has revealed that 45% of workers in the borders, customs and immigration industry want their agencies to adopt new methods and processes for innovation and 39% seek greater opportunities for cross-agency/private-sector collaboration[21].

A closer cooperation with businesses can help authorities determine innovative solutions to address the many challenges to customs risk management and to develop a targeted approach to manage the growth in e-commerce traded goods. In addition, the current cooperation between customs authorities within the EU, as well as with non-EU trading partners, can be expanded upon even further to address the need for clearer rules and more effective procedures that deal with the growth in cross-border illicit trade via e-commerce, and particularly the trade in excisable goods.

An example of a collaboration initiative between EU and non-EU customs authorities is the *Smart and Secure Trade Lanes (SSTL) Pilot Project* – a coordinated Border Management initiative undertaken by DG TAXUD, and the EU Member States', Hong Kong's, and China's customs authorities. The goal was to facilitate data exchanges on maritime, air and rail trade between the parties and to set up coordinated cargo clearance procedures at both exporting and importing ends[22]. Through jointly developed secure communication channels, the participating customs authorities exchange each other's inspection findings and share risk information to help reduce lead times. The latest project phase (Ph3) worked on developing an automated data exchange process between the parties. However, research from the Erasmus University of Rotterdam has shown that the SSTL

project is currently still in its infancy and lacks a common way to make the goals of compliancy and trade facilitation measurable[23].

Finally, when looking for solutions a balance between compliance/enforcement and trade competitiveness/facilitation must be considered. Customs and border processes and procedures can form both tariff (i.e., taxes) and non-tariff barriers to trade, bringing about a 'burden' or 'cost' to businesses that adversely impacts cross-border trade. Authorities can actively contribute to driving down logistics costs and indirect costs to trade by establishing policies and platforms that enable improved digital access to services and information, drive coordination and trust across the trade ecosystem and create an environment that fosters industry innovation.

3. Deep-Dive into Solutions and Best Practices

This section explores potential solutions centred around a closer public-private sector collaboration that can help customs authorities tackle the challenges posed by the growth of e-commerce and the illicit trade of contrabands and counterfeits of excisable goods.

3.1. Proposed Near-Term Solutions

Cross-border goods movements have a *physical*, *information* and *financial* layer, each intertwined with one another. In order to effectively address illicit trade, authorities need to have a grip on all three. A range of existing and nascent solutions and approaches enable them to do so. These solutions follow the guiding principles of a collaborative mindset across jurisdictions and organisational siloes, common standards, interoperability between systems, a data-driven culture, and the flexibility to learn and adapt at pace.

3.1.1. Inspection Feedback Loop

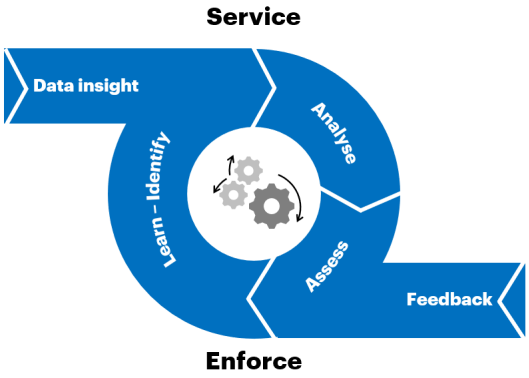
Currently, most of the risk intelligence in the EU happens at the Member State level. To address the challenges related to e-commerce and the excisable goods trade, we recommend Member States and DG TAXUD incorporating a real-time *Inspection Feedback Loop*. This entails using findings from physical inspections to recalibrate the existing risk-management rules and algorithms, both at the level of the Member States and DG TAXUD, and to evolve from a deductive to a prescriptive risk management model.

The centralised Analytics Hub the EU is currently building (see Section 2) is a step in the right direction. However, we recommend following the Circular Risk Management Process to ensure its correct implementation. The steps outlined below are to be repeated in a loop with a systematic recalibration of the risk management process from a linear to a circular process:

1. **Context:** Gather risk intelligence using a plethora of data sources available to Customs (e.g., declaration data, trader data, tax data) to gain a deep understanding of the stakeholders and trade context.
2. **Identify:** Identify for which purpose the gathered data can be used. Once the data sources are examined, they can be ingested into a data ecosystem out of which the risk intelligence team can derive insights for the development of new risk models.
3. **Analyse:** A decision engine then performs the risk analysis at the transaction, trader, and supply chain levels.
4. **Assess:** Based on the analysis, the engine assesses whether risk interventions are required.
5. **Control:** The decision engine generates recommended actions and notifies the relevant parties (intel officer, Member States, …). This feedback is internalised for future reference.
6. **Audit:** Post-Clearance Audits are performed by customs to verify the accuracy and authenticity of declarations and adherence to customs regulations. Lessons learned are taken from inaccurate clearances to evolve the risk model.

7. **Enforce:** Customs officers can take the recommended risk intervention/mitigation actions, choose an alternative action based on their expertise, or escalate to specialised teams. The actions undertaken, such as customs seizures and associated penalties, will be used to recalibrate the existing rules and algorithms.

Circular Risk Management Process



1. Blockchain Solutions

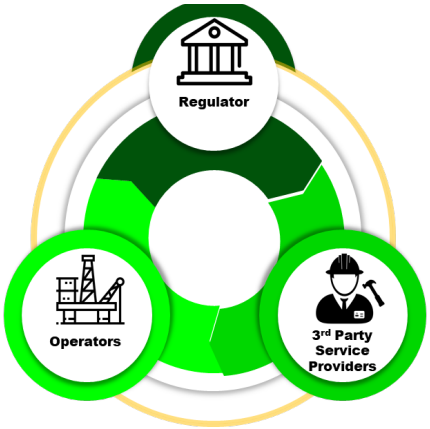
The European Commission is looking into modernising its customs administration systems with more efficient technologies. For instance, DG TAXUD has shown interest in modernising the EMCS with technologies such as blockchain[17]. This again raises the importance of the EU taking a central role in establishing a close collaboration with private sector actors who, with their technology expertise, can help realise this evolution.

The EU Commission is in a unique position to put in place a digital infrastructure that establishes trust and interoperability across networks. The EU Commission has recently launched its *Blockchain Strategy*[27], which supports blockchain on the policy, regulatory and budget fronts. The Strategy foresees building the *European Blockchain Services Infrastructure (EBSI)*: a blockchain infrastructure that will be interoperable with private sector platforms[28]. Amongst its use cases are the secure sharing of data amongst EU authorities on VAT identification numbers and import one-stop-shops amongst customs and tax authorities. EBSI would provide the EU with the comprehensive insight on trade supply chains required for intelligent risk management and trade facilitation.

Blockchain solutions can provide multiple advantages to the stakeholders involved:

1. **Trust**: Instead of each stakeholder (businesses, customs authorities) having to keep a separate database, blockchain uses a distributed ledger in which transactions are recorded concurrently in multiple locations and in which each stakeholder with permissioned access can consult the same information. It also keeps record of the entire transaction history between the parties, thereby eliminating any vulnerabilities to fraud.
2. **Decentralisation**: There is no central actor in charge of facilitating information sharing through blockchain solutions, as data is shared within an ecosystem of parties.
3. **Cost reductions**: Blockchain creates efficiencies by reducing the need for middlemen (e.g., vendors and third-party providers) for the processing of data, and it facilitates reporting and auditing.
4. **Security and privacy**: With blockchain, records can't be altered and are encrypted end-to-end. Robust access permissions are used, and information is stored across a network of computers, which makes it difficult for non-allowed individuals to get access. This helps put a stop to fraud and unauthorised activities.

Shared ecosystem vision



Industry blockchain initiatives exist, but often struggle to move beyond the pilot stage due to a lack of a clear governance structure. According to a study by the European Parliamentary Research Service (EPRS), several blockchain initiatives (including a pilot blockchain project undertaken by a European Customs Authority and industry experts, as well as other use cases in customs processes, trade finance and logistics), have revealed the need for the stakeholders involved to articulate a shared ecosystem vision that encompasses business, technology and operations[29]. This can only be realised with a closer and more pro-active government involvement, which will ensure business- and technology-related decisions are taken appropriately and swiftly.

Blockchain solutions have also been explored to tackle illicit tobacco supply chains. The currently used tax stamps solution is outdated and presents a series of challenges affecting actors across the supply chain. To reduce illicit trade and regain legitimate government revenues, a blockchain platform can optimize supply chain visibility by:

- Removing the need for physical shipping documents with a reduction of data duplication and operating costs while increasing supply chain visibility.
- Connecting end-to-end value chains and bringing about increased visibility that will help tackle inefficiencies by eliminating costs and delays with third party players and enable customs authorities to execute more targeted interventions and seizures[30].
- Fighting illicit trade on excisable goods to reduce the government's tax gap, without damaging industry or trade.

3.1.2. AI-Augmented Inspections

Surveillance systems have evolved, with the data captured by today's systems being far too large for humans to manage efficiently. Image and video analytics software are created to analyse the constantly growing volumes of video feeds and help resolve and prevent incidents. With these analytics software, customs authorities could benefit from more efficient surveillance systems, highly intelligent surveillance capabilities and better use of human security and management staff.

AI-Augmented Inspections enable customs authorities, law enforcement agencies and businesses to:

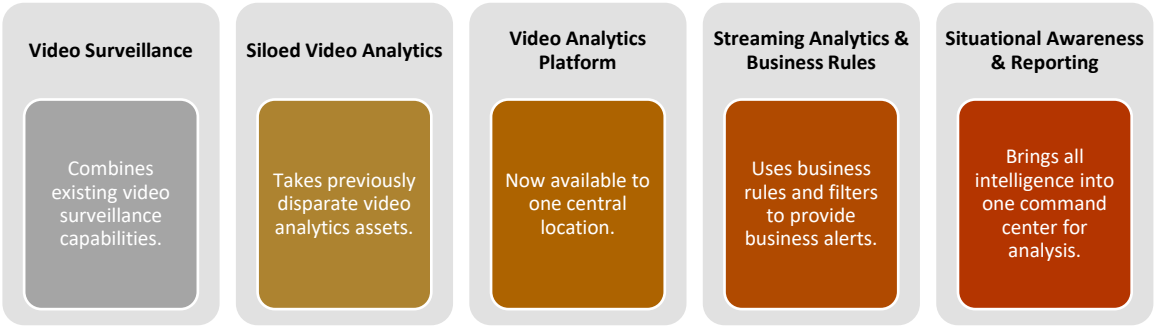
- Gain real-time insight into operations and interactions.
- Take appropriate action based on alerts generated by deep analytics and AI.
- See business processes from a new perspective.

- Leverage granular "ground truth" data for longer-term trend analyses.

AI-Augmented Inspections may use data on known characteristics of counterfeit products (e.g., from COPIS) and compare these with data on genuine products to train algorithms to identify potential counterfeits in images and video footage from X-ray scanning or physical inspections, such as when a border officer opens a package that had been flagged for inspection.

A case in point are Video Analytics Platforms, which apply analytics to data received from video feeds to deliver insights that support fast and accurate decisions. With these tools, customs authorities can take fast and accurate decisions on intervention/seizure actions based on alerts generated by Deep Learning (Machine Learning and AI). They allow authorities to see business processes from a new perspective, gain real-time insight into operations and interactions so they can take immediate action, and leverage granular "ground truth" data for longer-term trend analyses. The more information these solutions process, the more targeted the recommended actions can become via Deep Learning[31].

Five operational pillars, one comprehensive solution



Case study: Automated Comparison of X-ray images for Cargo Scanning (ACXIS)

Today, analytics in cargo scanning are focused on comparing transport declarations with X-ray imaging. However, under the ACXIS project[32], research is being done with the Dutch and Swiss Customs authorities into integrated solutions that provide automation, information exchange between customs authorities, and computer-based training modules for customs officers.

The project uses *Automated Target Recognition (ATR)* functions, enabled by Machine Learning, to analyse X-ray images of containers and detect targeted goods (such as cigarettes, weapons, and drugs). ATR transforms the X-ray images into manufacturer-independent formats through geometrical and spectral corrections and are stored into a database along with the user feedback. In addition, simulation training software is being developed to improve the image interpretation competency of customs officers.

The preliminary results show improved detection of anomalies in containers (including detection of cigarettes). However, further developments are required with a larger dataset to increase the detection probability of firearms and to further improve customs officers' efficiency and effectiveness at border checkpoints.

3.1.3. Multiple-Source Data Integrations

As the world becomes more connected, the information that *can* be checked by EU customs authorities is being outpaced by what *should* be checked. The risk of overlooking key information increases as well as the exposure to emerging threats. There is therefore a need for greater digital literacy with authorities and for the adoption

of new, highly specialised skills and tools to protect cross-border trade and infrastructures from money laundering, fraud, cybercrimes and terrorism.

Modern risk management approaches require a focussed methodology centred around a data-driven network. Highly relevant sources of data include regulatory/voluntary trade and logistics data, customs in-house data, national authorities' data, and EU and global community data. These data can feed into supply chain data networks (e.g., TradeLens, NxtPort), national customs and police systems, and EU systems to form interpretable goods, logistics, financial and economic operator data. In addition, these approaches are required to address criminal networks' use of encrypted communication platforms, dark web marketplaces and crypto payments. These new sources of information can only be unlocked and interpreted by modern analytics skills and tools.

Through the EU Customs Action Plan, DG TAXUD has already set out to establish a central Analytics Hub to collect, analyse and share customs data that support critical decision-making and help identify weak spots in the EU's external borders. The Analytics Hub currently uses data from the EU Customs surveillance database and will be using data from COPIS (counterfeit goods seizures), AFIS (anti-fraud), and VAT payments by the end of 2023. While it focuses on safety and security, we recommend considering a broader scope of data sources to further enrich the EU's data-led investigation capabilities.

1. Collaborations with surveillance cyber security authorities

For instance, the US Customs and Border Protection (CBP) agency has set up a Data Science Division to improve its border monitoring capabilities by leveraging technology for quicker security risk detections. They intend to leverage data retrieved from ground sensors, video surveillance systems and aerial platforms and to use Machine Learning capabilities for algorithmic targeting and situational awareness improvements[33]. Thanks to these efforts, the CBP will be able to classify risks much quicker, to identify what's coming before it gets to the border, and to be able to take the necessary actions.

As such, EU customs authorities' risk management efforts can be enhanced by engaging in:

- Web crawling and dark web investigations of online communication platforms and marketplaces to identify risk (e.g., use of certain words in posts and articles) and persons of interest (e.g., based on watchlists) in connection to actors involved in cross-border trade transactions
- Hacking into encrypted communication platforms allegedly used by criminal actors.
- These added sources will enable advanced analytics and simulation modelling to improve the current risk identifications and rules generation processes.

These capabilities exist at the national level but are fragmented and usually operate beyond the cross-border trade context. The EU therefore needs to establish a central EU capability with a focus on cross-border trade to complement and collaborate with the existing national capabilities. In addition, the EU could collaborate with EU industries for their technology expertise, thereby enhancing the customs staff's digital literacy and ensuring the correct implementation of surveillance technologies.

2. Collaborations with Payment Services Providers

Engaging with payment providers to access payment information of online purchases, will enable customs to execute, consolidate and audit payments easier, ultimately facilitating trade. It helps identify areas of risk and collecting customs and other taxes at the point of purchase. In the EU Customs Action Plan, DG TAXUD has already put forward plans to introduce new customs reporting requirements for online payment provider platforms such as PayPal and Amazon Pay. The new payment data reporting obligations on payment service providers, set in Council Directive (EU) 2020/284[34], will be imposed as of 1 January 2024.

3. Data-intelligence platforms

As the financial crime landscape continues to evolve, businesses are pioneering the use of data science and Artificial Intelligence to protect themselves against financial crimes. Ripjar's Torch is an example of a scalable platform that allows entities to better identify, monitor and mitigate financial crime risk by means of Machine Learning and AI-driven platforms. The platform allows entities to fuse, enrich, automate, and analyse any source of data, which can then be used to automate key processes and facilitate smarter investigations. The Torch platform has been used by compliance officers across global banking, capital markets and insurance institutions for anti-money laundering purposes.

Data-intelligence platform use cases

There are also other solutions in the market that leverage advanced technologies to map out financial crime, such as the Oracle Financial Services Crime and Compliance Studio, Quantexa Syneo Financial Crime and Fraud solution, Comarch Anti-Money Laundering software, etc. However, when aiming for large-scale implementations of these novel technologies, it is important to appeal to entities with deep industry experience and proven track records of next-gen technologies to facilitate these implementations. For instance, Royal Dutch Shell[35] has partnered with both Ripjar and Accenture in March 2021 to implement Ripjar's automated risk assessment platform.

4. Cryptocurrency Analytics

Cryptocurrencies have become the coin of 21st century cybercrime. EU law enforcement agencies and customs authorities must be able to navigate the complexities of analysing cyber and crypto transactions in the illegal trade of excisable goods, tracking actors across jurisdictions, and fusing data with other relevant sources.

Connecting cryptocurrency analytics across different sources of data will help build a more complete picture behind indications of cryptocurrency crimes. Possible data sources to be fused are the flows of payments, anti-fraud data, types of drugs being smuggled and past seizures of counterfeit goods.

Customs authorities will not be able to solve cybersecurity and challenges alone and will need to expand and rethink partnerships with the private sector and other areas of government (e.g., EU law enforcement agencies or European Union Agency for Network and Information Security) to adopt such data-led investigatory capabilities.

3.1.4. Trusted Supply Chains

Building upon the use of AEOs under the EU Customs Risk Management Framework (CRMF) to facilitate legitimate trade for economic operators, we propose customs authorities to expand the notion of *trusted traders* to *trusted supply chains.* This involves two key aspects:

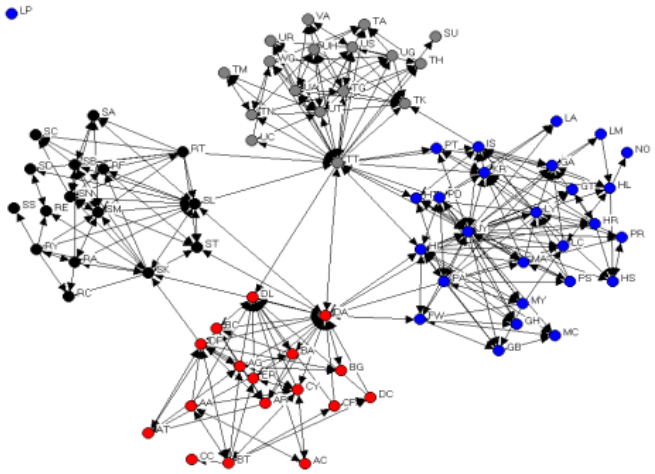
1. **Monitor not only the compliance of a singular economic operator, but the compliance of entire supply chains.**

Most customs agencies' current risk management practices are focused on Transaction and Trader Risk. For this solution, we need to look beyond this – i.e., towards the end-to-end Supply Chain Risk. Data analytics methods, such as Social Network Analysis (SNA), use networks and graph theory to understand social structures and can use the data sources available to Customs (e.g., declaration data, trader data, supply chain data, and other

public/private data) to gain in-depth insights on traders and the supply chains they operate in. These insights then provide the possibility to determine a risk level to the supply chain.

In the context of *interoperability*, the larger the dataset used for SNA, the more accurate the results. As such, this method can be enriched by including data from other EU and Member State systems, such as counterfeit data from COPIS, known criminal identifications from AFIS VAT payments data, data from the Union Customs Code (UCC) systems (expected to be fully realised by end 2025), and data from other verified EU authorities.

Graphical representation of a social network



Another example related to trusted supply chains is the Global Business Identifier (GBI) initiative[26] launched by the CBP. The goal of this initiative is to identify and track principal players in the global supply chain by creating unique identifiers that represent a company's primary legal entity and ownership, its specific business, its global locations, and the supply chain role it takes up within a transaction. The system has facilitated the identification of high-risk shipments.

2. Enable actors involved in trusted supply chains to self-assess risk in their supply chains.

Under the Union Customs Code (UCC), Autonomous Economic Operators (AEO) can be given the possibility to perform certain customs formalities and assessments that are normally done by customs authorities[36]. When authorised, these self-assessments would allow traders to perform risk assessments and verify their compliance with the customs regulations. Authorised traders perform these self-assessments based on the guidelines specified by customs authorities, and under their supervision. Traders thereby determine the amount of import and export duty payable and pay it within ten days. In case of infringements, Member States currently can impose penalties that seem appropriate to them, which can be used to cover the administrative burden the infringement has caused. As these penalties differ in nature and severity depending on the Member State, there is still room for improvement across the EU in the harmonisation and uniform application of customs legislation.

The prerequisite for being authorised to self-assess should involve the traders' ability to monitor risk across their end-to-end supply chain. Looking back at the Dentsu example where businesses have the capabilities in place to collect data from across their supply chains (and the technical capabilities to process such data), these businesses are better placed than customs agencies to interpret this data and monitor risk and compliance. These businesses however still need to collaborate with customs to ensure the definitions of risk and compliance are in line with current policies.

3.2. Our Future Vision

This Intertwining of physical and digital realms will greatly impact e-commerce supply chains in the future. The world of the Internet of Things (IoT) is evolving rapidly. Once the cost of embedding chips in goods becomes low enough, most products will have an IoT component, and this will massively improve the ability to track and trace products and ascertain their genuineness. With the number of IoT connected devices estimated to be around 50 billion by 2030[37], customs authorities will have to be able to navigate the massive web of interconnected devices and use it to its benefit.

Just like businesses, the customs authorities will have to invest in IoT technologies to drive operational efficiently, enhance EU traders' experience and enable new value-added services. Customs authorities will need to increasingly work together with industry representatives and technology experts to modernise, accelerate the digital transition, and develop policies that properly guide and manage Smart Supply Chains. Upcoming communication, monitoring and inspection technologies will help manage the proliferation of e-commerce and accompanying financial, counterfeit, compliance, safety, and security risks.

To tackle the challenges of illicit trade (particularly surrounding excisable goods), the public and private sectors must collaborate on further harmonising and strengthening standards, as well as improving the digital literacy of customs authorities' staff by investing in and acquiring highly specialised skills and tools. Indeed, the mission of customs is expanding with an increasing demand for greater facilitation and acceleration of legitimate trade, protection of EU citizens against financial and non-financial risks, as well as the protection of EU businesses against fraud. Taking the right actions now will ensure that customs authorities will be able tackle the challenges of the future.

4. Concluding Remarks

There are currently a number of risk management plans and initiatives in place that help give customs authorities the right priorities to risk management in e-commerce and the trade in excisable goods. However, there is a need to further strengthen national customs authorities' actual implementation of risk management activities.

The industry calls for an increased collaboration between the private sector (businesses) and public sector (EU customs and law enforcement authorities). Together, they can:

- Achieve more coherent and stronger Customs Union.
- Address the challenges brought about by the growth in e-commerce and the fight against criminal networks and fraud.
- Establish policies and solutions that are both effective in addressing illicit trade as well as safeguarding the EU citizens' interests and the economic competitiveness of EU businesses.

The industry presents several near-term solutions that follow the guiding principles of a collaborative mindset across jurisdictions and organisational siloes, common standards, interoperability between systems, a data-driven culture, and flexibility to learn and adapt. The solutions brought forward included the use of Inspection Feedback Loops, AI-Augmented Inspections, Social Network Analyses and Self-Assessments, Multiple-Source Data Integrations, and Data-Led Financial Crime Investigatory Capabilities.

These solutions consider the balance between compliance and trade facilitation, to avoid customs and border processes and procedures of forming tariff and non-tariff barriers to EU trade. With an increased collaboration with technology and trade experts from the private sector, authorities can drive coordination and trust across the trade ecosystem and create an environment that fosters industry innovation.

References

1. OECD, "Connecting Businesses and Consumers During COVID-19: Trade in Parcels", Jul 2020, link to article: Connecting Businesses and Consumers During COVID-19: Trade in Parcels (oecd.org)

2. Statista, "E-commerce in the European Union – statistics & facts", Oct 2021, link to article: E-commerce in the European Union – statistics & facts (statista.com)

3. World Customs Organization, "WCO Study Report on Cross-Border E-Commerce", Mar 2017, link to report: wco-study-report-on-e-commerce.pdf (wcoomd.org)

4. OECD, "Role of Small Shipments in Illicit Trade and Its Impact on Enforcement", 2018, link to report: Role of Small Shipments in Illicit Trade and its Impact on Enforcement (OECD-ilibrary.org)

5. European Commission, "Contraband and counterfeit cigarettes: frequently asked questions", Jul 2010, link to webpage: Contraband and counterfeit cigarettes: frequently asked questions (ec.europa.eu)

6. KMPG, "Illicit cigarette consumption in the EU, UK, Norway and Switzerland – 2020 Results", Jun 2021, link to report: Illicit cigarette consumption in the EU, UK, Norway and Switzerland – 2020 Results (stopillegal.com)

7. Babuta, A., Haenlein, C., Reid, A., "E-Commerce, Delivery Services and the Illicit Tobacco Trade", Apr 2021, link to paper: E-Commerce, Delivery Services and the Illicit Tobacco Trade (rusi.org)

8. Suddeutsche Zeitung, "Customs ensures untaxed tobacco product by mail", Jan 2021. Link to article: Kriminalität - Dresden - Zoll stellt unversteuerte Tabakwaren im Postversand sicher - Panorama - SZ.de (sueddeutsche.de)

9. ADM Lombardia, "Comunicato Stampa, Milano 1: Scoperte Spedizioni di Liquidi da Inalazione di Contrabbando Porvenienti dal Regno Unito", Apr 2021. Link to article: 44055dfa-b781-4830-8dbc-e795316fb11b (adm.gov.it)

10. WCO, "Cross-Border E-Commerce Framework of Standards", Jun 2018, link to framework: Cross-Border E-Commerce Framework of Standards (wcoomd.org)

11. Aigner, S., *"Mutual recognition of Authorised Economic Operators and security measures"*, Mar 2020, link to article: Mutual recognition of Authorised Economic Operators and security measures (worldcustomsjournal.org)

12. CBP, "CBP and Trade Partners are Taking Action to Secure eCommerce Supply Chains", Jan 2020, link to webpage: CBP and Trade Partners are Taking Action to Secure eCommerce Supply Chains (cbp.gov)

13. WCO, "USCBP latest initiatives to strengthen enforcement capacity for e-commerce shipments", Oct 2021, link to article: USCBP latest initiatives to strengthen enforcement capacity for e-commerce shipments (mag.wcoomd.org)

14. European Commission, "Customs Risk Management Framework (CRMF)", Oct 2021, link to framework: Customs Risk Management Framework (CRMF) (ec.europa.eu)

15. European Commission, "Taking the Customs Union to the Next Level: a Plan for Action", Sep 2020, link to communication: Taking the Customs Union to the Next Level: a Plan for Action (eur-lex.europa.eu)

16. European Commission, "Import Control System 2 (ICS2)", n.d., link to webpage: Import Control System 2 (ICS2) (ec.europa.eu)

17. European Commission, "Excise Movement and Control System (EMCS)", n.d., link to webpage: Excise Movement and Control System (EMCS) (ec.europa.eu)

18. EUR-Lex, "Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the on the application of Directive 2014/40/EU concerning the manufacture, presentation and sale of tobacco and related products", May 2021, link to report: Report on the application

of Directive 2014/40/EU concerning the manufacture, presentation and sale of tobacco and related products (eur-lex.europa.eu)

19. European Parliament, "Regulation on electronic Freight Transport Information", May 2018, link to article: Regulation on electronic Freight Transport Information (europarl.europa.eu)

20. European Commission. "Modernising VAT for e-commerce: Question and Answer", Dec 2017, link to webpage: Modernising VAT for e-commerce: Question and Answer (ec.europa.eu)

21. Accenture, "Border Services Survey on Future Workforce", Feb 2021, not publicly available.

22. Hong Kong Customs, "Hong Kong Customs achieves successes on SSTL Pilot Project and AEO Programme in facilitating trade", Jul 2016, link to article: Hong Kong Customs achieves successes on SSTL Pilot Project and AEO Programme in facilitating trade (customs.gov.hk)

23. Erasmus Universiteit Rotterdam, "SSTL Ph3 and the data pipeline. Using reliable data to achieve trade facilitation and compliancy", Jul 2020, link to research paper: SSTL Ph3 and the data pipeline. Using reliable data to achieve trade facilitation and compliancy (thesis.eur.nl)

24. European Commission, "First operational year of the EU system of tobacco traceability", Jun 2020, link to article: First operational year of the EU system of tobacco traceability (ec.europa.eu)

25. UK GOV, "Tobacco Track and Trace following the UK transition period", Oct 2021, link to paper: Tobacco Track and Trace following the UK transition period (gov.uk)

26. CBP, "Global Business Identifier (GBI) Initiative", Jul 2021, link to presentation: Global Business Identifier (GBI) Initiative (cbp.gov)

27. European Commission, "Blockchain Strategy", Jun 2021, link to webpage: Blockchain Strategy (digital-strategy.ec.europa.eu)

28. European Commission, "European Blockchain Services Infrastructure", Jun 2021, link to webpage: European Blockchain Services Infrastructure (digital-strategy.ec.europa.eu)

29. EPRS, "Blockchain for supply chains and international trade", May 2020, link to study: Blockchain for supply chains and international trade (europarl.europa.eu)

30. Derindag, O. F., et al., "International trade and blockchain technologies: implications for practice and policy, link to paper: International trade and blockchain technologies: implications for practice and policy (iopscience.iop.org)

31. Intel, Transforming Video Analytics into Business Results, n.d., link to solution brief: Transforming Video Analytics into Business Results (intel.com)

32. Visser, W., Schwaninger, A., Hardmeier, D., Flish, F. "Automated comparison of X-ray images for cargo scanning", link to paper: Automated comparison of X-ray images for cargo scanning

33. Cullum, J., "Faced with Multiple Threats, CBP Initiates Data Sciences Division to Aid Physical, Cyber Challenges", Nov 2018, link to article: Faced with Multiple Threats, CBP Initiates Data Sciences Division to Aid Physical, Cyber Challenges (hstoday.us)

34. EUR-lex, "Council Directive (EU) 2020/284 of 18 February 2020 amending Directive 2006/112/EC as regards introducing certain requirements for payment service providers", Feb 2020, link to Directive: Council Directive (EU) 2020/284 (eur-lex.europa.eu)

35. Smith, W., "Shell partners with Accenture and Ripjar on supply chain AI", Mar 2021, link to article: Shell partners with Accenture and Ripjar on supply chain AI (aimagazine.com)

36. Teong, Y. S., "The Impact of UCC for AEO", 2016, link to paper: The Impact of UCC for AEO (europesefiscalestudies.nl)

37. Statista, “Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025”, Apr 2016, link to article: Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (statista.com)

38. Mercer, L., “Making the commercial case for blockchain diamond tracking”, n.d., link to webpage: Making the commercial case for blockchain diamond tracking (everledger.io)

39. Jamasmie, C., “Nanotechnology platform to trace diamonds launched”, n.d., link to webpage: Nanotechnology platform to trace diamonds launched (mining.com)