HIDDEN LINKS:
FACILITATING CRIMINAL ACTIVITIES WHILE EXPLOITING E-COMMERCE

unicri
United Nations
Interregional Crime and Justice
Research Institute

TABLE OF CONTENTS

DISCLAIMER

The opinions, findings, conclusions and recommendations expressed herein do not necessarily reflect the views of the United Nations Interregional Crime and Justice Research Institute (UNICRI) or contributory organizations, and do not imply any endorsement. The content of this publication may be quoted or reproduced in part, provided that the source of information is acknowledged. UNICRI would like to receive a copy of the document in which this publication is used or quoted.

References to specific brand names, product images and commercial platforms (including links) in this report are provided solely for illustrative and analytical purposes, to explain the mechanisms through which hidden links operate in the context of online counterfeiting. The inclusion of such examples does not imply, suggest or establish any association between the brands, products or platforms mentioned and unlawful activities. Nor should these references be interpreted as affecting or reflecting their reputation, integrity or compliance practices. Examples are included only when essential to understanding the phenomenon under examination

The designation employed and presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations and UNICRI, concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitation of its frontiers or boundaries.

ACKNOWLEDGEMENTS

This report is the product of an initiative led by the United Nations Interregional Crime and Justice Institute (UNICRI). It was written by John Zacharia, and by Vasilis Katos and Emily Rosenorn-Lanng (both of Cyber Innovations Ltd.) under the guidance of Marco Musumeci, Programme Management Officer at UNICRI, with editing by Marina Mazzini and design by Pierluigi Balducci.

Viale Maestri del Lavoro,10
10127 Turin, Italy
Website: www.unicri.org
E-mail: unicri.publicinfo@un.org

1. EXECUTIVE SUMMARY

Leading up to and during the pandemic that began in 2020, many counterfeiters focused on trafficking in counterfeit goods online, particularly through e-commerce platforms. Although such online traffickers use various techniques to sell counterfeit goods on these platforms, this report focuses on one particularly difficult technique to combat: the use of hidden links.

In their most insidious form, hidden links are e-commerce listings that appear to offer a generic product for sale – for example, a generic green jacket – but when consumers go to the e-commerce listing and click the link to purchase the generic jacket, they instead receive a completely different product that bears a counterfeit mark, such as a handbag bearing an identical but counterfeit trademark of a famous luxury brand.

Counterfeiters' use of hidden links makes detection particularly difficult for brand owners and e-commerce platforms, because the methods they usually apply to detect counterfeit goods on their marketplaces are largely ineffective. By way of example, most major e-commerce platforms implement forms of image recognition and keyword filters to flag the unauthorized use of images of trademarks or descriptions of goods bearing counterfeit marks, which are typically tied to the sale of counterfeit goods. In the same vein, major brand owners regularly review listings searching for similar information showing that an e-commerce listing is, in fact, offering for sale a counterfeit product. With hidden links, however, these detection techniques are unavailing. Test purchases would support identifying listings that offer for sale generic items while actually trading in counterfeit goods, but making a test purchase of every generic listing on every major e-commerce platform would be both prohibitively expensive and overly burdensome, given the sheer volume of generic listings across e-commerce platforms.

This report explores how hidden links work and who the various actors are behind this technique in an effort to propose strategies to combat their use. In a nutshell, manufacturers of counterfeit goods and complicit third-party sellers work together to create an e-commerce listing using a hidden link. They then need to share the link with trusted influencers and affiliates who can, in turn, promote the hidden link to consumers looking for counterfeit goods sold through these links. Initially, the influencers and affiliates will use social media to share the hidden link in closed groups. Eventually, an influencer or consumer will begin to promote the hidden link outside the closed groups, so they are more publicly known. Websites or discussion boards/channels are commonly used for this purpose. Although e-commerce platforms can shut down hidden links once they are made aware of them, this is usually too late.

To effectively combat the hidden links problem, this report proposes two solutions. First, the creation of an artificial intelligence (AI)-enabled tool to simulate automated "test" purchases without completing them – i.e., a tool that could use digital packet inspection to simulate consumer behaviour and identify discrepancies between listed and delivered goods. Second, and until such a tool is created, greater cooperation between social media platforms and those actors seeking to combat hidden links, such as e-commerce platforms, brand owners, and law enforcement. In addition, social media companies that effectively deprive counterfeiters of the closed forums they need to communicate the existence of the hidden links, would make it much more difficult for counterfeiters to "scale up" the sale of counterfeit goods using this method.

2. INTRODUCTION

Trafficking in counterfeit goods is an ever-growing problem.[1] Today, both infringing and legitimate goods are increasingly sold in online markets such as e-commerce platforms, and third-party sellers command a significant share of the e-commerce retail pie. For example, since 2020, a majority of all physical goods sold on Amazon's e-commerce platform are sold by third-party sellers.[2] Traffickers in goods bearing counterfeit marks – *i.e.*, marks identical to, or substantially indistinguishable from, legitimate trademarks – have also shifted to selling counterfeit goods online.

E-commerce platforms have developed automated tools to detect listings for counterfeit goods before sellers have the chance to list such goods publicly on the platform. As the effectiveness of these automated tools has improved, counterfeiters have adapted their techniques to circumvent the platforms' countermeasures. One of the most insidious and successful techniques employed by counterfeiters is the use of hidden links. Hidden links are e-commerce listings that appear to sell a legitimate generic product, but once a consumer places an order, they will actually receive a counterfeit good.[3] The automated tools typically used by e-commerce platforms to detect listings for counterfeit goods – such as image recognition and keyword detection tools – will not be able to identify hidden links.[4] Accordingly, brand owners and e-commerce platforms dedicated to combatting hidden links must take a different approach to solve this problem.[5]

1 The number of seizures of goods infringing intellectual property rights at the U.S. border, for instance, increased from 3,244 seizures in 2000 to 33,810 seizures in 2018. William Mauldin & Alex Leary, U.S. Signals Crackdown on Counterfeit Goods Sold Online, The Wall Street Journal (Jan. 24, 2019). According to the U.S. Customs and Border Protection, between fiscal years 2020 and 2024, the total number of infringing goods seized at the U.S. border more than doubled, Intellectual Property Rights Seizure Statistics: Fiscal Year 2024 (Publication Number 3964-0125). The story is similar in Europe. The European Commission's Directorate-General for Taxation and Customs Union (DG TAXUD) and the European Union Intellectual Property Office (EUIPO) issued the joint report EU Enforcement of Intellectual Property Rights: Results at the EU Border and in the EU Internal Market 2024 (2025), indicating that the European Union seized over 112 million counterfeit items, with an estimated retail value of 3.8 billion euros, in 2024 alone. The Illicit Trade Reports of the World Customs Organization (WCO) also present a worrying picture for other regions. In 2017, seizures of counterfeit goods amounted to slightly fewer than 150 million products in the Middle East and around 180 million products in South America (World Customs Organization (Illicit Trade Report 2018). Subsequent WCO reports highlight the seriousness of trafficking in counterfeit goods, particularly regarding risks to consumers' health and safety. Seizures of falsified medicines in 2021 and 2022 reached alarming levels in several countries, including Benin, Guinea, Mali, Namibia, and Togo. In terms of the type of falsified medicines seized, the WCO Illicit Trade Report 2022 shows the prevalence of painkillers, antibiotics, erectile dysfunction drugs, antidiabetic drugs and also medical devices.

2 Jay Greene, Burning Laptops and Flooded Homes: Courts Hold Amazon Liable for Faulty Products, The Washington Post (Aug. 29, 2020): "Nearly 60 percent of all physical goods sold on Amazon's e-commerce marketplace come from third-party merchants, a fact that's lost on many shoppers."

3 E.g., https://www.alizila.com/alibaba-fights-hidden-links-ipr-intellectual-property-rights-marketplaces/: hidden links occur when "[o]nline sellers create a listing for a seemingly unrelated, innocuous product, but which actually offers a different and counterfeit item."

4 E.g., 11 Ways to Detect Aliexpress' Hidden Links: "Sellers resort to hidden links primarily to avoid legal issues and platform restrictions. [...] Hidden links provide a workaround for these challenges, so sellers can continue offering such products discreetly."

5 To increase knowledge on this issue and improve responses to counterfeiting as an organized crime activity, UNICRI established a fully-fledged programme dedicated to this issue. From 2007 (the year of publication of its first report on this topic (1) onwards, activities have progressively expanded to include several studies on actual trends and future developments (especially those linked to the use of new technologies); guidelines to help public law enforcement and prosecutors investigate IP crimes; manuals for IP owners on how to investigate and refer IP violations to public law enforcement and prosecutors; as well as training activities deployed in various regions on supply chain security issues linked to the trafficking in counterfeit goods.

3. HIDDEN LINKS IN E-COMMERCE

3.1 What are hidden links

Hidden links are e-commerce listings that appear legitimate but in fact facilitate the sale of counterfeit products. They may show a generic product — a plain belt, wallet, or handbag — but once consumers place an order, they receive a counterfeit branded item.

While they serve as the crucial bridge used by counterfeiters to connect their marketing efforts on social media with actual purchase transactions on e-commerce platforms, as elaborated later in this report, they also attempt to evade detection by brand-enforcement systems and marketplace controls.

Social media influencers have even coined phrases like *"Order this, get this"* to guide their followers on how to buy counterfeits using these hidden links. (Complaint in *Amazon v. Fitzpatrick,* Case No. 20-cv-01662 (W.D. Wash. Nov. 12, 2020).

Source:
Complaint in Amazon v. Fitzpatrick
Case No. 20- cv-01662
(W.D. Wash. Nov. 12, 2020).

At their core, hidden links are URLs that point to product listings on online marketplaces, but with critical obfuscation applied. These links may direct buyers to listings where brand names are stripped from descriptions, product images are deliberately blurred (especially for items with distinctive patterns), or – in more common cases – to completely unrelated "decoy" products that bear no resemblance to what will actually be delivered.

The need for hidden links arose as counterfeiters face two opposing challenges: on the one hand they need to advertise their products to as many potential customers as possible. As such, they primarily use social media to ensure broad outreach to their target customers and target groups. On the other hand, they need to avoid detection, as this will result in takedowns and removals of their listings and, if identified, legal action against them. In essence, hidden links are employed to circumvent marketplace controls restricting the sale of counterfeit goods. For this reason, hidden links are often made available for a short time to avoid detection.[6]

3.2 What is the impact of hidden links?

The impact of hidden links on trademark owners is difficult to overstate. Specifically, the use of hidden links negatively impacts trademark owners in at least two important ways. First, hidden links take advantage of the legitimate supply chain to sell counterfeit goods. Although traffickers have long used the illegitimate supply chain to sell counterfeit goods, this traditional

6 Alibaba Steps Up Fight Against 'Hidden Links' and IPR Vigilance Post Reorganization

approach limits a trafficker's customers to those who are willing to go to illegitimate markets to purchase counterfeit goods. However, when traffickers use hidden links in listings on legitimate e-commerce platforms to sell counterfeit goods, they increase the scope of potential customers to those who may only choose to use the legitimate online supply chain. In this way, traffickers can successfully syphon trademark owners' revenue streams from legitimate marketplaces by redirecting consumers from sales of authentic goods to sales of counterfeit goods in the same legitimate online marketplace – thereby increasing the likelihood of displaced sales of authentic goods and amplifying the overall harm to trademark owners.

Second, hidden links evade the investigative tools trademark owners' typically use to investigate trademark counterfeiting. For example, trademark owners will scan listings in online marketplaces for images associated with the sale of goods bearing marks identical to, or substantially indistinguishable from, the trademark owner's protected word mark or logo to see if these goods are sold at prices well below any authentic new or used good bearing the same trademark. Similarly, if the image is generic or otherwise conceals the counterfeit mark, a trademark owner can still scan for a description indicating, for example, that the good is a "replica" or "knockoff" of the trademark owner's brand. In either case, the trademark owner can demand that the e-commerce platform remove such listings, and most legitimate e-commerce platforms will comply with such demands. When a trafficker uses a hidden link, however, these investigative techniques will categorically fail. The trademark owners' scans will pass over the generic and unrelated product that does not include a description of the counterfeit good actually being sold. Without a way to identify well-designed hidden links, trademark owners cannot easily stop them from being used by traffickers to sell counterfeit goods online.

In this respect, the use of hidden links has an equally negative impact on e-commerce platforms that are making good faith efforts to root out listings for counterfeit goods. Unlike trademark owners, e-commerce platforms have more powerful tools to identify traffickers in counterfeit goods on their own platform. Operators of e-commerce platforms can vet third-party sellers to ensure that they are legitimate and properly identified *before* allowing them to place listings on their platform. These operators can also build AI-enabled algorithms based on historical data to proactively identify and remove (1) third-party sellers who they know have previously sold counterfeit goods or (2) listings of counterfeit goods before they are made available to the public. Furthermore, they can run algorithms based on customers' reviews (that are not always visible to trademark owners) to remove listings after they are posted on the online marketplace. Nevertheless, hidden links can evade even the most sophisticated AI-enabled algorithms that e-commerce platforms implement to detect traffickers in counterfeit goods. Thus, even well-intentioned e-commerce platforms struggle to identify and remove hidden links from their online marketplaces.

3.3 How criminals use hidden links in e-commerce to traffic in counterfeit goods (a.k.a. the hidden-links ecosystem)

The story of hidden links starts with the demand for counterfeit goods/replicas. In general, many consumers purchasing products for unusually low prices know that what they are purchasing is highly unlikely to be the genuine product. And virtually all consumers who choose to go to a hidden link do so because they have been advised, typically by an influencer, to use the link

and visit the listing for a generic product, knowing that through the hidden link, it is guaranteed that they will in fact be buying a specific counterfeit good at a specific, desirable price. In this way, hidden links are at the center of the purchase workflow for counterfeit goods through e-commerce platforms.

As set forth more fully below, the process through which hidden links work can be summarised as follows.

1) Manufacturers of counterfeit goods interested in supplying their illicit products will work in concert with third-party sellers who will create listings on e-commerce platforms containing hidden links. Initially, the existence of the hidden link will most commonly be shared in closed groups on peer-to-peer (P2P) platforms and on social media. Group or channels on messaging apps are popular platforms for disseminating hidden links to closed group members, as are closed groups on social media platforms. The clear purpose of these closed groups is to limit the group's membership to trusted affiliates of the third-party seller who intend to post the hidden link, as well as to select influencers. If the hidden link is revealed to a wide audience too quickly, then the e-commerce platform may learn about the hidden link and remove it before a meaningful number of counterfeit goods sales have occurred. In this way, the closed group provides some basic confidentiality and avoids detection by any scans trademark owners may be using on social media sites or P2P platforms to detect counterfeiting activity.

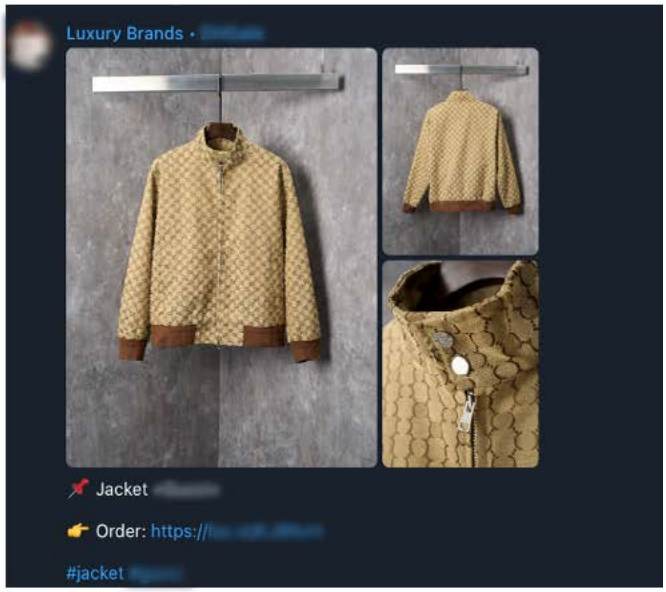
2) These affiliates will work to identify additional influencers who will "spread the word" to their followers in other closed groups. Eventually, an influencer or consumer will publicly reveal the existence of a hidden link, at which point either the third-party seller takes the listing down, the trademark owner learns of the hidden link and demands that the e-commerce platform take it down, or the platform learns of the hidden link and takes down the listing containing the hidden link.

3.4 The evolution of hidden links

Hidden links have evolved over time. In all cases, they may point to an actual product, or a so-called decoy product. Early on, traffickers used hidden links to point to a generic product or an image of the product, but with the brand name missing from the product description. This approach would evade infringement detection software initially. However, trademark owners and e-commerce platforms could eventually tailor their scanning tools to look for the image of any product made by the trademark owner, even if it does not include the trademark itself. In some cases, the hidden link would point to a product that is blurred – especially for products that show "unique" or otherwise brand-identifiable patterns. However, with the proliferation and advancement of AI-enabled detection tools, these obfuscation techniques are becoming less effective because even blurred versions of the trademark owner's product can be used to train AI-enabled tools. An example of pattern obfuscation is presented in the series of images on the right, which shows the original product with clear patterns, and the imposed blurred version posted on the marketplace, with the brand name missing from the description.

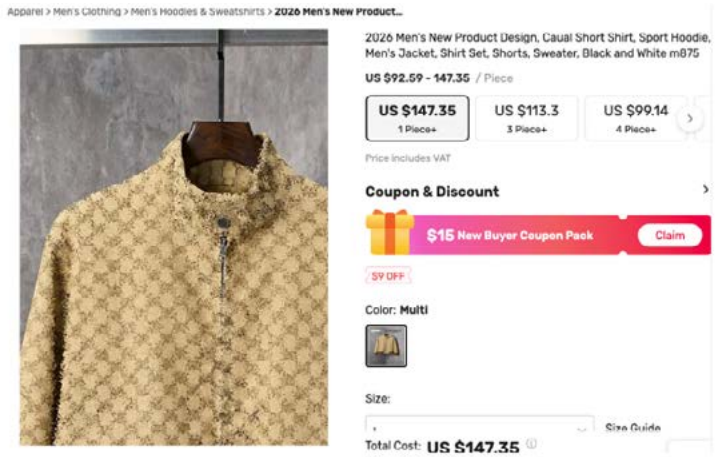
Figure 1: Examples of pattern obfuscation.

Original product



Source: P2P/Social media platform

Product linked through the hidden link redirects



Source: e-commerce platform

Detail of a photoshopped (blurred) image and omission of the brand name

For the common case of a **decoy product**, the hidden link will point to a completely different type of good from the counterfeit good actually being sold. This deliberate decoupling between the listed product and the item actually delivered maximizes the likelihood of evading detection.

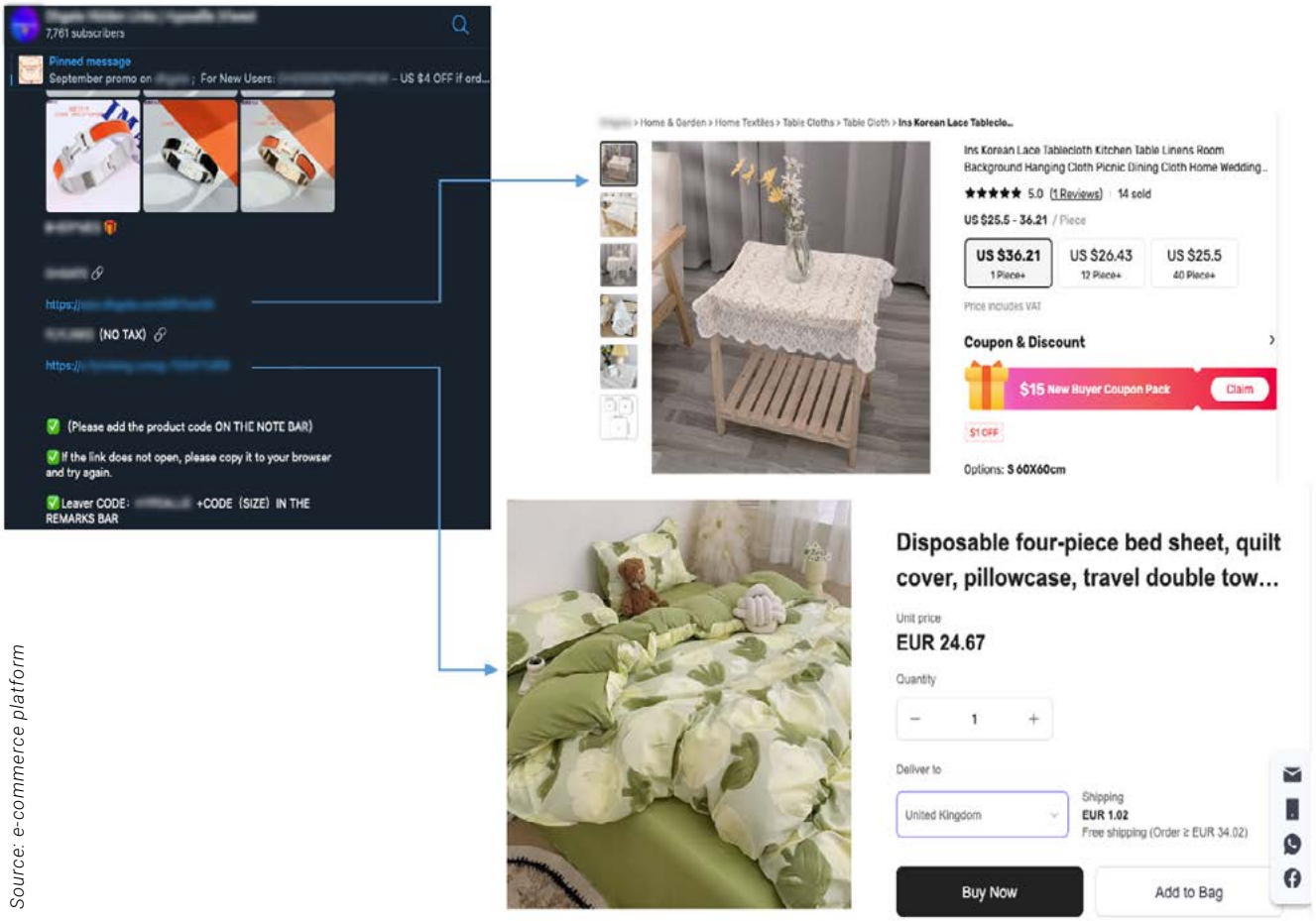
Another obfuscation technique consists of modifying the brand logo or trademark when it appears on the product.

Source: e-commerce platform

In the following example, there are two hidden links for buying a a famous luxury brand product, each pointing to a different third-party online platform, as shown in the figure below. The use of two hidden links is particularly interesting as it serves two purposes:

- Resilience: using two separate third-party platforms, diversifies risk by offering a backup if one link or vendor account is taken down.
- Increased competitiveness and attractiveness: In the counterfeit goods market, sellers often advertise “No Tax” as a benefit to attract buyers by promising lower prices, since none of the usual taxes levied on legal goods are charged or paid to authorities. This also signals to buyers that the transaction is “off the books,” further indicating illegal activity and removing a possible paper trail that law enforcement or tax agencies could follow. The broader impact includes lost public revenue, weakened law enforcement, and increased difficulty in tracking illicit sales.

Figure 2: Example of simultaneous use of two hidden links.



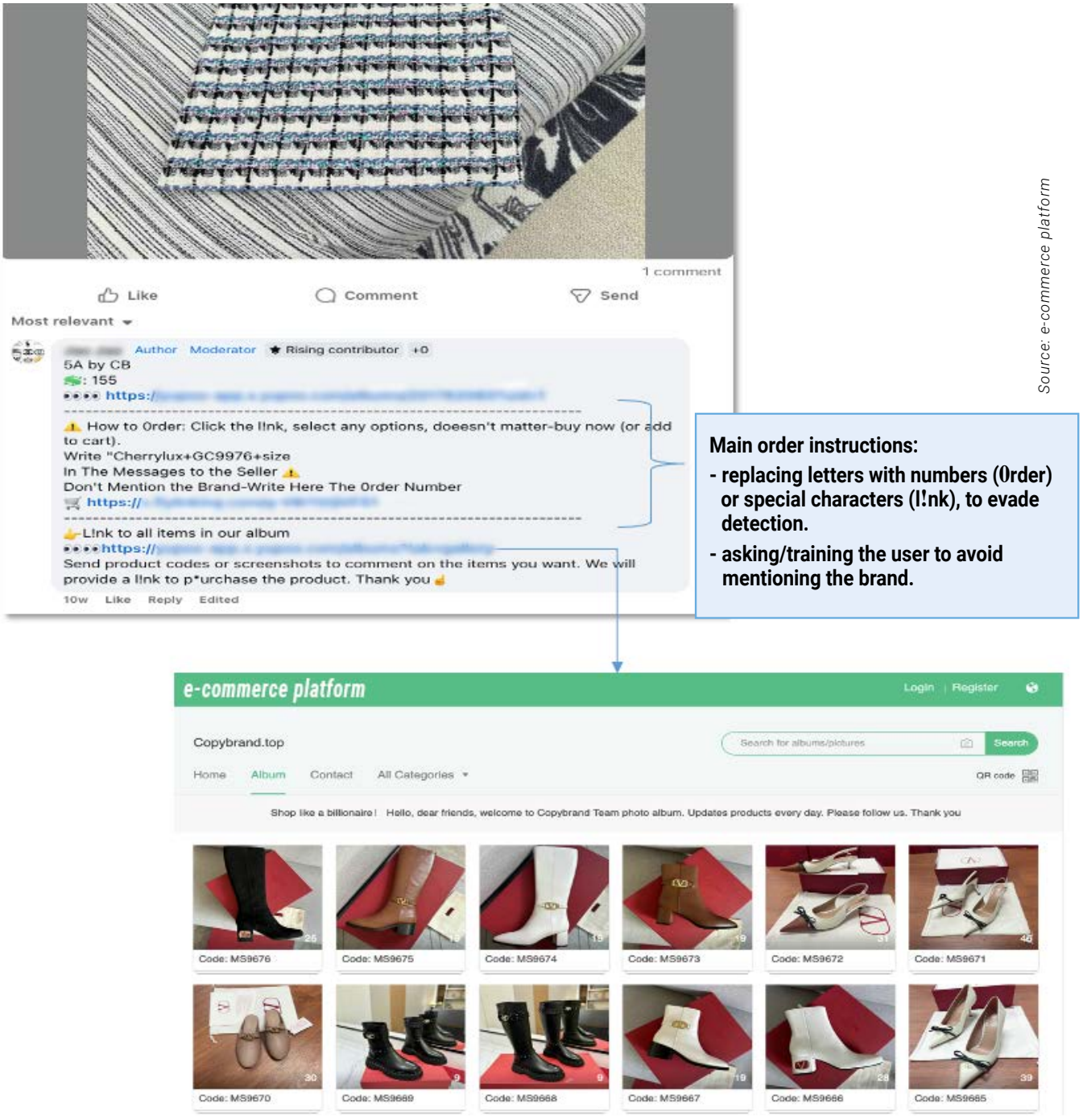
Source: e-commerce platform

3.5 Scalability challenges for counterfeit sellers

In the counterfeiters' world, evasion of detection and scalability are closely coupled. As legitimate online marketplaces have processes in place to remove sellers of counterfeit goods, these sellers cannot simply have their digital "store" on the marketplace showcasing all the available ranges of counterfeit goods on offer. At the same time, as mentioned earlier, many sellers use decoy products to evade detection by e-commerce platforms. In addition, the hidden-links channels are not user- or customer-friendly, since prospective buyers must endlessly scroll vertically through the posts in the group to find a product of interest and the associated hidden link. With a view to creating a more user-friendly mechanism for hidden links and boosting their sales, sellers of counterfeit products try to solve this problem by using digital "photo album" platforms. Although these types of sites are also used for legitimate purposes, since they are merely catalogues and not stores (i.e. one cannot purchase items directly from these sites), sellers use them to upload pictures and showcase their products, often including replicas or counterfeit goods. When buyers find an item of interest on these platforms, they need to contact the seller via a P2P messaging application or email, and they will receive the hidden link to the marketplace site with the necessary instructions for the purchase. It should be noted that when digital albums are used, they introduce an additional layer between the marketing realm (e.g. social media and P2P messaging platforms) and the online marketplace.

As can be seen in the example below, the hidden links with purchase instructions are left in the comments, with no need to use the P2P platforms.

Figure 3: Hidden link with purchase instructions left in the comments.

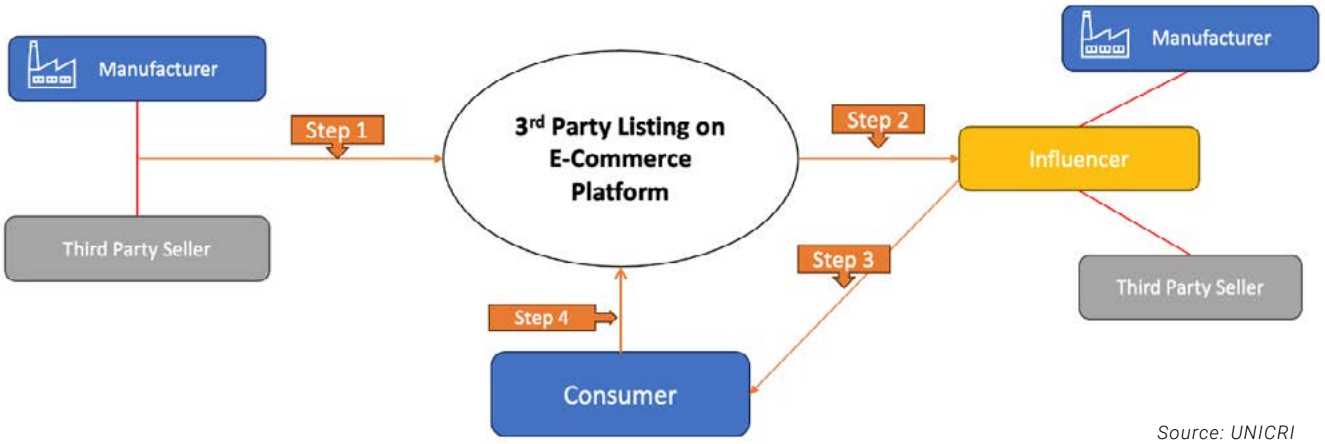


Source: e-commerce platform

3.6 The critical role of influencers

Influencers have become the critical nexus in modern counterfeit distribution networks, acting as the bridge between manufacturers and consumers while exploiting the trust and reach of social media. The diagram below illustrates this dynamic, showing how the workflow unfolds in four distinct steps, with influencers positioned at the core.

Figure 4: Workflow illustrating the central role of influencers in the hidden links ecosystem.



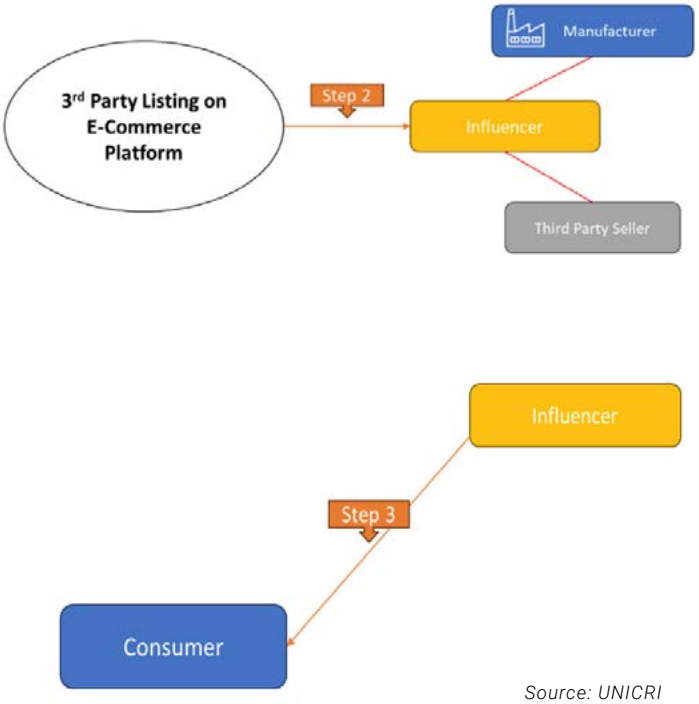
Source: UNICRI

Step 1: Product listing creation

The story begins when manufacturers work with third-party sellers to create listings on e-commerce platforms. These listings employ the obfuscation techniques described earlier — blurred images, missing brand names, or decoy products — to evade platform detection systems and are reachable by purchasers through hidden links.

Step 2: Influencer recruitment

The manufacturer and/or third-party seller then provides these hidden links directly to influencers. This represents a crucial handoff, as influencers become the discreet distributors of these concealed product pathways. The relationship may involve commission-based agreements, flat fees, or product exchanges, creating a financial incentive for influencers to promote counterfeit goods.



Source: UNICRI

Step 3: Audience amplification

Here's where influencers demonstrate their unique value to the counterfeit ecosystem: they leverage their established credibility and follower base to drive consumer to-

ward the hidden links. Unlike anonymous Telegram channels or obscure Facebook groups, influencers bring legitimacy, personality, and targeted reach. They frame counterfeits as "affordable alternatives", "budget finds", or "dupes", thereby normalizing the purchase of replica goods while maintaining plausible deniability about the products' authenticity.

This process was allegedly used by counterfeiters in the case *Amazon v. Fitzpatrick*, discussed more fully below, where influencers monetized their accounts by promoting counterfeit goods under the guise of "dupes." **Social media** also played a critical role here. Influencers used closed groups on social media platforms to alert followers of the hidden links and to coach them on how to navigate them.

Step 4: Consumer purchase

Consumers, influenced by the trusted voice of their favorite content creator, click the hidden link, land on the e-commerce platform and knowingly complete their purchases of counterfeit goods. The influencer has successfully converted their social capital into counterfeit sales.

Once hidden links gain traction and visibility, their existence becomes publicly known, allowing e-commerce platforms to eventually detect and remove them — but by then, a significant number of counterfeit sales have already occurred.

Source: UNICRI

The tables below summarise the hidden links ecosystem in relation to the sale of counterfeit goods, including those stakeholders (such as e-commerce platforms, transaction platforms, social media groups, and digital photo albums) that are exploited by counterfeiters.

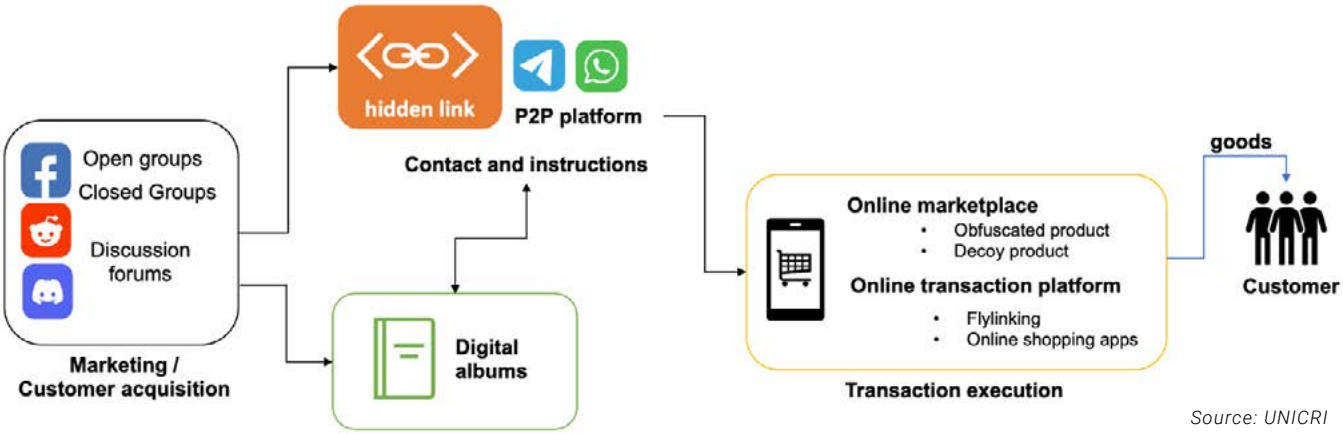
Key actors
Primary actors
Buyers: Generally aware they are purchasing replicas at low prices rather than genuine products. They actively seek out access to sellers through social media groups, digital catalogues, or direct contact channels.[7]
Third-party sellers: Employ sophisticated obfuscation tactics, including blurred product images, missing brand names in descriptions, and coded communication. They diversify operations across multiple platforms and maintain backup channels to ensure continuity.
Influencers: They play a crucial role in driving traffic and legitimizing counterfeit operations by promoting hidden links to their followers, often under the guise of "budget-friendly alternatives" or "dupes". Their endorsement lends credibility to sellers and significantly expands market reach, particularly when they have established trust with their audience. Some influencers may operate knowingly as part of the counterfeit network, while others may be unaware of the full extent of the illegal activity they are facilitating.

7 In most countries, purchasing counterfeit goods (even knowingly purchasing such goods) for personal use does not violate civil or criminal trademark law. Conversely, purchasing counterfeit goods with the intention of further distributing or trafficking them constitutes a violation of civil and criminal trademark laws in most jurisdictions.

E-commerce platforms/online marketplaces: E-commerce platforms that host actual product listings and facilitate payments. These can be exploited through hidden links pointing to obfuscated or decoy product listings.
Transaction platforms: Platforms used to facilitate and secure the payment process. Unlike the online marketplace, which allows both product browsing and payment execution, transaction platforms streamline only the online payment. In this case, the buyer, through the hidden link, is directed straight to the checkout. In essence, these platforms act as a **payment and logistics hub** for sellers who operate on social media, making the transaction process more convenient and secure for both parties. This enables sellers to convert a social media post into a direct point of sale without the need for a full-fledged e-commerce website.
Supporting infrastructure
Social media groups: The social media groups serve as primary advertising hubs. Closed groups offered by social media platforms provide basic access control and confidentiality while remaining relatively easy to join.
Digital photo album platforms: Services functioning as digital product catalogues scalability challenges by allowing sellers to showcase inventory without direct sales capability. Buyers contact sellers via P2P apps or email after viewing catalog items to receive hidden links.

Core ecosystem components
Hidden links
Hidden links serve as the central mechanism connecting marketing efforts to actual purchases. They exist primarily on peer-to-peer (P2P) platforms and may point to either actual products (with obfuscated information) or decoy products that completely decouple the delivered item from the marketplace record.
Obfuscation techniques
Product image manipulation: Images are blurred, especially for products with unique or brand-identifiable patterns. AI-based detection advances are making these techniques less effective.
Description sanitization: Brand names are omitted from product descriptions to prevent brand enforcement and infringement detection software from identifying counterfeits.
Communication coding: Sellers replace letters with numbers (e.g. 0rder) or special characters (e.g. l!nk) to evade automated detection systems. Buyers are trained to avoid mentioning brand names in communications. These can serve as indicators of customer complicity. As with product image manipulation, communication coding has become a less effective obfuscation technique as it can be used to train AI-based detection tools to recognise such coded patterns of communication.
Resilience and risk diversification
Sellers commonly use multiple hidden links pointing to different platforms, serving dual purposes: providing backup if one link or vendor account is taken down, and increasing competitiveness through features like “No Tax” offerings that signal off-the-books transactions.

Figure 5: Hidden links simplified ecosystem.



Source: UNICRI

4. HOW TO COMBAT THE USE OF HIDDEN LINKS IN E-COMMERCE TO TRAFFIC IN COUNTERFEIT GOODS

Hidden links are particularly difficult to investigate. In theory, an investigator for a trademark owner or e-commerce platform could conduct test purchases of every listing for a generic product in an online marketplace to establish whether a third-party seller is truly offering the product depicted in the listing and not a counterfeit good. In reality, this is both cost-prohibitive and incredibly inefficient. For this reason, this report proposes two different solutions – one technological and one cooperative – to more effectively combat the hidden links challenge.

4.1 How technology can be used to combat hidden links

The Open Source Intelligence (OSINT) cheat sheet provided in the figure below represents one possible configuration for outlining the modus operandi of counterfeiters while providing context for understanding the counterfeit ecosystem and detailing manual investigation approaches. However, the scale of the problem is substantial — with a significant number of counterfeit sellers employing sophisticated evasion techniques and quickly pivoting to different channels when detected — making manual investigation alone insufficient. To effectively combat this challenge, it is strongly recommended to leverage AI-enabled tools to streamline and automate searches and investigations.

Figure 6: Cheat sheet - counterfeiters' modus operandi and investigation approaches.

Source: UNICRI

Importantly, cheat sheets and investigation guides like this one can now serve as a knowledge base for AI systems through approaches such as Retrieval-Augmented Generation (RAG). RAG is an AI architecture that combines large language models with the ability to retrieve and reference specific documents from a curated knowledge base. In practical terms, this means an AI system can be supplied with multiple investigation guides, platform-specific techniques, legal frameworks, and historical case studies, and then dynamically access this information when conducting investigations. For example, when the AI encounters a new counterfeit seller using unfamiliar terminology, it can instantly retrieve relevant sections from the cheat sheet explaining that terminology and the appropriate investigation techniques, ensuring the consistent application of best practices across thousands of simultaneous investigations.

Brand owners have already successfully implemented image recognition technology to detect unauthorized use of their logos and trademarks across platforms. Today's advanced AI capabilities extend far beyond image analysis. Agentic AI systems — autonomous AI agents capable of planning, executing, and adapting their actions to achieve specific goals — can automate complex search patterns across multiple platforms simultaneously, map network connections to identify hidden associations between different sellers and channels, continuously monitor for new counterfeit operations using evolving tactics, and even initiate test purchases without completion to gather evidence while maintaining legal compliance. Machine learning algorithms can identify subtle patterns in seller behaviour, such as account creation patterns, linguistic markers, pricing strategies, and supply chain indicators that would be virtually impossible for human investigators to detect at scale.

These AI-driven approaches, particularly when grounded in expert knowledge through RAG systems, allow investigators to scale their efforts exponentially, identify patterns invisible to manual review, respond to the dynamic nature of counterfeit networks in real-time, and maintain institutional knowledge even as the investigation teams change. The combination of human expertise codified in resources like this cheat sheet and AI's ability to process and act on that knowledge at scale represents a significant enhancement to brand protection programs, enabling organizations to match the scale and adaptability of modern counterfeit operations.

4.2 How cooperation with e-commerce platforms can combat the use of hidden links

Until such autonomous AI agents are perfected, other solutions must be considered. Accordingly, this report proposes attacking the hidden links problem by targeting the closed groups on social media platforms and encouraging greater cooperation between social media platforms and those seeking to combat hidden links – such as e-commerce platforms, brand owners, and law enforcement authorities.

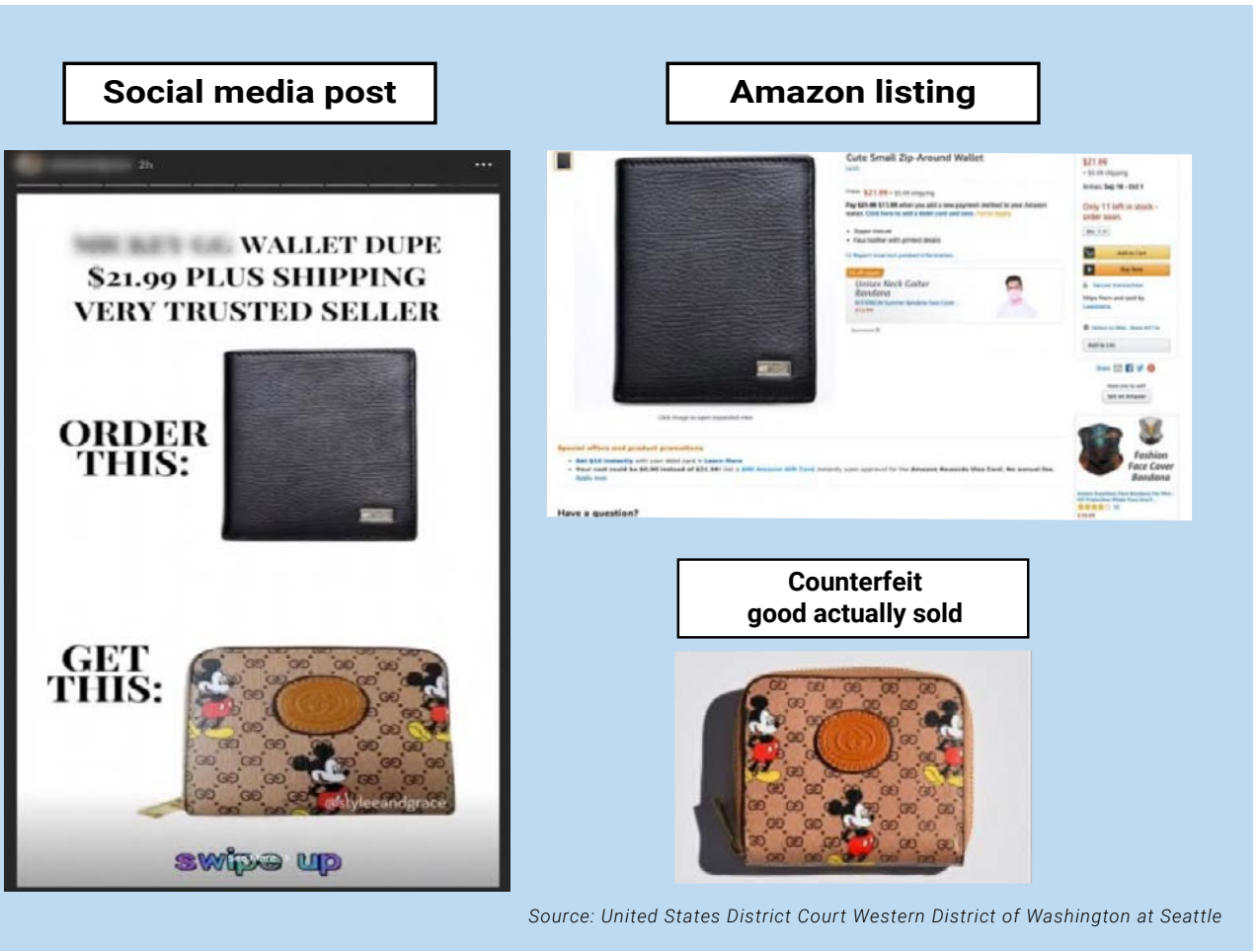
An examination of a civil case involving hidden links is useful at this stage to illustrate the key role that social media platforms play in promoting hidden links used to traffic counterfeit goods. In 2020, Amazon filed a civil case against defendants who allegedly employed hidden links to sell counterfeit goods, and against influencers who allegedly used social media to promote these hidden links.[8] As the manufacturers and sellers of the counterfeit goods in that case were

8 Amazon.com, Inc. v. Fitzpatrick, et al., Case No. 20-cv-01662, (W.D. Wash. Nov. 12, 2020);

unlikely to fall within the jurisdiction of the court, the complaint centered on "a pair of individuals, Defendants Kelly Fitzpartick and Sabrina Kelly-Krejci, who engage in social influencer activities on various websites and apps for the admitted purpose of promoting, advertising, and facilitating the sale of counterfeit luxury fashion goods by the Seller Defendants."[9] The complaint alleges that these influencers used their social media accounts to "publish videos, photographs, and detailed descriptions" of "obviously counterfeit goods that blatantly copy the registered trademarks of luxury brands."[10]

Although the Amazon listings that the influencers allegedly indentified "display only a generic, seemingly non-infringing product; the counterfeit nature of the product is revealed only to those who order and receive the product."[11] On Defendant Fitzpatrick's Instagram page, she allegedly described a "hidden link" as when "[y]ou order a certain product that looks nothing like the designer dupe in order to hide the item from getting taken down [by Amazon] and orders bring cancelled."[12] Amazon further alleged that she also provided the following image:

Figure 7: Images allegedly provided by the defendant on Instagram.



Source: United States District Court Western District of Washington at Seattle

9 Id. at 2.

10 Id. at 2.

11 Id.

12 Id. at 3.

Amazon alleged in its complaint that the influencers' goal was to falsely advertise a placeholder item on Amazon's online marketplace that was "designed to evade Amazon's counterfeit detection systems. Once the orders are placed, the Seller Defendants and other bad actors then ship counterfeit products to customers."[13] According to the complaint, "[O]nly Fitzpartrick's followers knew that the products for sale were counterfeits based upon Fitzpartick's explicit instruction and links" in her social media accounts.[14] In other words, Amazon alleged that was a classic scenario whereby manufacturers and third-party sellers work together to use hidden links to traffic in counterfeit goods, and where influencers promote these hidden links to their followers.

Notably, Amazon does not allege that it discovered this hidden-links activity while it was in its non-public phase. Instead, Amazon was only able to detect this activity after the influencers' activity became public and Defendants "Fitzpatrick and Kelly-Krejci ma[d]e no efforts to conceal their true motive."[15] The influencers in this case allegedly used other social media platforms to promote counterfeit products, including TikTok, Facebook, and Twitter.[16]

Even though Amazon could identify the social media accounts that the influencers were using to openly promote hidden links on Amazon's online marketplace, Amazon alleged that its efforts to take down the influencers' accounts were frustrated by the fact that the lax enforcement by the social media platforms allowed the influencers to create new accounts with ease. "When Instagram and other websites and apps have removed their social media accounts, Fitzpatrick and Kelly-Krejci have simply created new accounts to continue their illegal activities."[17]

For example, Amazon alleged that after Instagram removed Fitzpatrick's account for the first time at Amazon's request, Fitzpatrick successfully created a new Instagram account just 4 days later.[18] When Instagram again took down Fitzpartick's account, Amazon alleged that another replacement account appeared just one day later.[19] Through these Instagram accounts, Fitzpatrick allegedly was able to promote the following hidden links on Amazon's online marketplace, and Amazon was able to confirm the counterfeiting conduct through test purchases.

13 Id. at 3-4.

14 Id. at 14.

15 Id. at 4.

16 Id. at 13.

17 Id.

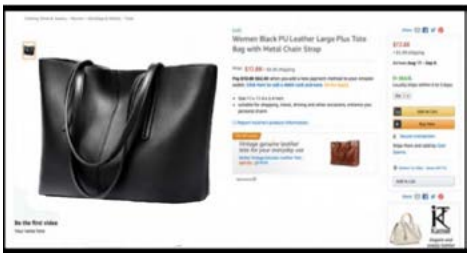
18 Id. at 15.

19 Id.

Figure 8: Images showing hidden links allegedly promoted by the defendant.

Social media post

Amazon listing



Counterfeit good actually sold

Source: United States District Court Western District of Washington at Seattle

Social media post

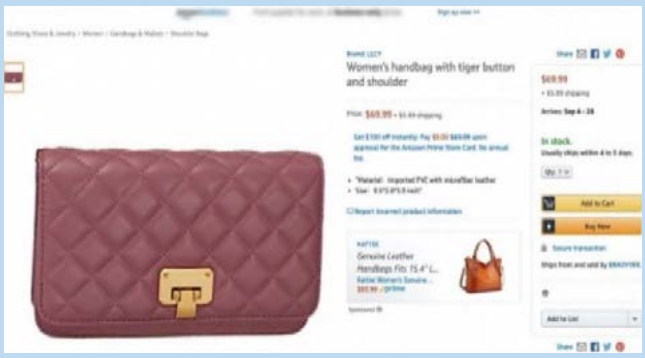
Amazon listing

Counterfeit good actually sold

Source: United States District Court Western District of Washington at Seattle

Social media post

Amazon listing



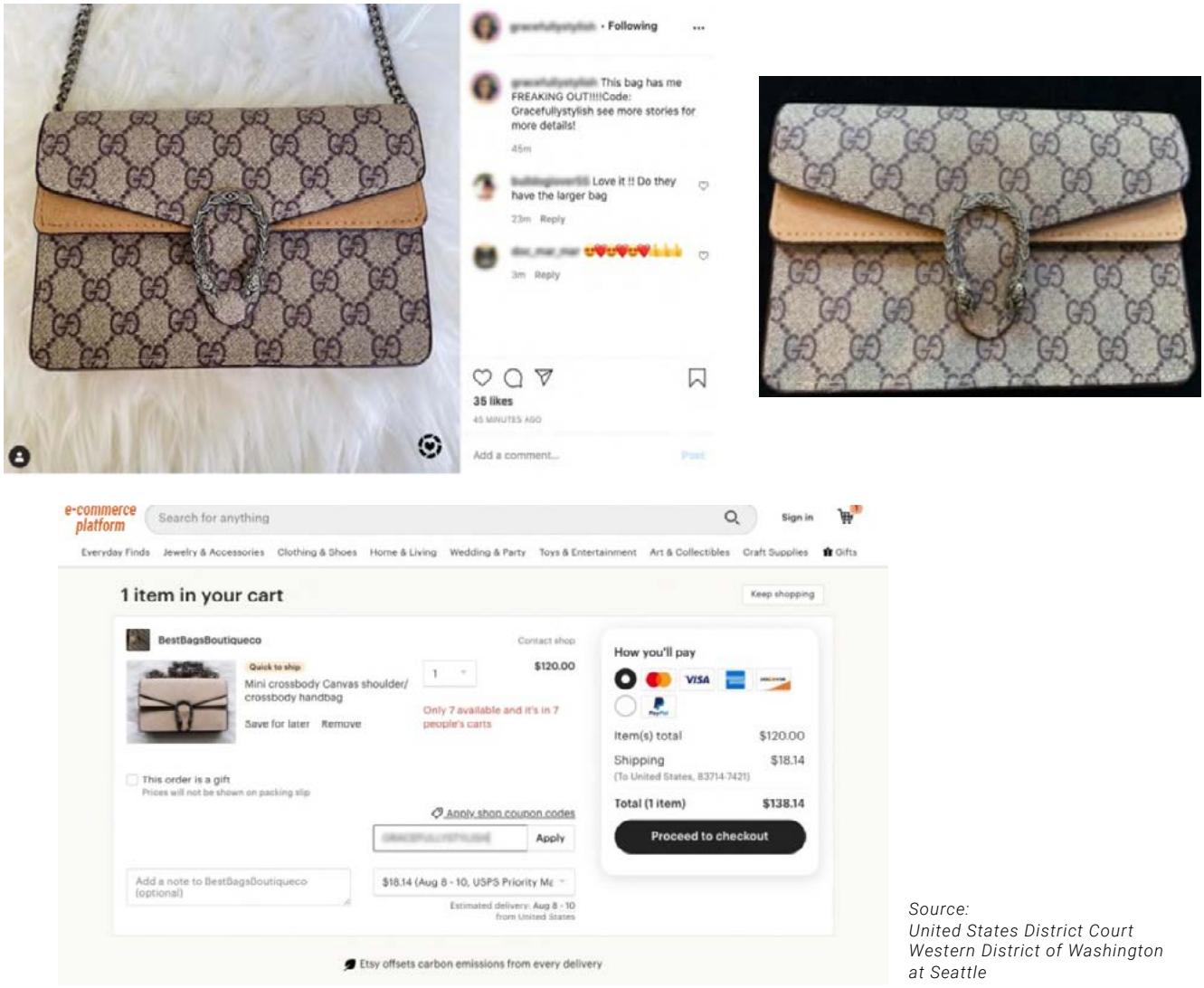
Counterfeit good actually sold

Source: United States District Court Western District of Washingt on at Seattle

And when Amazon shut down the Seller Defendants' listings containing the hidden links, they allegedly redirected their followers to other e-commerce websites where the same sellers allegedly could be.[20] For example, Amazon alleged that its investigators identified the following Instagram posts relying on hidden links on Etsy to enable the purchase of counterfeit goods:

20 Id. at 40-42.

Figure 9: Hidden links on Etsy allegedly promoted by the defendant on Instagram.



Source:
United States District Court Western District of Washington at Seattle

Although the Amazon complaint illustrates the hidden-links ecosystem and the vital role that social media and influencers play within it, it also underscores the difficulty in making a case against the easiest targets in that ecosystem: the influencers. In this regard, it is worth noting that the case did not lead to a judgment, since an out of Court settlement was agreed upon by the parties. This is notwithstanding the fact that most countries' civil trademark laws prohibit the manufacture and sale of counterfeit goods and, in addition, provide that those who knowingly contribute to, or knowingly profit from, the trafficking in counterfeit goods are also civilly liable in many jurisdictions under a secondary liability theory, such as contributory or vicarious trademark counterfeiting. Contributory liability generally occurs when a party has the right and ability to supervise, direct, or control the wrongful conduct at issue and has nonetheless knowingly allowed such conduct to continue, whereas vicarious liability generally rests on the theory that a party knowingly derives a direct financial benefit from the wrongful conduct.

Unlike the trafficking in counterfeit goods, buying counterfeit goods, even knowingly, is generally legal. This creates a dilemma when relying on a civil secondary liability theory against influencers in the hidden-links ecosystem. Although influencers undoubtedly have the ability to "influence" the purchase of counterfeit goods, they rarely, if ever, have the ability to control the manufacture or sale of counterfeit goods. This highlights the structural limitations of civil

enforcement efforts directed at influencers.

To resolve this problem in its secondary-liability theories, Amazon alleged that the influencers did, in fact, have "the right and ability to supervise, direct and control the wrongful conduct alleged in the Complaint, and derived a direct financial benefit from that wrongful conduct."[21] Amazon more specifically alleged that "Fitzpatrick was paid directly by Seller Defendants for her promotions"[22] and that she was in contact with the sellers on Amazon.[23] Amazon even alleged that Fitzpatrick "gloats about how she personally sources the supply of counterfeit products sold through deceptive tactics on Amazon" in her Instagram account.[24] In this way, Amazon's allegations, if proven, may have been sufficient to establish that the influencer defendants in their case were liable for either contributory or vicarious trademark liability. Ultimately, Amazon settled its case against the influencers in 2021, so we will never know if Amazon would have been able to overcome the difficulty in pursuing its secondary-liability theories against the influencers in their case.[25]

Unlike civil enforcement, criminal enforcement has well-established legal theories to account for the conduct of influencers. Specifically, most countries authorize prosecutors to pursue conspiracy or aiding and abetting theories against properly charged defendants. These forms of criminal liability cover a broader scope of conduct than do civil forms of secondary liability like contributory and vicarious liability. In addition, criminal enforcement has a greater deterrence effect than civil cases, and most countries are required to implement criminal laws prohibiting wilful trademark counterfeiting on a commercial scale.[26]

Public criminal investigative authorities and prosecutors should find hidden-links cases particularly compelling to pursue. The evidence that actors across the hidden-links ecosystem (manufacturers, third-party sellers, influencers, and even consumers) are acting wilfully makes these cases more attractive for criminal prosecution than the typical online trademark-counterfeiting matter. Furthermore, the tools available to public investigative authorities to investigate and infiltrate closed groups on social media accounts are generally more robust than those available to private parties in civil cases. Some jurisdictions may place stricter limits on the investigative options available to private parties than on those available to law enforcement, particularly with respect to "undercover" purchases, surveillance, and similar activities.

At least one e-commerce platform has successfully made a criminal referral of a hidden-links case. In the summer of 2024, e-commerce platform Alibaba successfully referred a hidden-links case to the Chinese Public Security Bureau (PSB).[27] The PSB's investigation led to an August 2024 raid in which authorities arrested 10 suspects and seized over 50,000 infringing items

21 E.g., id. at 5-6.

22 Id. at 14.

23 Id. at 14-15.

24 Id. at 16.

25 "Amazon Settles with Influencers Who Allegedly Peddled Counterfeits on Instagram and TikTok."

26 Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS Agreement"), Article 61 (1994) ("Members shall provide for criminal procedures and penalties to be applied at least in cases of willful trademark counterfeiting [...] on a commercial scale.").

27 Comment from Alibaba International Digital Commerce Group, Posted by the Office of United States Trade Representative on Oct 3, 2024.

targeting over 15 brands, most of them well-known luxury and sports labels.[28] To date, it appears that this criminal investigation is ongoing.

As the Amazon civil case in particular demonstrates, social media companies that effectively deprive counterfeiters of the closed forums and accounts that are needed to communicate the existence of hidden links would make it almost impossible for counterfeiters to scale up the sale of counterfeit goods. Limiting counterfeiters' ability to increase sales through hidden links means limiting the profitability of selling counterfeit goods through the use of hidden links.

Although social media platforms may be reluctant to monitor closed groups – whether out of concern for violating free-speech standards or for risking a loss of subscribers and related loss of revenue – these concerns cannot supersede the fact that the players in the hidden-links ecosystem are using closed groups to facilitate illegal activity. Most social media platforms have terms of service authorizing them to monitor and remove the content of chats for illegal activity – which is how some social media platforms monitor closed groups to determine if they are engaged in illegal activity such as the trafficking in child-exploitative materials. Extending such policies to more closely monitor, investigate, and shut down closed groups involved in the trafficking of counterfeit goods would not require a substantial policy shift for social media platforms.

Another area where social media platforms could improve their enforcement is by strengthening their "know your customer" ("KYC") standards to prevent influencers whose accounts have been removed from simply opening new accounts on the same platform. In the Amazon case, for example, if Instagram had implemented more rigorous KYC standards, it would not have allowed the influencer Defendant Fitzgerald to create additional Instagram accounts after her previous account had been taken down. In part because of legislation such as the European Union's Digital Services Act and the United States' more modest INFORM Consumers Act, e-commerce platforms have greatly improved their own KYC standards. Social media platforms must now take similar steps.

28 Id.

5. CONCLUSIONS

Hidden links represent a sophisticated response by counterfeiters to the increasing effectiveness of traditional detection and enforcement mechanisms on e-commerce platforms. By decoupling what is listed from what is actually delivered, and by routing promotion through influencers, closed social-media groups, digital catalogues, and specialised transaction platforms, counterfeiters exploit the legitimacy, reach, and convenience of mainstream online ecosystems while remaining largely invisible to conventional controls.

To address these challenges, two broad lines of action are essential. First, sustained investment in AI-enabled investigative tools such as Retrieval-Augmented Generation (RAG) and agentic AI can enable investigators to better identify hidden links, map criminal networks, and adapt to evolving tactics in near real time. Second, deeper cooperation between platforms, brand owners, social media platforms, and law-enforcement authorities is required to ensure that intelligence is shared, enforcement actions are coordinated, and recidivist actors are prevented from simply re-emerging under new identities.

Ultimately, limiting the profitability and scalability of hidden-link operations will not eliminate counterfeiting, but it can significantly raise the costs and risks for those who engage in it. By combining technological innovation, stronger platform governance, targeted criminal enforcement and sustained collaboration, stakeholders can meaningfully reduce the space in which hidden links operate and better protect consumers, legitimate businesses, and the integrity of the digital marketplace.

unicri

United Nations
Interregional Crime and Justice
Research Institute