crime&tech
Powered by Transcrime

UNIVERSITÀ CATTOLICA del Sacro Cuore

Project FATA
From Awareness To Action

Boosting the awareness and the public-private action against new counterfeiting threats

FATA
From Awareness
To Action

Final Report

April 2022

with the support of
amazon

Progetto FATA

From Awareness To Action

Boosting the awareness and the public-private action against new counterfeiting threats

Authors (Crime&tech):

Mirko Nazzari
Michele Riccardi
Flaminia De Biase

Authors (Ministero dell’Interno):

Stefano Delfini
Loredana Stamato

Suggested Citation: Ministero dell’Interno and Crime&tech-Università Cattolica del Sacro Cuore, 2022, *Project FATA: From Awareness To Action. Boosting the awareness and the public-private action against new counterfeiting threats,* Milan: Università Cattolica del Sacro Cuore.

Graphic project:

Ilaria Mastro

ISBN: 978-88-99719-33-3

Crime&tech s.r.l.
Spin-off di Università Cattolica del Sacro Cuore (UCSC) - Transcrime
Largo Gemelli 1, 20123 Milano
Tel. +39 02 7234 3715/3716
info@crimetech.it
www.crimetech.it

Table of contents

FATA

crime&tech
Powered by Transcrime
UNIVERSITÀ CATTOLICA del Sacro Cuore
with the support of amazon

Introduction

- **Counterfeiting has rapidly evolved in recent years**, because of changes in both consumer habits and purchasing channels.
- The **rapid growth in e-commerce** has generated new counterfeiting schemes, *modi operandi* and criminal actors as well as strengthening the links between **counterfeiting, payment fraud and cybercrime**.
- While both public authorities and online marketplaces are leading the fight against these emergent threats, a **new paradigm** is necessary with respect to **raising awareness, prevention, investigation, and cooperation**.
- The present study, which was carried out in accordance with the **From Awareness To Action (FATA) project** framework, aims to shed light on the **new counterfeiting threats** on online marketplaces, highlight the challenges associated with counterfeiting, present current best-practices from both the public and private sector as well as proposing future directions for intervention and cooperation.
- The study is based upon **in-depth review of case studies**, judicial documents, institutional reports and a wide variety of other information collected from **interviews with stakeholders and experts** at both the national and international level, along with representatives from law enforcement, public authorities, online marketplaces, postal operators, logistics operators, companies and brand owners.
- FATA is a project carried out by **Crime&tech**, a spin-off company of **Transcrime** – Joint Research Centre on Transnational Crime of the Università Cattolica del Sacro Cuore, together with the Italian **Ministero dell'Interno** (through '**Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale - Dipartimento della Pubblica Sicurezza**') and with the support of **Amazon**.

Counterfeiting and online markets: emerging threats and trends

Channels

- Today, counterfeiters simultaneously and interconnectedly employ the following range of online channels, both to promote and sell counterfeit goods and to carry out a host of other crimes:
  - social network;
  - fraudulent websites (e.g., website clones generated through *cybersquatting* and/or *typosquatting*);

  - marketplace;
  - instant messaging apps;
  - online forum and chats (e.g., videogame chats).

- Criminals can move across these various channels and bring end-consumers with them, by, for example, employing **cross-linking techniques** across different websites and forums, in addition to relying on disposable accounts and *spam* tools.
- Our analysis of case-studies, recent EUIPO reports, and extant scientific literature reveals an **increasing use of social networks** as a means through which both promote and sell counterfeits, which in itself is a consequence of the greater vulnerability of social media if compared to online marketplaces (see below for details).

Actors

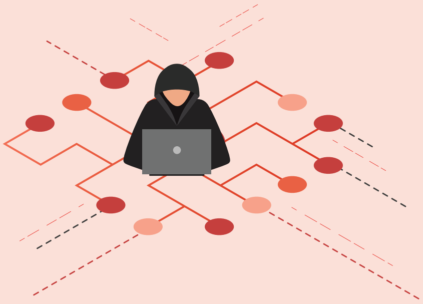
- New forms of online counterfeiting extend far beyond those actors involved in the manufacturing of counterfeit goods, to include a **wide array of other criminal subjects**, all of whom have different roles and expertise.
- **Influencers**: typically are young individuals, who act as intermediaries on social networks and forums to attract end-consumers and connect them with manufacturers, the latter of which are generally located in East-Asian countries and ready to send counterfeit goods to end-consumers by means of small parcels delivered via the postal system.

- **Brokers and IT developers**, who are often from Eastern Europe and Russian-speaking regions, support counterfeiters and criminal groups in both the development and management of IT services that are employed in the sale of counterfeits via online channels, such as:
  - design and management of fraudulent websites and website clones;
  - development of 'check-out' sections and fraudulent cash-out systems;
  - development of software and malware to be disseminated through fraudulent websites and online marketplaces;
  - development of systems that automatically produce content (*spam-bot*) that is employed in forums and chats for the purposes of promoting counterfeit goods and fraudulent marketplaces.

- **Brokers and professionals**, who facilitate the incorporation and management of shell companies, which are controlled by figureheads and often registered abroad (e.g., in countries with low levels of corporate transparency or *Free Trade Zones*), that are then used for a variety of reasons, namely:

- importing and concealing, via the creation of false invoices, counterfeit goods that are then sold online;
- managing fraudulent websites;
- laundering money and concealing illicit financial flows (e.g., the payment of illicit drugs) behind fictitious transactions on online marketplaces.

- **Organized crime groups**:
  - either of mafia origin (first and foremost, Camorra) or of a non-mafia or foreign nature (first and foremost, Chinese-speaking organized crime groups);
  - able to manage the entire online counterfeiting supply chain;
  - connected to foreign manufacturers and factories;
  - able to manage assembling and packaging centers in Italy;
  - able to manage the network of local illicit retailers (street sellers) and online retailers, by relying on the aforementioned modi operandi and channels;
  - potentially linked to terrorist and extremist groups.



Schemes

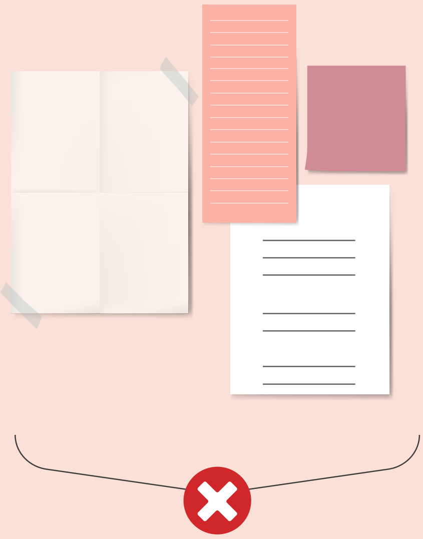
- These actors attempt to profit from their interactions with online channels by **exploiting and infiltrating all phases of online purchasing services**: account creation, purchase, payment, reimbursement, returns, interactions with other users and consumers.
- This behavior leads to increasing interconnection between crime schemes (***poly-criminality***) as well as strengthening the link between counterfeiting and **fraud, financial crime and cybercrime**.
- Counterfeiting is thus not a singular offense, but rather a process (***fraudster journey***) consisting of a wide variety of steps and crimes:
  - **sale of counterfeit goods**, via the aforementioned channels and methods;
  - **identity theft** targeting both consumers and sellers, which includes the theft of data related to payment methods, such as, for example, via *e-skimming* techniques[1] on website clones and *phishing*[2];

[1] E-skimming is a cybercrime hacking technique that steals information uploaded by consumers into an online shopping website.

[2] Phishing is a type of social engineering attack that aims at tricking users into believing that the e-mail they received comes from a legitimate institution (e.g., a bank). The e-mail, which refers to something the recipient may need/want, asks them to click on links to insert their credentials or download an attachment.

- **dissemination of malware** via fraudulent marketplaces and website clones, aimed at identity theft or ransomware;
- **payment services fraud**, which use previously stolen identification or credit cards;
- **returns fraud,** which follow online purchases, and which entail, among other things, returning counterfeit products rather than the originals for a refund.

Prevention and investigative activities: challenges and best practices

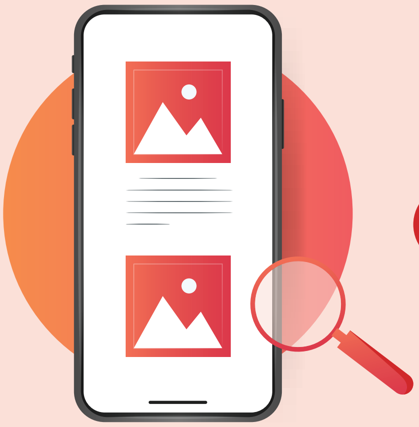


- Ensuring volume and prominence of enforcement against counterfeiting should represent a priority. The reintroduction of counterfeiting in the EMPACT priorities for the cycle 2022-2025 clearly points in this direction, highlighting the importance of holding bad actors accountable.
- Best practices in the fight against online counterfeiting can be classified into two main lines of intervention:
  - **prevention** through the control and monitoring of (a) products, (b) listings, (c) sellers on online marketplaces;
  - **cooperation and information exchange** across the different stakeholders, most notably between law enforcement authorities, online marketplaces, and brand owners.
- Despite these best practices, numerous challenges still exist; first and foremost, among these are the **differences between the different actors** (e.g., small vs. large marketplaces, marketplaces vs. social media) in terms of awareness of the problem, attitude toward cooperating with authorities, and the adoption of adequate prevention and investigative tools.
- In particular, both the case-study analysis and the interviews identified the **greater vulnerability of social networks** (in comparison to online marketplaces), as a result of both the less developed seller vetting activity and the lack of controls over sponsored campaigns.

Prevention through the monitoring of products, market, and sellers

Three control and monitoring lines can be identified:

- the **tracking and tracing of products** by brand owners, through both organisational and technological solutions, among which the following can be highlighted:



  - the use of track and trace systems of a material, electronic, chemical, and digital nature;
  - the employment of solutions based on *blockchain* and *Distributed Ledger Technology (DLT)*;
  - the use of other serialization services;
  - best practices in terms of both development and sharing of the same solutions by different brand owners can be observed.

- The monitoring of **listings and messages on marketplaces, social media and online forums**, aimed toward quickly identifying and removing listings of counterfeit goods. This occurs via the employment of:
  - solutions for automatic content and image recognition;
  - text-mining aimed at identifying false content and fraudulent text;
  - the identification of anomalous reviews, which may conceal fraud or selling counterfeits;
  - the screening of websites in order to identify website clones and fraudulent marketplaces.

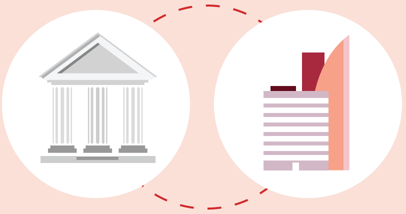
- **The due diligence of sellers** (*Know Your Business Customer* or *Seller vetting*) aimed toward screening and analysing the risks related to sellers (and potential new sellers) and ensuring that they cannot enter online marketplaces via the use of shell companies that are then used to sell counterfeits. However:
  - there is scarce knowledge about seller vetting practices and options are limited;
  - significant differences exist across different operators, with marketplaces generally more solidly equipped than, for example, social networks (in which on-boarding practices are de facto missing);
  - sophisticated on-boarding mechanisms can be identified, which combine digital verifications with 'material' checks (e.g., concerning the existence of real registered seats and local addresses);
  - instead, the use of sophisticated indicators and risk models to assess the risk of sellers appears to be limited, despite their wide employment in related domains (e.g., in anti-money laundering and anti-corruption, L. 231/2001[3]);
  - it is not possible to know the average rate of rejection in sellers' on-boarding, albeit there are some exceptions (e.g., only 6% of attempted new registrations passed the robust verification process of Amazon).

[3] Legislative Decree n. 231 of 8 June 2001 is an Italian Law that provides for a direct liability of legal entities, companies and associations for certain crimes committed by their representatives.

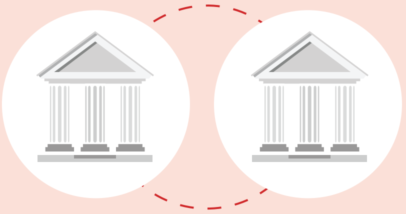
Public-private cooperation and information exchange:

Both in Italy and abroad, there are several best practices concerning cooperation and information exchange that can be found:

- **Between marketplaces, brand owners, postal operators**; for example, in terms of joint actions to investigate and prosecute counterfeiters, or in terms of sharing data on bad actors that have been identified (e.g., to avoid offenders simply moving from one marketplace to another).



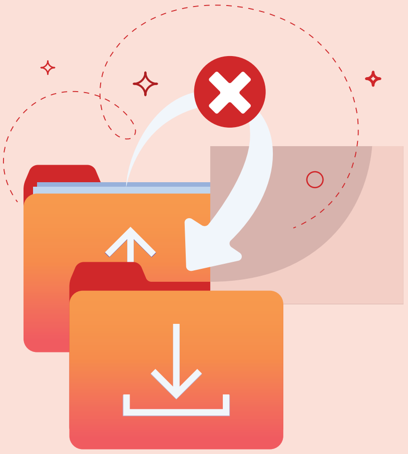
- **Between public authorities and the private sector**; for example, sharing data that are either useful for helping law enforcement more easily bad actors that need to be prosecuted, or for raising awareness among consumers.



- **Among different public authorities**, such as, for example, the *Desk Interforze Anticontraffazione*, coordinated by the Ministero dell'Interno – Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale, or the *Consiglio Nazionale per la Lotta alla Contraffazione e all'Italian Sounding (CNALCIS)*.

Key challenges

Despite these best practices, the fight against counterfeiting on online markets is hindered by two key problems, which, in turn, limit prevention and investigative activities on behalf of both public and private actors:

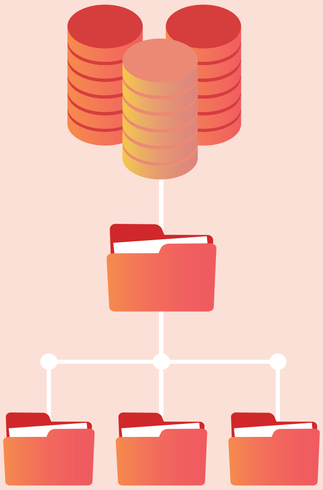


- **The lack of dedicated channels and the difficulties associated with exchanging information between actors. This occurs in various directions:**
  - *from public authorities to the private sector*; for example, data on seizures and the outcome of judicial procedures and prosecutions against individuals who have previously been reported to police by the same marketplaces and brand owners;
  - *from the private sector to public authorities*: relevant asymmetries exist among different stakeholders in terms of cooperation and data sharing with law enforcement authorities. For example, interviewees report less established data sharing practices with social media, if compared to marketplaces;
  - *from brand owners to other stakeholders*, albeit limited to the sharing of traditional guidelines on distinctive marks, despite the possibility of sharing more sophisticated data (e.g., 2D and 3D templates which may facilitate the identification of counterfeits);
  - through the voluntary sharing between private (and public) actors of information on individuals and bad actors, suspicious accounts or suspicious or stolen credit cards and payment methods that have already been identified (and blocked).

- **Difficulties in *cross-channel* online *cross-border* investigations.** The interconnection of the schemes and channels used by counterfeiters, not to mention their transnational nature, requires an integrated approach that is currently hindered by:
    - the segmentation of the responses from law enforcement and investigative authorities, which, in turn, makes it difficult to conduct a singular dialogue between the different specialist units that deal with counterfeiting, fraud, economic crime and cybercrime, respectively;
    - problems associated with international cooperation, especially with respect to some extra-EU countries and particularly when it is difficult to clearly discern the territoriality principle.

Recommendations and future interventions

Based on this study's analysis of both the new counterfeiting threats and the vulnerabilities of current prevention systems, **three directions for future interventions** can be identified. Specific recommendations can be made for each of these interventions:



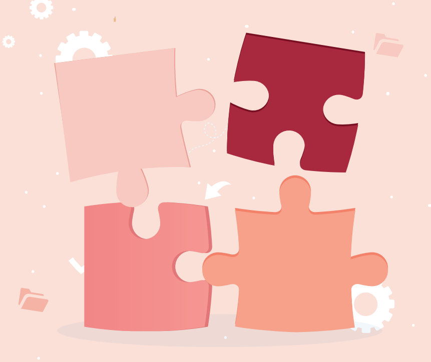
Strengthening the monitoring of the phenomenon

- By **setting up a scientific observatory** which could build, manage, and update a repository:
    - that could include schemes and cases (anonymized) of both counterfeiting on the web and of fraudulent behavior on online marketplaces;
    - that could be accessed by public authorities and private stakeholders;
    - inspired by similar initiatives in the anti-money laundering field (e.g., the collections of *Modelli e schemi di comportamenti anomali* published by the Italian UIF – Unità di Informazione Finanziaria, or the FATF periodic reports on money laundering methods and trends).

Empowering technological and data analytics skills and tools

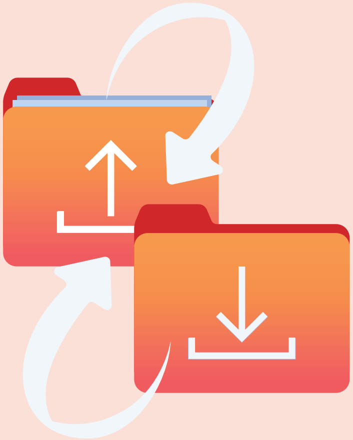
- By **developing and disseminating new tools for analysis and early-detection**, especially among those actors who are less equipped and leveraging the resources and opportunities made available by the recent Italian recovery plan (PNRR) – for example, the possibility to set up 'Extended Partnerships' between firms and universities on the topic of Artificial Intelligence and Made in Italy.

- By **training private and public stakeholders in data analytics skills**, with dedicated courses that describe the instruments which are currently available, their added value, and discuss their constraints from both a technological and legal perspective, first and foremost, those related to privacy and personal data protection.



Expanding cooperation and information exchange

- By **launching a new alliance among stakeholders**, in the form of a stable and multidisciplinary working group, which could be aligned to the new counterfeiting threat, and which could therefore:
  - group public authorities (law enforcement, judicial authorities, supervisory agencies aimed at protecting the legitimate markets) and private stakeholders (online marketplaces, social networks, brand owners, postal operators, payment service providers);
  - include authorities active in the fight against cybercrime (e.g., Italian Postal Police, Italian Agency for the National Cybersecurity) and financial intelligence units (e.g., Bank of Italy – UIF);
  - Include university experts and research centers.



- By **exploring new mechanisms for exchanging and sharing information**, even of a confidential kind, among stakeholders, to foster a shared early-detection approach, multiply economies of scale and reduce redundancy costs. These new mechanisms could:
  - be based on last generation secure exchange technologies (e.g., *federated learning*);
  - take inspiration from similar initiatives launched in other countries (e.g., the collaboration between Amazon and other online marketplaces to create a data exchange program to share information about known counterfeiters);
  - take inspiration from similar sharing systems in other domains (e.g., among obliged entities in the anti-money laundering field, such as, for example, in the Netherlands and Singapore);
  - be compliant with the constraints and obligations of all the involved parties, in terms of personal data protection regulation, protection of consumer rights and entrepreneurial freedom.

- By supporting **legislative amendments or Commission guidance** to clarify privacy and other frameworks where needed to give confidence to stakeholders to operate such exchanges.

Preface

Preface by the 'Ministero dell'Interno – Dipartimento della Pubblica Sicurezza – Direzione Centrale della Polizia Criminale – Servizio di Analisi Criminale'

The phenomenon of counterfeiting, to which those of multimedia piracy and commercial illegal are closely related, is one of the most relevant, consolidated and transversal forms of economic crime, now almost entirely the prerogative of transnational organized crime.

This is an illegal activity that:

- manifests itself in an articulated way, structured in at least four phases (production, transport, wholesale distribution and retail), according to the canons of the "supply chain", typical of advanced economic systems;
- is characterized by the ability to adapt quickly to the evolution of international trade, the development of new technologies and changes in consumer orientations and needs, as well as for the reactivity with which it is able to adopt its own countermeasures to the strategies of law enforcement prepared by the police forces.

The most up-to-date and reliable quantitative analyses on the scale of world trade in counterfeit and counterfeit products (EUIPO and OECD 2021a) estimate that, in 2019, the volume of international trade of these products amounted to as many as 464 billion U.S. dollars, equal to 2.5% of world trade and that, in the same year, imports of counterfeits in the European Union amounted to 5.8% of total imports, amounting to 119 billion euros[4].

In this context, recent studies reveal that Italy is, after the United States of America, the country in the world most penalized by counterfeiting and piracy (OECD 2018).

From a commodity point of view, the phenomenon - originally limited almost exclusively to luxury goods - has gradually expanded to the most diverse categories of products, to the point that each type of item at the which intellectual property adds economic value and thus creates price differentials, is currently the subject of interest for counterfeiting or piracy, including those that are particularly sensitive in terms of health (medicines, food, tobacco, etc.) and safety (e.g. toys, electric drills).

In recent years, there has been a considerable increase in the falsification of so-called "ITC" devices, a category in which mobile phones, computers, tablets, DVD players, headphones, earphones, microphones, etc.: as a whole, they are the sector that ensures, today, the greatest illicit revenues. From a quantitative point of view, however, leather goods, games and toys, clothing, footwear, watches and glasses are still the most common goods in illegal circuits.

The main factors that, by combining with each other, have led to the expansion of the "fake industry" that has occurred in recent decades, can be summarized as follows:

- the crisis situation that affects many small businesses;
- the rise in unemployment, which makes workers available to provide work benefits in a clandestine, occasional and low-cost way;

[4] According to previous OECD-EUIPO studies, based on the same methodology, trade in fake goods was 2.5% of world trade in 2013 and 3.3% in 2016 with an overall value of, respectively, USD 461 billion and 509 billion. As a result, both in absolute value and in percentage, the overall value of trade in fakes has remained constantly high over the last years, getting close to PIL of countries such as Austria and Belgium.

- the rationalization of production processes, by large and medium-sized enterprises, through the relocation and outsourcing of some intermediate phases, with the consequent exposure to the risk of misappropriation of industrial "know-how";
- the growing availability on the market of tools and technical equipment capable of making it easy to duplicate protected products;
- the established tendency, by consumers, to search for and buy items, even counterfeit, provided that they are "branded", as they are considered representative of a certain lifestyle;
- the increase in large illegal migratory flows, given that foreign citizens, illegally present in the territory of the State, can, in an easy and immediate way, draw the means of livelihood illegally selling false goods or being recruited for the packaging of the same;
- indulgence or tolerance towards counterfeiting and piracy on the part of public opinion, due to a lack of knowledge of the harmful effects of these phenomena;
- the interest of organized crime, which has understood the significant opportunities for illicit enrichment offered by this "business", with high profitability and low risk, for which the associations involved are able to take advantage of those forms of 'illegal land control' that they also use for other criminal activities, as well as the experience they have historically acquired in other illegal sectors, such as the smuggling of cigarettes (Tabacchi Lavorati Esteri) and the international trafficking of drugs, which require, due to their articulated dynamics, structured criminal organizations, capable of infiltrating large transport infrastructures and to manage a composite and sophisticated network of people and resources essential to the functioning of the illicit supply chain.[5] Therefore, it was easy to integrate the same partnerships even in the "false" business, when it became clear that the cost-benefit ratio was significantly unbalanced in favor of this last.

Ministero dell'Interno – Dipartimento della Pubblica Sicurezza – Direzione Centrale della Polizia Criminale – Servizio Analisi Criminale

The 'Direzione Centrale della Polizia Criminale', through its 'Servizio Analisi Criminale', an interforce unit involving members of 'Polizia di Stato', 'Arma dei Carabinieri', 'Guardia di Finanza' and 'Polizia Penitenziaria', manages, in collaboration with the 'Prefetture', the monitoring system called 'Co.Ab' ('Collaborazione e Abusivismo'), that collects data related to the operations carried out by Police and Local Police and the relative results.

The 'Servizio Analisi Criminale' also contributed to the evaluation document of the S.O.C.T.A. (*Serious and Organized Crime Threat Assessment*), together with the MISE, providing an updated overview on several criminal phenomena, such as food fraud, counterfeiting of textiles, pharma crime, online piracy, product counterfeiting and intellectual property crime.

The aforementioned contribution, used by the Europol analysts for the final document, has been submitted to the C.O.S.I. ('Comitato Permanente per la Cooperazione Operativa in materia di Sicurezza Interna') and approved for the next programmatic cycle of the European Union in 2022-2025. Therefore, the E.M.P.A.C.T. (European Multidisciplinary Platform Against Criminal Threats) will include as a priority also the fight against counterfeiting and intellectual brand protection.

[5] In the smuggling of foreign processed tobaccos, besides the network of contacts necessary for the supply and payment of illicit shipments and the relevant logistics infrastructure to manage the reception, conservation and transport of tobaccos, it is also necessary to have professionals who can provide the fictitious documentation to avoid potential scrutiny by law enforcement and carry out successful shipments.

Preface by Crime&tech – spin-off company of Transcrime – Università Cattolica del Sacro Cuore

The growth of both e-commerce and online markets has brought counterfeiting to new heights. Although its true scale is hard to quantify, online counterfeiting is characterised by new actors, new criminal schemes, new *modi operandi* and new offenses. Today, the sale of counterfeits on online marketplaces occurs in conjunction with a wide array of economic and financial crimes, such as, for example, payment fraud or identity theft, and with new forms of cybercrime. In this respect, counterfeiting is not a singular offense, but rather forms part of a *fraudster journey*, as one of the interviewees in this study referred to it.

The rise of these new criminal schemes not only changes the profile of the criminal actors involved, but also the nature of the victims, which expands to include many consumers and web surfers, who are often wholly unaware, vulnerable and poorly equipped. Consequently, the harms caused by counterfeiting multiply exponentially to affect consumers, firms, and the public sector.

Both the difficulties associated with investigating counterfeiting on online markets and the relative dearth of studies on this issue inspired the researchers to conduct the present study. Crime&tech, the spin-off company of the research centre Transcrime of the Università Cattolica del Sacro Cuore, has been glad to share this view with both the Italian Ministero dell'Interno and Amazon, which supported the present study.

Together with these partners, we produced the present report, which only constitutes one of the results of project *FATA – From Awareness To Action*. FATA was conceived with the express aim of combining, on the one hand, the experience and knowledge of public authorities, and, on the other, that of online marketplaces; that is to say, the expertise of those stakeholders that are at the forefront of the ongoing fight against online counterfeiting. FATA also aims to share this knowledge with all of the other parties (e.g., e-commerce and logistics operators, brand owners, public bodies, consumers), who are, albeit in manifold ways, involved in this domain.

We believe that FATA represents the first milestone in the establishment of a **new observatory capable of continuously monitoring** the new schemes of online counterfeiting, which would require constant input and updating from all the necessary stakeholders, that is, researchers, public authorities, and the private sector. In this respect, FATA marks the first output of a **new alliance between the public and private sector** and, at least we hope, plants the first seed in the development of a new paradigm in terms of both the prevention and investigation of online counterfeiting, one which is integrated, comprehensive and able to keep a pace with the evolution of this criminal phenomenon.

Crime&tech - Università Cattolica del Sacro Cuore

Crime&tech srl is the spin-off company of Transcrime, the Joint research centre on transnational crime of the Università Cattolica del Sacro Cuore. Crime&tech translates Transcrime's research in data analytics services and technological instruments for the assessment, identification, and prevention of criminal risks. Crime&tech supports public and private actors in a number of domains, including anti-money laundering, anti-corruption and fraud prevention in the retail sector.

Preface by Amazon

At Amazon, we have a zero-tolerance policy for counterfeiting and piracy: we believe we have a responsibility to protect consumers, brands, and our store from counterfeit products, and we work hard to do that.

As per Netcomm estimates[6], 29 million Italians habitually buy online today and they do all deserve to get the authentic products they purchased. Also, the country competitiveness system must be protected, and counterfeiters should not undercut honest entrepreneurs and deprive brand owners of the value of their intellectual property.

The pandemic played as an accelerator of the online commerce, but it also attracted bad actors who tried to take advantage of the situation. Despite their attempts, we continued to make strong progress driving counterfeits to zero in our store through robust proactive controls and powerful tools for brands, and increasing our litigation efforts and collaboration with law enforcement agencies.

In 2020 alone, Amazon invested over $700 (€600) million and employed more than 10,000 people to protect our store from fraud and abuse; as a result, we prevented over 6 million attempts to create new selling accounts, stopping bad actors before they published a single product for sale, and fewer than 0.01% of all products sold on Amazon received a counterfeit complaint from customers.

While we are proud of the progress made, we know that counterfeiting remains a persistent global retail-industry challenge, and that bad actors will not stop but move their operations across many other channels, including their own websites, online marketplaces, offline channels, and more.

The complexity of online counterfeiting is expected to grow along with market changes and technological innovation. We believe it is of strategic importance to investigate new scenarios and to understand the extent and nature of existing links with other criminal phenomena. As the Ministry for Economic Development stated, "a modern approach to the protection of industrial property cannot be limited to playing on the defensive"[7], it is necessary to deepen the knowledge of online counterfeiting in order to adapt and effectively direct prevention and contrast policies.

It has also become increasingly clear to us that we have to make bold changes in how we work together across sectors to stop it. At Amazon, we strongly believe that we need an enhanced partnership across industry and governments to better protect our borders from counterfeit goods, and to shut down confirmed counterfeiters across the retail industry.

Likewise, we believe that counterfeit prosecution should be regarded as a priority, more than ever for sometimes it is a predicate crime to far more nefarious activity. More resources should be allocated to law enforcement authorities to this end, and we regard the reinstatement of counterfeiting amongst the priorities of the European Union multidisciplinary platform against criminal threats (EMPACT) to be a relevant step in that direction.

Project FATA originates from a deep reflection on all of the above, and from the need to investigate the characteristics of the actual online market for counterfeits.

[6] https://www.consorzionetcomm.it/il-lockdown-triplica-i-nuovi-consumatori-online-in-italia-tra-gennaio-e-maggio/

[7] Ministero dello Sviluppo Economico. 2021. Strategic intervention Lines on industrial property for the three-year period 2021-2023, pag. 7. https://uibm.mise.gov.it/images/LINEE_DI_INTERVENTO_approvate.pdf

Two excellent institutions joined forces to this end, the Ministry of Interior Criminal Analysis Service, detaining and mastering data collection and analysis and setting contrast strategies at national level, and Crime&Tech from the Catholic University of Milan, an internationally renowned research center. We are proud we had the opportunity to support their work, and we hope we will all join forces to foster synergies, encourage integrated prevention policies, and facilitate the updating of regulations to hold counterfeiters accountable.

Amazon

Amazon is guided by four principles: customer obsession rather than competitor focus, passion for invention, commitment to operational excellence, and long-term thinking. Amazon strives to be Earth's Most Customer-Centric Company, Earth's Best Employer, and Earth's Safest Place to Work. Customer reviews, 1-Click shopping, personalized recommendations, Prime, Fulfillment by Amazon, AWS, Kindle Direct Publishing, Kindle, Career Choice, Fire tablets, Fire TV, Amazon Echo, Alexa, Just Walk Out technology, Amazon Studios, and The Climate Pledge are some of the things pioneered by Amazon. For more information, visit www.aboutamazon.it and follow Amazon.it on Instagram, Facebook and Twitter.

1.

Introduction

1.1 The rationale for the study

The globalization of markets, the spread of **information and communication technologies (ICT)** and the **growth of e-commerce** have profoundly transformed the market over the last two decades. These changes have generated manifold new opportunities for both businesses—by allowing them the chance to enter new markets—and consumers—who are now able to buy ever-more products at lower prices.

In parallel with this, these changes have also fostered **new criminal opportunities for distributing illicit goods**, particularly **counterfeit products**. In addition to the traditional distribution channels — stands, peddlers, illegal shops— and, albeit on a smaller scale, the legal supply chain (Guardia di Finanza 2020b), the sale of counterfeits **has increased on the internet** in recent years, as evidenced by various reports from public authorities and law enforcement agencies (see, for example, Europol 2021). While traditional distribution channels remain predominant in the counterfeiting market, bad actors also exploit e-commerce and online auctions in order to benefit from the growth of online shopping and reach a wider array of consumers (see Box 1), in addition to exploiting specific characteristics of e-commerce which facilitate criminal behaviour (Consiglio Nazionale Anticontraffazione 2019), such as:

- the **opportunity for bad actors to conceal their identities** by using, for example, shell companies or e-commerce vendors as figureheads;
- the **variety of existing marketplaces and virtual channels**, which can be employed, even simultaneously, to move and displace, to disorient law enforcement investigations;
- the **possibility to reach an increasing number of consumers**, who are unaware of the risks and poorly equipped to handle them.

These factors, which will be discussed in detail in the sections that follow, significantly undermine the effectiveness of those **measures designed to prevent and combat counterfeiting**.

Box 1. The growth of e-commerce during the COVID-19 pandemic

According to the latest round of the 'E-commerce statistics for individuals' survey (Eurostat 2021), around 73% of internet users shopped online in 2020, in comparison to 62% in 2015, with the highest prevalence found among those aged 16-24 (78%) and 25-54 (79%). As highlighted by OECD (2020), the COVID-19 pandemic and attendant governmental measures has significantly impacted upon the growth of e-commerce. Indeed, online purchases in the EU in April 2020 were 30% higher compared to the previous year. The COVID-19 pandemic also altered consumer patterns, insofar as even non-habitual consumers (e.g., elderly people) began to buy online. While the vast majority of purchases are still made offline, the pandemic has clearly accelerated the widespread acceptance of online shopping as a purchasing channel for a wider array of goods.

As underscored by a recent joint report by Censis and Ministero dello Sviluppo Economico (2021), the COVID-19 pandemic also profoundly influenced the counterfeiting market. Despite counterfeit goods are still predominantly sold through offline channels, bad actors adapted to the new scenario (e.g., slowdown of international trade, difficulties in moving large shipments) by increasingly selling their counterfeits online, where, in addition to traditional products, we also saw a preponderance of goods related to the pandemic (e.g., face masks, sanitizers, medicines and rapid COVID-19 tests). Several criminal investigations and studies have shown the massive sale of counterfeit medical devices, both nationally and internationally (OECD e EUIPO 2020; Ministero dell'Interno 2021). Online marketplaces have responded relatively strongly to this threat, in turn, leading to an active collaboration with law enforcement agencies. For example:

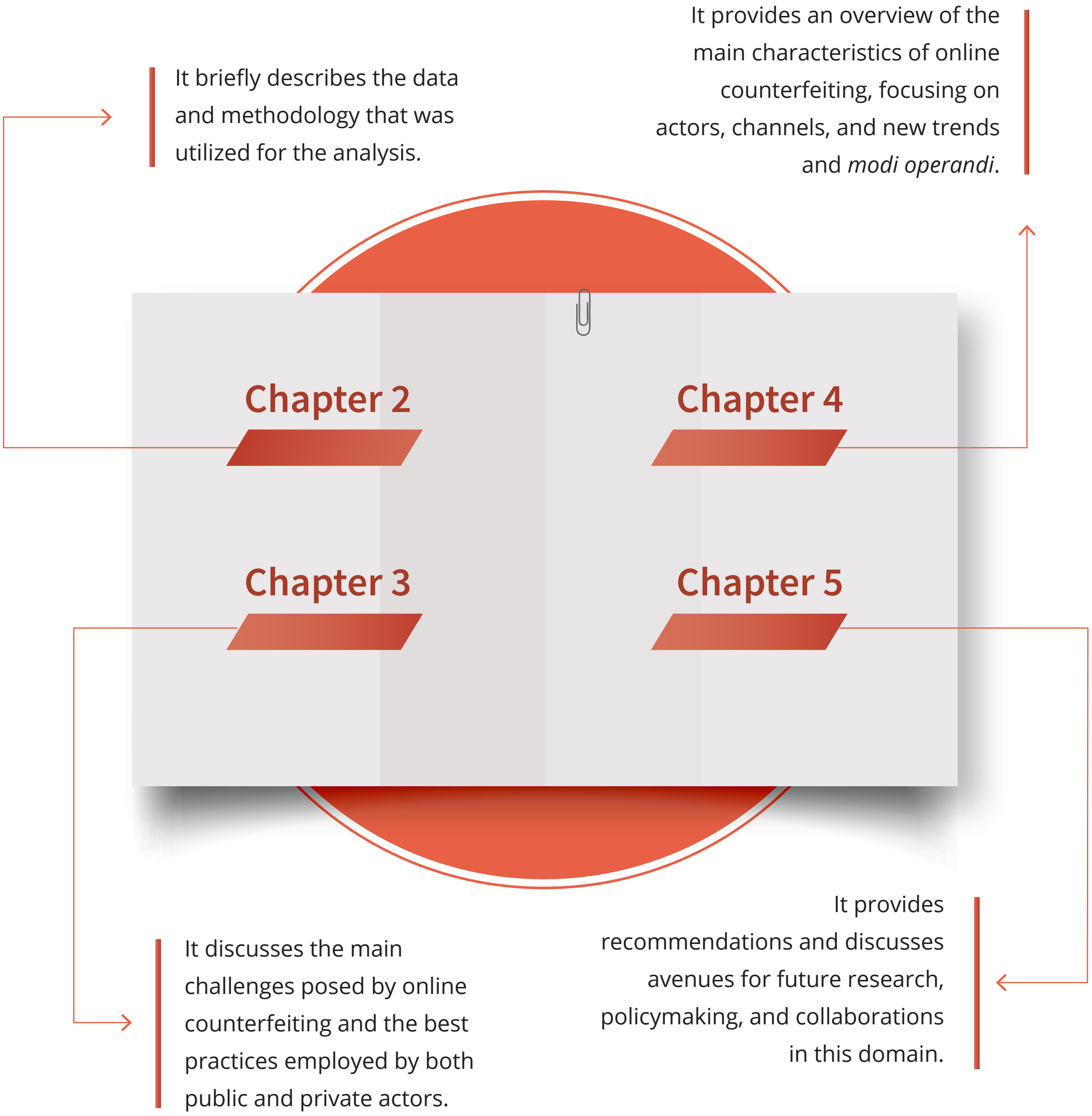
- Amazon proactively removed 6.5 million healthcare products from its marketplace in 2020 (e.g., sanitizers, face masks) because they were fraudulently advertised as being effective against COVID-19, in conjunction with closing 10,000 vendor accounts that sold healthcare products at a significantly higher price than average (ICE 2020). Amazon also joined (together with Pfizer, 3M, Citi e Alibaba) the task-force that was set up by the Homeland Security Investigations (HSI) and the National Intellectual Property Rights Coordination Center (IPR Center) to combat fraud linked to the COVID-19 pandemic (ICE 2020);
- in 2020, Alibaba cooperated with law enforcement agencies from 19 Chinese provinces in relation to 1711 cases involving the sale of counterfeit products linked to the COVID-19 pandemic, actively contributing to the arrest of 716 counterfeiters (Alibaba Group 2020).

Despite the undoubted relevance of the topic, there is a relative dearth of knowledge on how counterfeiters exploit e-commerce. Indeed, no previous study in Italy has provided a systematic overview of either the new trends and *modi operandi* in online counterfeiting or the countermeasures implemented by public authorities and private companies to prevent it. For example, it would be important to understand to what extent websites, as opposed to online marketplaces, are employed for the sale of counterfeits. Recent criminal investigations have demonstrated that some type of counterfeit goods – e.g. medicines – are mostly sold via websites. For example, the XIV edition of Operation 'Pangea' by Interpol (May 2021), coordinated for Italy by the Servizio per la Cooperazione Internazionale di Polizia della Direzione Centrale di Polizia Criminale, led to the seizure of 9.089.549 counterfeit medicines/medical devices and the 113.000 websites through which these counterfeits were sold (AIFA 2021b). Similarly, the IX edition of the joint EU-US Operation 'In Our Sites' (December 2021) led to the seizure of 33.654 websites distributing counterfeit goods online (Europol 2021b). However, despite such insights, a comprehensive and systematic analysis of these new trends is still missing. This **knowledge gap**, on the one hand, makes it more difficult to identify, investigate and prosecute counterfeiters, while, on the other, it serves to undermine **the trust of customers,** who are often unable to understand who they are buying from, which, in turn, could lead them to lose confidence in shopping online.

Project **FATA** aims to address this gap. In particular, this present study will:

- shed light on the **new forms and *modi operandi*** of online counterfeiting, particularly the simultaneous use of numerous online channels and the employment of various concealment schemes (e.g., shell companies) in the sale of counterfeits;
- increase **awareness over the links between counterfeiting and other forms of organized crime**, including financial and cyber offenses;
- improve **cooperation between public authorities and the private sector** (e.g., online marketplaces, brand owners, logistic companies);
- promote **new initiatives and tools** through which to increase the effectiveness of countermeasures designed to prevent and combat online counterfeiting.

The report is organized as follows:



Chapter 2

It briefly describes the data and methodology that was utilized for the analysis.

Chapter 3

It discusses the main challenges posed by online counterfeiting and the best practices employed by both public and private actors.

Chapter 4

It provides an overview of the main characteristics of online counterfeiting, focusing on actors, channels, and new trends and *modi operandi*.

Chapter 5

It provides recommendations and discusses avenues for future research, policymaking, and collaborations in this domain.

1.2 The magnitude of counterfeiting online

1.2.1 An underestimated phenomenon?

Current estimates of the magnitude of counterfeiting are produced using a variety of methodologies, which are grounded in both **demand-based** and **seizure-based** approaches. The most recent of these estimates comes from a joint report by OECD and EUIPO (2021b), which estimates the overall volume of counterfeits in 2019 to be equivalent to 461 billion USD at a global level (equal to 2.5% of the overall value of global trade). In 2015, a European study by Transcrime (Camerini, Favarin, e Dugato 2015) that used data on seizures and consumer habits (both online and offline) - the latter of which was collected by OHIM via a survey (OHIM 2013) - estimated the overall value of counterfeiting to be 41 billion euros each year. Despite serving as clear indicators of the severity of this criminal phenomenon, these estimates **are not able to distinguish between online and offline counterfeiting**.

Also, administrative statistics related to the **number of crimes and offenders** reported to the judicial authorities (see Box 2), do not provide a comprehensive overview of the size of counterfeiting, due to, among other things, both the high 'dark figure' (i.e., the rate of crimes that are not reported to the police), the challenge in investigation and the priority given to such offences. In Chapter 3 we review how uncovering criminals concealed behind online accounts - also located in foreign jurisdictions - is hard for law enforcement agencies.

The lack of representativeness offered by official data has been exacerbated even further in recent years by the fact that, between the period 2018-2021, counterfeiting was not listed as a priority in the **EMPACT *(European Multidisciplinary Platform Against Criminal Threats)***.[8] This exclusion inevitably diverted resources and the attention of law enforcement agencies toward those priorities that were on the EMPACT list, which, in turn, had a deleterious impact upon the number of counterfeiting crimes and offenders that were reported to or identified by the judicial authorities. Hopefully, the re-inclusion of counterfeiting as an EMPACT priority will be mirrored also in terms of bad actors reported to the police.

1.2.2 Signals that online counterfeiting is on the rise (but offline is still predominant)

Despite the absence of reliable estimates on the overall volume of counterfeit trade online, there are several indicators that it is **on the rise**. At the same time, there are data indicating that, in terms of volume and value, 'offline' counterfeiting is still predominant.

- A recent report by OECD and EUIPO (2021b) on **the illicit trade of counterfeits linked to e-commerce**, based on the EU customs seizures, highlights that:
    a. **56%** of customs seizures in the EU during 2017-2019 are related to online sales. However, in terms of economic value, **only 14% of seized goods are related to online sales**, while 86% is not (Figure 1);

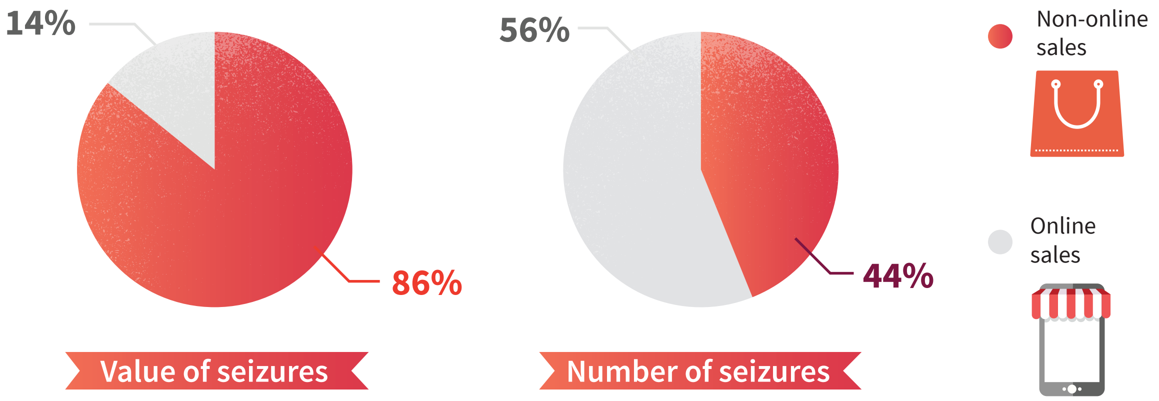
[8] The EMPACT is the integrated approach to EU internal security. The EMPACT periodically defines the EU priorities in the fight against organized and serious crime, thus representing the flagship instrument for multidisciplinary and multiagency operational cooperation to fight organized crime at the EU level (https://www.europol.europa.eu/empact).

b. while for online counterfeiting the role of 'small parcels'[9] is crucial (see Chapter 3), most of the seized goods are still related to offline counterfeiting and shipped through other channels (e.g., containers) (OECD e EUIPO 2021a);

c. it is also important to clarify that in this report, OECD and EUIPO refers to the definition of counterfeiting reported in the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (see section 2.1 for more information), referring to a wider spectrum of tangible goods that infringe trademarks, design rights or patents.

Unfortunately, the study - the first to specifically focus on e-commerce - only includes figures at the EU aggregate level as opposed to figures for individual countries, which means it is not possible to ascertain current counterfeiting trends in Italy.

Figure 1. Distribution of value of seizures related to online sales and not related to online sales. *Source: OECD and EUIPO (2021).*



- **11% of conversations on social networks about physical products** are related to counterfeits, according to a recent study by EUIPO (2021c);
- A recent study (Stroppa et al. 2019) detected 56,769 Instagram accounts that were being misused by criminals to sell counterfeits, a **171% increase** in comparison to the 20,892 Instagram accounts detected in the 2016 edition of the study that used the same methodology (Stroppa e Di Stefano 2016). In 2019, these accounts published more than 64 million posts and, on average, 1.6 million stories each month, reaching more than 20 million users via their followers;
- on TikTok, posts with hashtags linked to counterfeits exceeded **100 million visualizations** worldwide (Lince 2020);
- EUIPO (2021b) analyzed 1,000 internet domains of 20 brand owners. **49%** of these were **deemed to be 'suspicious'** and linked, among other things, to the **sale of counterfeits**, the spread of malwares and the theft of personal information.

Although they provide an incomplete view of the phenomenon, and despite the predominant role played by 'offline' counterfeiting, both the official statistics and the above-presented data clearly show that counterfeiting **is growing online**, and adopting new schemes, *modi operandi*, channels, and transportation methods. Investigating these new trends constitutes the aim of this study.

[9] 'Small parcels' refer to packages containing less than 3 items that can be seized under the simplified procedure;

Box 2 – Counterfeiting trends in Italy (2015-2021)

Box by 'Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale - Dipartimento della Pubblica Sicurezza - Ministero dell'Interno'

The enforcement activities carried out by law enforcement agencies on the national territory has highlighted that the number of reported crimes, during the period 2015–2021 (data for 2021 refers to the first six months of the year and may change due to future consolidations) has decreased overall. The crimes considered in the analysis are those referred to by the Italian Criminal code in the articles 473 c.p. "*Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni*", 474 c.p. "*Introduzione nello Stato e commercio di prodotti con segni falsi*" e 517 ter c.p. "*Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale*".

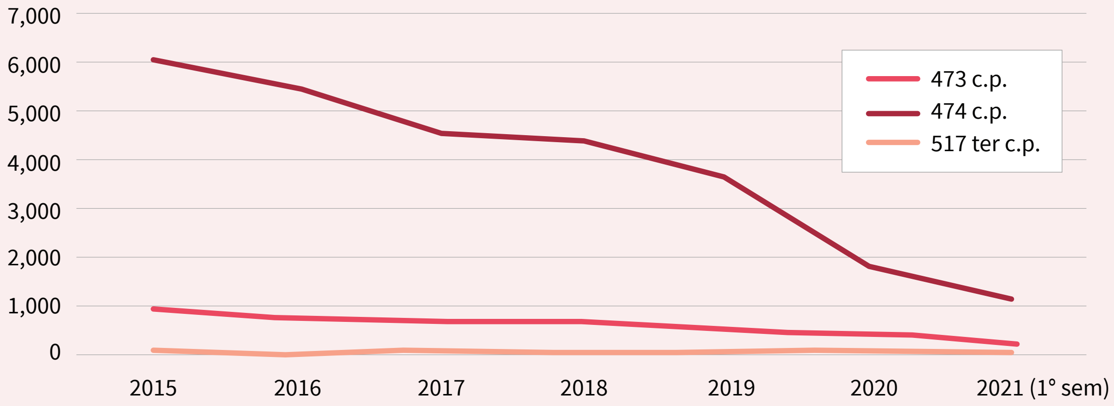
The data included in the table was extracted from the Servizio per il Sistema Informativo Interforze, which manages the Centro Elaborazione Dati (C.E.D.) of the Italian Ministry of the Interior, and have been elaborated by the Servizio Analisi Criminale, which are both units of the Direzione Centrale della Polizia Criminale.

Table 1 and Figure 2 – Crimes related to counterfeiting reported by law enforcement agencies to the judicial authority

Source: Elaboration by 'Servizio Analisi Criminale' on data extracted from the C.E.D. of the Italian 'Ministero dell'Interno'.

Crimes distinguished by violated articles of the Italian Criminal Law

	2015	2016	2017	2018	2019	2020	2021 1° sem
473 c.p.	930	795	695	672	577	433	209
474 c.p.	6,061	5,537	4,611	4,420	3,617	1,804	1,046
517 ter c.p.	57	54	42	38	37	40	17



The overall decreasing trend in this criminal phenomenon—even if we consider the fact that Italy has one of the most advanced prevention and enforcement systems—suggests that the sale of counterfeits is shifting onto the Internet, therefore making it difficult to identify and prosecute the criminals involved in such illegal activities.

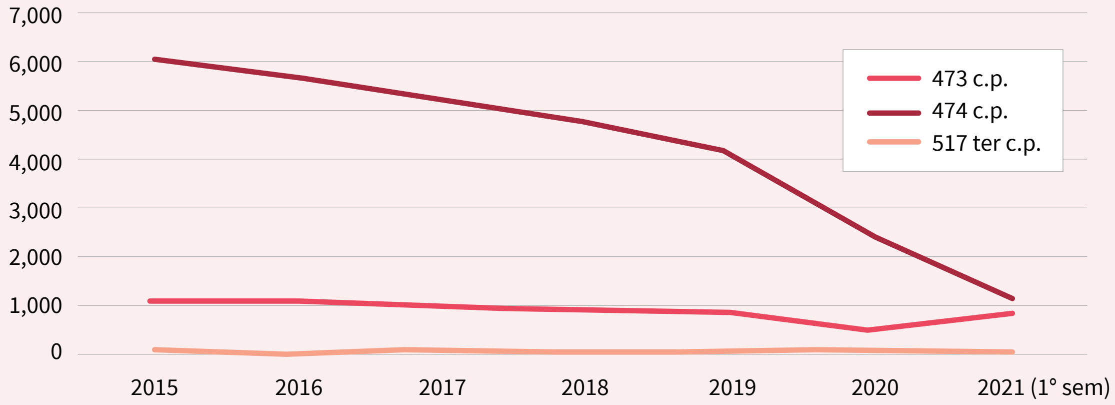
With respect to the same time frame, the number of individuals prosecuted by the judicial authority for counterfeiting does not follow a clear pattern: overall, there is a decrease in the number of offenders related to article 474 c.p., a steady trend for article 517 ter c.p., while for article 473 c.p. an overall decrease up until 2020 can be observed, followed by a relevant increase in the first six months of 2021.

Table 2 and Figure 3 – Individuals reported by law enforcement agencies to the Judicial Authority for crimes related to counterfeiting

Source: Elaboration by 'Servizio Analisi Criminale' on data extracted from the C.E.D. of the Italian 'Ministero dell'Interno'.

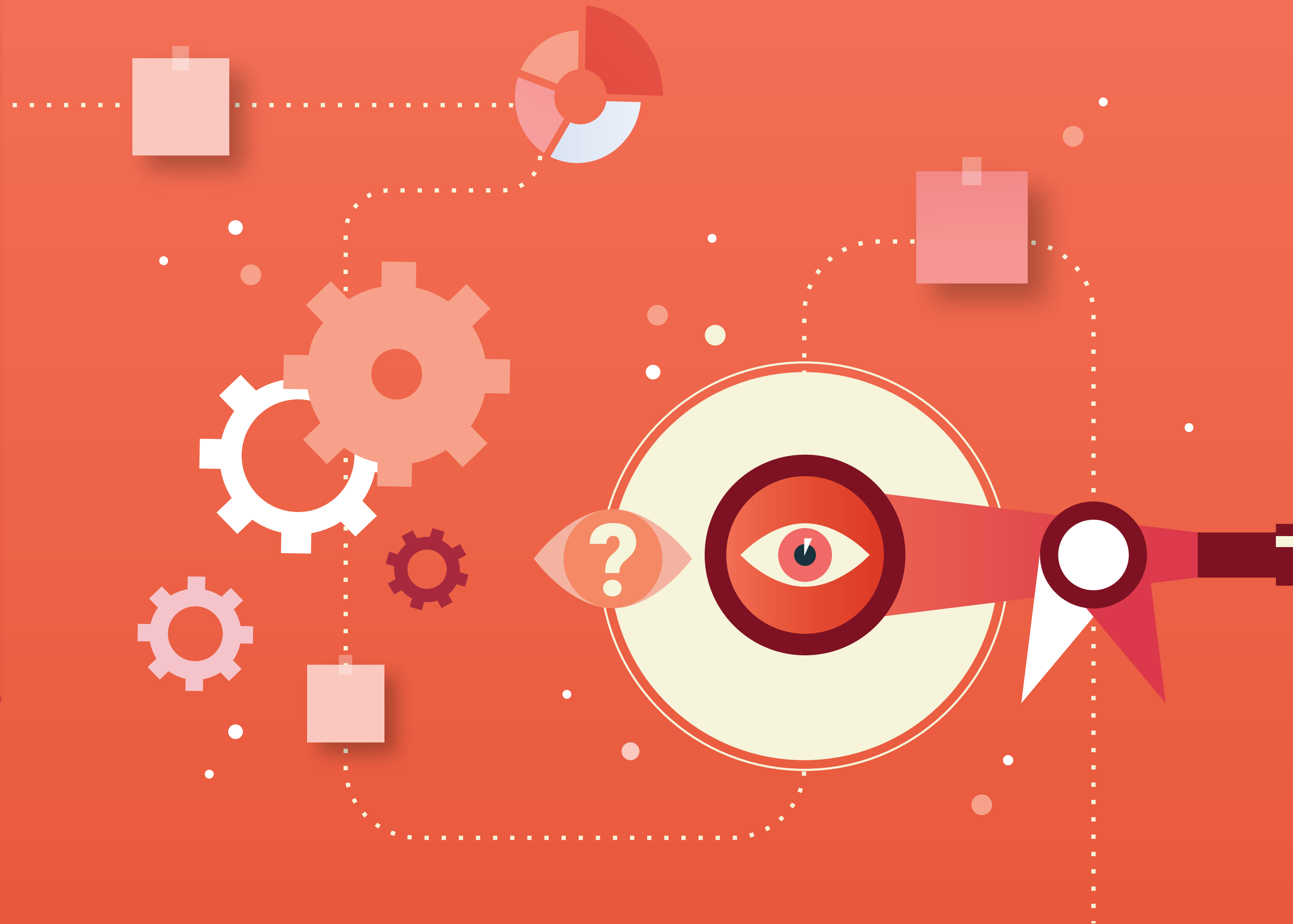
Criminally persecuted people

	2015	2016	2017	2018	2019	2020	2021*
473 c.p.	1,048	1,030	938	896	793	480	753
474 c.p.	6,051	5,606	5,153	4,690	4,131	2,379	1,151
517 ter c.p.	68	67	43	50	47	65	47



2.

Methodology



2.1 Definitions

The present study analyzes counterfeiting on online markets. For this purpose, it is useful to provide an operational definition of the two key concepts - counterfeiting and online markets - that are employed in the analysis.

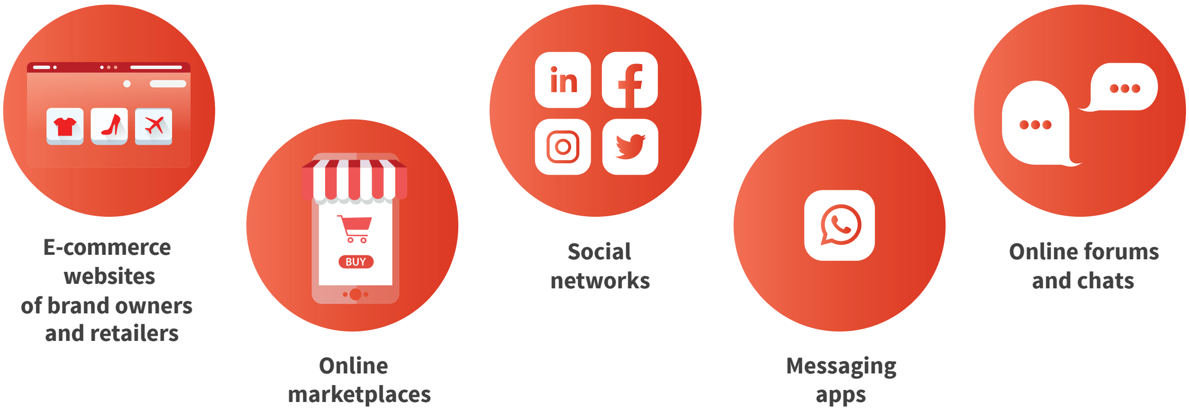
Counterfeiting

By counterfeiting, we are referring to the violation of intellectual property rights (IPR) by means of the illicit copying of a product and its resulting sale *uti originalis* (Senato della Repubblica Italiana 2017, 12). In particular, we use the definition of counterfeiting delineated in the following articles of the Italian Criminal Code: **473 c.p.** (*Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni*), **474 c.p.** (*Introduzione nello Stato e commercio di prodotti con segni falsi*) and **517 ter c.p.** (*Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale*).

It is important to specify that the definition employed in the present study differs from the one adopted by OECD in its reports, the latter being wider in scope than that of the Italian Criminal Code. OECD employs the definition of counterfeit goods as foreseen in the enforcement section of the agreement on Trade-Related aspects of Intellectual Property Rights (also known as TRIPS Agreement), negotiated and administered by the World Trade Organization. This Agreement states that counterfeit trademark goods '*shall mean 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 under the law of the country of importation*' (WTO 1994, 342).

Online markets

By online markets, we are referring, in broad terms, to the wide array of **online channels** via which products and services may be advertised and sold, namely:



The use of such a broad definition is necessary given counterfeiters' increasing employment by all commerce, including counterfeiters of online channels that are not specifically designed for selling products and services, such as social media, forums and online chat rooms (Kennedy 2020). Chapter 3 will discuss this trend in greater detail.

2.2 Data and sources

Given the novelty of the phenomenon under investigation, not to mention limited previous research and statistics on the topic, the present study adopts a 'hybrid' methodological approach, which is based on **three main data sources**:

- **judicial and police documents** of counterfeiting-related cases, both in Italy and abroad;
- **reports, both publicly available ones and those that are confidential in nature**, by public authorities and private stakeholders (e.g., marketplace, social media, logistics and postal operators and brand owners);
- **interviews with stakeholders** from both the public and private sector.

Interviews and e-mail exchanges for sharing relevant documents were conducted with **25 professionals, both in Italy and abroad**, who represent different stakeholder categories:

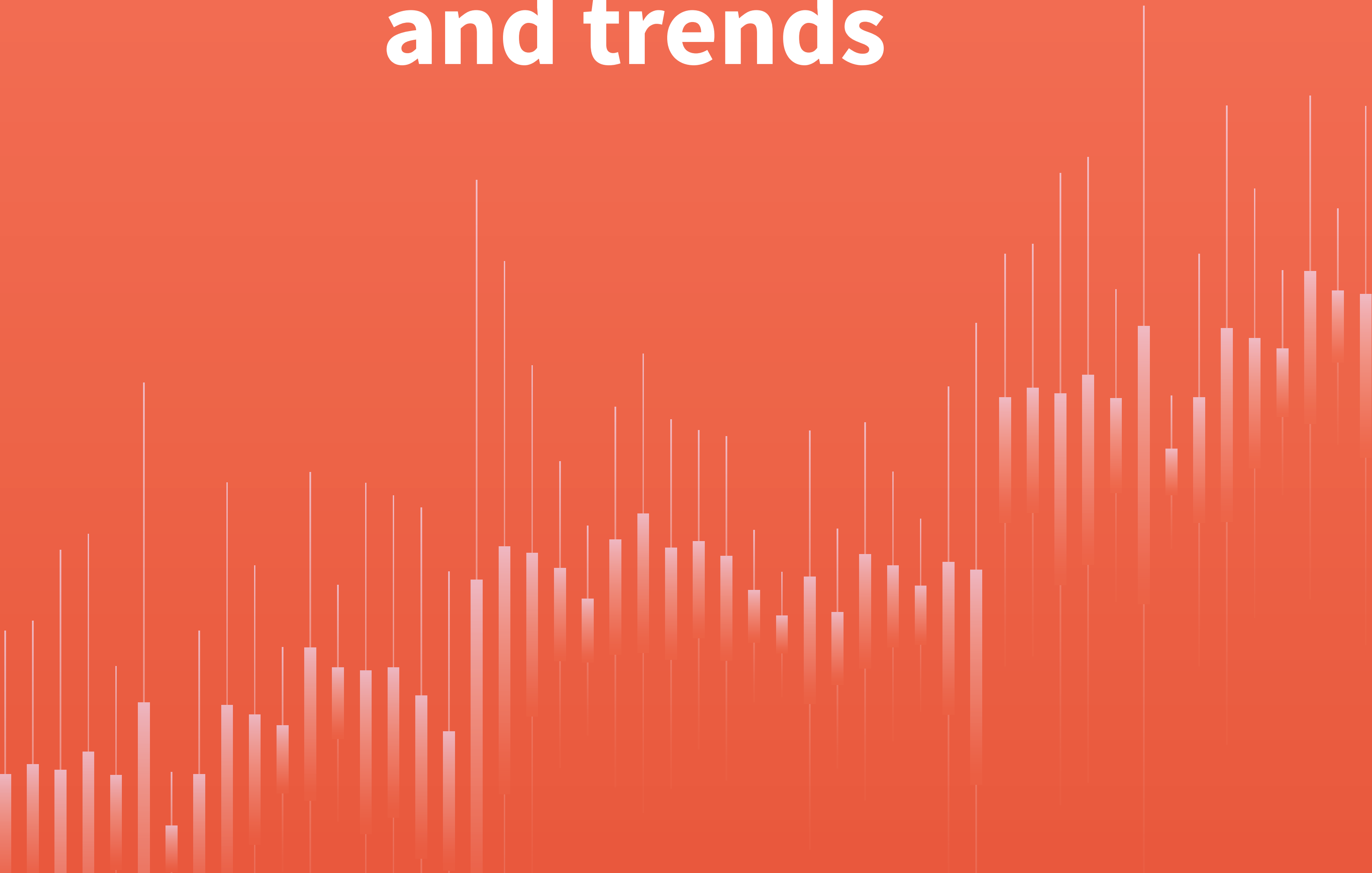
- law enforcement agencies and public authorities;
- online marketplaces;
- social media;
- brand owners (from several businesses) and trade associations;
- logistics operators;
- postal operators;
- research centers and universities.

The interview guides were tailored to fit the role and expertise of each of the interviewees and shared with them in advance. Some interviewees were also able to share relevant documents for the study, both prior to and after the interviews. When authorized, these documents are explicitly referenced. Otherwise, these references are anonymized.[10]

[10] Not all the interviewees, or the institutions to which they belong, provided consent to be explicitly cited in the study. Among those who authorized to be cited, we would like to thank: the Ministero dell'Interno, and in particular Dr. Stefano Delfini, Dirigente Superiore della Polizia di Stato e Direttore Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale – Dipartimento della Pubblica Sicurezza, Dr. Loredana Stamato, Primo Dirigente of the Polizia di Stato, Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale - Dipartimento della Pubblica Sicurezza, and Ten. Col. CC Alessandro Giordano Atti, Director of the V Sezione – III Divisione "Interpol" Servizio per la Cooperazione Internazionale di Polizia della Direzione Centrale della Polizia Criminale - Dipartimento della Pubblica Sicurezza; la Guardia di Finanza, and in particular Ten. Col. Francesco Basile, Comandante 2° sezione del Gruppo Anticontraffazione e Sicurezza prodotti del Nucleo Speciale Beni e Servizi, e il Ten. Col. Giacomo Scilì Bellomo, Capo Sezione Tutela Mercato Beni e Servizi dell'Ufficio Tutela Uscite e Mercati del III Reparto Operazioni del Comando Generale; Amazon; INDICAM, and in particular Dr. Lucia Toffanin, Direttore Generale; Michigan State University, and in particular Dr. Jay Kennedy, Assistant Professor at the School of Criminal Justice and the Center for Anti-counterfeiting and Product Protection; Poste Italiane, and in particular Dr. Rocco Mammoliti, Chief Information Security Officer, and Dr. Massimiliano Aschi, Senior IT Security Specialist; Yoox-Net-A-Porter Group and in particular Dr. Gianluca Gaias, Chief Security Officer, and Dr. Arianna Vitalini, Corporate Digital Governance Manager. We would also like to thank all the other interviewees, belonging to public authorities and private entities who prefer not be explicitly mentioned in the study, for the inputs provided.

3.

Counterfeiting online: emerging threats and trends



The evolution of counterfeiting on online markets can be discerned by examining three dimensions:

- the **channels employed** to sell counterfeits;
- the **criminal actors** involved;
- the **schemes** used.

The interconnection of these three dimensions produces new forms and *modi operandi* in the production and sale of counterfeits on online markets.

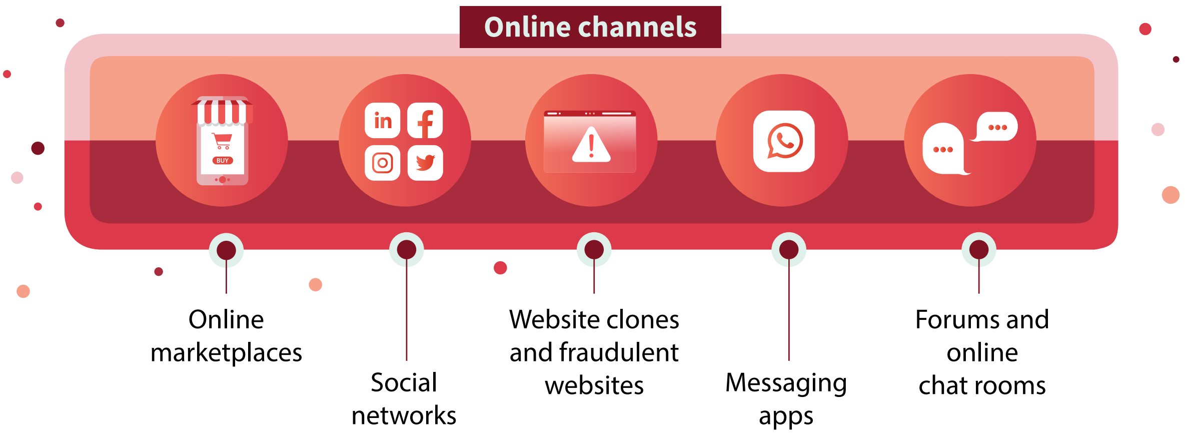
3.1 Channels

Recent police investigations have shown an **increased diversification and interconnection** of the online channels that are used for advertising and selling counterfeits. Counterfeiters (both individuals and organized groups) use several channels **at the same time** through employing cross-links, which enables them to:

- reach a larger volume of potential clients;
- circumvent the countermeasures implemented by providers;
- hinder police investigations by exploiting the asymmetries between the different channels in terms of information sharing with law enforcement agencies.

The members of law enforcement agencies and public authorities interviewed by the authors highlighted **different levels of cooperation** between the various online marketplaces, especially when these are registered abroad or use extra-EU servers. Furthermore, they underscored that there are **different capabilities in terms of the technological and preventive tools** that are used to proactively monitor listings and vendors (see Chapter 4). The law enforcement agents and brand owners that we interviewed agreed that although, on the one hand, **large marketplaces** are equipped with cutting-edge automatic detection systems of illegal goods, on the other, **social networks** are not as well equipped to prevent the sale of counterfeits. Also, **smaller e-commerce websites** do not generally have adequate tools even though, in contrast to larger players, may lack the necessary resources to implement such countermeasures.

The next sections will delve further into the main online channels currently being abused by counterfeiters. In particular:


Online channels
BUY
Online marketplaces
Social networks
Website clones and fraudulent websites
Messaging apps
Forums and online chat rooms

3.1.1 Online marketplaces

Online marketplaces, such as Amazon, eBay, Alibaba and others have become ever-more relevant in the shopping habits of consumers, which is why they have caught the attention of counterfeiters. As already indicated by a joint study by EUIPO and Europol, (2019), the misuse of online marketplaces is becoming a key source of profits for organized crime groups involved in the sale of counterfeits. However, both the interviews and the analysis of the case studies in the present study demonstrate that these channels are usually well **equipped and controlled**, therefore being and, as such, less vulnerable to illicit activities, especially compared to other e-commerce channels. For example, large marketplaces, such as Amazon, have implemented next-generation automatic detection systems and strict seller vetting procedures (see Chapter 4). Box 3 shows that the fraudulent schemes detected on online marketplaces are becoming ever-more sophisticated, in order to circumvent the **advanced countermeasures** implemented by these operators.

Box 3. Online counterfeiting and cross-channel schemes

In November 2020, Amazon prosecuted two influencers in the United States who, via their social media accounts (Facebook, Instagram and TikTok), promoted counterfeits that were on sale in several online marketplaces, including Amazon, Etsy and DHgate (CNBC 2020; Amazon 2021b). The fraudulent scheme was detected by Amazon thanks to the activities of its Counterfeit Crimes Unit (CCU), which, besides the Amazon marketplace, proactively monitors other online channels (e.g., websites, social networks). The two influencers, together with eleven Amazon sellers, engaged in a sophisticated scheme to circumvent the anti-counterfeiting controls implemented by the marketplace:

- the sellers listed **generic, non-infringing items** on the marketplace, without including trademarks in either the pictures or the descriptions of the listings (thus preventing Amazon's automatic controls from detecting potential infringements – see Chapter 4);
- the two influencers promoted these listings on their social media accounts by posting side-by-side photos of the generic, non-infringing products and the counterfeit products with the key slogan: ***"order this/get this"***;
- the followers of the two influencers were then redirected to the listings of the generic, non-infringing products on Amazon using **hidden links**;
- after placing the order, rather than sending the generic products (**order this**), the sellers would ship the counterfeit products to consumers (**get this**).

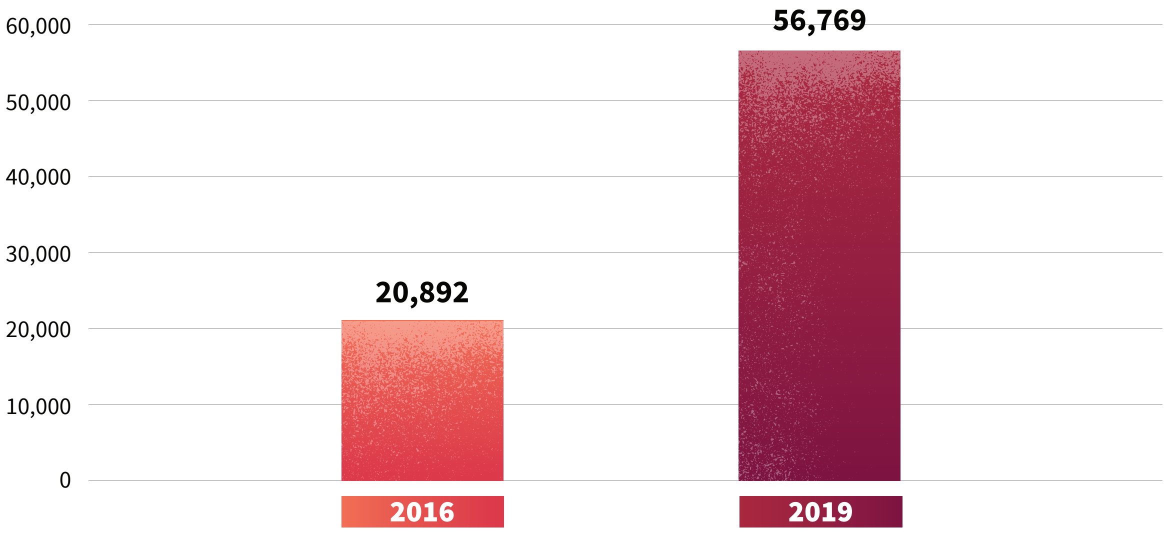
The two influencers recently accepted a civil settlement, paying a penalty that Amazon devolved to the development of brand protection activities, including awareness campaigns on online counterfeiting (Amazon 2021b). Amazon will now pursue the sellers that fraudulently declared to be located in the United States, while in fact they were in China (CNBC 2021).

3.1.2 Social networks

In recent years, several social networks have introduced marketplace sections and services to allow their users to sell and buy products (the so-called social commerce). There is growing interest among counterfeiters in these non-traditional platforms (Kennedy 2020; EUIPO 2021d; EUIPO e OECD 2021). The counterfeiters exploit social networks for their 'multiplicative' power, that is, for their likes and share content functions, which allow them to reach a wide number of users (EUIPO e OECD 2021). Several estimates from recent studies show these patterns:

- a study by EUIPO (2021c) estimated that almost **11% of conversations** about physical products on Facebook, Instagram, Reddit and Twitter were related to counterfeits;
- in Italy, the Ministry of Economic Development (2020) highlighted that the **IPR infringements related to online markets** reported through the '**Linea Diretta Anticontraffazione**' (a tool offered to consumers and brand owners in collaboration with the Guardia di Finanza), spiked over the course of the last several years, accounted for **86% of all reports** - with a high proportion of these being related to social networks such as Facebook and Instagram;
- a recent study (Stroppa et al. 2019) detected 56,769 Instagram accounts were being misused worldwide to sell counterfeits, **a 171% increase** on the 20,892 Instagram accounts that were detected in the 2016 edition of the study (Stroppa e Di Stefano 2016). The study estimated that, in 2019, these accounts published more than 64 million posts (a significant increase compared to the 14.5 million posts in 2016), reaching, via their followers, more than 20 million users;
- posts with hashtags related to counterfeits exceeded **100 million visualizations** worldwide on TikTok alone (Lince 2020).

Figure 4. Number of Instagram accounts selling counterfeits. Source: Stroppa and Di Stefano (2016) and Stroppa et al. (2019)



Counterfeiters not only employ social networks to advertise counterfeits, but also to exploit several other features:

- **posts and stories** on personal accounts and in private groups. The above-mentioned study estimated that the 56,769 social accounts misused by counterfeiters on Instagram published 64 million posts and, on average, 1.6 million stories every month (Stroppa et al. 2019);

- **live streaming** carried out by individuals (e.g., *influencers*) with a high number of followers (Lince 2020; EUIPO 2021f);
- **sponsored advertising campaigns**: a recent report by TRACIT and AAFA (2020) highlighted that, from May 2017 onwards, more than 70 major international brands were targeted by fraudulent adverts on social networks. These advertisements exploit the potential reach of social networks to redirect consumers toward third-party websites selling counterfeits. Even after being reported and subsequently removed, fraudulent advertisements are typically posted back online in a relatively short space of time, albeit with slightly different content. According to Carpani (2020) the rapid proliferation of this phenomenon is primarily due to:
    - the low operational costs;
    - lack of controls by social networks over accounts used to launch the sponsored campaigns (e.g., if the account has been opened recently, if the contents of the sponsored campaign are in line with the account);
    - lack of controls by social networks over the websites the sponsored campaigns redirect users to.
- **fraudulent comments and reviews** on the posts published by the brand owners on their official accounts, mainly through employing burner accounts and spam bots[11] (EUIPO 2021f).

Several **police investigations and judicial hearings**, both in Italy and abroad, have shown that counterfeiters use social networks contextually with other marketplaces and websites (see Box 4).

Box 4. Online counterfeiting and social networks: operation 'Aphrodite II'

Operation 'Aphrodite II', which was jointly launched by Europol and EUIPO, significantly addressed the violation of IPR on social networks, fostering a collaboration between brand owners and law enforcement agencies to both exchange relevant information and implement comprehensive enforcement actions. As part of Operation 'Aphrodite II' (June 2019), law enforcement agencies from 18 EU Member States, with the support of Europol, seized 4,700,000 counterfeit products and shut down 16,470 social media accounts and 3,400 websites (Guardia di Finanza 2019). Criminals promoted counterfeits on social networks, showing photos and prices of the products in chats and private groups. In several cases, hidden links redirected users to online marketplaces hosted by extra-EU servers. Negotiations between counterfeiters and clients took place on messaging apps or over the telephone through a number of figureheads. Clients paid with prepaid cards, PayPal, money transfers and other electronic payment methods, while counterfeits were shipped to end-consumers through postal services and couriers.

The investigation benefited from an effective information exchange between law enforcement and brand owners, especially thanks to take-down initiatives implemented by the latter. In particular, the information that was shared pertained to: (a) listings of suspicious products; (b) involved accounts; (c) third party websites that users were re-directed to.

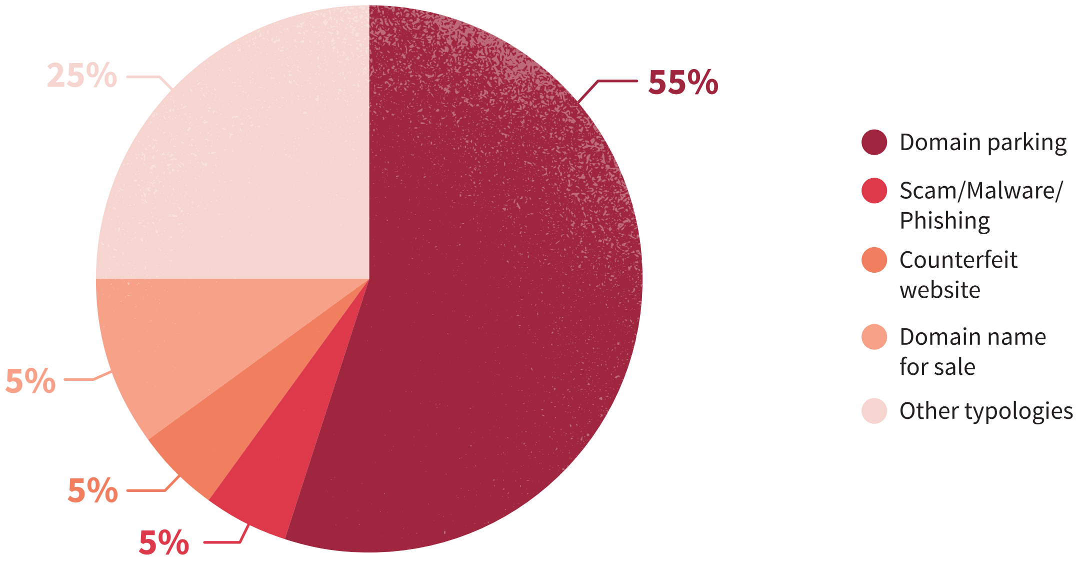
[11] Burner accounts are social media accounts (often disposable ones) that are used to post contents anonymously. Spam bots are software that allow actors to easily spam on chats, forums, and e-mails.

3.1.3 Website clones and fraudulent websites

Online counterfeiting has traditionally been associated with the sale of counterfeits through **fraudulent websites**, namely websites that mirror brand owners' legitimate websites in terms of having a similar domain, content and layout (Consiglio Nazionale Anticontraffazione 2019). The violation of an internet domain occurs by fraudulently registering at the *Internet Corporation for Assigned Names and Numbers* (ICANN)[12] either an identical (***cybersquatting***) or similar domain (***typosquatting***) to that of a registered brand. With respect to the former, another extension of an already existing internet domain is registered (e.g., .com, .info, .net, .org,). In the case of the latter, intentionally modified versions of already existing internet domains are registered (e.g., reversal of two letters, misspelling, inclusion of a prefix/suffix), in an attempt to exploit potential typing errors of users during internet queries.

A recent study by EUIPO (2021b) analyzed almost 1,000 internet domains (993) of 20 brand owners, concluding that **49% of them (486) were 'suspicious'**. 55% of these 486 internet domains were parked (*domain parking*)[13], 10% were on sale, while the remaining ones were employed for illegal purposes, such as, for example, hosting websites that sell counterfeits (5%), spread malware, or steal personal information (5%). In addition, another report by EUIPO (2017) interestingly found out that counterfeiters systematically re-register internet domains which were once registered by a different organization, thus trying to benefit from the popularity of the previous owner (e.g. search engine indexation, positive reviews). For example, the study reported that, in the United Kingdom, **71%** of 14.182 websites suspected of selling counterfeit goods were connected to an internet domain which was previously registered under the name of a different organization.

Figure 5. Type of use of internet domains considered to be 'suspicious' (N=486). Source: EUIPO (2021b)



[12] The *Internet Corporation for Assigned Names and Numbers* (ICANN) is a non-profit public-benefit corporation whose role is to both administrate and coordinate the global Internet's systems of unique identifiers and ensure the stable and secure operation of these systems.

[13] *Domain parking* refers to the registration of an Internet domain without associating it with any service (e.g., website, e-mail hosting).

In addition to fraudulent websites, the interviewees in this study pointed out the rapid proliferation of websites that **overtly sell counterfeits** as well as having internet domains that include specific keywords which are easily recognizable by clients (e.g., *replica, simulation, buying fake, best fake*). The sale of counterfeits adapted in response to the growing demand from certain clients (who are often very young) who are not interested in purchasing original products. In 2019, the *International Trademark Association* (2019) conducted a survey that involved 4,712 individuals, aged between 18 and 23 years of age (the so-called 'Gen Z'), in 10 different countries. 79% of these individuals reported that they willingly purchased counterfeits in the year prior to completing the survey, primarily because these products were easier to find (58%) or they simply could not afford the genuine ones (57%).

Box 5. Practices employed by counterfeiters to improve the rank of fake and clone websites

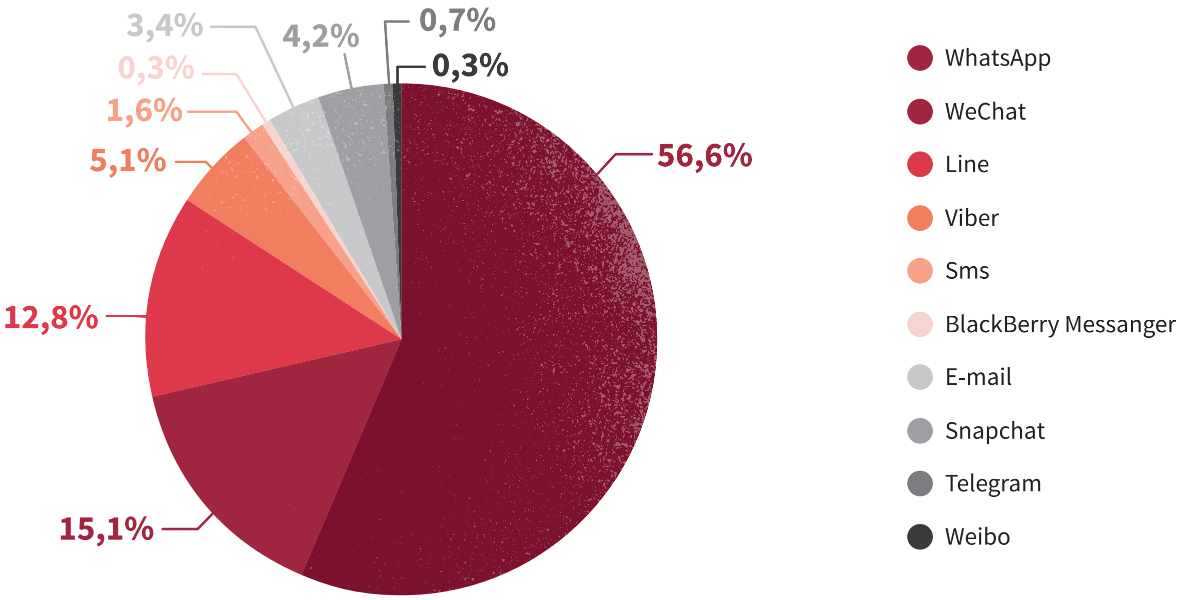
The layout and graphics of fraudulent websites imitate both the ***look and feel*** of legitimate brand owners, thus misleading users to believe that they belong to authorized sellers (Heinonen, Holt, e Wilson 2012; Kennedy 2020). Products are often promoted using **images taken from official catalogues** and sell for **plausible prices** that match those offered by authorized outlets (i.e., not extremely low as was the case a few years ago). Besides content and layout, the **rank of these fraudulent websites on popular search engines** is often a misleading factor. These websites are usually highly ranked in web queries due to:

- ***defacement:*** a cyber-attack that exploits the vulnerabilities of legitimate websites to include web pages selling counterfeits (often hosted by foreign servers);
- ***hidden keyword advertising:*** the registered trademarks of unaware brand owners are illicitly included (a) in a small font in the homepage of a website selling counterfeits, (b) in a font of the same color of the background of the homepage, (c) directly in the HTML code (meta-tags) or (d) in the JavaScript code (cloaking) of the website;
- ***linking:*** links that redirect users to websites that are external to the one they are surfing on.

3.1.4 Instant messaging apps

Among the several channels abused by counterfeiters, instant messaging apps also play a significant role in the sale of counterfeits. The above-mentioned study by Stroppa and colleagues found that 56.6% of the Instagram accounts involved in the sale of counterfeits communicated with their clients via WhatsApp, followed by WeChat (15.05%) and Line (12.8%), while only 5% used more traditional channels such as e-mail and SMS (Stroppa et al. 2019).

Figure 6. Instant messaging apps employed by individuals selling counterfeits on Instagram (N=56.769). Source: Stroppa et al. (2019)



These apps allow counterfeiters to:

- show **the list of counterfeits on sale**, for example in private groups;
- send **hidden links to the potential clients that redirect** them to other online marketplaces (also extra-EU);
- provide clients with details about **products** and **payment methods**;
- receive information on the **addresses** to which the counterfeits are to be shipped;
- **recruit individuals** to be involved in the sale of counterfeits.

Moreover, these apps are safer than traditional channels, insofar as, at least in most cases, they employ end-to-end encrypted chats and rarely close accounts for violation of the terms of service. Indeed, even in the rare cases that accounts are closed, counterfeiters can easily get new phone numbers and open new accounts (Stroppa et al. 2019).

Box 6. Recruiting individuals through social networks and instant messaging apps to sell counterfeits

In February 2020, the Guardia di Finanza of Luino (Varese, Italy) dismantled, as part of operation 'Falsi online', a complex criminal organization that was involved in the sale of counterfeits online (Guardia di Finanza 2020). The criminal scheme was as follows:

- counterfeiters posted on several social networks **job offers**, promising easy money without any need for prior work experience;
- the interested individuals were included in **private group chats on WhatsApp**;
- in these groups, the recruited individuals were then informed about how to advertise and sell counterfeits online.

In particular:

a. criminals at the top of the organization sent the new members (social sellers) photos of counterfeits and related prices;
b. the social sellers posted these photos **on their social media accounts**;
c. the clients **paid in advance by sending money to the PostePay cards** of social sellers themselves;
d. after receiving the payments and withholding a commission, **social sellers forwarded the money to the PostePay cards** of criminals at the top of the organization;
e. counterfeits were **mailed to the addresses of social sellers**, who then arranged the shipping to the end users.

How did law enforcement agencies and brand owners cooperate in this criminal investigation?

The Guardia di Finanza detected this criminal scheme by screening both e-commerce websites and social networks for listings of products on sale at extremely convenient prices. The analysis allowed for the identification of several sellers, acquiring the photos of the products for sale with details of the related trademarks (e.g., tags, zips). At this point, the **affected brand owners were brought into the fold** and, through specific technical reports, ascertained the non-originality of the products. Later, Guardia di Finanza carried out an **OSINT investigation** to collect relevant information for identifying the individuals behind the social media accounts (e.g., profile photo, birthdate, birthplace).

3.1.5 Online forum and other chats

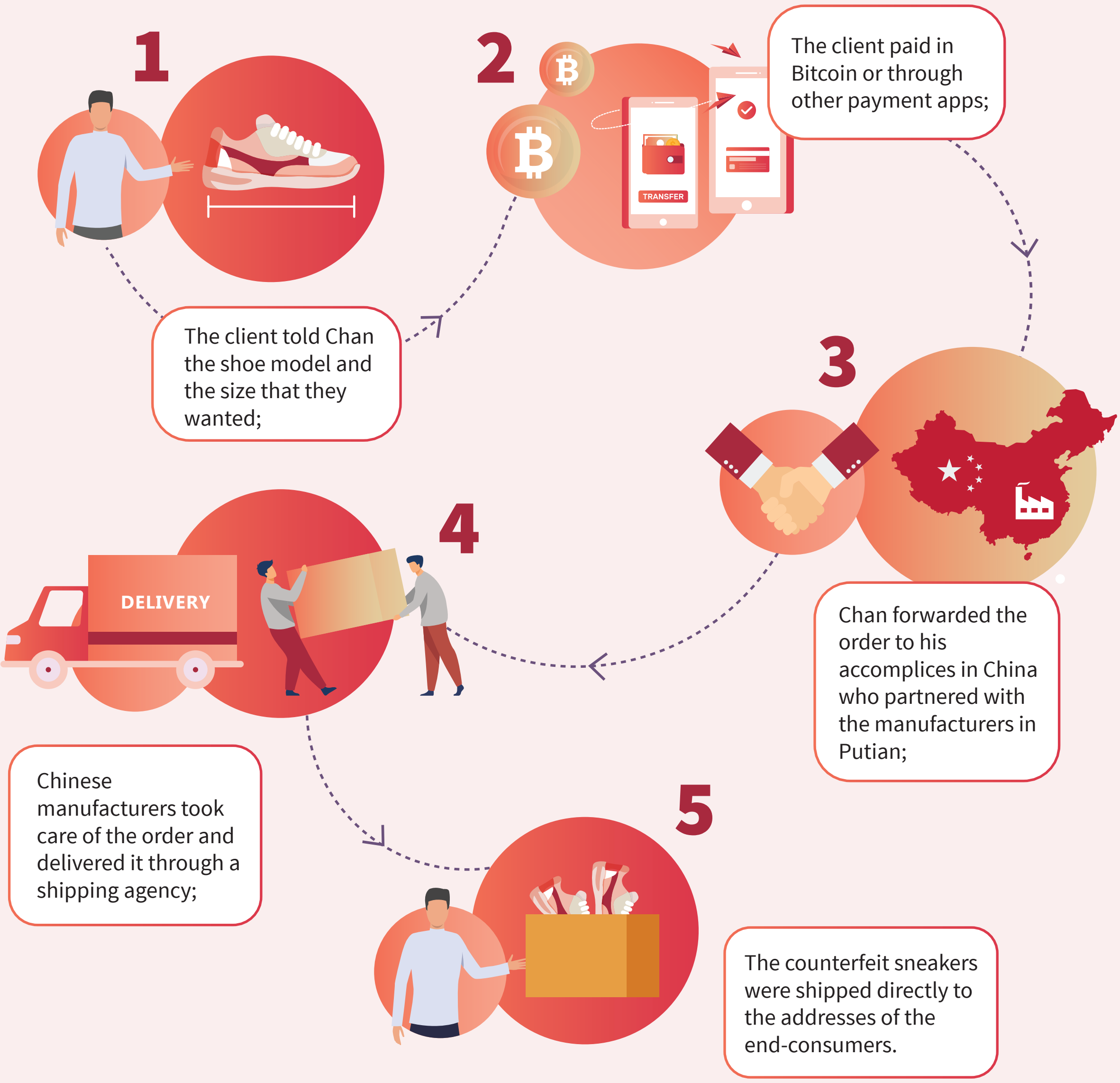
This channel is often linked to clients who willingly focus on the secondary market and buy products that, both given the characteristics and the sale methods, are clearly identifiable as counterfeits (***non-deceptive counterfeiting***). For these clients, counterfeiting represents the possibility to buy products at significantly lower price than the official listings. **Forums are among the preferred channels for sharing information** about where to buy the best counterfeits, who are the most reliable sellers, and how to spot low-quality replicas (Kennedy 2020). For this reason, these users have also developed a specific terminology for communicating among each other. For example, on *r/FashionReps* (a subreddit with more than 647,000 members that is entirely dedicated to fashion replicas) there is a guide for new members that explains the most frequently used terms, such as (Reddit 2018):

- **QC (Quality Control):** a user posts the photo of a purchased replica to ask the other users for feedback on its quality;
- **GL (Green Light):** a user answers a request for quality control and confirms the good quality of the replica;
- **LC (Legit Check):** a user posts a photo of a purchased product to ask the other users about its legitimacy;
- **W2C (Where to Cop):** a user asks where to buy a specific product;
- **1:1 (One to One):** the replica is identical to the genuine product;
- **B&S (Bait & Switch):** a seller is not reliable and users should not buy from them.

Box 7. Replicas and forums: the parallel market of sneakers

The sneakers market is characterized by a large community of enthusiast consumers (the so-called *sneakerheads*), who are willing to spend a lot of money for the most desirable models. These are often sold in limited editions and in selected shops, which drives **those who are not willing to spend a lot of money** to buy them on the secondary market. On Reddit, for example, the subreddit **r/Repsneakers** has almost 480,000 members who post daily photos of the replicas that they want to buy and ask advice from other users, as a sort of quality control check. If the replica fails the test, then the client reports the detected flaws and differences to the manufacturers, asking for better products (Wall Street Journal 2019).

In 2018, a Chinese medical student in the United Kingdom posted on r/Repsneakers in an attempt to gauge the potential interest of the community in buying counterfeit sneakers that he could provide as a result of his personal contacts with Chinese manufacturers in Putian (Vice 2018). Satisfied with the feedback, Chan open his dedicated subreddit (r/chanzhfsneakers) and, shortly afterwards, had more than 10,000 clients and a waiting list of more than 3,000 individuals. The scheme was as follows:



The client told Chan the shoe model and the size that they wanted;

The client paid in Bitcoin or through other payment apps;

Chan forwarded the order to his accomplices in China who partnered with the manufacturers in Putian;

Chinese manufacturers took care of the order and delivered it through a shipping agency;

The counterfeit sneakers were shipped directly to the addresses of the end-consumers.

Videogame chats are another channel that can be exploited to sell illegal goods, ranging from stolen personal data to counterfeits (CBS News 2019). This adds up to the criminal risks related to in-game transactions, such as money laundering and terrorist financing (Moiseienko e Izenman 2019; Wronka 2021).

3.2 Actors

Both the analysis of the case studies and interviews highlighted **the wide variety** and **increasing professionalization** of the criminal actors involved in the sale of counterfeits. Counterfeiters are now capable of both manufacturing copies that are close replicas of the genuine products and carrying out more complex schemes to sell and distribute such counterfeits goods, due, in part, to their extensive technological, cyber, and financial/corporate expertise. Generally speaking, three main categories of criminal actors can be identified:

- ***'influencers':*** individuals, who are often young, who act as intermediaries on social networks in order to attract end-consumers and connect them with the manufacturers of counterfeits;
- ***'brokers':*** professionals, both individuals or criminal groups, who provide expertise and services in both the cyber and financial/corporate domain;
- **organized crime groups:** ranging from Italian Mafias to foreign criminal groups, in addition to sometimes being linked to terrorist actors.

3.2.1 'Influencers'

The presence of individual actors, who are often young, who act as intermediaries between the supply of counterfeits (usually located in south-east Asia) and the demand, and abuse social networks and **drop-shipping** models (see Box 8). The latter refer to a wholly legal practice, which allows sellers to trade products without storing them, instead relying on one or more third-party vendors. The seller collects the orders and then forwards them to vendors, who then directly ship the products to clients through postal or courier operators.

The increased misuse of small parcels in online counterfeiting is well documented in the statistics reported in the last report by OECD-EUIPO (2021). The **91% of the counterfeit goods seized** in the EU which are linked to e-commerce sales involve the postal system. In contrast, **only the 45% of goods not linked to online sales** involved the postal system, since they are also frequently shipped via other transportation channels (e.g., containers). Unfortunately, the study - the only one that provides statistics on counterfeits related to online sales that have been seized - does not provide figures for Italy.

Box 8. Sale of counterfeits and drop-shipping: the operation 'Bologna Luxury'

Operation 'Bologna Luxury' benefited from the cooperation between brand owners and law enforcement agencies. The **starting point** of the police investigation was the **take-down** of a website selling counterfeits that was successfully carried out by a fashion brand owner during its activities of internet brand protection. The legal department of the brand owner formally shared with the Nucleo Speciale Beni e Servizi of Guardia di Finanza information on the activities being carried out, reporting the **social media accounts that were involved, and the social media posts that had been removed**. The information exchange allowed Guardia di Finanza to employ it in the related police investigation, which subsequently identified the offenders and traced the illicit financial flows. The investigation later ascertained that a **young influencer who acted as an intermediary** between consumers and Chinese manufacturers was behind one of these social media accounts (called *'Follie_di_lusso', luxury madness*), which was active on both Facebook and Instagram. The scheme, that generated more than 200,000 euros of revenues in a few weeks, was as follows:

- the client chose the products from the list;
- the client negotiated the price with the seller via private chats on WhatsApp;
- the influencer, after receiving the payment (through wire transfers or PostePay), forwarded the illicit proceeds (after withholding a fee) to the PayPal accounts of the Chinese manufacturer;
- the influencer, always using WhatsApp, reported to the Chinese manufacturer the details of each order, including the addresses of where to ship the counterfeits;
- the Chinese manufacturer shipped the counterfeits in small parcels directly to the address of the client, without allowing for any returns or reimbursements.

As part of the police investigation, Guardia di Finanza also started **a formal interlocution with the social networks**, by means of an international letter rogatory, to collect the necessary elements to identify the criminals behind the social media accounts, such as **log files, phone numbers and payment methods**. After identifying the e-mail address of the suspected influencer, Guardia di Finanza also made a request to PayPal, by means of the Safety Hub – PayPal Law Enforcement, to share transactional data associated with the influencer's accounts, to confirm the illicit financial flows which had already been identified and traced thanks to the financial investigation carried out with PostePay.

3.2.2 'Brokers'

Counterfeiting benefits from collaborations with criminal groups specializing in ***crimes-as-a-service*** **(C-A-A-S)**, which is also the case for other economic and organized crimes at the EU level (Europol 2020). In the counterfeiting schemes analyzed in the present study, professionals who provide their expertise and knowledge **in the cyber/IT and financial/corporate domain** are frequently involved.

IT and cyber specialists

These brokers support counterfeiters in the:

- **design and development** of fraudulent websites;
- development of **shopping carts** and cash-out systems for websites, both legitimate and fake ones;
- development and management of **malwares** to be conveyed via fraudulent websites to steal the personal data of unaware consumers, before subsequently being used to extort money or be resold on the dark web;
- **development of bots** that are then employed on forums and online chat rooms to promote counterfeit goods and fraudulent marketplaces (e.g., *spam-bots*).

Within this domain, actors from **Eastern Europe and Russian-speaking countries prevail** and are frequently involved in other types of online fraud and cybercrime (Europol 2020). In this regard, it is interesting to note that **7.6%** of the 56,769 Instagram accounts used by counterfeiters redirected users to e-commerce websites with Russian Internet domains (.ru) (Stroppa et al. 2019).

Box 9. Web-developers, fraudulent websites, and online counterfeiting

As part of operation 'Zombi' (December 2019), the Guardia di Finanza of Genova seized and took down **475 websites** used to sell fake clothing and accessories. The criminal organization benefited from the help of **professional web-developers**, who used the Internet domains of bankrupt and failed companies which, because they were still available, could be abused to host e-commerce websites selling fake shoes. The websites were hosted on **foreign servers** and registered to **foreign individuals**, who were registrants of several other fraudulent websites (Ministero dell'Interno, 2021).

Corporate and financial intermediaries and shell companies

These are individuals - not to mention professional firms - that provide their expertise and knowledge for setting up and managing shell companies that are engaged in selling counterfeits, both online and offline. Shell companies are employed for various reasons, according to the cases studies collected for the purposes of this study:

Importing counterfeits to be sold online

Several police investigations have demonstrated how shell companies import and sell counterfeits through **false invoicing and false documents** (e.g., false certification of origin, fraudulent delivery notes) (FACT Coalition 2019). For example, these companies, which are often registered abroad and in countries with low levels of corporate transparency, were even used to justify the purchase of medicines (counterfeited or stolen ones) that were then resold through online pharmacies (Savona e Riccardi 2018; AIFA 2021a).

Box 10. Fake Rolex watches, websites, and accountants

As highlighted by Ministero dell'Interno (2021), as part of operation 'Right Time' (September 2019), the Guardia di Finanza of Viareggio e Pisa arrested 6 individuals who were in charge of a complex fraudulent scheme that sold luxury watches, both in physical markets and online marketplaces. The criminal organization benefited from **the consultancy work of an accountant**, who helped to open and manage shell companies that were **registered in the names of figureheads** (usually, low-income individuals) and which were used to both make the watches appear to be original goods (by means of **false invoices**) and for laundering the illicit proceeds.

Registering and managing fraudulent websites

Shell companies, registered in the name of figureheads, may be used to **set up and manage websites** that are used for selling counterfeits, stealing card information and identity cards, and spreading malware. As also highlighted by a recent joint report by OECD and EUIPO (2021b), counterfeiters employ shell companies to **register payment accounts** that allow them to receive payments over fraudulent websites. Such providers, which are also known as *rogue payment facilitators* (McCoy 2016), offer services that allow counterfeiters to avoid both the use of traditional payment circuits and related countermeasures (Tian et al. 2018).

Opening seller accounts on online marketplaces

Shell companies can be used as sellers on online marketplaces as well as eventually covering the sale of counterfeits. Despite seller vetting procedures being significantly enhanced in recent years (see Chapter 4), the largest marketplaces continue to be victimized by fraudulent sellers (FACT Coalition 2019). Nevertheless, if large marketplaces as Amazon and eBay have proper tools in place to detect and proactively block anomalous sellers' behavior, smaller ones are often unequipped and may easily fall prey to fraudulent sellers, eventually spreading counterfeits among their consumers.

Box 11. Fraudulent sellers are prosecuted for selling counterfeit smartphones

In 2018, ten individuals were prosecuted by the Federal Court of Idaho for selling counterfeit smartphones on Amazon and eBay. The collaboration between these marketplaces and law enforcement agencies allowed for the dismantling of a complex fraudulent scheme that involved the import of goods from Hong Kong, their repackaging in the United States and subsequent selling on the above-mentioned platforms via seller accounts opened using shell companies (U.S. Attorney's Office 2018; FACT Coalition 2019). The scheme generated almost 2 million USD in criminal proceeds, which were later seized by the authorities.

Counterfeiting and money laundering

Shell companies can be used to obfuscate or facilitate the laundering of illicit proceeds deriving from the sale of counterfeits, employing well-known typologies that are also used for other criminal activities (for a review see Does de Willebois et al. 2011; Savona e Riccardi 2018; Bosisio et al. 2021). In this sense, it is worth mentioning Operation 'Pinar', which was carried out in 2016 by the *Spanish Policia Nacional and Agencia Tributaria* with the support of Europol. The operation dismantled a criminal organization involved **in both the selling of counterfeits and money laundering**, seizing almost 265,000 counterfeits, 30 luxury cars, eight pieces of real estate and 150 bank accounts (Europol 2016). The criminal organization laundered more than 9 million euros **through false invoices between shell companies (registered in the names of figureheads)**, while also moving the illicit proceeds abroad. The criminal group employed four financial advisors, who helped them to launder the illicit proceeds.

Transaction laundering is a lesser known phenomenon, but is equally relevant to our discussion here. It allows criminals to use **e-commerce to cover for illicit payments or transactions** (Moiseienko 2020). A shell company can open a seller's account on a marketplace to carry out fictitious transactions with an accomplice, individual or company that buys apparently legitimate goods or services, in order to conceal several criminal purposes (Cassara 2016; Miller, Rosen, e Jackson 2016), namely:

- **buying illegal goods or services** (e.g., drugs, weapons, paedo-pornographic material), distributed via parallel channels;
- **disguising the movement of illicit proceeds**, for the purposes of laundering money or financial terrorism, in addition to using mispriced transactions (in other words, 'e-commerce trade-based money laundering').

The case US vs Mohamed Elshinawy (n. 18-4223) serves as an illustrative example of this strategy. The criminal investigation uncovered a **terrorist financing scheme which used fictitious e-commerce transactions** on eBay (US District Court of Maryland 2018). Mohamed Elshinawy, a US citizen, was recruited in 2015 by another man, S.S. (anonymized), a Pakistani engineer who lived in the United Kingdom. S.S. sent funds to the recruits through fictitious transactions on eBay carried out by Ibacstel Electronics Limited, an electronics company located in Cardiff. S.S. issued false invoices for fictitious purchases from Elshinawy (who pretended to sell printers on the marketplace) and wired the funds using PayPal. FBI investigators traced, over the course of a four-month period, transactions amounting to almost 8,700 USD that Elshinawy planned to use for carrying out a terrorist attack on US soil.

To highlight the growing relevance of transaction laundering, it should be noted that several **suspicious transaction reports** have been filed to the Financial Intelligence Units (FIUs) of several foreign countries, such as the United Kingdom, by those online marketplaces who also manage the transactions, and also act as obliged entities subject to anti-money laundering regulation (Couvèe 2019; Moiseienko 2020). Chapter 5 provides recommendations concerning how to take inspiration from successful examples **in the anti-money laundering domain**, in order to strengthen the fight against online counterfeiting.

Box 12. Characteristics and anomalies of shell companies acting as legitimate sellers on online marketplaces to sell counterfeits

From the analysis of the case studies, it is evident that most of the shell companies disguised as legitimate sellers on online marketplaces are characterized by several **red-flags and anomalies** that mirror the alerts already highlighted by anti-money laundering guidelines, such as:

- being located in countries characterized by low levels of corporate transparency, or in Free Trade Zones (FTZs) (FACT Coalition 2019; Ministero dell'Interno 2021);
- ownership control by opaque corporate vehicles (e.g., trusts, foundations, fiduciaries) and lack of information about beneficial owners (Bosisio et al. 2021);
- anomalous ownership complexity, not justified by the firm's size and business sector (Jofre et al. 2021);
- registered office located in an address where several other companies, in different business sectors, are also registered;
- financial anomalies (e.g., low fixed assets, low cash flow, low personnel costs) (Pellegrini et al. 2020);
- frequent and unjustified changes of company name, type of company and registered office;
- anomalous characteristics of shareholders and administrators (e.g., too young, too old, professional background not compatible with the role).

3.2.3 Organized crime groups

Section by 'Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale - Dipartimento della Pubblica Sicurezza - Ministero dell'Interno'

The countermeasures to be adopted in the fight against organized crime and counterfeiting groups must consider several key elements that define the evolution of this criminal phenomenon across the globe, such as:

- the ever-increasing **transnational dimension** of this illegal activity, characterized by the shift from manufacturing in traditional industrial districts in Italy to large countries, such as China and India, but also Turkey, Egypt and Hong Kong for specific product categories;
- the **change of trade routes** through which counterfeit goods reach Italy from their country of origin. These routes do not typically employ the biggest national ports, but rather follow complex itineraries: illegal goods may transit through countries such as the United Arab Emirates, Singapore, Morocco, prior to entering the EU customs area via countries like Greece, Slovenia and Bulgaria, where customs controls are laxer, before finally being transported by land to Italy;

- the exponential increase in the online sale of counterfeits mainly stems from the **wide array of virtual shops** provided by the Internet as well as the anonymity it affords to criminals;
- the emergent **trend of fractionating illicit shipments into smaller units** that are then delivered by either couriers or passengers at airports/ports or large shipment companies;
- the emergent trend of applying **counterfeit trademarks** to the products immediately prior to the sale, so as to prevent law enforcement agencies from seizing the products during the shipment;
- the increasing number of Free Trade Zones,[14] which are often employed in illicit schemes.

Box 13. Counterfeiting and Free Trade Zones

Free Trade Zone (FTZs) are industrial and commercial zones that, despite their heterogeneity, are generally territorially delimitated areas, which are often located near large airports and port infrastructures. The companies registered in these areas may import, manufacture and export goods benefiting from lower customs fees, more favorable tax conditions and lower administrative and corporate obligations compared to those established by the national law of the country in which the FTZs are located. However, FTZs can be abused by counterfeiters as logistics transit areas to:

- disguise from customs officials the origin of illicit goods from high-risk countries;
- set up shell companies that hinder, in the case of police investigation, the identification of criminals involved in the illicit trade;
- break down the shipments into smaller parcels in order to limit the potential losses in the event of seizure;
- hide counterfeits among legitimate goods;
- apply trademarks to unlabeled goods.

According to a study by OECD and EUIPO (2018), the existence, number and dimension of FTZs are correlated with the overall value of counterfeits exported from the country in which they are located. The establishment of a new FTZ causes a 5.9% increase, on average, of the overall value of these exports.

In the Italian context, **three different criminal organizations** (which are in any case interconnected) take part in the illicit market of counterfeit goods: Italian mafias, non-mafia organized crime groups and foreign organized crime groups.

The main police investigations that have been conducted from 1990s until the present day indicate that Camorra is the Italian mafia organization with the most interest in counterfeiting and piracy. Camorra groups do not only participate directly in counterfeiting by employing, for example, their members and economic resources, but rather also participate in a more indirect manner, by providing to other criminal groups that are active in this illicit market, in return for a share of the illicit proceeds, their economic resources, protection and contacts.

[14] Free Trade Zones, which were only 79 in 25 countries in 1975. Today, there are almost 3,500, FTZs covering 130 countries: to, compared to 79 FTZs in 25 countries in 1975. To better understand their economic role, it should be noted that in the "Jafza Free Trade Zone" alone, which was established at Dubai (EAU) in 1985, hosts more than 7,000 companies from more than 100 countries and employs 144,000 workers.

The foreign criminal groups active in this illicit activity in Italy are mainly Chinese, who benefit from their business relationships with the motherland and the large Chinese communities in other EU countries; however, criminal groups from the Balkans and Eastern Europe are also actively involved in importing and distributing counterfeit cigarettes, while African criminal groups (from Morocco, Nigeria and Senegal) are involved in the retail sale of counterfeits in the territory. Finally, it should not be overlooked that counterfeit trade may represent an expedient channel for financing other serious and organized crimes, including terrorism (Box 14).

Box 14. Links between counterfeiting and terrorism

The potential links between counterfeiting and terrorism have been highlighted previously, especially in relation to extremist organizations like the Irish Republican Army (IRA), the Euskadi Ta Askatasuna (ETA), the Fuerzas Armadas Revolucionarias de Colombia - Ejército del Pueblo (FARC) and the 'Ḥarakat al-Muqāwama al-Islāmiyya (HAMAS), who have been involved in the counterfeiting of veterinary medicines, cigarettes and CDs. Indeed, AL QAEDA, in some training manuals that were retrieved in 2002, explicitly recommended to its terrorist cells to sell counterfeits to finance their activities (AACP 2002). These connections remain relevant today. One of the members of the terrorist cell that carried out the attacks in Paris in November 2015 was also involved in importing counterfeit sneakers into France from China (UNIFAB 2016).

In this context, law enforcement activities should aim, first and foremost, to identify and dismantle the criminal groups that manage the illegal supply chain of counterfeit goods, thus damaging the supply of the entire market. In addition to investigations aimed at tracing the supply chains of counterfeit goods, territorial controls should also be implemented that aim toward:

- controlling the imported goods to seize counterfeits intended for the national market;
- opposing the distribution of these goods in the geographical areas most frequented by the public.

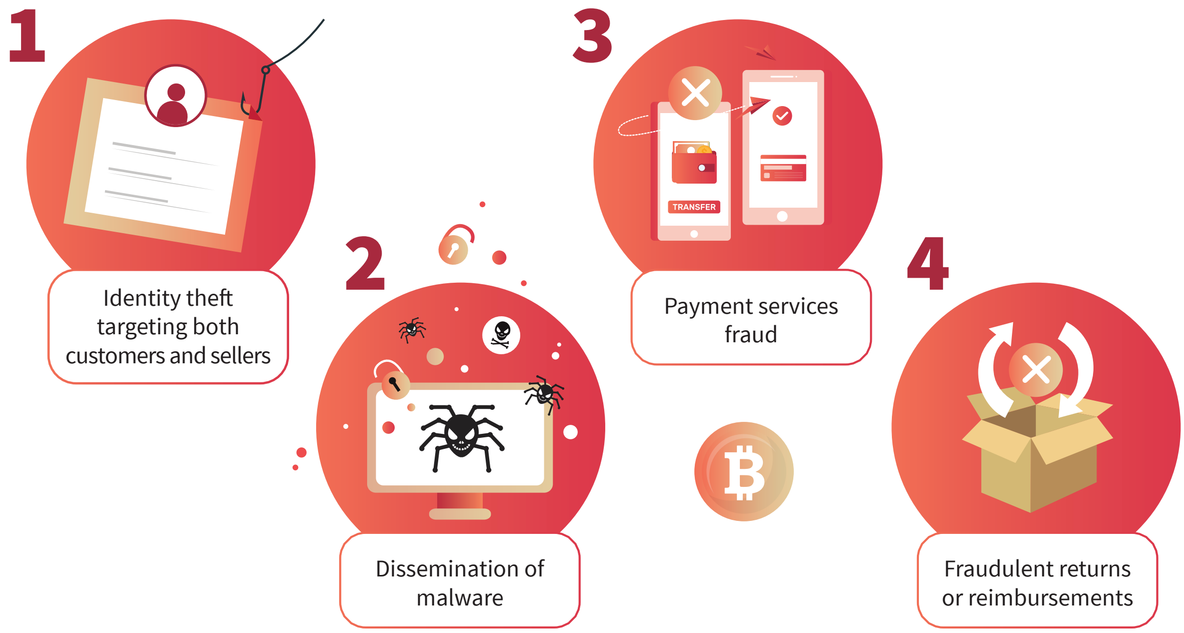
The long-term aim of such enforcement strategies would be to produce:

- a reduction in the illicit activities related to the injection of counterfeit goods onto the market, due to lowering the number of illegal street vendors operating in the territory;
- more significant results, since investigations based on intelligence activities would focus on the production, importation and wholesale distribution phases.

3.3 Schemes

The heterogeneity of the aforementioned channels and criminal actors involved in counterfeiting manifests itself in **the growing interconnection between criminal schemes**, which is symptomatic of the increasing poly-criminal nature that has already been identified at both the national and international level (Europol e EUIPO 2020; Europol 2021a). The sale of counterfeits constitutes only a part of a far more complex environment, where cross-links with **other economic crimes and cybercrime** have become ever-more frequent and relevant.

The criminal actors involved in the sale of counterfeits online attempt to benefit from the interaction with online marketplaces, **exploiting all the services offered**: purchases, payments, returns, reimbursements, and account registrations. The aim of counterfeiters is not merely to sell their illegal goods, but rather to also benefit from a wide array of other criminal activities, such as:


1
Identity theft targeting both customers and sellers
2
Dissemination of malware
3
TRANSFER
Payment services fraud
4
Fraudulent returns or reimbursements

Alongside the 'customer journey', then, we can also speak of the fraudster journey, which comprises several steps and crimes, not all of which are always necessary, but are often carried out simultaneously. These offenses will be discussed in greater detail below.

3.3.1 Identity theft targeting both consumers and sellers

Account takeover (ATO) occurs when bad actors steal a user's credentials and take control of their e-commerce account. In a recent study, TransUnion (2020) observed that there had been a **347%** increase in these types of attacks worldwide between 2018 and 2019. After gaining access to the account, criminals modify the related information (e.g., passwords), transfer money to their bank accounts, make fraudulent purchases on online marketplaces or even gain access to other accounts of the victim. Criminals obtain this information in different ways (Vigderman 2021), such as:

- purchasing stolen personal information on the ***dark web*** (or that comes from data breaches/leaks);
- stealing the personal information of consumers surfing on **fake and other fraudulent websites** (e.g., advertisement banners that download malware);
- stealing through **cyber-attacks** (e.g., phishing emails, social engineering, compromised business e-mails, brute force attacks).

Alongside customers' accounts, sellers' accounts are also targeted by counterfeiters. In this case, credentials are also stolen by using **social engineering techniques**, particularly phishing emails[11]. After gaining access, counterfeiters then modify:

- the payment method registered on the platform. As a consequence, **proceeds from orders are redirected to the bank accounts of counterfeiters and fraudsters**;
- the inventory of sellers, **including counterfeits**. In several cases, counterfeiters themselves buy these goods, using cloned credit cards, and then ask for reimbursement for non-delivery (*reimbursement fraud*) or launder the illicit proceeds.

3.3.2 Payment service fraud

Once they have gained access to e-commerce accounts and the related details of payment methods (e.g., credit cards), criminals often employ **scripts or bots to automatically make several small purchases** to both determine if the stolen card information is still valid and to assess potential spending limits (Canfield 2018). After these tests are run (***card testing***), the stolen card information is then either used to make large purchases until the credit runs out or is resold on the Dark web (CyberSource 2020).

When the cardholder notices the fraudulent transactions, they generally dispute them to their bank that subsequently issues a **refund** (***chargeback***) and charges a fee to the merchants involved. After receiving the refunds, clients generally do not report being victimized to law enforcement agencies, which, on the one hand, penalizes online marketplaces, especially those that are unrelated to the fraud, and, on the other hand, hampers the monitoring capabilities of law enforcement agencies themselves. Some initiatives have been launched to address this problem. For example, in 2012, '**Project Chargeback-Leading the Charge(Back) against fakes**!' was launched in Canada (see Box 23 in Chapter 4).

Box 15. Employment of cloned credit cards in fraudulent schemes

Between May 2019 and October 2020, a marketplace interviewed for the FATA project detected suspicious behavior related to some of its accounts (recently created) while monitoring activities related to orders and returns. The scheme was as follows:

- criminals opened an account as customers;
- **after a few minutes**, the same account **placed an order of a significant amount**, paying with a credit card and **requesting express delivery**;
- **when the order was not delivered yet**, the account requested a return with reimbursement in the form of credit to spend on the marketplace (transferable to other payments methods associated with the consumers);
- during the delivery, the courier did not find anyone at the address associated with the order, while **the associated phone number was disconnected**;
- the order was returned to the warehouse, and, after a couple of days, the return was accepted, and the **reimbursement issued**;
- **the credit issued to the customer was then transferred** to other payment channels of the offenders, namely its PayPal account.

After a detailed investigation, the marketplace discovered that the credit cards used for purchasing goods **had been cloned** and that the bank had already reimbursed the cardholders. The marketplace sent all the relevant documents to PayPal, requesting the closure of the account. After more than a year and several reminders, PayPal closed the account. Despite this intervention, the criminal **simply modified their fraudulent scheme**, creating a new PayPal account for each new account opened on the marketplace. At this point, the marketplace started analyzing all transactional data to detect potential fraud red-flags. By cross-checking data on the **geographical area, IP addresses, payment methods and chosen delivery**, the marketplace detected several fraudulent orders placed using the same procedure, probably by the same criminal actor using a smartphone (detected requesting a password change from one of the accounts) and/or from a public Internet point (the orders were always placed between Monday and Friday from 9:00 AM to 17:00 PM).

3.3.3 Fraudulent returns

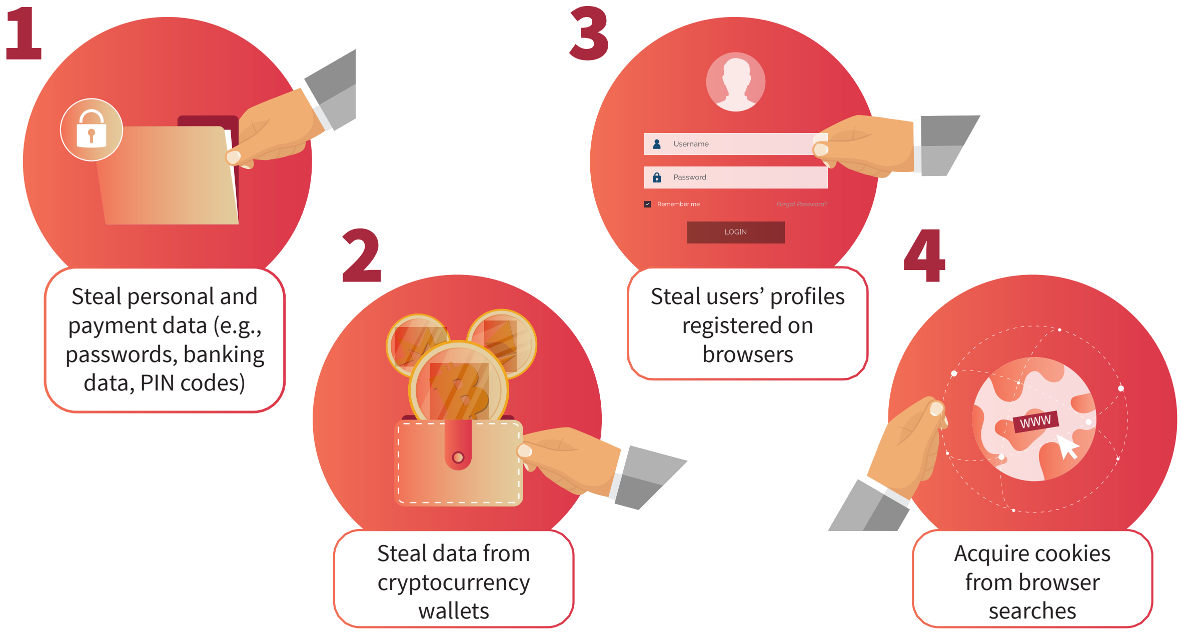
Counterfeiters, using either ad-hoc accounts or violated ones, make purchases on e-commerce marketplaces but, after receiving the goods, return **counterfeit products** instead of the original ones. The genuine products are then used to study trademarks to produce more similar copies or to be resold on the secondary market (Bosisio et al. 2017). These fraudulent schemes are also facilitated, according to the researchers of Flashpoint (2019), by the sale of serial numbers of genuine products and false receipts on forums in the Deep Web.

Box 16. Fraudulent returns and counterfeits

Between March and April 2021, an online marketplace interviewed for the FATA project identified a fraudulent scheme involving the returns of counterfeits. The accounts involved (all associated with the same EU country) purchased luxury clothing on the marketplace and, immediately after, returned counterfeit versions. These copies were proactively detected by the marketplace thanks to specialist operators, who ascertained differences in materials, tags and logos compared to the genuine products. In this sense, the marketplace further enhanced the collaboration between brand owners who ask for 2D and 3D scans of their products, thus facilitating the automatic detection of fraudulent returns.

3.3.4 Diffusion of malware

Fake and fraudulent websites for selling counterfeits may also be used to **spread malwares**[15] to infect the devices of unaware users to:



1. Steal personal and payment data (e.g., passwords, banking data, PIN codes)
2. Steal data from cryptocurrency wallets
3. Steal users' profiles registered on browsers
4. Acquire cookies from browser searches

[15] Malware (or malicious software) is an umbrella term that includes any program or file that is intentionally harmful to a computer, network or server.

Box 16. Fraudulent returns and counterfeits

On September 2021, both the *Cybersecurity and Infrastructure Security Agency* (CISA) and the Federal Bureau of Investigation (FBI) acknowledged the proliferation of the ransomware-as-a-service (RaaS) 'Conti' in cyber-attacks to several organisations at the global level (CISA 2021). Among the access to users' devices (es. *spear phishing*[16], *vishing*[17]), criminals also employed counterfeit *software*, advertised through ad-hoc developed portals, which were then downloaded by users. Once access to clients' devices had been obtained, the criminals then implemented the so-called 'double extortion' strategy, that is, the collection, encryption and then publication of the stolen personal data if the ransom was not eventually paid (usually asked for in cryptocurrencies).

[16] Spear phishing is a type of fraud that targets a specific company or individual. In contrast to phishing, criminals tailor their attacks by using information on victims collected via social engineering techniques, as to increase their efficacy.

[17] Vishing (or *voice phishing*) is the name given to a type of phishing that involves the use of voice calls and voice audio.

4.

Preventing and combating counterfeiting: challenges and best practices

As discussed in the previous chapter, current best practices in the fight against emergent online counterfeiting threats, in addition to improved enforcement against the counterfeiters, can be classified into two main branches:

- **prevention** through the control and monitoring of (a) products, (b) advertisements and listings, (c) sellers active on online marketplaces;
- **cooperation and information exchange** between the different stakeholders, particularly among law enforcement, marketplaces, and brand owners.

Chapter 4 describes in detail these two lines of activities, and highlights, on the one hand, **the challenges associated with these approaches**, and, on the other hand, the **best practices** implemented by actors in this field. Based on the interviews, case-studies and scientific literature, where available, the following elements are discussed:

- a description of the prevention and cooperation initiatives undertaken by the parties active in this field;
- information, where available, on the positive impact that the selected best practices have generated.

4.1 Prevention

Prevention of online counterfeiting aims, first and foremost, at ensuring that counterfeiters cannot access the online market, to minimise the number of counterfeit goods on the web, protect consumers and increase their trust in e-commerce. In this sense, three activities appear to be particularly relevant:

The **tracking and tracing** of original products

The **monitoring of listings and messages** on online channels

The **due diligence of sellers** (*Know Your Business Customer or Seller vetting*)

Box 18. OECD guidelines to address emerging challenges of online counterfeiting

In December 2021, the OECD published the study 'E-commerce Challenges in Illicit Trades in Fakes: Governance Framework and Best Practices' (OECD 2021) to provide an overview of both public and private countermeasures designed to address the abuse of online platforms by counterfeiters. OECD suggests addressing the following issues in periodic re-examination of such measures:

- engaging e-commerce platforms in detecting illicit transactions and taking actions against the responsible;
- promoting the establishment of industry-led solutions including, for example, voluntary 'codes of conduct' to allow private stakeholders to show their excellence;
- promoting industry self-regulation to address emerging threats;
- reviewing and amending both international and national anti-counterfeiting policies to significantly alter the risk-reward ratio for counterfeiters;
- promoting data sharing among shareholders to overcome jurisdictional and institutional gaps;
- engaging all the intermediaries including postal, courier, social media logistics providers and payment processors;
- reviewing the adequacy of information on small shipments and the role of intermediary vendors;
- applying the WTO-TRIPS Article 60 *de minimis* exemption only to goods accompanying incoming passengers and not small parcels;
- enhancing vetting of third-party vendors;
- protecting the privacy of online stakeholders.

4.1.1 Monitoring of products

Anti-counterfeiting track and trace systems rely on **different technological and organisational solutions**, which guarantee the origin of the product, from the manufacturing process itself right up until the end consumption. The main approaches are discussed here in turn alongside the relevant best practices.

Track and trace solutions

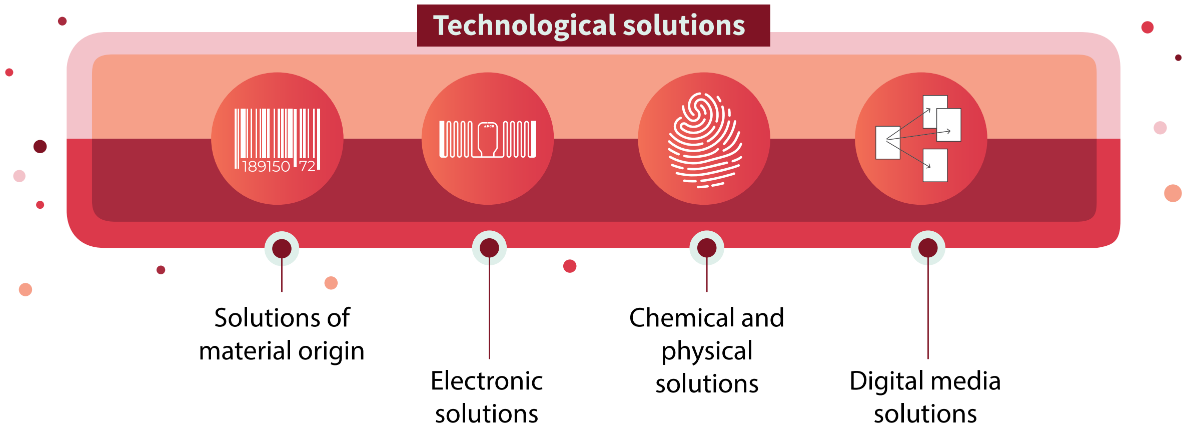
To ensure the integrity of the supply chain and IPR, several technological solutions have been developed to both uniquely identify a product and guarantee its origin. In particular, as reported in a recent EUIPO (2021a) study, these solutions can be classified as follows:

- **solutions of material origin**: these include machine-readable barcodes (both one- and two-dimensional ones), inks, watermarks, and ID marks;
- **electronic solutions**: these include RFID (Radio-Frequency Identification)[18], NFC (Near Field Communication)[19], magnetic stripes and chips;

[18] This is a technology which allows the automatic identification, via a radio transponder, of tags applied to products.

[19] This is a technology which, in contrast to RFID, allows bidirectional communication between an *initiator* and a *target*.

- **chemical and physical solutions**: these include *Surface Fingerprint* and *Laser Surface Analysis* technologies[20], or glue- and tracer-based coding;
- **digital media solutions**: these include *Digital Rights Management* (DRM) systems[21].



A selection of best practices in this domain are listed in the table below. Brand owners are active in monitoring their supply chain (e.g., suppliers, vendors, resellers), so as to avoid counterfeit products from being, wittingly or unwittingly, sold to end-consumers, and they are often supported by marketplaces.

Table 3. A selection of initiatives undertaken by marketplaces and brand owners to trace their products

▶ Initiative: **Amazon 'Transparency'**
In 2019, **Amazon launched 'Transparency**', a product serialisation service that helps identify individual units and proactively prevent counterfeits from reaching customers. It currently covers 10 countries at the global level and includes more than 15,000 registered brands (Amazon 2021b). Those brand owners which adhere to the programme apply on the external packaging of each unit of the enrolled product a 2D alphanumeric code (nonsequential), which is scanned by Amazon to ensure only authentic units are shipped to customers. At fulfillment centers, each barcode is submitted for authentication at order download, if a product fails this authenticity check, it is immediately set aside for further investigation. The 2D code allows clients, through the Transparency *app*, to verify the originality of the product regardless of where it is purchased, and obtain detailed product information (e.g., manufacturing date, manufacturing place, expiry date). At the same time, registered brand owners have access to a report which both allows them to monitor the performance of Transparency and provides information on the number of: • units that prevented from reaching customers because they are not equipped with valid Transparency code; • unsuccessful code scans due to codes in incorrect products; • listing attempts that were rejected when sellers were unable to provide valid Transparency codes;

[20] These are technologies which analyze the composition of materials' surfaces, identifying possible structural differences and allowing for the identification of the product.

[21] All those technologies which manage IPR in digital format.

- Reports of suspected counterfeit infringement.

There are numerous benefits for brand owners and sellers from participating in the programme. Stefano Bolzicco, owner of a furniture firm, LoryArreda, reported that "*I have been selling on Amazon since 2016 and I have immediately adhered to Transparency. In the short-term, it had a psychological benefit: I felt protected. In the long-term, I observed an increase in my brand's reputation. Turnover increased by 35%*" (Il Sole 24 Ore 2021a).[22]

▶ Initiative: **eBay 'Authenticity guarantee'**

In September 2020, **eBay launched the 'Authenticity Guarantee'** programme for luxury watches that were sold at a price higher than 2,000 USD in the United States, before extending it in October 2020 to include all sneakers sold at a price higher than 100 USD (eBay 2021). Those sellers who adhere to the programme, after receiving an order, send the product to the eBay authentication center, which then carries out a range of checks, both of a physical and chemical nature, to guarantee the originality of the product. The process can produce two outcomes:

a. if the product is accepted, then the center applies an NFC tag to the product (which acts as a certificate of guarantee) and sends it to the final client;

b. if the product does not pass the controls, then eBay immediately reimburses the client and initiates an array of further due diligence checks with the seller. If the product then appears to be counterfeit, then eBay immediately removes listings from the marketplace and initiates legal action against the seller.

The programme acts as a sort of guarantee in terms of potential fraud. Should the customer return the product, then this is once again examined by the eBay center before being returned to the seller, to avoid the restitution of fraudulent products (e.g., counterfeit, or stolen goods).

▶ Initiative: **Luxottica GLOW**

Luxottica has developed GLOW (Guaranteed Luxottica Origin Worldwide), a traceability system based on RFID technology which verifies both the originality of the products and the security of the retail channels through a RFID tag, which is embedded in eyeglass frames. The tag includes some key information that allows for the unique identification of each pair of glasses, from the manufacturing process itself right up until the sale-point, to avoid that:

a. counterfeit products enter the supply chain;

b. original products become displaced toward non-authorised sale channels.

Other good practices

Since 2009, **Moncler** has applied an anti-counterfeiting tag on each of its products, which can be verified on a specific website (*code.moncler.com*). From 2016 onwards, besides this verification approach, Moncler also adopts RFID-based tags which, through an app, allow actors to read QR codes and NFC tags associated with each product.

[22] Translation by authors.

Salvatore Ferragamo, after carrying out the first pilot projects in 2011 and 2013, equips all his leather clothes with NFC tags to ensure their traceability. The client, through a dedicated app, is thus able to verify the originality of the product and acquire an array of further information related to the product.

Brembo, in 2021, developed the app **'Brembo Check'** that enables its clients and resellers to identify potential counterfeit products. Once they have acquired the product UPGRADE, a client/reseller can verify its originality by scanning, through the app, the QR code associated with each part. To avoid adulteration, the tag is produced through a particular printing mechanism that makes the QR unusable should somebody try to remove it. The launch of this app empowered the anti-counterfeiting system of Brembo, which, already from 2016, was selling some of its products (*performance aftermarket*) along with an 'anti-counterfeiting card' in a sealed envelope. The client could obtain from the card a six-digit code, which, once uploaded to a dedicated section of Brembo's website, could certify the originality of the product.

Distributed Ledger Technology (DLT) and Blockchain solutions

Within the framework of supply-chain management, DLT technologies ensure that products are easier to trace, which, in turn, allows for the monitoring of their originality. Each transaction/action (from manufacturing to the market) can be registered in a distributed ledger in which the inclusion of the information is allowed only after the verification of the user (e.g., through an electronic signature) to avoid non-authorised modifications.

The potential of the blockchain in the anti-counterfeiting domain has been acknowledged at the European level, which led to the creation of the Anti-counterfeiting Blockathon Forum. This was implemented by the European Commission and EUIPO and groups experts from a multitude of disciplinary backgrounds in order to set up a common standard infrastructure, based on blockchain technology, which connects all involved stakeholders (e.g., intermediaries, brand owners, law enforcement) to share and exchange data and information designed to protect the integrity of the supply chain from the infiltration of counterfeit products (EUIPO 2019b).

The use case and adoption of DLT-based solutions, remains uncertain or theoretical, with limited trials or adopt such as the IPR Protection Tech Brain' of Alibaba (2020) and the Aura Blockchain Consortium (launched in April 2021 by Prada, LVMH e Richemont) which has developed an in-house blockchain solution, open to all luxury brands at global level, which allows clients to easily trace product life-cycle, from manufacturing to distribution. Many vendors are keen to develop viable offerings as well (see Box 19).

Box 19. Anti-counterfeiting and blockchain solutions

In October 2021, a Swiss start-up active in the area of brand protection developed a solution which, by combining blockchain and NFC, ensures the originality of products in the beauty and cosmetics industry (Il Sole 24 Ore 2021b). Each product is sealed with a NFC tag, which protects, for example, against the fraudulent actions aimed toward topping up or diluting the content of perfumes and bottles. Once sealed, a digital copy of the product is created and then uploaded on the blockchain, thus limiting then any potential adulteration and modification. NFC tags allow manufacturers and the end-consumers to communicate end-to-end: manufacturers can monitor their supply- chain, and early-detect fraudulent activities earlier, while consumers may check the originality of their products in a contactless way.

4.1.2 Solutions to monitor listings

Despite the organisational and technological solutions adopted, some counterfeiters are still able to operate online. In order to block the sale of counterfeits, some marketplaces have adopted artificial intelligence (AI) algorithms, which allow them to monitor large volumes of listings and early-, detect earlier and proactively remove any which could potentially violate IPR. A detailed list and description of these technologies is included in a recent report by EUIPO (2020). Some selected *best practices* are reported here below.

In 2019, **Alibaba launched 'IPR Protection Tech Brain'**, a proprietary suite based on AI, cloud computing and blockchain, which proactively monitors listings (Alibaba Group 2020). Since their launch, the suite algorithms have analyzed 13.7 billion images and have been trained based on a sample of listings violating IPRs (shared by the same brand owners). In 2020, according to Alibaba, this mechanism led to the removal of 96% of all listings which violated IPRs as soon as they were published. These algorithms apparently contributed to a 33% reduction in both the listings removed after being reported by clients and the rate of returns toward clients because of purchasing counterfeit goods (1.1 for every 10,000 transactions).

In 2019, **Amazon launched 'Project Zero'**, an anti-counterfeiting system which protects clients and brand-owners (currently more than 18,000 brands are enrolled) through two main tools:

- **automatic protections**: Amazon's machine learning algorithms continuously scan attempted changes to product detail pages for signs of potential abuse. In 2020 they scanned over 5 billion of attempted changes daily (e.g., changes to title/description, price change) (Amazon 2021c);
- **self-service removal of counterfeit products**: the brands enrolled in Project zero have the ability to autonomously directly remove listings from the marketplace. Removed listings are then used to train the AI algorithms and improve the future identification of counterfeit goods.

At the present juncture, more than 75% of the *brands* enrolled in Project Zero have never used the self-service counterfeit removal tool, thanks to the automatic checks which, proactively, block suspected bad product listings before they are published (Amazon 2021c).

In 2020, **eBay** blocked and removed around 31.5 million listings which were violating IPRs, while 1.9 million listings were removed after reporting from third parties, leading to the cancellation of **53,000 eBay users' accounts** (eBay 2021). AI algorithms allow to both block those listings which potentially violate IPRs (by sending the seller a message informing them about the detected violation) and mark those listings which warrant further manual due diligence checks by eBay staff.

31,5 milioni listings removed

1,9 milioni listings removed after reporting from third parties

53.000 user accounts cancellation

4.1.3 Seller vetting and due diligence

As discussed in Chapter 3, counterfeiters attempt to open accounts as sellers on online marketplaces, both as individuals and/or behind fictitious companies, to distribute counterfeit goods and carry out illicit activities (see 3.3). This risk makes it necessary to carry out **due diligence checks of third-party sellers**, as requested by the recommendations issued in this domain (Consiglio Nazionale Anticontraffazione 2019) and in related fields (e.g., anti-money laundering, anti-corruption, 231/2001). Despite the relevance of the topic, **information on the practices** currently employed by marketplaces **remains scarce**.

- on the one hand, the topic of *Know Your Customer / Know Your Vendor* is not usually the subject of scientific research, while dedicated studies on this topic are also lacking;
- on the other hand, the interviewees in this study reported that it was impossible for them to share more detailed information justifying it, due to the existence of internal constraints and obligations. On the contrary, we thank Amazon for sharing information on its seller-vetting practices, which are described in Box 20.

When fully implemented, the seller vetting activity is structured in multiple layers that creates a sort of **'informative funnel'**, which, in turn, makes it difficult for counterfeiters to open a seller's account. The due diligence is aimed at:

- identifying more easily the **fictitious information** which has been provided during the registration process. Fraudsters may provide actual information about figureheads (e.g., email contacts, phone contacts, payment methods), but also fake information (e.g., addresses) in order to create **'artificial identities'** that are as real as possible;
- identify **anomalous behaviour** during the registration process, such as, for example, unjustified changes to contacts and addresses;
- identify potential links between the sellers and other individuals/entities that have previously been targeted by **adverse media or negative events** (e.g., sanctions, arrests, seizures) and which may be symptomatic of fraudulent behaviour or which, in any case, would justify enhanced due diligence controls.

Box 20. Amazon's *Know Your Business Customer* processes

The process employed by Amazon to verify the identity of third-party sellers combines AI approaches and manual audits by staff. In 2020, Amazon has stopped over 6 million attempts to create a selling account – a significant increase compared to the 2.5 million attempts in 2019 (Amazon 2021c). On average, **only 6% of attempted new registrations passed their robust verifications process**. To complete the registration, third party sellers should undertake in person or live video verification process, provide government-issued ID documents (with personal pictures) along with an array of additional information, including, among other things, addresses, bank details and taxpayer information. The information is then counterchecked with third-party data providers, including the list of individuals and entities previously reported because of anomalous and illicit behavior. In particular, Amazon:

a. connects with each prospective seller via video chat or via an in-person meeting in Amazon offices, so as to verify both the identity and coherence of the provided documentation;

b. verifies the addresses provided by the applicant, by sending information including a unique code to the registered seat;

c. verifies the bank details with the payment service providers to check where funds are deposited, and to identify their beneficial owner(s).

Once authorised, the sellers are in any case subject to continuous monitoring aimed toward identifying potential anomalous behavior over time. In this sense, the analysis of both clients' and products' reviews are key. Machine learning algorithms can be employed to cross-check the reviews with third-party data providers, which allows for the identification in real-time of any risk cluster (e.g., generic reviews, excessively positive reviews, recurrent reviews, the number of reviews does not correspond to the number of items sold). As is widely acknowledged, reviews may be manipulated by counterfeiters to increase the reputation of sellers (Mayzlin, Dover, and Chevalier 2014; Luca and Zervas 2016).

A recent study analyzed 23 closed Facebook groups in which the sellers of a marketplace agreed with colluding clients a system for producing false reviews (He, Hollenbeck, and Proserpio 2021). The clients made purchases on the marketplace and were then reimbursed by the seller, who added on top a fee for the service provided by the fake customers.

Seller vetting controls adopted in the framework of anti-counterfeiting are inspired by the **equivalent on-boarding systems** that are already in place for banks and other obliged entities in the anti-money laundering domain. These first level controls—which are of a documental nature—are then supported by second order controls, which typically employ more sophisticated predictive and risk assessment models that can enrich the information collected during the on-boarding process with data and indicators stemming from third-party repositories (Box 21).

Box 21. Next-generation systems for the risk assessment of sellers, vendors and third parties

Transcrime, a research centre of the Università Cattolica, has developed some risk indicators that condense in a synthetic manner some anomaly metrics related to different characteristics of the analyzed firms and individuals (e.g., ownership structure patterns, localization and business sector, economic and financial data), which could be employed in customer due diligence and supply-chain controls. The following risk dimensions are found:

- the complexity of the ownership structure, which is not justified by the peer group (size and sector of activity);
- anomalous or unjustified changes in name, shareholding structure, directorship, legal forms;
- links to opaque legal arrangements (e.g., trusts, fiduciaries, etc.);
- anomalies in income statements or balance sheets.

The risk indicators and models developed by Transcrime have been tested and validated on several million firms in nine European countries, by employing as a target variable the evidence of sanctions and enforcement measures upon the firms and its owners/directors. In particular, several machine-learning methods (logistic regression, naïve Bayes and decision tree) have been employed as part of the training and testing activity. The results of the analysis demonstrate the strong predictive capacity of these models, which are capable of identifying more than 85% of the firms that are subsequently targeted by negative actions (Jofre et al. 2021). The models, once embedded in IT applications, are then utilized by public authorities to support their investigations and supervisory operations, while private firms employ them to control third-parties and protect the supply chain and procurement integrity.

Despite the good practices of some stakeholders, the *Know Your Business Customer* activity is often approached in an 'artisanal' way by most firms, especially outside the regulated sectors (e.g., anti-money laundering, anti-corruption). Besides the acquisition of personal information and first level controls, the following are not yet fully exploited:

- the **entire information asset** available on the seller, stemming from both internal sources (e.g., links with other clients or sellers already registered, references in messages and reviews) and external ones (e.g., repositories and open sources). The poor use of this information (e.g. registry records, adverse media, ownership information) is due to various reasons: (a) lack of publicity of certain data (e.g. ownership information); (b) costs, when distributed by commercial providers; (c) lack of accessibility via Application Program in Interface (API) for many jurisdictions;
- the **potential of *data analytics***, which allows to combine information of a diverse nature and identify anomalies based on comparisons with peer groups and clusters.

Despite the strict rules in terms of privacy protection—see, for example, the *Deliberazione del 12 giugno 2019 del Garante della protezione dei dati personali* (2019)[23] —it is still possible to implement effective solutions which fully respect personal data.

[23] The document is available at the following link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9119868.

4.2 Cooperation and information exchange

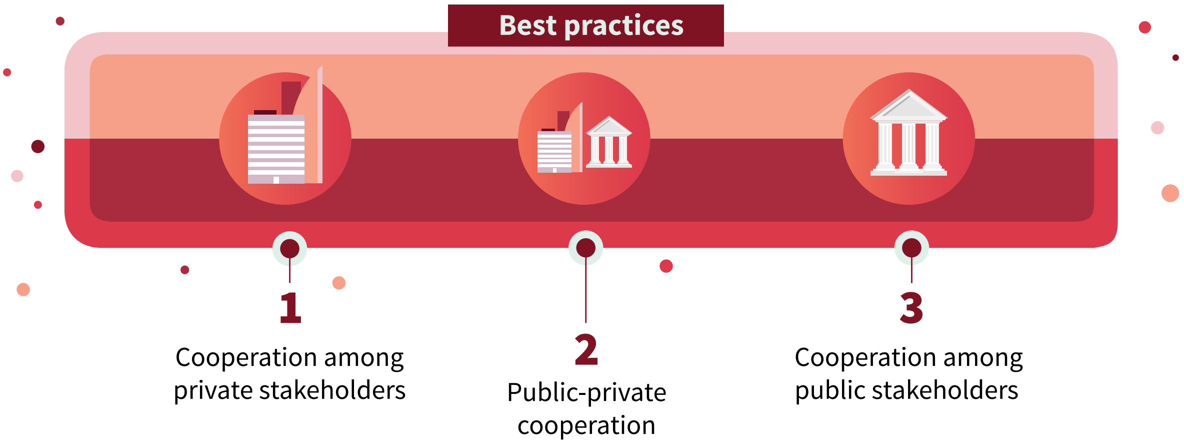
Sharing good practices, experiences, data, and knowledge among public and private stakeholders is a critical component of fighting counterfeiting on online markets. In recent years, the cooperation between marketplaces, brand owners and public authorities has increased exponentially. However, many of the interviewees, from both the private and public sector, drew attention to certain difficulties associated with the effective exchange of information among the interested stakeholders. More specifically, information exchange was said to be challenging in various directions:

- **from public authorities to the private sector**, namely in terms of exchanging either data on seizures carried out by customs and law enforcement agencies or the outcomes of prosecutions targeting individuals or cases reported by the same private sector organisation to the judicial authority. Sharing this information with marketplaces, brand owners and postal operators may improve their capacity to detect fraudulent products and bad actors earlier as well as having a multiplying effect on their prevention activity;
- **from the private sector to public bodies**, which would allow authorities to expand their information and intelligence sources, in turn, constituting a valid form of support to traditional investigations. Unfortunately, as aforesaid, different degrees of cooperation exist between marketplaces and other operators (e.g., social media, other online forums), especially when the latter are based outside the EU or if they are smaller and less equipped stakeholders;
- **from brand owners to marketplaces, postal operators, and public authorities.** Exchanges are too often limited to the sharing of traditional guidelines on distinctive marks, while today it is possible to include more sophisticated data, such as 2D or 3D templates and scans, which may facilitate the detection of counterfeit goods thanks to the novel technologies, image recognition systems and new-generation scanners that are at the disposal of customs and logistics operators;
- in the **voluntary exchange among all stakeholders** - both public and private ones - of information related to previously identified bad actors, in order to avoid them easily being displaced across different online channels and markets. Here, the exchange of information could apply to both suspicious actors (individuals and legal persons) who act as sellers, in addition to those customers who have already been reported because of illicit activity (e.g., fraudulent returns or payment fraud).

However, despite notable innovations at both the policy and regulatory level (see Chapter 5), the information exchange between stakeholders is often hampered by presumed problems related to **personal data protection and protection of sensitive information at the industrial, commercial, or investigative level**. These are often unjustified excuses, insofar as similar exchange initiatives already exist within other domains (e.g., anti-money laundering, see Chapter 5), and because a vast array of new technologies now allow for the secure exchange of information without infringing upon the integrity, secrecy and anonymity of the data shared (e.g., *federated learning* mechanisms and others).

For this reason, it is worth noticing that the European Commission plans to step up the fight against counterfeiting by, among other initiatives, developing an EU Toolbox (expected for the Q3 2022). Its objective is to clarify roles and responsibilities of brand owners, intermediaries and law enforcement authorities, thus fostering their active cooperation and incentivizing data sharing. Building on existing best practices (e.g., Memorandum of Understanding on the sale of counterfeit goods on the internet), it aims at specifying clear principles for sharing more and better data, improving the interoperability between databases and expanding existing tools (e.g., IP Enforcement Portal), while continuously ensuring the protection of data.

Both the review of extant literature and the analysis of the case studies have shed light on an array of best practices which are worthy of being reported and discussed. These best practices can be classified into three categories:


Best practices
1
Cooperation among private stakeholders
2
Public-private cooperation
3
Cooperation among public stakeholders

Cooperation among private stakeholders

The exchange of data among brand owners and online marketplaces allows for the more effective identification of listings from sellers that infringe IPRs. However, some interviewees noted that there were a lack of dedicated mechanisms to facilitate this information flow. The table below describes a selection of best practices in this domain.

Table 4. Best practices in terms of collaboration among private stakeholders

▶ Initiative: **eBay VeRO**
In 1998, eBay launched the *Verified Rights Owner* (VERO) programme, which allows the enrolled brand owners (which currently amounts to more than 97,000) to report and request the removal of listings from sellers which violate their IPRs. In the event that the infringement is verified, eBay removes the listing and initiates legal action against the identified seller. According to eBay, to date only 2.2% of the 19 million sellers active on the platform have had listings removed because of a report from the VeRO programme.

▶ Initiative: **Alibaba 'Intellectual Property Protection Platform'**

In 2016, Alibaba launched the '*Intellectual Property Protection Platform*' (IPP), a unique platform that combines two additional programmes, *AliProtect* and *TaoProtect*, which launched in 2008 and 2016, respectively. Brand owners may open an account on this platform to issue a request to remove content deemed to infringe their IPRs on all the seven group's marketplaces. In 2020, the number of brand owners listed on the IPP increased by 40% compared to 2019. According to Alibaba, 98% of the requests to take-down content are dealt with within a 24-hour period (Alibaba Group 2020).

▶ Initiative: **Amazon 'Brand Registry'**

In 2017, Amazon launched '*Brand Registry*', a free-of-charge service which allows registered brand owners to access an array of tools that allow them to protect their brands. In particular, brand owners can verify in detail the textual data, pictures, and contents of the listings on the marketplace, in conjunction with checking that the information provided to end-customers is always correct and precise. Moreover, through this system brand owners can provide Amazon with further information that the marketplace can then use to improve its proactive measures to automatically detect infringements on its online channels (See above). In 2020, more than 500,000 brands enrolled on the programme and, according to Amazon, since its launch brands reported, on average, 99% fewer suspected infringements than before (Amazon 2021c).

Box 22. Working groups of private actors for the fight against online counterfeiting

In 2010, the European Commission invited e-commerce marketplaces, brand owners and sectoral associations to sign a ***Memorandum of Understanding*** **(MoU)** on the prevention of the sale of counterfeit goods on online markets (countersigned in 2011). The objective of the MoU is to both define new practices in the fight against online counterfeiting and to promote the cooperation between the signatory members in order to improve the effectiveness of the fight against online counterfeiting. The MoU envisages three critical lines of defence:

- raising the awareness of clients over the risks and the negative consequences stemming from counterfeiting. In this sense, e-commerce platforms commit to providing consumers with all the necessary information to be able to prevent the purchase of them purchasing counterfeit goods;
- the adoption of proactive measures (of both of a technological and organisational nature) to identify quickly and effectively the trade of counterfeit products;
- the adoption by online marketplaces and e-commerce platforms of suspicious reporting systems and removal services for counterfeit products and related listings.

In 2017, the European Commission published a document presenting the outcome results one year after 1 year from the start date of the (revised) MoU. The results were based on certain KPI envisaged by the MoU and computed by the same signatory parties. For example, out of the first 100 results stemming from queries carried out on marketplaces between May and June 2017, 14.3% referred to potential counterfeit products. Moreover, 97.4% of the listings which potentially infringed IPRs were removed directly by marketplaces, while only 2.6% were removed based on a report by a brand owner.

As reported in a recent position paper by Amazon (2021a), several online marketplaces have actively worked to establish mechanisms in the United States for the creation of a mechanism to share information on verified counterfeiters. The results of this initiative are very promising: Amazon has recognised that 16% of the sellers reported as suspicious by other e-commerce platforms had in fact also attempted to sell goods via the Amazon marketplace, too.

Cooperation among marketplaces and brand owners is not limited to the identification and removal of listings infringing IPRs, but also consists of reporting identified counterfeiters to the competent authorities and **initiating legal proceedings** through joint civil suits against the identified actors. In this sense, certain joint civil actions are particularly relevant, such as those initiated together by **Amazon and Ferragamo** (Amazon 2021a), **Amazon and HanesBrands** (Amazon 2021c) and **Facebook and Gucci** (Reuters 2021) that filed joint lawsuits after due investigation by the same brand and Amazon CCU against suspected bad actors.

However, it is important to highlight that the attention of marketplaces toward brand owners is not solely limited to the major players, such as, for example, luxury brands, but rather also includes small- and medium-sized enterprises (SME). Amazon, for example, has launched joint actions together with smaller firms like JL Childress or DutchBlitz, a family firm that produces board games (Il Sole 24 Ore 2021a). This point is not insignificant because, according to a recent investigation by EUIPO (2019a), only 9% of SME have registered their IPRs in comparison to 36% of larger companies. Considering this discrepancy, Amazon developed an initiative, called *IP Accelerator*, that aims to support SME in protecting their IPR. As emphasized by Mary Beth Westmoreland, Amazon's vice president, "the IP Accelerator has been designed specifically for small firms, which are engaged with a selected network of legal firms specializing in IPRs which have accepted to work at fixed and competitive prices" (Il Sole 24 Ore 2021a). In 2020, more than 7,000 SME enrolled on this programme and accessed the services made available by the *Amazon Brand Registry*.

Public-private cooperation

Another especially relevant point highlighted by the interviewees concerns the cooperation between private stakeholders and law enforcement agencies in terms of information exchange to support investigations. Best practices can be identified in this domain. For example, eBay developed the '**Regulatory Portal**' which allows law enforcement agencies to send data and information requests. In 2020, eBay received 38,497 requests at the global level, providing - in compliance with personal data protection rules - information on 42,071 clients and sellers (eBay 2021). At the same time, PayPal launched the '**Safety Hub - PayPal Law Enforcement Tool**', a web-based platform which allows law enforcement agencies and judicial authorities to request information and data on PayPal users more easily. The platform replaces the previous methods that were employed to contact PayPal (e.g., post, e-mail, fax), while the received requests are manually processed by a *Global Investigation Team* and dealt with within 10 working days.

Besides these information exchange mechanisms, several case studies - already mentioned in previous sections - also provide best practices, which ensured both a positive outcome for the investigations and the identification of bad actors.

Table 5. Best practices in terms of information exchange between law enforcement and private stakeholders, according to the selected judicial investigations

▶ Initiative: **'Internet brand intelligence' activity**

▶ Name of the investigation(s): **Bologna Luxury, Aphrodite II**

The 'Internet brand protection' supervision carried out by several brand owners allowed for the identification and take-down of listings on various online channels which were infringing their IPRs. The results of this activity were then promptly shared with law enforcement, who then launched investigations to identify the individuals who were hiding behind the accounts on social media and online channels.

Which information has been shared between law enforcement and brand owners? Information on (a) removed posts/listings and (b) involved accounts.

▶ Initiative: **Proactive monitoring of the web by law enforcement**

▶ Name of the investigation(s): **Falsi Online**

The proactive monitoring carried out by the Guardia di Finanza of Luino (Varese province) allowed for the identification of accounts that were promoting and selling counterfeit products. After this intelligence activity, the Guardia di Finanza engaged with the interested brand owners to ascertain, through appropriate technical reports, that the advertised products were not original.

Which information was shared between law enforcement and brand owners? Information on (a) images of the products sold online; (b) the employed sale channels; (c) selling prices.

▶ Initiative: **Involvement of social networks in law enforcement investigations**

▶ Name of the investigation(s): **Bologna Luxury**

In this investigation, the Guardia di Finanza engaged in close dialogue with the social networks involved in the case (Facebook and Instagram) to acquire further information on accounts involved in the advertisement and sale of counterfeits, to facilitate the identification of the bad actors involved.

Which information was shared between law enforcement and social networks? Information on (a) log files; (b) mobile phone numbers; (c) payment methods.

▶ Initiative: **Involvement of payment service providers to trace the financial transactions of counterfeiters**

▶ Name of the investigation(s): **Bologna Luxury**

In this investigation, the Guardia di Finanza, via the use of innovative software, was able to identify the user ID of the PayPal account stored in the cookie of the browser of the mobile phone that was seized from the individual under investigation. This allowed the law enforcement agency to engage with PayPal (through the Safety Hub – PayPal Law Enforcement Tool) to share data from the transactions related to the account. The provided data allowed them to trace a number of payments that favored Chinese manufacturers, thus confirming what already emerged from the conversations on WhatsApp.

Which information was shared between law enforcement and social networks? Information on the PayPal transactions related to the account under investigation.

Box 23. Public-private cooperation against online counterfeiting in the United States and Canada

At the end of 2020, Amazon shared information with US Customs (CBP) and the Department of Internal Security (HSI), which led to the freezing of some counterfeits prior to being handled by logistics operators. The information provided by Amazon, which was supported by further investigations carried out by CBP and HIS, allowed law enforcement agencies to seize eight truckloads of counterfeit car parts. This cooperation has also worked well in the opposite direction. In 2020, CBP informed Amazon about the seizure of a shipment of earphones bearing non-authorised Champion's trademarks. Amazon contributed to the freezing of the items of the counterfeiters who were present in Amazon's network as well as cancelling their accounts. Amazon's Counterfeit Crimes Unit (CCU) then worked together with the brand owner, which owned the related IPRs (HanesBrands), in order to issue joint suits to 13 counterfeiters.

In 2012, in Canada, a project called 'Project Chargeback-Leading the Charge (Back) against fakes!' was launched, which involved the Canadian Anti-fraud Centre (CAFC) of the Royal Canadian Mounted Police, banks, payment service providers and brand owners. The initiative sought to combat the sale of counterfeit products via the following steps (WIPO 2017):

- customers who acknowledge the purchase of counterfeits issue a report to CAFC, providing information on, among other things, the brand of the purchased product, the price they paid, the name of the seller and the online channel on which the purchase was ordered;
- the CAFC contacts the brand owner to verify the originality of the product reported;
- if the product is proven not to be original, then the client's bank is authorised to chargeback him/her;
- the client is required not to return the product, but rather to destroy it once they receive the chargeback;
- the seller's account is then cancelled by the payment service provider, which subsequently charges the seller the chargeback cost;
- both the bank and the payment service provider may be sanctioned in the event that the number of chargebacks is deemed to be excessively high.

Since the beginning of the project, the CAFC has managed more than 35,000 requests, which have brought up to 10 million dollars of reimbursements and led to the take-down of more than 8,000 sellers who were promoting counterfeit goods on 25,000 websites.

Beyond cooperation on operational activities, the public-private cooperation also aims at raising the awareness of customers and firms concerning the risks of online counterfeiting. For a detailed list of these initiatives, please see '*Piano Strategico Nazionale* 2019-2020' (Consiglio Nazionale Anticontraffazione 2019). Of particular interest in this regard is the *Settimana Anticontraffazione* (*Anti-counterfeiting week*), organized by the DGTPI-UIBM of the Ministero dello Sviluppo Economico (Ministry of the Economic Development) (see Box 24).

Box 24. Awareness raising: the *Settimana Anticontraffazione*

The *Settimana Anticontraffazione* is an awareness raising campaign from the DGTPI-UIBM of the Ministero dello Sviluppo Economico that started in 2016, and is usually held in October. It aims to foster discussion over both the magnitude and effects of counterfeiting, in an attempt to raise awareness among consumers, particularly younger consumers, and encourage them to adopt more responsible consumer behaviour. During the week, information events are organized within specific cities across the entire national territory, which present the results of the reports edited by the Direction together with CENSIS on both the impact and diffusion of the counterfeiting phenomenon. The initiative, which involves various institutional partners and stakeholders from the private sector, focuses on several topics, such as, for example, IPR-related crimes, the involvement of organized crime and money laundering in the sector, counterfeiting in the luxury industry, and the fight against counterfeits at the local level.

Cooperation among public stakeholders

As illustrated in Section 4.1, the segmentation of Public Authorities and law enforcement does not always allow for an integrated and coordinated response against new forms of online counterfeiting. In this regard, it is worth mentioning the recent constitution, established at the end of October 2021, of the **Consiglio Nazionale per la Lotta alla Contraffazione e all'Italian Sounding (CNALCIS)**, which is a renewed version of the Consiglio Nazionale Anticontraffazione (CNAC). This body seeks to:

a. identify the strategies and operational activities aimed at combating counterfeiting and 'Italian sounding' practices;

b. propose joint actions between law enforcement authorities and the private sector and new policy measures to address key counterfeiting priorities identified by the CNALCIS itself.

The CNALCIS is supported by the '**Commissione Consultiva Permanente FF. OO**', which is composed of representatives from law enforcement agencies, and the '**Commissione Consultiva permanente delle forze produttive**', which comprises representatives from sectoral and consumers' associations. This structure aims at operationalizing the strategies designed by the CNALCIS, while ensuring the representation and safeguard of both public and private interests. However, the definition of clear metrics and KPIs to monitor both the outputs and the outcomes of their activities over time would be highly desirable. For example, it could be useful to monitor the number of operational activities supported for each of the key counterfeiting priorities identified by the CNALCIS itself, allowing to timely spot potential criticalities to address.

Regarding the cooperation between law enforcement agencies, of particular relevance is the ‘**Desk Interforze Anticontraffazione**’, which meets periodically at the premises of the **Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale**. This Desk’s duty is to develop operational and strategic synergies in the fight against counterfeiting and to design joint interventions, which are agreed with representatives from the Comandi Generali dell’Arma dei Carabinieri, the Guardia di Finanza, the Direzione Centrale Anticrimine della Polizia di Stato, the A.N.C.I. - Associazione Nazionale Comuni Italiani (acting as link with Municipality Police), and of the S.I.A.E. - Società Italiana degli Autori ed Editori, the latter addressing multimedia piracy.

Box 25. Combating counterfeiting *online* and *offline*

Box by ‘Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale - Dipartimento della Pubblica Sicurezza - Ministero dell’Interno’

With specific directives dated, respectively, 8 August 2014, 15 November 2014, 6 July 2015 - with the attached “Guidelines on the Prevention and Counter to Counterfeiting Phenomenon” - and July 6 2018, the Minister of the Interior has ordered a systematic intensification of the action to prevent and combat counterfeiting and commercial illegal, in order to defend the free and correct competition, protecting the legal economy and safeguarding consumer health.

Special attention was paid, with the first, to tourist resorts and, in particular, seaside resorts, where there is a significant increase in the presence of subjects dedicated to these pipelines.
The directive was then extended to the entire national territory in the following month of November, becoming a permanent model of impulse.

On 6 July 2015, the Minister of the Interior again intervened in the matter, in order to raise awareness among the Prefects to implement, within the Provincial Committee for Order and Public Security, the initiatives for the containment and repression of the illicit phenomena under consideration, highlighting the need to identify and disarticulate the entire false chain, from the criminal centers of various reasons involved in the production, import, distribution and marketing of illicit goods up to the terminals of this pervasive illegal activity.

On this occasion, the importance of joint action between all the institutions involved was recalled, through which to be able to pursue the relevant purposes of public interest mentioned above.

Finally, the latest directive, on 6 July 2018, confirmed the previous guidelines and reiterated the need to give a strong and renewed vigor to the action to prevent and contrast counterfeiting and commercial illegal - especially in seaside resorts and in those with a strong tourist, artistic and cultural vocation or that are the venue for holding events of particular importance - through strengthening of the measures already indicated and the use of the new tools made available by the recent regulatory provisions on the subject.

In particular, the prefectural authorities have been notified of the opportunity to ensure, among other things:

- the maximum enhancement of the role of local police, due to their specific skills in the field of trade discipline and widespread knowledge of the territory;
- the verification of any availability, by the trade associations of the production sectors most damaged by the phenomenon, to contribute financially to local security programs in the forms permitted by current regulations;

- the execution of operational intervention plans that include, in relation to the most complex situations, the activation of targeted inter-force services;
- the intensification of the control activity on the presence of irregular immigrants;
- the identification, by the Municipalities, of the areas in which the access ban (the "Urban DASPO" or "DACUR.") provided for by the legislation on urban security is applicable;
- the adaptation of the memoranda of understanding, stipulated with all public and private entities interested in the fight against these forms of illegality, to the models that have made it possible to achieve the best results in terms of scaling the phenomenon and increasing the perception of security.

The positive results found, in implementation of the aforementioned lines of intervention, then suggested allocating[24] an 18% share of the Urban Security Fund to coastal municipalities, for the support of projects, proposed by the municipalities most exposed to the negative effects of the illicit phenomena in question, aimed at strengthening ordinary law enforcement activities in the two-year period 2019-2020.

[24] With the Decree of the Ministry of the Interior, adopted in agreement with the Ministry of the Economic Development on the 18 December 2018, illustrating the allocation criteria of the Urban Security Fund set up by Article 35 quater of the Legislative Decree n.133 of the 4 October 2018, as modified by the Law n.132 of the 1 December 2018.

5.

Recommendations and future directions

The emerging threats, the new schemes employed by counterfeiters, the challenges and the vulnerabilities of anti-counterfeiting systems require both a **paradigm shift** and a new approach in terms of **awareness, prevention, investigation, and cooperation**. In this respect, three directions to complement the increased enforcement against counterfeiters directly through future interventions can be identified:

- strengthening the monitoring of the emergent threats related to counterfeiting online;
- empowering technological and data analytics skills and the tools of public and private stakeholders to trace products and sellers;
- expanding cooperation and information exchange among public and private stakeholders.

For each of these three directions, it is possible to identify specific proposals, which are discussed in turn below.

5.1 Strengthening the monitoring of the emerging threats

All of the actors—from both the public and private sector—involved and interviewed during the course of this project highlighted the importance of developing a **more structured approach to monitoring and keeping involved parties up-to-date** regarding the new schemes of online counterfeiting. As highlighted in Chapter 3, threats are rapidly evolving—both in terms of new actors and crimes—and only a few stakeholders have a comprehensive perspective on this *fraudster journey*. This has a negative impact upon the capacity of stakeholders to both detect counterfeit goods earlier and implement effective solutions at both the organisational and technological level.

An observatory on the new threats and *modi operandi* of online counterfeiting

This report is the first picture, at least at Italian level, of how counterfeiting on online marketplaces takes place. In order to monitor its evolution, numerous interviewees recommended that a **scientific observatory** could be established to continuously collect and classify knowledge on the topic, which would be available to public and private stakeholders in a structured and accessible manner. This observatory would help to maintain a strong awareness of the phenomenon, monitor the threats as they continue to evolve, and assess the effectiveness of the implemented countermeasures.

This hub could set up, manage and periodically update an **online repository** that is accessible by both public authorities (e.g., law enforcement) and private actors (e.g., marketplaces, social media, logistics and postal operators, brand owners) and which could include a **collection of schemes and case-studies** (anonymized or in any case managed in compliance with the privacy regulation) of counterfeiting and other fraudulent schemes related to e-commerce and online markets. These cases would be collected at the global level from a variety of sources (judicial documents, police, and institutional reports, scientific literature, and open sources), analyzed and classified via a scientific method, so that they could be searched using tags and other keywords. The repository would offer a **constantly updated picture** of the online counterfeiting phenomenon, in turn, contributing to building a knowledge-base which is horizontal to all the involved stakeholders. Specifically, the information included in the database could be used to:

- train staff members that are involved in the fight against counterfeiting;
- update the automatic risk assessment and detection models employed by marketplaces and brand owners;
- provide in-depth knowledge that is useful for designing new regulatory and policy measures.

Both the observatory and the repository could take inspiration from **similar developments in the anti-money laundering field** at both the national and international level, which has not only increased knowledge (and awareness) of the problem, but has become the basis for each organisational and technological solution implemented by banks and other obliged entities in the field (see Box 26).

Box 26. The utility of constant monitoring in the anti-money laundering field

For a long time, in the anti-money laundering and counter-terrorist financing domain (AML/CFT), supervisory authorities have set up an array of initiatives aimed at monitoring the threats and schemes of anomalous activity, in order to increase the knowledge and awareness of obliged entities (e.g., banks, professionals and other intermediaries) of the phenomenon:

- in Italy, the UIF - Unità di Informazione Finanziaria periodically publishes reports which highlight **models and schemes of anomalous behaviour** (*modelli e schemi di comportamenti anomali*) at the AML/CFT level, related to different sectors and typologies. For example, the most recent ones focus on anomalous behaviour related to tax crimes, pre-paid cards, both in the gaming and gambling sector and in the factoring/leasing industry;
- at the international level, the **FATF - Financial Action Task Force periodically** produces reports on emergent **'Methods and trends'** related to money laundering and terrorist financing. Over the course of the last few years, the FATF published more than 75 reports, including (anonymized) cases collected from a variety of sources.

UIF and FATF schemes and cases are employed by banks, professionals and other obliged entities to **update their early-detection and risk assessment models** (UIF 2021). Notwithstanding these reports, banks also benefit from risk assessment exercises carried out at the national level by both the Comitato di Sicurezza Finanziaria del Ministero dell'Economia e delle Finanze (MEF 2018) and the European Commission (2018b).

According to a recent survey carried out by Crime&tech, with the support of SAS on Italian obliged entities (equivalent to 50% of the Italian financial market), **all interviewed intermediaries employ UIF and FATF anomalous schemes** reports as a starting point for their AML solutions, both at the organisational and technological level (Crime&tech 2021).

5.2 Empowering technological and data analytics skills and tools

New tools for analysis, due diligence, and early-detection

Marketplaces, social media, and postal operators have an **enormous volume of information** at their disposal, which, thanks to AI, *big data analytics*, and new technologies, and in full compliance with personal data protection, could be employed to enhance their capacity to detect counterfeits and fraud at a higher level. At the moment - albeit with some exceptions, as described in the previous chapter - the potential embedded in this information is **only partially being exploited**, and only by select actors and operators.

Based on the interviews with public authorities and other private stakeholders (e.g., brand owners), relevant differences in terms of analytical capacity can be observed across different marketplaces and sales channels. While larger marketplaces appear to be equipped with more advanced tools, the interviews revealed that (some) social networks are more vulnerable and less able to quickly detect fraudulent behaviour and counterfeits.

At the same time, also smaller e-commerce marketplaces face similar issues, even though for different reasons. While in the case of smaller e-commerce marketplaces, this vulnerability stems from a lack of resources (of both the human and economic kind) to devote to the fight against counterfeiting, in the case of social networks, this vulnerability is related to a lack of interest in viewing the problem as a priority. For example, **seller vetting controls are missing** when accounts are opened by for-profit firms, while the products of sponsored campaigns are not fully verified. These differences across marketplaces may generate **displacement effects** of criminal activities toward weaker channels, eventually undermining the entire e-commerce system and potentially generating problems of unfair competition.

As suggested by the good practices illustrated in section 4.1, the technological and analytical skills of the involved stakeholders could be empowered in three directions:

1. Better control over the origin of products,
through:

a. the employment of track and trace solutions of a material, electronic, chemical nature, such as RFD, NFC and other serialization systems (see 4.1.1);

b. the adoption of *blockchain* and DLT solutions, which could involve the entire supply chain (until the end-consumer);

c. a widely shared employment of these solutions among different stakeholders (e.g., different brand owners, or between these and other marketplaces), where possible;

d. the extension of these solutions to SME that are unable to devote resources to innovation in this domain, by, for example, supporting them with incentives or 'umbrella' initiatives fostered by sectoral associations;

e. the employment of new scanning technologies (e.g., 3D scanners, neutron-based scanners), which may help to identify anomalies related to goods along the whole logistics chain (for example, detecting returns fraud with counterfeit goods).

2. More effective monitoring of advertisements and othe web activities,

through a more intensive employment of:

a. AI and machine-learning;

b. text-mining of content posted on marketplaces, social media, and other forums, in order to detect anomalous posts;

c. image recognition of pictures of products posted on the web;

d. the sharing by brand owners of more accurate 2D and 3D scans of their products to facilitate their image recognition;

e. large-scale screening of websites to identify website clones and fraudulent websites.

3. Better seller vetting and due diligence,

through:

a. the use of procedures during remote on-boarding (e.g., verification of the address and mailbox), which may help to ensure that the prospective seller is a real firm and not a 'shell company' employed for illicit purposes;

b. the expansion of information about sellers and related individuals (e.g., owners, directors), through the employment of business data providers and 'compliance lists'[25] and the improvement of publicly available electronic company records in all jurisdictions;

c. the employment of next-generation indicators and risk models capable of identifying anomalies in the characteristics of sellers (e.g., in the ownership structure, of an accounting or financial nature, other anomalies with respect to peer groups);

d. the continuous monitoring of the activities of sellers, and the identification of anomalous activities (e.g., unusual or unjustified variations of advertised products, of contacts, of registered seats);

e. the monitoring of the reviews left on marketplaces in order to identify anomalous activity, collusion and fraud (e.g., the use of the same review across products or sellers);

f. the exploitation of economies of scale with related domains (e.g., AML, anti-counterfeiting), so as to take inspiration from the best practices already implemented by obliged entities.

[25] These are databases which are frequently employed in the AML/CFT domain, and which, on the basis of open sources (e.g., sanction lists, press releases by the police, certified open sources), provide the names of individuals targeted by previous sanctions (e.g., OFAC, UN, EU), enforcement measures (e.g., arrests and seizures, administrative measures) or who are listed in categories which are subject to, at least in the AML field, to enhanced due diligence (e.g., PEP – Politically exposed persons).

To invest in the development of these instruments, and ensure their adoption by all stakeholders active in the e-commerce domain, one could leverage the resources provided by the **Piano Nazionale di Ripresa e Resilienza (PNRR)**. For example, the PNRR can finance the constitution of Extended Partnerships which would involve universities and firms on specific topics identified by MIUR, chief among which: **'Artificial intelligence'** and **'Made in Italy'**. Within this framework, it would be possible to set up cooperative initiatives between universities and the private sector to develop and test new instruments and advanced analytical approaches, in order to improve the traceability of the products and empower the early detection of the 'supply chain of fakes' - both online and offline.

Training public and private sector representatives on *data analytics*

Applying these analytical and technological capacities on a broader scale is not limited only by material investment, but rather by the training of the involved stakeholders. Indeed, a number of interviewees stressed the need for dedicated training, organized with the support of universities and sectoral associations, which, among other things, would:

- highlight the available data analytics tools and approaches (e.g., machine-learning, neural networks, text and image recognition) and the potential offered by these approaches;
- review the variety of information and data sources which could be employed for analysis and predictive analytics;
- highlight and discuss the constraints, both at the legal and technological level, which prevent the use and elaboration of these data, above all, those related to personal data protection and automatic profiling.

Box 27. Artificial intelligence, anti-counterfeiting, and personal data protection

Although advanced technological solutions can play a key role in the anti-counterfeiting domain, their adoption must also consider what is requested by the relevant regulation in terms of personal data protection. In particular, AI algorithms must comply with specific requirements (e.g., compliance with the criteria used for training the models, replicability and verifiability of the results).

All these principles ensure that AI algorithms are not based uniquely on automatic processing, which is explicitly denied by EU regulation as well as at the national level. While these are important constraints, they should not be regarded as obstacles to the adoption of advanced technological solutions. That is to say, it is wholly possible in fact to adopt technical and organisational measures, which adhere to these criteria, while, at the same time, allowing for an effective use of advanced solutions. On the one hand, *pseudo anonymisation* techniques could be employed, while, on the other, AI-based solutions could be employed, such as, for example*, federated learning*.

The possibility of simultaneously employing compliant and effective solutions has been further underscored by the publications of various EU bodies on this topic, namely:

- the Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (Commissione Europea 2018a);
- the resolution of the European Parliament on the implications of Big Data on fundamental rights (Parlamento Europeo 2017);

- the guidelines in the field of artificial intelligence and personal data protection related to the Convention 108 (Consiglio d'Europa 2019);
- the white book on artificial intelligence – a European approach (Commissione Europea 2019).

In this regard, the inclusion of clear principles on the issue by the European Commission in the IP Action Plan toolkit is desirable. The inclusion of these principles would encourage the adoption of advanced technologies in the fight against counterfeiting, removing the existing barriers and ensuring the full compliance with the data protection regulation.

5.3 Expanding cooperation and information exchange

A new multidisciplinary alliance at the national level

The increased interconnection of fraudulent schemes (listings of counterfeits, payment fraud, cybercrime) requires the **institution of stable and multidisciplinary work (an 'alliance')**, which could both take an operational lead and include all stakeholders actively involved in the prevention and fight against online counterfeiting:

- **public authorities** (law enforcement, supervisory agencies of the legitimate supply chain, judicial authorities) involved in the prevention and fight against online counterfeiting;
- **private stakeholders**, in particular:
  a. marketplaces;
  b. social media;
  c. brand owners;
  d. logistics and postal operators;
- **research centers** and universities;
- representatives of providers of **technological and *data analytics* solutions**.

Considering the interconnection between counterfeiting and financial crimes (e.g., payment service fraud) and cyber offenses (e.g., identity theft, phishing, and malware), it is appropriate that the working group includes representatives from:

- public authorities involved in the **investigation of and fight against cybercrime** (e.g., the Italian Postal Police);
- intelligence **authorities in the financial and AML domain** (e.g., Bank of Italy – UIF; the Italian Financial Corps).

The working group, which would benefit from the positive experiences of similar initiatives launched at the international level (e.g., the Memorandum of Understanding on the sale of counterfeit goods on the internet) would aim to:

- share data and information on the **new schemes and *modi operandi*** of online counterfeiting, in accordance with the aforementioned observatory;
- discuss and design **new mechanisms and instruments for information exchange** which, on the one hand, could facilitate information flows and, on the other, ensure compliance with all the involved parties' interests (e.g., personal data protection, protection of sensitive information at the commercial and industrial level);
- support the private sector to **cooperate more strictly with law enforcement and public authorities**, and encourage the latter to share more broadly with the private sector outcomes and information related to prosecutions against bad actors;
- set up joint-investigative teams on topics, cases, individuals, and specific sectors (e.g., agricultural supply-chain, made in Italy, luxury, engineering supply-chain).

As in the case of the Memorandum of Understanding on the sale of counterfeit goods on the internet, this 'alliance' could definitely benefit from setting up clear metrics and KPIs to monitor its outputs and outcomes over time. For example, members in the private sector may measure the effectiveness of new mechanisms and instruments for information exchanges discussed in the working group by monitoring the number of offers of alleged counterfeit goods, and the number of listings removed/accounts of bad actors closed.

Box 28. Collaboration between marketplaces, law enforcement and payment service providers

In February 2021, Amazon launched the *Payment Service Provider Programme* to further improve both the prevention and detection of illicit behaviour and payment fraud. Those sellers that decide to use payment service provider to receive their payments from the platform must select one of those that are enrolled on the programme, and who therefore satisfy the agreed criteria on security and compliance. This initiative was also identified as a best practice in a recent paper by EUIPO (2021e) and allows for the identification of the accounts of the sellers which receive the payments and their beneficial owners. Moreover, it limits the employment of current accounts at a higher risk, such as those opened at virtual banks. Amazon then shares with those payment service providers enrolled on the programme the information provided by the seller, to verify it. In the case of false or fraudulent information, or of illicit activities which are subsequently detected, the seller's account is then cancelled, and the funds frozen for paying pending transactions, including for returns and chargebacks.

New mechanisms for sharing and exchanging information

As mentioned in Section 4.1, the lack of agreed mechanisms for exchanging information among all involved parties represents one of the biggest challenges for effective cooperation in the fight against online counterfeiting. The increasingly **hybrid and poly-criminal nature** of the actors that are active in the sale of counterfeits on the web, who are often simultaneously present on multiple channels (**cross-channel**), requires instead a broad spectrum of collaboration, capable of ranging from counterfeiting to payment fraud, to cybercrime. As reported by several interviewees from the private sector, the **segmentation of public authorities** makes it difficult to combat in a comprehensive and integrated fashion the phenomenon as it stands at this juncture. Despite the existence of specialist units and centers of excellence within each of these public authorities, the cooperation between these agencies, not to mention with the private sector, is far from straightforward.

These difficulties are exacerbated by the fact that counterfeiting schemes are of a **transnational nature**. The identification of who lies behind the sale of counterfeits on the web does not always allow for tracing back the physical supply chain involved in the manufacturing and storage of counterfeit goods, which are often located in foreign countries and managed by third individuals. Often, the same servers which host websites - clones or fraudulent ones - that are used to sell counterfeits are located abroad, either off-shore or typically extra-EU countries. The difficulties associated with defining the territorial principle in cybercrime cases as well the challenges of international cooperation and information exchange with certain jurisdictions (or certain foreign entities) hamper the international fight against counterfeiting.

By leveraging those initiatives launched by **online marketplaces in foreign countries** (see box 22), **payment service providers** (see box 28) and also *stakeholders* in **other sectors**, such as anti-money laundering (see box 26), it is possible to explore new information exchange mechanisms and channels which, based on advanced technologies (e.g., *federated learning*), would allow for the sharing of data among public and private actors, and within the same private firms, even when competing against each other, on:

- accounts involved in illicit behaviour;
- related payment methods;
- selling strategies and *modi operandi*;
- related IP addresses.

This is the direction that was also taken by the *European Commission IP Action Plan* of the European Commission which, among the key elements of the future 'EU Toolbox against counterfeiting', specifically includes the "sharing of the data related to products and commercial operators, in compliance with personal data protection law" (Commissione Europea 2020, 18). The analysed cases and interviews in this study have demonstrated that counterfeiters, if identified and removed from a certain *marketplace*, move to another channel to sell their counterfeits. Setting up real-time information exchange systems between stakeholders in this domain would **reduce this 'displacement effect'** and serve to limit repeat offenders, which, in turn, would make the **entire e-commerce environment more secure**. In particular, sharing this information would benefit smaller stakeholders who are not equipped with the same level of resources (both of the human and monetary kind) to devote to combating counterfeiting.

In this sense, the blacklists issued by some payment service providers (the so-called ***Terminated Merchant Files***) are incredibly helpful: they include all the merchants (and related accounts) that have been suspended by payment providers due to, for example, anomalous number of chargebacks, money laundering or IPR violation. These lists, which are usually updated in real-time (such as in the *Mastercard Alert to Control High-risk Merchants*), are employed by those providers which have to on-board new merchants. They have been identified as a best practice by EUIPO (2021e) for addressing the phenomenon of repeat offenders, while EUIPO (through its *Expert Group on Cooperation with Intermediaries*) also called to **extend the sharing of these lists with marketplaces also**, so as to empower their seller vetting processes and improve the fight against counterfeiting.

Box 29. Sharing data across private entities to fight crime: the anti-money laundering experience

The *Monetary Authority of Singapore* (MAS) recently announced that they would launch a digital centralised platform in 2023, which will allow obliged entities (e.g., banks, financial institutions, professionals) to share between themselves in real-time information on clients and transactions, in order to more effectively money laundering and terrorist financing (Monetary Authority of Singapore 2021). The new platform, named COSMIC (*Collaborative Sharing of ML/TF Information & Cases*), will initially be employed by the six largest banks in Singapore (DBS, OCBC, UOB, SCB, Citybank and HSBC) and will allow for easier detection of complex money laundering schemes, which the same offender may carry out through bank accounts and transactions across different financial institutions.

Similarly, in the Netherlands, the main national banks (ING Bank, ABN Amro, Rabobank, Triodos Bank and de Volksbank) have promoted an initiative called *Transaction Monitoring Netherlands* (TMNL), which is a centralized monitoring system of financial transactions (Transaction Monitoring Netherlands 2021). TMNL shares data provided by the five banks in order to identify patterns and red-flags, which may signal potential suspicious transactions.

Conclusion

The present report represented the first systematic analysis in Italy of new trends and modi operandi in online counterfeiting and the countermeasures implemented by public authorities and private companies to prevent it. Online counterfeiting is often perceived as an increasing threat worldwide since bad actors look with interest at the opportunities offered by internet. However, while certainly being a relevant facilitator, online is still minimal in comparison to offline channels when it comes to selling counterfeit goods. Moreover, certain intermediaries, such as e-commerce marketplaces, are at the forefront of the ongoing fight against counterfeiters, allocating increasing resources to develop cutting-edge technologies and up-to-date countermeasures. The report findings and the related recommendations discussed in the previous sections may be summarized in three main working areas that need to be properly addressed in the future:

- **enforcement:** removing the barriers in the Italian framework that do not reflect the actual scenario of counterfeiting, thus making it difficult to hold bad actors accountable;

- **data sharing**: sharing relevant and up-to-date information on counterfeiting activities is essential to dismantle the criminal networks involved in this criminal market. To encourage such practice, Italy could actively participate to the framing of the EU Toolbox that sets out a coordinated European approach on counterfeiting. The Toolbox should indeed clarify roles and responsibilities of all the actors involved in fight against counterfeiting, also identifying ways to upgrade data sharing and cooperation between right holders, intermediaries (both online and offline) and law enforcement authorities. The establishment of a national working group on the topic could strengthen the Italian position at the international level in the fight against counterfeiting;

- **prevention**: setting common shared standards to prevent the advertisement and selling of counterfeit goods. In this regard, referring to the OECD guidelines published in the recent study ‘E-commerce Challenges in Illicit Trades in Fakes: Governance Frameworks and Best Practices’ (OECD 2021) is highly recommended. Also identifying and promoting best practices, in both the public and private domain, would help in sharing knowledge among the affected stakeholders, thus enhancing the fight against bad actors.

References

AACP. 2002. «Proving the connection: links between intellectual property theft and organized crime».

AIFA. 2021. «Medicinali online: in aumento le segnalazione di prodotti contraffatti acquistati da canali non autorizzati».

Alibaba Group. 2020. «Alibaba Group 2020 Annual Report on Intellectual Property Protection».

Amazon. 2021a. «EU Policy Position Paper - Accountability for Counterfeiters».

———. 2021b. «Press release Amazon Counterfeit Crimes Unit Reaches Settlement with Influencers Who Ran Social Media Counterfeiting Scheme, Permanently Banning them from Amazon's Store and Securing Financial Payments to be Donated to Support Anti-Counterfeiting Awareness September 30, 2021 at 9:16 AM EDT». https://press.aboutamazon.com/news-releases/news-release-details/amazon-counterfeit-crimes-unit-reaches-settlement-influencers.

———. 2021c. «Report sulla protezione dei marchi».

Bosisio, Antonio, Carlotta Carbone, Maria Jofre, Michele Riccardi, e Stefano Guastamacchia. 2021. Developing a Tool to Assess Corruption Risk factors in firms' Ownership Structures - Final report of the DATACROS Project.

Bosisio, Antonio, Lorella Garofalo, Marco Dugato, e Michele Riccardi. 2017. La sicurezza del retail in Italia. Uno studio su furti, rapine e nuovi sistemi di sicurezza. Milano: Crime&tech - Università Cattolica del Sacro Cuore.

Camerini, Diana, Serena Favarin, e Marco Dugato. 2015. «Estimating the counterfeit markets in Europe». Transcrime Research in Brief 3.

Canfield, John. 2018. «The Ever-Changing Landscape of Bots and Credit Cards Testing». https://www.business.com/articles/bots-credit-card-testing/.

Cassara, John A. 2016. Trade-based money laundering: the next frontier in international money laundering enforcement. Wiley & SAS business series. Hoboken, New Jersey: John Wiley & Sons.

CBS News. 2019. «Cybercriminals are doing big business in the gaming chat app Discord». https://www.cbsnews.com/news/cybercriminals-are-doing-big-business-in-the-gaming-chat-app-discord/.

Censis e MISE. 2021. «Rapporto conclusivo sulla contraffazione in 20 province italiane: un'analisi comparata».

CISA. 2021. «Alert (AA21-265A) - Conti Ransomware». https://us-cert.cisa.gov/ncas/alerts/aa21-265a.

CNBC. 2020. «Amazon sues two influencers for peddling counterfeit goods on Instagram and TikTok». https://www.cnbc.com/2020/11/12/amazon-sues-influencers-for-allegedly-marketing-counterfeits.html.

———. 2021. «Amazon settles with influencers who allegedly peddled counterfeits on Instagram and TikTok».

Commissione Europea. 2018a. «Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679».

———. 2018b. «Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities».

———. 2019. «Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia».

———. 2020. «Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni. Sfruttare al meglio il potenziale innovativo dell'UE. Piano d'azione sulla proprietà intellettuale per sostenere la ripresa e la resilienza dell'UE.»

Consiglio d'Europa. 2019. «Linee guida in materia di intelligenza artificiale e protezione dei dati personali».

Consiglio Nazionale Anticontraffazione. 2019. «Piano Strategico Nazionale 2019-2020».

Couvèe, Koos. 2019. «Fintechs Fuel Surge in UK Defense Against Money Laundering Requests». https://www.moneylaundering.com/news/fintechs-fuel-surge-in-uk-defense-against-money-laundering-requests/.

Crime&tech. 2021. «Next Generation AML: indagine tra le banche e gli altri soggetti obbligati in Italia sull'uso dei big data e dell'intelligenza artificiale in ambito antiriciclaggio».

CyberSource. 2020. «What you need to know about card testing fraud». https://www.cybersource.com/en-us/blog/2020/what-you-need-to-know-about-card-testing-fraud.html.

Does de Willebois, Van Der Emile, Emily M. Halter, Robert A. Harrison, Ji Won Park, e J.C. Sharman. 2011. The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It. The World Bank. https://doi.org/10.1596/978-0-8213-8894-5.

eBay. 2021. «2020 Global Transparency Report».

EUIPO. 2017. «Research on Online Business Models Infringing Intellectual Property Rights - Phase 2. Suspected trade mark infringing e-shops utilising previously used domain names.»

———. 2019a. «2019 INTELLECTUAL PROPERTY SME SCOREBOARD». https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IP_sme_scoreboard_study_2019/executiveSummary/executive_summary_2019_en.pdf.

———. 2019b. «Anti-counterfeiting Blockathon Forum. Blockchain Use Case». https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Blockathon/Blockathon-Forum_Blockchain-Use-Case.pdf.

———. 2020. Automated Content Recognition: Discussion Paper. Phase 1, Existing Technologies and Their Impact on IP'. LU: Publications Office. https://data.europa.eu/doi/10.2814/52085.

———. 2021a. Anti-Counterfeiting Technology Guide. LU: Publications Office. https://data.europa.eu/doi/10.2814/665780.

———. 2021b. Focus on Cybersquatting: Monitoring and Analysis. LU: Publications Office. https://data.europa.eu/doi/10.2814/14926.

———. 2021c. Monitoring and Analysing Social Media in Relation to IP Infringement: Report. LU: Publications Office. https://data.europa.eu/doi/10.2814/235275.

———. 2021d. «New and existing trends in using social media for IP infrigement activities and good practices to address them». Socila Media - Discussion paper. European Union Intellectual Property Office.

———. 2021e. «Payment - Discussion Paper. Challenges and good practices for electronic payment services to prevent the use of their services for intellectual property-infringing activities».

———. 2021f. Vendor Accounts on Third Party Trading Platforms: Research on Online Business Models Infringing Intellectual Property Rights : Phase 4. LU: Publications Office. https://data.europa.eu/doi/10.2814/279240.

EUIPO e Europol. 2019. «Intellectual Property Crime Threat Assessment 2019».

EUIPO e OECD. 2021a. Global Trade in Fakes : A Worrying Threat. Spain: EUIPO. https://data.europa.eu/doi/10.2814/374693.

———. 2021b. «Misuse of E-Commerce for Trade in Counterfeits». Illicit Trafficking. Paris: OECD Publishing. https://doi.org/10.1787/1c04a64e-en.

Europol. 2016. «MAIN EUROPEAN UNION HUB FOR DISTRIBUTION OF COUNTERFEIT GOODS DISMANTLED».

———. 2020. «Internet Organised Crime Threat Assessment».

———. 2021. «European Union Serious and Organised Crime Threat Assessment. A corrupting influence: the infiltration and undermining of Europe's economy and society by organized crime».

Europol e EUIPO. 2020. IP Crime and Its Link to Other Serious Crimes: Focus on Poly Criminality. Luxembourg: Publications Office. https://data.europa.eu/doi/10.2814/090414.

Eurostat. 2021. «E-commerce statistics for individuals». https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics_for_individuals.

FACT Coalition. 2019. «Anonymous Companies Help Finance Illicit Commerce and Harm American Businesses and Citizens. A need for Incorporation Transparency».

Flashpoint. 2019. «Refund Fraud and Fake Receipts Proliferate on the Deep & Dark Web». https://www.flashpoint-intel.com/blog/refund-fraud-fake-receipts/.

Garante per la protezione dei dati personali. 2019. «Deliberazione del 12 giugno 2019 - Codice di condotta per il trattamento dei dati personali in materia di informazioni commerciali».

Guardia di Finanza. 2019. «Social media e contraffazione - Conclusa l'operazione Aphrodite II». https://www.gdf.gov.it/stampa/ultime-notizie/anno-2019/giugno/social-media-e-contraffazione-conclusa-loperazione-aphrodite-ii.

———. 2020a. «Contraffazione sul web, denunciati 92 responsabili, sequestrato oltre mezzo milione di prodotti illegali». https://www.gdf.gov.it/stampa/ultime-notizie/anno-2020/febbraio/contraffazione-sul-web-denunciati-92-responsabili-sequestrato-oltre-mezzo-milione-di-prodotti-illegali.

———. 2020b. «Smantellata associazione per delinquere dedita al traffico di abbigliamento contraffatto». https://www.gdf.gov.it/stampa/ultime-notizie/anno-2020/maggio/smantellata-associazione-per-delinquere-dedita-al-traffico-di-abbigliamento-contraffatto.

He, Sherry, Brett Hollenbeck, e Davide Proserpio. 2021. «The Market for Fake Reviews».

Heinonen, Justin A., Thomas J. Holt, e Jeremy M. Wilson. 2012. «Product Counterfeits in the Online Environment: An Empirical Assessment of Victimization and Reporting Characteristics». International Criminal Justice Review 22 (4): 353–71. https://doi.org/10.1177/1057567712465755.

ICE. 2020. «HSI partners with Pfizer, 3M, Citi, Alibaba, Amazon, Merck to protect consumers against COVID-19-related fraud». https://www.ice.gov/news/releases/hsi-partners-pfizer-3m-citi-alibaba-amazon-merck-protect-consumers-against-covid-19.

Il Sole 24 Ore. 2021a. «Amazon contro falsi e contraffazioni: bloccate 10 miliardi di offerte sospette».

———. 2021b. «Blockchain ed Nfc contro il mercato miliardario della contraffazione – Il caso Authena-Masque Milano». https://guiomarparada.nova100.ilsole24ore.com/2021/10/20/blockchain-contraffazione-authena/.

International Trademark Association. 2019. «Gen Z Insights: Brands and Counterfeit Products».

Jofre, Maria, Michele Riccardi, Antonio Bosisio, e Stefano Guastamacchia. 2021. «Money laundering and the detection of bad companies: A machine learning approach for the risk assessment of opaque ownership structure». In .

Kennedy, Jay P. 2020. «Counterfeit Products Online». In The Palgrave Handbook of International Cybercrime and Cyberdeviance, a cura di Thomas J. Holt e Adam M. Bossler, 1001–24. Palgrave Macmillan.

Lince, Tim. 2020. «'Dupe culture' grows on TikTok; why this helps counterfeiters and harms brands». World Trademark Review. https://www.worldtrademarkreview.com/anti-counterfeiting/dupe-culture-grows-tiktok-why-helps-counterfeiters-and-harms-brands.

Luca, Michael, e Georgios Zervas. 2016. «Fake It Till You Make It: Reputation, Competition, and Yelp Review Fraud». Management Science 62 (12): 3412–27. https://doi.org/10.1287/mnsc.2015.2304.

Luxottica. 2017. «Il nostro modo di proteggere brand e clienti». https://www.luxottica.com/it/chi-siamo/operiamo/tutela-brand.

Mayzlin, Dina, Yaniv Dover, e Judith Chevalier. 2014. «Promotional Reviews: An Empirical Investigation of Online Review Manipulation». American Economic Review 104 (8): 2421–55. https://doi.org/10.1257/aer.104.8.2421.

McCoy, Damon. 2016. «Bullet-Proof Credit Card Processing». In . San Francisco, CA: USENIX Association.

MEF. 2018. «Analisi nazionale dei rischi di riciclaggio di denaro e di finanziamento del terrorismo elaborata dal Comitato di sicurezza finanziaria». http://www.dt.mef.gov.it/it/news/2019/aggiornamento_analisi_rischio_riciclaggio.html.

Miller, Rena S., Liana W. Rosen, e James K. Jackson. 2016. «Trade-Based Money Laundering: Overview and Policy Issues». Congressional Research Service.

Ministero dell'Interno. 2021. «Contributo del Servizio Analisi Criminale del Dipartimento della Pubblica Sicurezza - Direzione Centrale del Servizio Criminale del Ministero dell'Interno al progetto FATA».

Moiseienko, Anton. 2020. «Understanding Financial Crime Risks in E-Commerce». RUSI, Occasional Paper, .

Moiseienko, Anton, e Kayla Izenman. 2019. «Gaming the System: Money Laundering Through Online Games». Rusi Newsbrief, 2019.

Monetary Authority of Singapore. 2021. «MAS and Financial Industry to Use New Digital Platform to Fight Money Laundering». https://www.mas.gov.sg/news/media-releases/2021/mas-and-financial-industry-to-use-new-digital-platform-to-fight-money-laundering.

OECD. 2018. Il commercio di beni contraffatti e l'economia italiana: Tutelare la proprietà intellettuale dell'Italia. Paris: OECD Publishing.

———. 2021. E-Commerce Challenges in Illicit Trade in Fakes: Governance Frameworks and Best Practices. Illicit Trade. OECD. https://doi.org/10.1787/40522de9-en.

OECD e EUIPO. 2018. Trade in Counterfeit Goods and Free Trade Zones: Evidence from Recent Trends. Illicit Trade. Paris/European Union Intellectual Property Office: OECD Publishing. https://doi.org/10.1787/9789264289550-en.

———. 2020. Trade in Counterfeit Pharmaceutical Products. Illicit Trade. Paris: OECD Publishing.

———. 2021a. Misuse of Containerized Maritime Shipping in the Global Trade of Counterfeits. Illicit Trade. OECD. https://doi.org/10.1787/e39d8939-en.

———. 2021b. Misuse of E-Commerce for Trade in Counterfeits. Illicit Trade. OECD. https://doi.org/10.1787/1c04a64e-en.

OHIM. 2013. European Citizens and Intellectual Property: Perception, Awareness and Behaviour. Alicante: Office for Harmonization for Internal Markets.

Parlamento Europeo. 2017. «Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto».

Pellegrini, Antonio, Pierpaolo De Franceschis, Chiara Bentivogli, e Eleonora Laurenza. 2020. «Un indicatore sintetico per individuare le società cosiddette cartiere». Quaderni dell'antiriciclaggio 15.

Reddit. 2018. «[Guide] "Help,I'm New Where Do I start?" FashionReps Newbie Guide + Frequently used Terms!» https://www.reddit.com/r/FashionReps/comments/ae540e/guide_help_im_new_where_do_i_start_fashionreps/.

Savona, Ernesto Ugo, e Michele Riccardi, a c. di. 2018. Mapping the risk of Serious and Organised Crime infiltration in European Businesses Final report of the MORE Project. Milano: Transcrime - Università Cattolica del Sacro Cuore.

Senato della Repubblica Italiana. 2017. Lotta alla contraffazione e tutela del made in italy. Documento di Analisi n.5.

Stroppa, Andrea, e Daniele Di Stefano. 2016. «Social media and luxury goods counterfeit: a growing concern for government, industry and consumer worlwide». A cura di Bernardo Parrella.

Stroppa, Andrea, Davide Gatto, Lev Pasha, e Bernardo Parrella. 2019. «Instagram and counterfeiting in 2019: new features, old problems».

Tian, Hongwei, Stephen M. Gaffigan, D. Sean West, e Damon McCoy. 2018. «Bullet-proof payment processors». In 2018 APWG Symposium on Electronic Crime Research (eCrime), 1–11. San Diego, CA: IEEE. https://doi.org/10.1109/ECRIME.2018.8376208.

TRACIT e AAFA. 2020. «Fraudolent Advertising Online: Emerging Risks and Consumer Fraud».

Transaction Monitoring Netherlands. 2021. «What is TMNL?»

TransUnion. 2020. «Global E-Commerce in 2020: Redefining the Retail Experience as Shopping Patterns Change».

UIBM. 2020. «Rapporto sulle Politiche Anticontraffazione 2018-2019». Ministero dello Sviluppo Economico, UIBM. https://uibm.mise.gov.it/images/documenti/Rapporto_Politiche_Anticontraffazione_20182019.pdf.

UIF. 2021. «Indicatori e schemi di anomalia». https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/index.html?com.dotmarketing.htmlpage.language=102.

UNIFAB. 2016. «Counterfeiting & Terrorism. Report 2016». https://euipo.europa.eu/ohimportal/documents/11370/71142/Counterfeiting+%26%20terrorism/7c4a4abf-05ee-4269-87eb-c828a5dbe3c6.

U.S. Attorney's Office. 2018. «Sixteen Treasure Valley Residents Indicted in Federal Court». https://www.justice.gov/usao-id/pr/sixteen-treasure-valley-residents-indicted-federal-court.

US District Court of Maryland. 2018. «UNITED STATES OF AMERICA, Plaintiff, v. MOHAMED Y. ELSHINAWY, Defendant.»

Vice. 2018. «Uno studente ha creato un impero di sneaker false su Reddit - finché non è sprofondato». https://www.vice.com/it/article/vbjkj4/vendere-repliche-sneaker-reddit.

Vigderman, Aliza. 2021. «Account Takeover Fraud: A Consumer's Guide to Protecting Yourself». https://www.security.org/digital-safety/account-takeover-prevention/.

Wall Street Journal. 2019. «Meet the Sneaker Collectors Who Intentionally Buy Fake Shoes».

Wronka, Christoph. 2021. «"Cyber-Laundering": The Change of Money Laundering in the Digital Age». Journal of Money Laundering Control ahead-of-print (ahead-of-print). https://doi.org/10.1108/JMLC-04-2021-0035.

WTO. 1994. «Annex 1C. Agreement on Trade-Related Aspects of Intellectual Property Rights.»

crime&tech

Powered by Transcrime

UNIVERSITÀ CATTOLICA del Sacro Cuore

with the support of

amazon