TRANSNATIONAL ALLIANCE
TO COMBAT ILLICIT TRADE
TRACIT.ORG

The Landscape of Lawlessness Online

Illicit trade through online marketplaces and social media

TRACIT.ORG

ABOUT TRACIT

The Transnational Alliance to Combat Illicit Trade (TRACIT) is an independent, private sector initiative to drive change to mitigate the economic and social damages of illicit trade by strengthening government enforcement mechanisms and mobilizing businesses across industry sectors most impacted by illicit trade. For more information, visit www.TRACIT.org

MEDIA

All media enquiries should be directed to media.inquiries@TRACIT.org

SOCIAL MEDIA

LinkedIn: www.linkedin.com/company/tracitorg
X: @TRACIT_org

ACKNOWLEDGEMENT

Under the supervision of TRACIT's Director-General Jeffrey Hardy, this publication was drafted by principal author Suriya Padmanaahban, TRACIT's Director of Programs, with support from TRACIT Deputy Director-General Stefano Betti and TRACIT Research Associate Ryan Rothermel. Thanks also to Camilla Bosanquet of George Mason University, for her insights and contributions. TRACIT expresses its gratitude to its member companies for their support, resources, valuable feedback and contributions of information, case studies and viewpoints.

THE LANDSCAPE OF LAWLESSNESS ONLINE

ILLICIT TRADE THROUGH ONLINE MARKETPLACES AND SOCIAL MEDIA

TABLE OF CONTENTS

I. Executive summary 3

Objectives 4

Findings 4

Assessment 5

TRACIT recommendations 6

II. Introduction 9

Evolution of illicit activities in the digital age 9

Voluntary platform responses and their limits 9

Regulatory frameworks have not kept pace 10

Beyond IP crime: a widening scope of illegal activity grows online 11

Objectives 12

III. Unauthorized sale of regulated products 14

Examples by sector 15

Alcohol 15

Pesticides 17

Pharmaceuticals 20

Tobacco products 23

Wildlife products 24

IV. Enabling sales of stolen goods 26

V. Circumvention of consumer health and safety regulations 30

VI. Violation of product safety laws and regulations 33

OECD's October 2021 Product Safety Sweep 34

VII. Examining platform compliance 37

Assessment 38

Have platforms established clear rules for sellers, and explained how these rules are enforced? 38

Do platforms enforce their own policies governing illicit trade-related activity? 41

Do platforms maintain meaningful measures that deter violations? 47

VIII. Conclusions and Recommendations 52

Conclusions 52

Recommendations 54

Establish a regime for platform liability 56

IX. References 60

I. Executive Summary

Although online platforms have positively transformed global commerce, they have evolved at an unprecedented speed and scale, outpacing the security controls necessary to ensure their resilience to a widening landscape of illegal commercial activity.

E-commerce marketplaces, social media platforms, and encrypted messaging apps are widely exploited by criminal actors who take advantage of structural weaknesses and limited oversight to advertise, sell and distribute illicit products directly to consumers – at a scale that could never be achieved through traditional physical sales outlets.

What began primarily as a problem associated with the online sale of counterfeits and other intellectual property (IP) infringing goods has evolved into a much more significant problem. Today, counterfeiting is just the tip of the iceberg, and criminal activities have deepened to include the unauthorized sale of regulated products, the laundering of stolen goods, the circumvention of consumer health and safety laws, and the sale of products that violate product safety regulations. For example, prescription medicines are sold without verification of prescriptions or pharmacy licenses; pesticides are listed without registration or authorization checks; tobacco and alcohol products are sold without meaningful age verification; stolen goods are laundered through online marketplaces; and risky, unsafe or non-compliant products of all types are available at the doorstep of consumers worldwide.

These illegal activities undermine established regulations that governments around the world have pioneered to protect consumers, workers, and the environment. To catch up, governments must urgently modernize regulatory frameworks and aggressively apply these controls to meaningful governance of the online world.

Strengthening regulatory controls starts with assessing the measures platforms already have in place to prevent illegal transactions that expose customers to risk. In other words, where the private sector can effectively protect its infrastructure obviates the need for government controls.

A review of the major platforms shows that substantial technical and operational capabilities to police illicit transactions exist and can be proactively deployed regardless of regulatory mandates to do so. For example, a few platforms have invested heavily in efforts to protect their infrastructures from abuse and have endeavored to develop increasingly sophisticated tools and compliance programs, including comparatively detailed seller policies, proactive detection systems, onboarding procedures, and monitoring and enforcement capabilities.

Moreover, in some cases, industry-led initiatives and cross-sector collaborations have helped to close gaps and demonstrate that progress is possible.

Nonetheless, these measures are extremely limited or are not consistently or systematically applied across the broad spectrum of illicit trade activities taking place online. This suggests that governments have a role to implement clear regulatory controls that ensure platforms sufficiently and consistently prohibit illegal activity.

Objectives

The objectives of this report are to:

i. **Reveal that illicit trade-related activities taking place through online platforms** are widespread and extend well beyond IP infringements.

ii. **Inform that a critical set of controls exists and can be applied by platforms**, which would significantly mitigate the occurrence of illegal and otherwise illicit activities.

iii. **Call on governments to immediately adopt and implement effective regulations** to ensure that online platforms carry out the necessary controls on third-party sellers and their product listings, as well as to impose a regime of liability for platforms that do not conform to such measures.

Findings

This report finds that IP infringements are only the tip of the iceberg, and that illicit activity taking place on online platforms has expanded far beyond what online shoppers are aware of. The report identifies four major categories of illicit activity now taking place extensively through online platforms:

- **Unauthorized sale of regulated products**: Prescription medicines, pesticides, alcohol, tobacco, wildlife products, and other highly regulated goods are routinely sold online without adequate verification of licenses, registrations, prescriptions, age requirements, or other statutory conditions.
- **Fencing stolen goods**: Organized retail crime groups increasingly rely on online marketplaces and social media platforms to launder stolen merchandise, taking advantage of weak seller verification and limited traceability.
- **Circumvention of consumer health laws, regulations, and standards**: Illicit sellers exploit online platforms to market products that evade regulatory controls designed to protect consumers, including falsified medicines, contaminated cosmetics, unsafe supplements, and products containing hazardous substances.

- **Circumvention of product safety laws, regulations, and standards**: Unsafe, banned, recalled, or non-compliant products remain widely available online despite extensive national and international product safety frameworks.

Assessment

Guidance on where government regulatory interventions are needed can be found in how effectively – or ineffectively – a selected number of platforms govern illegal activity on their services. This assessment derives from three salient questions:

1. Have platforms established clear rules for sellers, and explained how such rules are enforced?

Clear, accessible, and operational seller policies are a critical first step in preventing illicit trade online. In a well-governed marketplace, platform policies should clearly define prohibited and regulated goods, specify seller obligations and documentation requirements, explain how compliance is verified, and outline the consequences for violations.

This report finds significant shortcomings and variations across platforms, where only some have established detailed governance models (e.g., category-specific rules, seller-verification requirements, licensing obligations, or enforcement procedures).

While the efforts of leading platforms demonstrate that strong controls are possible, these standards are not applied consistently across the broad online platform ecosystem. Many platforms continue to provide only generic or minimal policy language for highly regulated or high-risk product categories. In most cases, policy clarity declines sharply outside the anti-counterfeiting context. While policies addressing counterfeit goods often specify documentation requirements, takedown procedures, and repeat-offender consequences, policies relating to pharmaceuticals, pesticides, tobacco, alcohol, wildlife products, stolen goods, or unsafe consumer products are frequently limited in scope, fragmented, or difficult to locate.

2. Do platforms enforce their own policies governing illicit trade related activity?

To evaluate the extent to which online platforms comply with their own self-prescribed rules and policies aimed at addressing illicit trade-related conduct, this report examines how platforms: (i) prevent abuse by sellers and ii) proactively and continuously screen and monitor product listings. The report finds a substantial gap between published platform policies and practice. The report identifies seller onboarding and pre-listing verification as critical

weaknesses. Unfortunately, many platforms permit sellers to operate with minimal identity verification, limited business authentication, and insufficient validation of licenses or regulatory authorizations.

Similarly, despite the availability of advanced technologies and their application to detect counterfeits, equivalent screening tools are not consistently applied to other illicit product categories. As a result, regulated products, stolen goods, unsafe goods, falsified medicines, wildlife products, and prohibited pesticides continue to circulate online with limited scrutiny.

The report also highlights growing challenges in social media environments, including disappearing content formats, closed groups, and migration of transactions off-platform.

3. Do platforms maintain meaningful measures that deter violations?

The report examines whether platforms are willing to impose effective consequences on non-compliant sellers. The clearest indicator of effective deterrence is the imposition of measures that prevent offenders from returning to their platform. Without measures that impose significant cost or permanently block repeat offenders, the rules governing sellers carry little weight, and enforcement remains largely cosmetic.

Across all the illicit trade typologies reviewed, this report finds the enforcement of deterrent measures to be consistently weak. In practice, the most widely used penalty is notice-and-takedown, a system originally introduced to remove listings of counterfeit goods. While this remains a necessary enforcement tool, its effectiveness is limited when used in isolation. The process can be slow and cumbersome, particularly where illegal listings reappear quickly or are replicated across multiple accounts and platforms. Beyond notice-and-takedown, permanent bans are rare and inconsistently applied, while stay-down measures are used mostly for IPR cases and patchily implemented.

TRACIT recommendations

The role of governments

While nearly all platforms outwardly prohibit illicit trade and illegal commercial activity, application and enforcement remain limited and uneven. This state of play is unacceptable and creates opportunities for criminal actors to exploit platform weaknesses and circumvent regulatory controls.

Consequently, voluntary measures by platforms have not delivered sufficiently consistent outcomes across the full range of illicit trade risks now present online. Governments therefore have an important role to play in establishing clearer

statutory expectations, ensuring consistent enforcement, and strengthening accountability frameworks for online commerce.

Several jurisdictions—including Vietnam, the European Union, the United States, India, and China—have already begun introducing stronger due diligence, seller verification, transparency, and enforcement obligations for online platforms. These developments demonstrate that stronger and more enforceable standards are achievable, although approaches remain fragmented and are often focused on narrow categories of risk rather than the broader spectrum of illicit trade occurring online.

The OECD's Draft Voluntary Guidelines for Countering Illicit Trade in Counterfeit Goods on Online Marketplaces could help establish baseline standards to support governments in strengthening oversight of online platforms and developing clearer accountability.

Summary of TRACIT recommendations

The following is a summary of the recommendations addressed to governments based on this report's findings and assessment. The full text of the recommendations is found in Chapter 8.

1. **Establish online–offline regulatory parity.** Governments should ensure that licensing, inspection, labeling, age-verification, and product-safety obligations that apply offline are equally applied to online commercial activity.
2. **Require stronger platform enforcement controls.** Platforms should be mandated to implement tighter seller vetting, pre-listing verification, compliance checks for regulated products, proactive monitoring and takedown systems, and effective stay-down mechanisms to prevent repeat offending.
3. **Strengthen record-keeping and traceability obligations.** Platforms should be required to retain seller, transaction, and takedown records and ensure that listings can be traced back to responsible sellers.
4. **Mandate transparency, audits, and regulatory cooperation.** Platforms should be mandated to publish transparency reports, maintain designated enforcement contact points, and cooperate with regulators and law-enforcement authorities.
5. **Improve consumer redress mechanisms.** Platforms should be required to provide accessible complaint channels, timely responses, refunds for illegal goods, and rapid removal of unlawful or harmful listings.

Establishing platform liability

While there may be instances where platforms should be immune from the illegal

behavior of their users, this rationale erodes in cases where platforms profit from the transaction in the collection of listing fees, sales commissions, and targeted advertising. This incongruency is even more pronounced when platforms wield full control over listings, logistics, payments, and data through vertically integrated fulfillment networks. The mismatch between platforms' *de facto* control and claimed neutrality calls for the determination of modern rules for subjecting platforms to liability for transactions involving unlawful goods listed and sold on their sites.

The establishment of legal liability regimes for platforms whose services are used by third parties to conduct illicit trade would be consistent with regulatory approaches in other critical sectors where intermediaries owe a duty of care, such as finance, transportation, and healthcare. In establishing platform liability for non-compliance, governments should:

- Establish conditions for excluding illicit goods from safe-harbor protections for e-commerce marketplaces and social media platforms. .
- Establish clear statutory conditions under which platforms may be held accountable for failing to exercise reasonable oversight of commercial activities conducted through their services.

II. Introduction

Evolution of illicit activities in the digital age

The internet has long been vulnerable to exploitation and illicit activity. Its revolutionary connectivity created new pathways for identity theft, credit card fraud, stalking, hacking, and a wearisome litany of other crimes. The emergence of digital copyright infringements of music in the early 1990s extended the scope of illegal activities to the intellectual domain, and marked a transition from personal risk (i.e., identity theft) to wholesale market risk, where corporations and entire commercial sectors became vulnerable to supply chain and security weaknesses online.

The sweeping proliferation of pirated digital music during the 1990s and thereafter—primarily through peer-to-peer (P2P) file-sharing services—enabled users to evade copyright protections and download digital music for free. The subsequent impact on the music industry was massive and unprecedented. Billions in annual revenues were erased. Music sales and licensing plunged by 50 percent and remained there for over a decade.

As internet applications expanded in focus and type, opportunities for misuse multiplied beyond digital piracy, giving rise to new forms of illicit trade, including opportunities for trademark counterfeiters to offer a wide spectrum of counterfeit and illegal products directly to consumers. Whereas early counterfeiting (for example, fake luxury handbags) had primarily been conveyed through street markets, internet-enabled counterfeiters found they could easily manipulate and penetrate online marketplaces to gain access to consumers nationally, regionally and eventually, globally.

More recently, social media platforms are being exploited to direct users to wide ranges of fraudulent content (like websites designed to sell fakes or look-alikes) or to facilitate illegal transactions through their private messaging channels. At the same time, vanishing (ephemeral) content has emerged as a powerful tool for driving users to websites selling fake and fraudulent products – with little risk of detection.

Counterfeiting and piracy are now more prevalent than ever. According to the OECD, the magnitude of counterfeiting continues to grow in both size and scope, where essentially every product category is now vulnerable.[1]

Voluntary platform responses and their limits

The emergence of illegal activity online, in the form of copyright and trademark infringements, has challenged online platforms to introduce controls to protect their business from exploitation and safeguard their customers from fraud.

For the purposes of this paper, the term "online platforms" includes: (i) e-marketplaces (both Business-to-Business ('B2B') and Business-to-Consumer ('B2C')) and (ii) social media websites and/or electronic device applications ('apps'), all of which facilitate third-party product listings and transactions.

For the past 20 years, in fact, most major platforms have had to invest significantly in various controls, such as trust-and-safety systems, seller controls, notice-and-takedown programs, automated detection tools, and partnerships with brand owners and regulators. And to monitor progress, some platforms now publish transparency reports, operate dedicated reporting portals, and maintain specialized teams focused on platform integrity and consumer trust.

These efforts have established important precedents for preserving the integrity of commercial transactions online – pioneering rules of use, developing structural security measures, and punishing abusers. Today, many major platforms maintain significantly stronger policies and operational controls against counterfeit goods than existed a decade ago. This process demonstrates that internet-based governance of commercial activity is evolutionary, and that platforms can implement sophisticated compliance systems at scale when reputational risk, customer risk, and commercial incentives align.

However, these improvements have not been applied consistently across the broader spectrum of illicit trade now occurring online. While platforms increasingly dedicate substantial resources toward addressing counterfeit goods and piracy, far weaker controls often exist for other high-risk categories such as unlicensed pharmaceuticals, banned pesticides, stolen goods, unsafe consumer products, wildlife trafficking, and regulated products sold without proper authorization. In many cases, policies remain vague, enforcement inconsistent, and seller verification minimal.

As a result, voluntary measures alone have not produced a consistent or system-wide standard of accountability across digital commerce. The uneven application of platform controls has created significant enforcement gaps that continue to be exploited by criminal actors.

Regulatory frameworks have not kept pace

Despite the growing scale and diversity of illicit activity online, regulatory frameworks have not evolved at the same pace. While governments have invested heavily in consumer protection, product safety, customs enforcement, and licensing regimes for physical commerce, equivalent obligations and enforcement expectations have not always been clearly or explicitly extended into online commercial environments.

Even where legal frameworks already exist, enforcement often remains fragmented, inconsistent, or insufficiently adapted to the realities of digital commerce. Regulatory agencies frequently struggle to keep pace with the scale and speed of illicit activity occurring across online platforms, allowing illegal listings and repeat offenders to persist online.

Some jurisdictions have begun modernizing their approaches. Measures such as the U.S. INFORM Consumers Act and the EU Digital Services Act introduce stronger due diligence, transparency, and seller-traceability obligations for online platforms. These developments reflect growing recognition that platforms play a crucial role in shaping online commercial activity and therefore carry responsibilities that extend beyond merely hosting third-party content. However, these reforms remain uneven across jurisdictions and are still relatively limited in scope.

At the same time, platforms have continued to rely heavily on safe-harbor protections, arguing that they merely provide technical infrastructure for third-party sellers. Courts have increasingly begun narrowing these protections in cases where platforms actively facilitate unlawful activity. In *L'Oréal SA v. eBay International AG* (2011), the EU Court of Justice held that platforms could lose safe-harbor protections where they actively optimize or promote infringing offers and fail to act after notice. Similar reasoning emerged in *Yi Nian Fashion Trading Co. v. Du & Zhejiang Taobao Network Co. Ltd.* (PRC, 2011) and more recently in *Puma v. IndiaMart* (2025), where courts clarified that platforms carry legal responsibilities to prevent the sale of illegal goods.

While important, these judicial precedents remain narrow and fact-specific and have not yet translated into comprehensive statutory duties governing platform accountability.

Beyond IP crime: a widening scope of illegal activity grows online

The same gaps in platform governance, regulatory enforcement, and seller oversight that initially enabled the growth of online counterfeiting are now facilitating a much broader range of illicit trade activity online. Increasingly, platforms are being exploited for activities that extend well beyond intellectual property infringements and directly implicate consumer protection, public health, product safety, and market integrity frameworks. This report focuses on four broad categories of illicit activity increasingly occurring through online platforms:

- **Unauthorized sale of regulated products.** Highly regulated products—including pharmaceuticals, pesticides, alcohol, tobacco, nicotine products, and

wildlife products—are increasingly sold online in circumvention of licensing, registration, prescription, age-verification, and permitting requirements. Investigations routinely identify sellers offering regulated products without verified authorization or compliance with national laws.

- **Sale of stolen goods.** Organized retail crime groups increasingly use online marketplaces and social media channels to resell stolen merchandise obtained from retailers, cargo theft, freight transport, and distribution networks. Online platforms enable rapid resale at scale while reducing traceability and facilitating repeat offending through multiple seller identities.
- **Circumvention of consumer health and safety regulations.** Illicit sellers increasingly market products outside the regulatory safeguards that legitimate supply chains must follow. This includes non-compliant cosmetics, falsified pharmaceuticals, unregistered supplements, contaminated food products, and products containing hazardous substances sold without adherence to applicable health, labeling, or ingredient standards.
- **Violation of product safety laws and standards.** Unsafe electrical products, toys, chargers, cosmetics, and other consumer goods continue to be widely available online despite existing product safety frameworks. The OECD's Product Safety Sweep found widespread non-compliance across online marketplaces, including the continued availability of banned or recalled goods, inadequate labeling, and products failing to meet mandatory or voluntary safety standards.

In short, consumers face a digital marketplace where unsafe and non-compliant products are no longer isolated incidents, but rather reflect gaps in regulatory clarity, uneven and insufficient platform action, and limited policing by law enforcement.

Objectives

This report is intended to support policymakers in understanding the scale, diversity and evolving nature of illicit activities online, and to identify impactful and effective pathways for strengthening regulatory responses. This report seeks to:

i. **Demonstrate that illicit trade-related activities taking place through online platforms** are widespread and extend well beyond IPR infringements (e.g., counterfeiting and piracy). Most online platforms do not do all they could to prevent (i) the unauthorized sale of regulated products that would normally require a license or permit to sell or buy, (ii) the trafficking of stolen products, (iii) the circumvention of laws to protect consumer health and ensure product safety.

ii. **Establish that a critical set of controls should be applied by platforms**, which would significantly mitigate the occurrence of illicit trade-related activities. These measures include (i) Mandatory seller vetting with compliance verification, (ii) pre-listing verification, (iii) Proactive monitoring and takedown and stay down, not just for IPR, but for all regulatory and country breaches, and (iv) Strong measures, including permanent bans for repeat offenders.

iii. **Call on governments to immediately implement stronger regulations** that deliberately require the systematic application of the above measures by online platforms. Such controls must be underpinned by a regime of legal liability for platforms.

III. Unauthorized sale of regulated products

The unauthorized sale of regulated products[2] now takes place on a wide range of e-commerce platforms worldwide.

Governments typically regulate the manufacture, distribution, and sale of products like pharmaceuticals, alcoholic beverages, cigarettes, and pesticides to protect consumers, markets, or the environment from various product risks. To do so, they usually require licenses, registrations, or permits.

For example, regulatory controls dictate that pharmaceuticals can only be legally sold by licensed entities (such as doctors or pharmacies), and their distribution is typically restricted to individuals with valid prescriptions. When chemicals like pesticides present environmental and health hazards, sellers are required to hold specialized certifications or licenses. Consumers who wish to purchase alcohol or nicotine products must meet legal age requirements. Trade in natural commodities like wildlife, forestry products, and precious gems is heavily regulated to protect ecosystems, ensure sustainability, and prevent environmental damage.

In the online environment, the application of regulatory controls by platforms worldwide has been found to be considerably less stringent, enabling widespread, unauthorized sales of regulated products. This runs in contravention of long-standing and carefully developed legal and regulatory directives by governments to mitigate consumer and market risks.

While platforms have implemented controls to mitigate IP theft, similar levels of due diligence have not consistently been extended to preventing the unauthorized sale of other regulated products.

For example, across most online platforms, core gatekeeping functions are applied unevenly or performed with minimal attention to "know-your-user" due diligence practices that would be useful. Often, platforms do not require sellers of regulated products to authenticate their legal permission to sell (i.e., through proof of license) before posting a listing of, inter alia, pharmaceuticals, pesticides, tobacco, vapes or alcohol. Similarly, platforms are not systematically validating whether buyers meet statutory conditions to acquire regulated products, such as age thresholds for alcohol and tobacco, prescription requirements for medicines, or professional certifications for dangerous chemicals. Where such verification mechanisms exist, they are often based on self-declared information, which may be vulnerable to circumvention.

At the same time, while challenges remain, it is important to recognize that some online platforms have taken steps to strengthen responsible marketing, age-gating, and safety controls. Most major social media platforms, including

Twitter (now X), Facebook, Instagram, and TikTok, already set a minimum age requirement of 13, even before and beyond legal mandates, effectively creating a baseline industry standard. Platforms such as TikTok, Instagram and YouTube also maintain built-in age-gating systems, including age-restricted account creation, view-only modes for under-13 users (such as TikTok's limited experience mode) and parental-consent flows where available. However, in practice, the effectiveness of these measures varies, and in some cases, they may not be sufficiently robust to prevent circumvention. For example, Meta regularly fails to implement effective age-gating on Facebook and Instagram, enabling underage shoppers users to purchase regulated products, view adult-only advertising, and purchase restricted products without meaningful verification by the platforms.

These cases illustrate deeper, systemic weaknesses: platforms have developed technical capacities to screen sellers for IPR violations but do not deploy these tools with the same rigor to mitigate the unauthorized sale of regulated products online. This points to the need for clearer expectations, stronger incentives, and more consistent enforcement mechanisms to ensure that established controls—such as licensing, age verification, and product registration—are applied effectively in digital contexts.

Examples by sector

The following section examines how these challenges manifest in key regulated sectors: alcohol, tobacco, pesticides, pharmaceuticals, and wildlife products. Across these areas, available evidence suggests that required controls, including registrations, prescriptions, or age checks, are not consistently applied in online environments, resulting in instances of unauthorized sales in violation of national regulations.

Alcohol

Most countries strictly regulate the sale of alcohol, such as by requiring sellers to have trade licenses, limiting cross-border shipments, prescribing product labeling parameters, and requiring age verification for buyers. Some countries also have additional controls that would need to be accounted for when transactions are conducted online. For example, in the US, many states impose a regulatory model that limits transactions to a closed chain where producers sell to wholesalers, wholesalers to retailers, and retailers to consumers. Normally, these controls help to ensure the integrity of the supply chain, safeguarding the system from the intrusion of illegitimate supplies, unlicensed suppliers, and unauthorized consumers.

Online, however, legal structures can be more easily circumvented by people who use the internet to bypass physical controls on accessibility, such as restricted points of sale and age checks. Similarly, illicit sellers are able to access broader markets that are not always monitored to the same standard as physical retail.

At present, based on research collected for this study, the abuse of online platforms for illicit alcohol trade online appears more limited in scale compared to other sectors. However, the nature of the risks are similar: regulated products are offered online, often circumventing restrictions normally applied to sellers and buyers, including access by underage consumers and evasion of tax and excise controls.

Efforts by platforms to mitigate these abuses vary. Some established marketplaces have introduced controls aimed at limiting the availability of alcohol listings. For example, eBay limits alcohol listings to pre-approved, licensed sellers, which appears to have reduced the volume of listings; however, these requirements are not enforced to a zero-tolerance standard, and unlicensed sellers still surface. Similarly, Temu has implemented a more structured age-gating framework across its EU and UK platforms, centered on a third-party identity verification system operated by GBG Group Plc. Users attempting to access age-restricted products are redirected to a secure verification interface, where they submit identification documents directly to GBG. The system then returns a binary "pass/fail" token to Temu before access to relevant listings is granted. In the UK, this digital verification layer is further complemented by Royal Mail's adult signature service at the point of delivery. While this represents a more robust and multi-layered approach than is commonly observed across the industry, its effectiveness will ultimately depend on the consistency of enforcement throughout the entire transaction lifecycle.

In other environments, risks appear more pronounced.

- Instagram and Facebook Marketplace are routinely used to advertise and facilitate the sale of alcohol directly to consumers, potentially bypassing licensing, tax obligations, and age verification requirements.
- In Latin American border cities, social media platforms are used to advertise branded spirits and arrange delivery of untaxed stock sourced from lower-tax jurisdictions.
- Emerging evidence also points to challenges on certain fast-growing and relatively less regulated platforms such as Taobao or Pinduoduo.

The legal spirits industry has long been working to address these risks, including through sustained collaboration with digital platforms to strengthen safeguards and promote responsible online practices. Notably,

- The IARD Global Standards Coalition, where major digital platforms work with the alcohol industry to strengthen and align age-screening, responsible marketing rules, and protections for minors.[3]
- The Digital Guiding Principles, a cross-industry framework developed with platforms to establish common standards for responsible online alcohol marketing, including age affirmation, audience targeting, and transparency.[4]

Taken together, these dynamics suggest that while the magnitude of alcohol traded illicitly online is somewhat limited, it nonetheless represents a developing area of concern. Consequently, as with other regulated sectors exposed to illicit sales online, forward-looking legal frameworks must account for these vulnerabilities, and platforms must commit to consistent application and enforcement of their policies to prevent illicit sales of alcohol.

When lawful components facilitate illicit alcohol trade

Turning to less commonly considered aspects, online channels facilitate the sale of regulated products in indirect ways. Online platforms facilitate the sourcing of the "dry goods" that enable the production and sale of illicit alcohol: blank or pre-printed labels, bottle closures (including corks or caps), shrink sleeves, and even counterfeit or look-alike excise stamps intended to signal tax compliance. While many of these components are lawful in isolation, their aggregated availability online supports the manufacturing of counterfeit products.

Pesticides

All countries maintain regulatory frameworks governing the manufacture, sale, and use of pesticides, typically including requirements for product registration, licensing of distributors and retailers, adherence to labeling and safety standards, and restrictions on cross-border movement. These measures aim to safeguard agricultural productivity, protect environmental integrity, and ensure human and animal health.

Online, however, the application and enforcement of these regulatory controls is often uneven. Evidence indicates that unregistered, banned or counterfeit pesticides are available across a wide range of online platforms, enabling a parallel illicit supply chain that extends across national borders, especially where regulations differ. This undermines years of regulatory effort designed to safeguard agricultural productivity, environmental integrity and human health.

Regulations that have traditionally been applied to physical retail sales, such as requiring valid trade licenses, have not been uniformly applied to govern online sales. In addition, systemic weaknesses within online platforms, such as

inadequate due diligence during the seller onboarding process and weak category policing that allows pesticides to be listed under generic headings, make it easier for criminals to evade detection. Consequently, these vulnerabilities enable illegitimate sellers to:

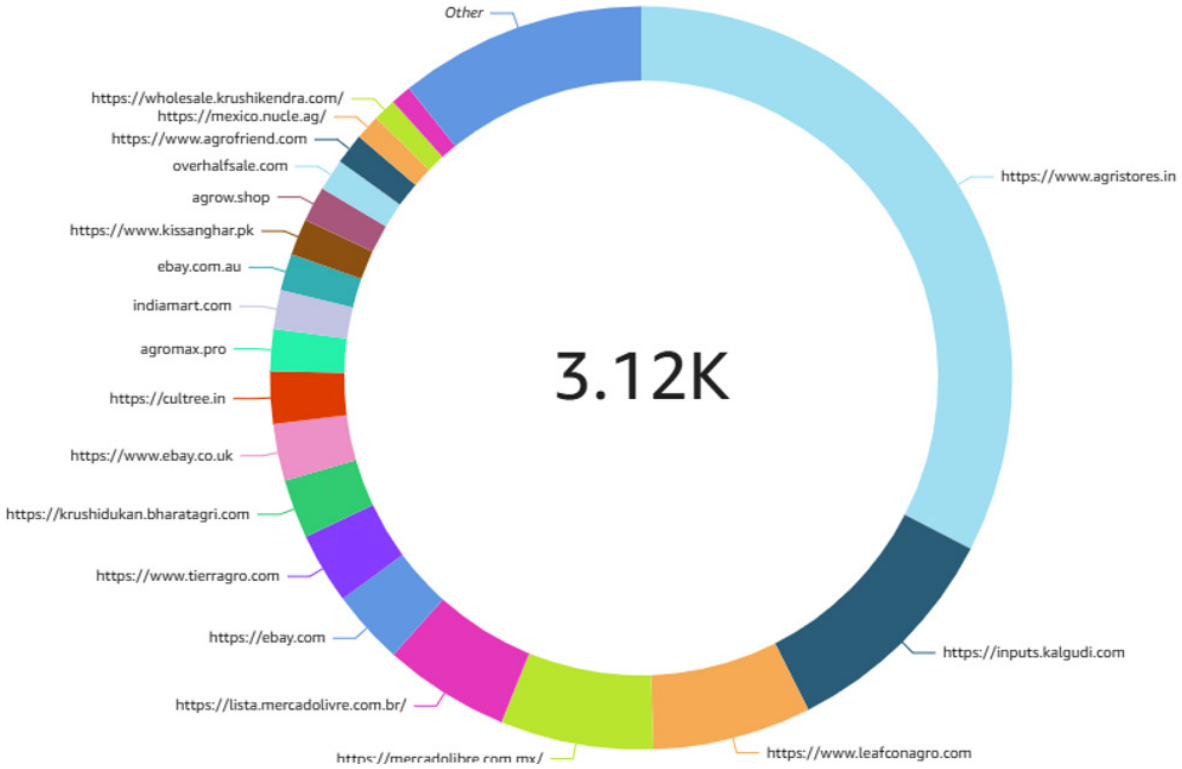
- Offer for sale unregistered and prohibited pesticides.
- Sell counterfeit pesticides or conceal banned or discontinued pesticides by labeling them with well-known brand names of major pesticide companies, thus lending them an appearance of legitimacy.
- Disguise pesticides as herbicides or organic fertilizers to evade registration and licensing requirements.
- Facilitate the diversion of pesticides from countries where they are legally permitted to countries where they are prohibited, by passing registration requirements in the 'country of intended sale'.

An investigation by Pesticide Action Network Asia and the Pacific (PANAP) found that HHPs - paraquat, endosulfan and profenophos are openly listed on mainstream marketplaces such as Shopee and Lazada.[5] To avoid detection, fraudulent sellers routinely strip their listings of identifying details, pixelate label images, omit the product name, or describe the pesticide in vague, benign terms to conceal its toxicity. Some fraudulent listings go further by falsely claiming that the restricted chemical is "ecologically safe" or "suitable for home-garden use," thereby luring unsuspecting consumers into handling a a highly hazardous pesticide banned in Malaysia.[6]

Industry monitoring efforts further highlight the problem's scale and reach. One leading agricultural-inputs company monitors more than 500 e-commerce sites and major social media platforms on a permanent basis, dedicating significant technical and investigative capacity simply to identify and remove illicit or non-compliant listings (see image on page 19).

The investigation reveals that high-volume sites such as Agristores, Kalgudi, Mercado Libre and several regional marketplaces account for a large share of infringements, and the long list of smaller platforms shows how widely violations are dispersed across digital marketplaces worldwide. IndiaMart has demonstrated limited effectiveness in addressing requests for the removal of illegal products. The platform is notably unresponsive to such takedown requests. According to industry data,[7] IndiaMart defends its contribution to illegal sales in stating that it acts solely as an intermediary, with transactions occurring directly between vendors and consumers. This suggests the platform may neglect its fundamental responsibility to safeguard consumers from threats to their health and the environment. This position is further contradicted by the platform's claim that illegal products originate from "verified exporters."

IndiaMart appears not to recognize that feedback and calls to action from industry regarding suspicious sellers should be a critical component of the internal risk assessment for "verified exporters." Products that were eventually removed after multiple requests troublingly reappeared 3 months later in their Featured Products section.



In April 2024, TRACIT released a report, "*Tackling the sale of illicit pesticides on e-commerce platforms: Risks, challenges and solutions*,"[8] highlighting rapid increases in the availability of illegal pesticides on online platforms and the serious concerns this trend raises. The report reviews major global online platforms and found that illicit pesticides are available on almost all of them. It provides examples of illegal pesticide listings and showcases measures that some platforms have undertaken to mitigate illicit trade in pesticides.

- Illicit pesticides and active ingredients, some of which are banned for use in many countries, are found for sale on Alibaba. Orders received by customers in EU and non-EU countries were illicit pesticides with logos belonging to well-known brands. This includes listings for "integrated packages" which include customized formulation using active ingredients, personalized packaging and graphics including logos (see image below). Further, some of these illicit listings were also from "Verified Suppliers" (i.e. the sellers' identity has been verified by Alibaba).[9]

- Lazada is a platform that operates in Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam. Online listings of illicit pesticides that were unregistered, contained banned substances, or had misleading labels have been found on Lazada.[10]
- On the platform Made in China, pesticides are falsely declared as insecticides or organic products and contain banned active ingredients. Also similar to the situation at Alibaba, sellers on Made in China offer "integrated packaging", and they ship illicit pesticides and active ingredients globally.[11]
- In addition to online marketplaces, the UN Environmental Program (UNEP) notes that criminals are increasingly using social media channels to advertise the sale of illicit pesticides.[12] For example, illicit pesticides are advertised through network "Stories" on Instagram. Criminals are also relying increasingly on Facebook groups to list offers for illicit pesticides.[13]

Pharmaceuticals

This section focuses on the distinct challenges posed by prescription-only medicines and over-the-counter (OTC) drugs available for sale on online marketplaces and social media platforms. We acknowledge that unlicensed online pharmacies are another form of lawlessness in online commerce; however, they fall outside the scope of this paper.

The pharmaceutical sector operates under one of the world's strictest regulatory regimes: every step—from manufacturing and marketing authorization to import-export controls, wholesale distribution, and prescription-only dispensing—is tightly licensed and monitored.

Despite these controls, evidence shows that these safeguards are not consistently applied or enforced by a range of online platforms. Prescription drugs such as Ozempic, Mounjaro, Adderall, Xanax, and Metformin are offered for sale without requiring sellers to demonstrate licenses, without requiring buyers to present prescriptions, or without scrutiny of whether the product can be legally sold across a border.

The World Health Organization (WHO) has specifically warned about the role of e-commerce as a contributory factor to the harmful distribution of substandard and falsified pharmaceuticals. Illicit pharmaceuticals pose significant risks to patient safety and public health worldwide. These products may contain incorrect ingredients, improper dosages, or harmful substances, leading to treatment failures, adverse reactions, and even fatalities.[14] The expansion of online access to medicines has amplified these risks, particularly where regulatory safeguards are not consistently enforced.

INTERPOL Operation Pangea XVII

INTERPOL's 2025 Operation Pangea XVII, annual operation targeting the online sale of illicit pharmaceuticals, confirmed the scale of the shift, seizing more than 50 million illicit doses across 90 countries with more than 750 arrests – about 10 times higher than the previous operation.

"The rapid growth of online platforms has made it easier for these unsafe drugs to reach people as well as opening new opportunities for criminal networks to exploit," said David Caunter, Director, Organized and Emerging Crime, INTERPOL.

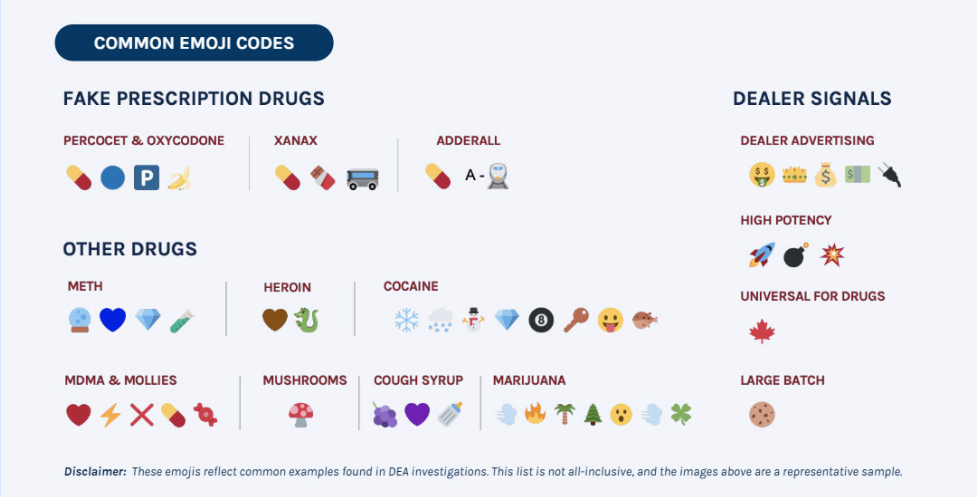
- In 2025, the U.S. Food and Drug Administration (FDA) warned that Amazon had introduced illegal drug products into U.S. interstate commerce.[15] The FDA noted that the concentrations of active ingredients in these products exceeded the limits permitted in the U.S. for non-prescription drugs and are classified as "unapproved new drugs" and "misbranded".[16] These products were handled through Fulfillment by Amazon (FBA), a system where Amazon stores, packs, and ships products to consumers. This follows another transgression in 2023, when the FDA issued two formal warning letters to Amazon, citing the illegal listings and sale of homeopathic products and products containing active pharmaceutical ingredients that lacked FDA approvals.[17]
- In 2024, a seller was jailed for selling sildenafil (Viagra), tramadol, zopiclone and pregabalin on Amazon and eBay under false "natural" claims. The MHRA described these as illegal, imported prescription-only medications.[18]
- The WHO issued a medical product alert in June 2024 regarding falsified

versions of Ozempic (semaglutide),[19] a medication used for diabetes management and weight loss. These falsified products are available for sale in several countries globally and are primarily marketed through unauthorized online platforms such as TikTok and sold on TikTok Shop thereafter.

- In 2023, EUROPOL authorities dismantled a criminal network that was producing and distributing illegal pharmaceuticals, including anabolic steroids, across the EU.[20] This network utilized popular social media influencers to promote to steer their followers on dietary and nutrition channels to markets for counterfeit performance-enhancing substances.
- A study by the US National Association of Boards of Pharmacy (NABP) uncovered widespread violations across major platforms. On Pinterest, 38% of posts promoting medications were linked to illegal online pharmacies; similar results were found through keyword searches on Instagram, Facebook, X (formerly Twitter), Reddit, and eBay. Listings included birth control pills, tretinoin, albuterol, codeine-based painkillers, and prescription drugs such as Adderall®, Xanax, and metformin—all sold without prescriptions. Platforms like Snapchat and Instagram have faced scrutiny for facilitating the sale of fentanyl-laced counterfeit pills—extremely potent opioids driving a major public health crisis.[21]

One Pill can Kill Campaign

The US's Drug Enforcement Administration's 'One Pill Can Kill'[22] campaign illustrates how criminal networks have transformed online platforms into a one-stop-shop to purchase dangerous prescription medicines and other lethal synthetic drugs.



Emojis for advertising, high potency, universal drug tags, and large-batch offers so viewers can recognize coded posts online.

EU Digital Services Act: Regulating illicit pharmaceuticals online[23]

In March 2024, the EU Commission initiated proceedings against AliExpress under the Digital Services Act (DSA) for the alleged sale of illegal products, including falsified medicines. The proceedings focused on:

- Compliance with the DSA obligations related to the assessment and mitigation of the systemic risks of dissemination of illegal content and consumer harm.
- The lack of enforcement of AliExpress' terms of service prohibiting certain products posing risks for consumers' health (such as fake medicines and food as well as dietary supplements); and
- The lack of effective measures to prevent such illegal content.

Tobacco Products

Tobacco is one of the most tightly controlled consumer products in the world: health warnings are mandated on every label, and retailers must have a license to sell and are mandated to check customers' age before sale. Online, this regulatory framework has largely been applied inconsistently. Evidence indicates that illicit tobacco products, including counterfeits and associated nicotine products, are available across a range of online channels, creating new pathways for access that can bypass regulatory controls designed to protect consumers.

Globally, illicit tobacco products can now be ordered online on marketplaces and social media in ways that do not consistently require sellers to demonstrate licensing or buyers to verify age, with delivery mechanisms that remove traditional face-to-face checkpoints for compliance.

Online platforms have inadvertently become critical enablers of the illicit tobacco and nicotine products trade, offering sellers a low-risk, high-reach environment with minimal oversight. In many cases, these platforms do not require proof of licensing to list tobacco products, nor do they conduct any form of pre-listing review or authorization before publication. Listings can be published instantly, with limited verification of legality or compliance with tobacco control laws. Age-verification measures vary in effectiveness and, in some cases, may not be sufficiently robust, allowing underage consumers easy access to restricted products. Sellers may use vague descriptions, misleading imagery often using typos, mis-categorization, adapted copyright, code words and cryptic images to evade detection, and social media platforms facilitate transactions through private groups, direct messaging, and disappearing content.

Examples

- Facebook and Instagram have become primary channels for the sale of illicit tobacco,[24] despite Meta's policies aimed at restricting tobacco promotion across its platform. These violations include promoting tobacco products on pages, in advertisements, and through commerce channels, often circumventing restrictions on underage access.[25]
- On TikTok, sellers promote vapes—often disguised as "stationery"—and appear to target under-18 consumers; many accounts persist even after being reported. TikTok videos posted by small business owners advertise discreet shipping practices that evade age verification to sell nicotine products.[26] Gaps in seller verification and the absence of mandatory buyer ID checks create major loopholes that make illicit nicotine products easy to purchase.[27]

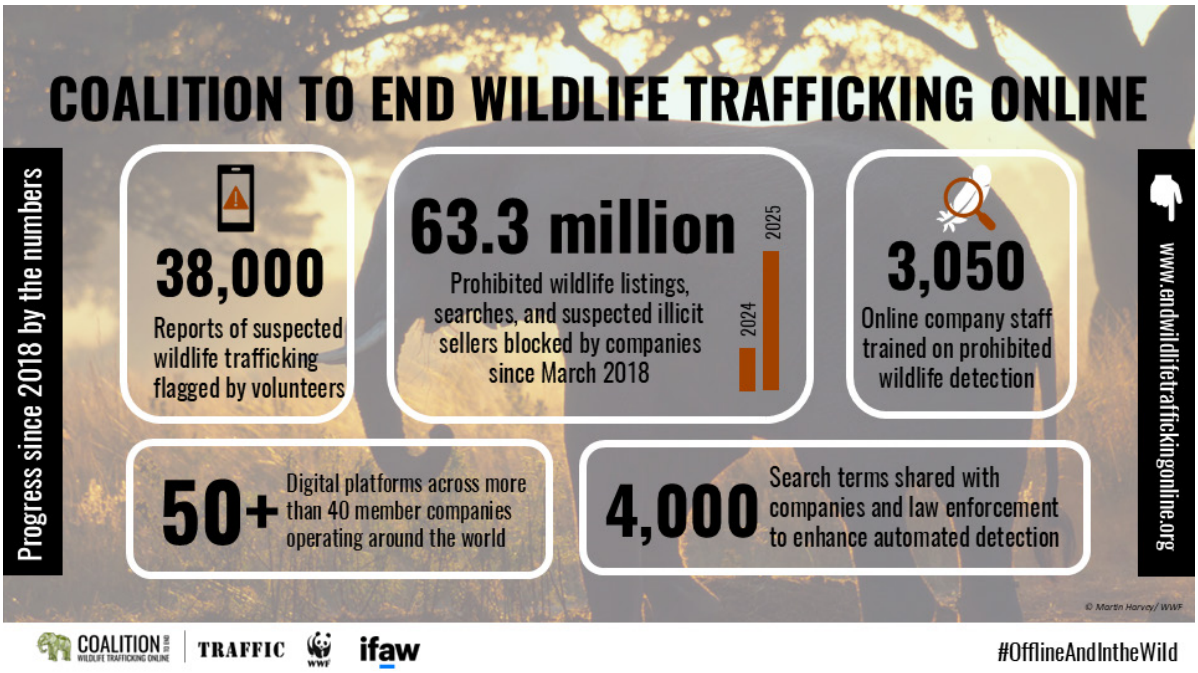
> *"It's the responsibility of social media platforms to ensure that products sold on their platforms, whether it's TikTok, Facebook, or Instagram, are legal for sale."*
>
> *- Kate Pike, Chartered Trading Standards Institute*

Wildlife Products

Illegal wildlife trade (IWT) generates billions in criminal proceeds annually, with online platforms playing a growing role in facilitating the trade. Online marketplaces, social media platforms, and encrypted communication platforms increase the ease with which illegal wildlife transactions are brokered between buyers and sellers.[28]

Simple keyword searches on online platforms reveal a substantial volume of wildlife products available for sale. These include both live animals and products from endangered species such as songbirds, tiger bones, lion parts, bear gall bladders, elephant ivory, and rhino horns. Other traded products include pangolin scales, shark fins, and parts from various marine and terrestrial species, some of which are protected under international regulations like CITES (the Convention on International Trade in Endangered Species of Wild Fauna and Flora).[29]

Online marketplaces like eBay, Etsy, TikTok Shop and Amazon, social media platforms like Instagram and Facebook and messaging apps such as WhatsApp, WeChat and Telegram are widely used by traffickers to advertise wildlife or related products.[30] Sellers and buyers operate in plain sight with limited regulation or enforcement. These online platforms provide spaces where advertisements for illegal wildlife and their products become accessible.



Between March 2018 and September 2024, over 24 million prohibited wildlife listings and suspected illicit sellers were blocked on online platforms by the Coalition to End Wildlife Trafficking.

Examples

- Listings of dozens of different rare bat species were found on eBay, Etsy and Amazon. Prices range from USD 8.50 for smaller bats to USD 2,500 for flying foxes. Most bats only produce one offspring a year, meaning commercial harvest, even at low levels, presents a serious threat to their conservation. Bats carry over 60 viruses, many of which are transmissible to humans, raising significant health concerns.[31]
- Despite Meta's participation in the The Coalition to End Wildlife Trafficking Online, convened by WWF, TRAFFIC and IFAW,[32] investigations have uncovered persistent issues. A 2020 investigation identified hundreds of Facebook pages and groups openly selling pangolins, rhino horns, turtles, orangutans, tiger claws, and other endangered species products.[33] Meta primarily relies on user-reported posts rather than actively searching for illegal listings. Meta's algorithms often amplify illegal listings instead of limiting them.[34]
- Between July 2021 and June 2023, TRAFFIC's USAID-supported research uncovered around 22,500 online advertisements for illegal wildlife products in Vietnam—averaging 30 posts per day—with Facebook (51.3%) and Zalo (35%) identified as the dominant platforms. These listings included items made from live animals and products from the targeted species groups, such as tigers, elephants, rhinos, pangolins, tortoises, and freshwater turtles.[35]

IV. Enabling sales of stolen goods

Organized retail crime (ORC) has rapidly evolved from traditional "fencing" rings into sophisticated, cyber-enabled enterprises. Although fencing is not new, its migration to the digital space – and the associated access to much wider marketplaces – has escalated this form of illegal commercial activity.

> *"What fuels [organized retail crime] as an enterprise is the ease of reselling stolen merchandise on online marketplaces,"*
>
> *- Illinois Attorney General Kwame Raoul*[36]

ORC networks steal merchandise in bulk from brick-and-mortar stores, freight trains, transport vehicles, ports and distribution hubs, then launder those products through online platforms. They routinely target high-turnover products, including electronics and tools, health and beauty items, over-the-counter medicines, fragrances, toiletries, apparel and footwear, alcohol and tobacco. These goods are then channeled onto online platforms and advertised as "new-with-tags" or "available in bulk", at significantly reduced prices.[37]

The role of online marketplaces is increasingly central to the economics of ORC. Online platforms provide ORC groups with rapid access to consumers, low barriers to entry, limited seller scrutiny, and the ability to operate across jurisdictions. The scale and efficiency of these online resale channels have transformed ORC from opportunistic theft into a highly organized and profitable criminal business model.

This growing organized theft has triggered mounting concern among policymakers, retailers and law enforcement agencies, particularly in the United States. Most notably, the US introduced the first major standalone legislative framework specifically targeting ORC and its connection to online marketplaces. The Combating Organized Retail Crime Act (CORCA) of 2025, passed by the US House of Representatives in May 2026, reflects a growing recognition that organized retail crime increasingly depends on online platforms to distribute and monetize stolen goods at scale. Notably, the legislation's stated purpose is to combat organized crime involving the illegal acquisition of retail goods and cargo for resale through both physical and online retail marketplaces. In doing so, Congress explicitly acknowledges that online marketplaces are no longer peripheral to organized retail crime, but form part of the infrastructure through which stolen goods are laundered back into consumer markets.

The legislative push toward addressing the online sale of stolen goods was already taking shape prior to the introduction of the CORCA in April 2025.[39] In 2023, the United States adopted the INFORM Consumers Act, which, although

initially framed around counterfeit goods, also reflected growing concerns about how easily stolen merchandise was being resold through online platforms. The Act directs online platforms to implement stringent transparency measures—chiefly, mandatory verification and public disclosure of high-volume third-party sellers—designed to expose bad actors and keep illicit products out of consumers' shopping carts. The legislative provisions addressing stolen goods required the U.S. Federal Trade Commission to protect consumers from unsafe merchandise, including stolen goods, illustrating how governments are beginning to address gaps in accountability and enforcement in digital marketplaces.[40]

US retail companies demand accountability in online platforms

The expanding scale of losses from ORC crimes online, along with the reputational risk to legitimate sellers, was highlighted in a petition from 20 major retailers including Home Depot, Best Buy, Walgreens and Kroger. These retailers formally urged Congress to require far stricter seller-verification rules for online platforms.[38] They highlighted that anonymity in online transactions, combined with gaps in seller verification, enables the resale of stolen goods at scale, distorting competition and reducing transparency for consumers. They further argued that greater transparency on online supply chains should be mandated so that buyers know exactly who they are buying from, whether purchased in-store or online.

> *"The INFORM Consumers Act requires online marketplaces to protect consumers from counterfeit, unsafe, and stolen goods by verifying their high-volume third-party sellers' identities, and making it easier for consumers to report suspicious marketplace activity,"*
>
> *- FTC's Bureau of Consumer Protection*

Examples

- Following the October 2026 unrest in France, goods suspected of having been stolen from shops appeared for sale on online marketplaces, prompting the government to summon Vinted, eBay, Leboncoin and other platforms and demand the removal of listings linked to stolen goods.[41] Vinted reported removing suspected looting-related listings, increasing monitoring and warning of permanent account bans, while eBay stated that it could not confirm an increase in such listings and would remove stolen items and take action against sellers upon confirmation from law enforcement.[42] Following government intervention, these platforms committed to intensified monitoring for indicators

such as abnormally low prices, bulk listing of new products and visible security tags, alongside sharing information to identify sellers and providing quantified enforcement reports, with an initial report due within 48 hours.[43] This intervention demonstrates that online platforms have both the technical capacity and operational tools to proactively identify suspicious listings, investigate sellers and cooperate with enforcement authorities. Crucially, it also shows how government intervention can rapidly mobilize these capabilities.

- eBay, Facebook and Craigslist have been repeatedly identified by New York law enforcement as major channels for the resale of stolen goods.[44] Retail theft in New York resulted in an estimated USD 4.4 billion in losses in 2022, and officials note that a significant share of this is enabled by the ability of criminals to fence the stolen products through online marketplaces. The 64% increase in shoplifting in the city between 2019 and 2023 corresponds to the growth in online listings and widespread resale of ORC-targeted goods such as OTC medicines, diapers, and detergents – many of which still featured "new-with-tags" labeling.[45]

A backroom of the illegal pawnshop in Brentwood, NY, busted by the Suffolk County DA was stuffed with stolen goods, including kitchen goods, luxury items and even professional building supplies, that were destined to be sold onlint. (Source: see footnote 43)

- In the UK, large quantities of consumer items including personal care items (razor blades, toothpaste, electric toothbrushes), meat, cheese, alcohol, OTC medicines, and electronics—are routinely stolen by "professional" shoplifters and then resold on Facebook Marketplace and via invitation-only groups, often with security seals still intact. Meta's reliance on community-led moderation, limits effective oversight, particularly where participants have no incentive to report illicit activity.[46]
- eBay was exploited to resell stolen power tools, kitchen appliances, construction materials, and designer clothing in a major Suffolk County case, where stolen inventory was systematically listed through multiple seller accounts to avoid detection.[47]
- An industry representative interviewed for this report cited that cargo theft

incidents have been reported across France, the UK, Los Angeles, and Brazil, with stolen merchandise repeatedly resurfacing on online platforms. For example, more than 2,000 items of footwear and apparel that were destined for retail stores in France were stolen and were later found being promoted by a store in Algeria on TikTok. Similarly, ORC groups hijacked a truck in Los Angeles with more than 120,000 pairs of footwear worth over USD 3 million and soon after made them available for sale on Facebook Marketplace in Tijuana.

- ORC groups used third-party seller accounts on Amazon and eBay to sell products from retailers such as Apple, Sunglass Hut, CVS and Walgreens. These platforms allowed products to be listed at prices far below legitimate offers, even undercutting "Amazon Prime" listings.[48]
- A storefront seller on Amazon and eBay listed merchandise stolen from local retailers by ORC groups, and between 2018 and 2023 more than 150,000 transactions went unnoticed on these platforms. The seller made USD 4.5 million from stolen goods,[49] while the platforms collected commissions on these transactions, profiting from the sale of stolen merchandise.

V. Circumvention of consumer health and safety regulations

Amongst the landscape of lawlessness online, illicit traders are able to circumvent or bypass laws that have been specifically promulgated to protect consumers from health and safety risks.

This presents a significant challenge to long-standing consumer protection regimes that were put in place to ensure that, for example, food is safe to eat, and medicines are effective and not contaminated. Because markets do not always self-regulate effectively, governments have stepped in to impose strict obligations on manufacturers, importers and distributors.

- As early as 1906, the U.S. established the Food and Drug Administration to protect consumers from adulterated and misbranded foods. That early mandate expanded into thousands of food and drug controls over ingredients, labeling, additives, and manufacturing practices associated with hundreds of consumer products – all aimed at bolstering consumer protection.
- In Europe, the EU now protects consumers from dangerous cosmetic products, prohibiting additives injurious to human health and requiring safety assessments and product notification through a Cosmetic Products Notification Portal.[50]

These consumer protection regimes have expanded over the past century as products, supply chains and risks have become more complex. Across countries, the approach is similar: regulators impose testing, certification, labeling and traceability requirements for products that could harm consumers if misused, adulterated or poorly manufactured. Safety controls are now deeply embedded in national regulatory systems. These systems, while resource-intensive for both industry and regulators, form the backbone of modern consumer protection.

However, in today's online commercial transactions, safeguards are applied unevenly. As a result, accountability remains limited, whether for platforms, importers, or sellers to verify that product listings meet applicable safety standards. These gaps enable illicit traders to misrepresent product information and sell products in circumvention of established regulatory controls or safety standards designed to protect consumers.

For example, an online listing may be published without a physical address or country of origin, circumventing registration requirements, verification of ingredients, traceability rules and labeling standards. In such cases, for example, products marketed as "extra-virgin" olive oil or "artisan" honey may not have been produced under applicable regulatory controls, increasing potential risks to consumers. Consumers may also lack the information needed to assess whether products have undergone required inspections or meet safety and labeling standards.

This trend is evidenced by a report from the UK Food Standards Agency (FSA), which notes that online platforms have made the internet sale of food easier and more widespread, enabling vendors globally to trade without physical shopfronts, creating new challenges to enforcement. In response, the FSA has called on social media companies to assume responsibility for transactions on their platforms — urging them to verify seller credentials and to promptly remove dangerous listings.[51]

Growing awareness of these risks has also prompted legislative proposals. For example, the US SHOP SAFE Act (Stopping Harmful Offers on Platforms by Screening Against Fakes in E-Commerce), aims to legislate strong "know-your-vendor" controls on e-commerce platforms selling products presenting consumer health and safety risks. A key provision uniquely calls for platform liability where compliance checks are not performed.

Examples

- In 2025, Vietnam's Department of Food Safety found that several functional foods being sold on Shopee and Lazada, including Omega 3-6-9 supplements, Natto Kinase, Estroven Complete, and Kirkland glucosamine products, were being marketed without any registration or approvals. These items had not undergone the required product-declaration registration certificates, exposing consumers to unknown health risks, including undeclared ingredients, inaccurate dosages, or potential health complications associated with interactions with existing medications.[52]
- In 2025, the US FDA found that Amazon sold "tattoo-numbing" creams with dangerously high levels of lidocaine and unapproved drug formulations. The products were marketed as ordinary OTC pain-relief creams but posed risks of systemic toxicity when used on large or broken areas of skin. The FDA warned Amazon that it was legally responsible for investigating and determining the causes of any violations and for preventing their recurrence or the occurrence of other violations, and to ensure that the firm complies with all requirements of federal law, including FDA regulations preventing the introduction of unsafe medicines into the market.[53]
- A concerning trend in the cosmetics industry is the advertisement of low-cost 'dupes' on online marketplaces like TikTok Shop and Facebook Marketplace. While a dupe is a knock-off product that imitates another without actually violating a trademark, they nonetheless circumvent laws designed to protect consumers from potential health risks.[54]
- Counterfeit Korean brands like Innisfree and Laneige are often sold on Temu and AliExpress in circumvention of consumer health standards. These products are now found in customs seizure operations around the world, including in

South Korea, India, and the EU – arriving from Chinese sellers. Product testing revealed many seized products had levels of mercury up to 1000 times government mandated limits, E. Coli bacteria, and staphylococcus aureus.[55]

- In 2025, a Which? investigation found that over 65% of cosmetics bought on online marketplaces were fake. Major online marketplaces, including Amazon, eBay and TikTok Shop, were exposed for selling counterfeit versions of popular cosmetics brands. Counterfeit cosmetics can contain cancer-causing and toxic ingredients and can cause skin irritation, infections or chemical burns. Despite buyers flagging fakes in reviews, platforms continued to host listings by sellers that had sold thousands of units.[56]
- In 2025, a CNBC investigation into Walmart Marketplace identified sellers offering counterfeit health and beauty products. Twenty products examined during the investigation, including brain-health supplements, were found to be counterfeit through brand authentication or laboratory testing. The findings raised concerns about consumers unknowingly purchasing potentially unsafe products.[57]
- Listings on Shein routinely expose children to dangerous chemicals. A 2025 Greenpeace investigation found that Shein was selling clothing containing hazardous chemicals at levels that are a thousand times above EU safety limits, directly exposing consumers, especially children, to substances linked to cancer, infertility, hormone disruption and organ damage.[58]
- A 2024 investigation by the Danish Consumer Council found that over 60% of slime dough toys purchased from online marketplaces such as Temu, Wish, Shein and Amazon contained dangerously high levels of boron, far above EU safety limits, which are dangerous for children.[59]

VI. Violation of product safety laws and regulations

While the previous section focused on online platforms' frequent non-compliance with the specific obligations laid down in consumer-protection legislation, a further and distinct problem concerns the failure of many of those platforms to comply with product safety laws and standards. These are not necessarily limited to consumers' protection in the narrow sense, but aim more broadly to maintain a safe, fair and competitive marketplace and confidence in commerce.[60] Accordingly, when unsafe goods are listed and supplied through online platforms, the resulting harm is not merely a breach of consumer-protection norms (e.g., information duties or fairness rules), but also a failure to respect a regulatory framework aimed at preventing physical (and, increasingly, digitally mediated) risks from products reaching end-users.

In the legal supply chain, corporations invest significantly in rigorous testing protocols to verify that products comply with national product safety standards and are safe for consumer use. An important part of the process involves third-party audits to ensure a company's products and processes meet these product safety standards. For example, SGS, a multinational company specializing in inspection, audits, verification, testing, and certification, works across various industries to ensure product safety and compliance with regulations. Their GS Mark service requires ongoing annual audits to ensure continued compliance. For companies, investments in certifications such as this are a cornerstone of their compliance with product safety standards and their commitment to consumers.

Product safety rules are so important that intergovernmental organizations like UNCTAD and the OECD partner with national governments to promote product safety frameworks. For example, the OECD issues a consolidated Recommendation on Consumer Product Safety—outlining core elements such as risk assessment, injury-data collection, and management approaches—and promotes cross-border cooperation via tools like the GlobalRecalls portal for swift alerts and removal of unsafe products.

The OECD delineates three categories of product safety risks that consumers are exposed to while shopping online:

- Availability of banned or recalled items: platforms routinely list products that national authorities have prohibited or recalled — spanning apparel, automotive parts, chemicals, cosmetics, foodstuffs, household electrical and non-electrical goods, sporting and recreation equipment, and toys and games—despite clear regulatory orders to remove them.
- Inadequate product labeling and safety warnings: many listings for regulated goods omit or display illegible the mandatory elements—hazard pictograms,

age-and-use warnings, conformity marks, batch/serial numbers, manufacturer/importer details, and user instructions in the local language—leaving buyers unaware of critical safety information.

- Failure to meet voluntary or mandatory safety standards: online platforms often offer items subject to defined electrical, mechanical, or chemical specifications without providing any proof of conformity—such as certification marks, technical data sheets, or safety declarations—undermining the whole premise of regulated product safety.

OECD's October 2021 Product Safety Sweep

One of the clearest illustrations of the pervasiveness of product safety risks online can be found in the OECD's Product Safety Sweep.[61] The survey looked at 4,000 products across 21 OECD and partner economies to assess the three categories of risk discussed above.

The results for online marketplaces reveal significant levels of non-compliance, as well as widespread gaps in the ability to verify compliance based on the information available in product listings:

- 54% of products listed on online marketplaces were found to be non-compliant with applicable product safety standards and laws. This reflects confirmed cases of non-compliance identified during the sweep.
- From the list of banned or recalled goods identified in the sweep, a shocking 92% remained available on online marketplaces. Coupang listed every single banned or recalled item on the list, followed closely by Wish at 98.7 %, AliExpress at 93.6 %, eBay at 92.9 %, and Amazon at 64.9%.
- For labeling requirements, approximately one-third of marketplace listings were non-compliant. In around 40% of cases, authorities were unable to determine compliance due to insufficient information in listings, such as missing hazard warnings, manufacturer details, or conformity markings.
- Almost 40% of the products inspected did not meet certain product safety standards (voluntary or mandatory) per national requirements. Ezbuy had the greatest rate of non-compliance (80%), followed by Lazada (70%) and Wish (62%)
- The sweep also found that foreign sellers exhibited significantly higher confirmed non-compliance rates (around 68%) compared to domestic sellers (approximately 26%), highlighting the challenges associated with cross-border enforcement in online marketplaces.

- Certain product categories, particularly toys and games, showed especially high levels of non-compliance or inability to verify compliance, reflecting heightened risks for vulnerable consumers such as children.

Importantly, the OECD distinguishes between confirmed non-compliance and cases where compliance could not be verified due to missing or incomplete information in product listings. This distinction is critical. The inability to determine compliance is itself a significant regulatory concern, as it limits both consumer awareness and enforcement authorities' ability to assess whether products meet required safety standards.

Collectively, these results point to a global online marketplace environment where unsafe or non-compliant products remain accessible, and where the information required to verify compliance is frequently absent or insufficient. For policymakers, this highlights the need for stronger requirements on seller traceability, product information, and verification of compliance, as well as more effective mechanisms to ensure the removal of unsafe and recalled products.

Emerging platform-led product compliance controls

A handful of platforms have begun introducing more structured product compliance measures. Recently, for example, Amazon, has implemented a framework that relies on third-party Testing, Inspection, and Certification (TIC) providers for certain high-risk product categories. Sellers of products such as children's goods, electronics, and dietary supplements are required to submit safety testing and compliance documentation through Amazon-recognized third-party laboratories before products can be listed. While this approach is not comprehensive and remains limited to selected categories, it nevertheless demonstrates that platforms have the technical capability to introduce more robust verification and compliance controls where they choose to do so.

Examples

- In November 2025, the Competition and Consumer Commission of Singapore (CCCS) found that almost 80% of children-oriented products sold on Shopee and Lazada, including baby cots, strollers and accessories, were unsafe and failed to meet applicable international safety standards.[62]
- A Which? investigation found that every plug-in mini heater it tested failed basic U.K. safety standards and was illegal to sell. These unsafe heaters were widely available on Amazon, eBay, and Wish, and were also promoted through Facebook and YouTube.[63]

- In a 2025 investigation, over 96% of children's products purchased on Temu were non-compliant with product safety standards, and many posed high-severity risks such as choking, suffocation, hazardous chemicals and structural failures. Similarly, only 1 of 27 tested USB chargers bought from Temu met basic electrical-safety requirements, with multiple models presenting overheating, fire, or insulation hazards.[64]

> *"The EU has the world's strictest toy safety rules, yet online platforms continue to allow the sale of toys from non-EU sellers that endanger children … So online platforms should not abuse EU consumer trust. Online platforms and marketplaces such as Temu need to take responsibility for weeding out and not allowing traders that sell illegal, unsafe toys."*
>
> *- Catherine Van Reeth, Director General of Toy Industries of Europe*[65]

- A 2025 investigation found that "not a single" children's item on Shein passed compliance tests, and platform responses depended upon the complaining party: Reports made as ordinary consumers received standardized replies without action. When consumer organizations reported the findings, Shein removed all affected items within days. However, similar or equivalent products remained available.[66] Electrical products were similarly deficient in meeting established safety standards: about half the USB chargers bought on Shein presented serious electrical-safety defects such as overheating, insufficient insulation, and risks of fire.[67]
- In June 2025, the European Commission found that AliExpress violated EU safety standards through its "systemic failure" to prevent the listing of illegal and dangerous goods, and routinely hosted counterfeit clothing and unsafe children's toys. Regulators said AliExpress had underestimated the general risk of illegal products and lacked adequate content-moderation systems, concluding that the platform's safety controls "do not work properly."[68]
- In May 2025, the UK Office for Product Safety and Standards published a recall notice for lithium-ion chargers sold via TikTok Shop after finding that they posed an electric-shock risk. The listings lacked required labeling, documentation, and compliance markings.[69]
- A 2024 investigation revealed that unsafe and recalled toys continued to be sold on eBay and Facebook Marketplace, including products with choking hazards, excessive lead levels, and dangerous high-powered magnets. After these harmful product listings were taken down, they reappeared on the same platforms, under new seller accounts or with slightly altered descriptions. Although these platforms state they remove harmful listings, unsafe toys remain widely available across their marketplaces.[70]

VII. Examining platform compliance

The preceding chapters have shown that illegal activities taking place online now extend well beyond the circumvention of laws to protect IP rights. Chapters 2-5 delineated four online commercial activities that occur in disregard for or in neglect of existing legal frameworks:

(i) the unauthorized sale of regulated products that require a license or permit to sell or buy,

(ii) the trafficking of stolen products,

(iii) the circumvention of consumer health and safety laws, and

(iv) the circumvention of product safety laws.

These findings point to a systemic gap between the legal frameworks governing commercial activity and how those rules are applied online. While digital commerce has expanded rapidly, the controls that underpin legal markets—licensing, verification, traceability, and enforcement—are not being applied with the same consistency online. In practice, much of the day-to-day governance of online commerce is currently determined by platform-level policies and controls, which vary significantly in scope, clarity, and effectiveness. This variation is not a marginal issue—it directly shapes the extent to which illicit trade can occur within platform ecosystems.

This raises the question of whether voluntary approaches alone are sufficient, and whether the scale and persistence of illicit activity point to the need for governments to play a more active role in regulating platforms.

Against this backdrop, this report evaluates platform compliance with the law against three benchmarks:

1. **Have platforms established clear rules for sellers, and explained how such rules are enforced?**

   Have platforms published clear, easily accessible policies governing seller conduct, including rules on prohibited products, defined seller obligations, and expectations on compliance? Furthermore, do these policies explain how such policies are meant to be enforced and how violations will be detected, addressed, and penalized to ensure accountability?

   Unless the rules are clear and sellers can access them, understand what is expected of them, and know how platforms monitor and enforce compliance, we cannot reasonably expect full adherence, whether in theory or practice.

2. **Do platforms enforce their own policies governing illicit trade-related activity?**

   To what extent do platforms operationalize their own rules into effective enforcement actions? In addition to instituting controls, this includes examining the effectiveness of mechanisms in place to enforce compliance, such as seller onboarding checks and product listing screening to ensure seller adherence to platform rules.

   Unless platforms actively enforce their rules through meaningful implementation, oversight and review, rogue sellers will continue to operate undetected and unchecked.

3. **Do platforms maintain meaningful measures that deter violations?**

   Do platforms meaningfully implement deterrent measures, such as takedown systems and stay-down actions to ensure sellers cannot repeatedly trade in illicit goods?

   Without meaningful deterrent sanctions, rules alone fail to prevent repeat offenses and deter illicit trade.

This report evaluates these questions from two perspectives:

A. **Products involved.** Platform policies and compliance programs can be broad and can apply to multiple types of commercial activities. Therefore, this report evaluates performance on terms of service language, rules, community standards or other provisions relating to transactions that might be vulnerable to (i) intellectual property rights violations, (ii) theft, (iii) circumvention of mandated licensing or certification or (iv) illicit or illegal activities involving otherwise highly regulated products, including alcohol, tobacco (including electronic cigarettes, vaping paraphernalia and nicotine products), pharmaceuticals (especially involving prescription medications) and animal and wildlife products (including the trade in protected species and the production of derivative products).

B. **Critical junctures in the online sales process** where rules, compliance practices and measures might be applied with the greatest potential effectiveness: (i) Seller onboarding (seller verification), (ii) Proactive product screening, (iii) Deterrent penalties.

Assessment

a. Have platforms established clear rules for sellers, and explained how these rules are enforced?

For platforms, the first line of defense against illicit trade is the establishment of clear sets of rules to govern seller conduct. These rules are typically codified in seller agreements, which form the foundational framework for acceptable behavior on the platform. These terms are designed to prevent the listing and sale of illegal, unsafe, or non-compliant products by explicitly defining prohibited goods and commercial activities. They also signal the platform's commitment to legal and ethical standards, offering a basis for enforcement actions when violations occur.

In principle, these rules should function like a compliance manual: they should clearly define which products are prohibited, what documentation sellers must provide (e.g., a permit), how sellers' identities and licenses will be verified, how product listings will be screened before going live, and which penalties apply when violations occur. A comprehensive policy should also explain how the platform checks compliance when a product is banned or regulated, what evidence is required from sellers, and what enforcement steps follow when rules are breached.

Virtually all e-commerce platforms now explicitly prohibit listings that violate intellectual property protections broadly, or involve counterfeit goods specifically. These policies are often detailed, operational, and supported by structured enforcement mechanisms, demonstrating that platforms are capable of implementing robust governance frameworks when expectations are clear. This progress has been largely driven by sustained pressure from brand owners and industry coalitions over the past decade.

In contrast, policies addressing other forms of illegal activity—such as the sale of regulated goods, stolen merchandise, or unsafe products—are often less detailed, less specific, and/or less clearly operationalized. This disparity is not merely a drafting issue; it has direct implications for enforcement. Where rules are vague or incomplete, compliance becomes difficult to monitor, and violations are easier to conceal.

Findings show that even among some of the world's most well-known platforms, detailed and operational policy language is largely limited to the governance of intellectual property rights, while rules for other high-risk product categories are vague, incomplete, or entirely absent. For example:

- IndiaMART provides minimal and largely non-operational policy guidance across several high-risk product categories. Policies are often limited to high-level prohibitions, with little or no detail on licensing requirements, compliance checks, or enforcement mechanisms. Stolen goods, for example, receive only a single, generic prohibition line with no supporting detail. Overall, IndiaMART's seller rules do not meaningfully reference licensing

requirements, compliance checks or enforcement consequences. This absence of operational detail significantly limits the effectiveness of the platform's policy framework in guiding seller behavior or supporting enforcement.

- DHgate's policies governing alcohol, pesticides, tobacco, pharmaceuticals and wildlife are basic, relying primarily on item-category lists within general prohibitions documents. Moreover, these policies do not clearly address how sector-specific licensing, documentation or regulatory compliance are verified. Some high-risk categories, such as stolen goods, are vague and only tangentially referenced under separate policies for overarching illicit goods frameworks and seller conduct. DHgate does provide some information on violation penalties and distinguishes them between tiers of violation severity. Depending on the type of infraction and any history of previous infractions, these can range from a warning, imposition of fines on the seller, the restriction of listings for a predetermined period, to the closure of an account. Shopee's guidance on pharmaceuticals is minimal and largely limited to references to compliance with local legislation. It does not address licensing or registration obligations or how it verifies these documents for sellers. Similarly, for alcohol, Shopee states that a license must be submitted by the seller, but the policy does not clearly define the scope of these licensing requirements or explain how such documentation is verified. Shopee's policies on pesticides, tobacco and wildlife are generally limited to brief statements within broader restricted-goods lists and lack product examples or sector-specific details. Stolen goods are only covered by a single, generic prohibition with no further explanation. The platform notes that "violations can result in listing deletion, account restrictions, suspension, or legal actions", but does not clearly define the conditions under which such measures are applied or how enforcement decisions are determined. This creates a gap between stated rules and their operational application.

Some platforms have developed more structured and operational policy frameworks, demonstrating that stronger approaches are both feasible and already in practice.

- Amazon maintains a detailed and structured restricted-products policy. For each category of product, it provides specific guidance on applicable restrictions, supported by references to relevant legislation and product examples. In certain high-risk categories, pre-approval is required through third-party Testing, Inspection, and Certification (TIC) service providers before a product may be listed. These requirements are supported by ongoing verification mechanisms, reflecting a more structured approach to managing compliance risks.
- TikTok Shop has developed detailed seller policies outlining product restrictions, required licenses and documentation, verification processes, and

associated penalties for violations. The policies are clearly structured and articulate expectations in a way that supports both seller understanding and enforcement.

- Mercado Libre applies differentiated policies depending on the destination country, aligning product restrictions with national regulatory requirements. Through structured classification systems, the platform provides sellers with clear guidance on whether products are permitted, restricted, or prohibited in specific jurisdictions.

The presence of detailed and enforceable policies in certain areas—notably intellectual property rights protection—demonstrates that platforms have the capability to implement robust controls. The absence of comparable frameworks in other high-risk areas would therefore reflect differences in prioritization rather than technical feasibility.

For policymakers, this distinction is critical. Voluntary approaches alone may not ensure consistent standards across platforms, and clearer regulatory expectations may be required to ensure that all categories of illicit trade are addressed with equal rigor.

b. Do platforms enforce their own policies governing illicit trade-related activity?

Because a platform's policies are central to its operations, it is therefore reasonable to examine what measures are implemented to enforce its own prescriptions and ensure compliance.

Despite platforms' efforts to implement security measures, enforcement remains weak and inconsistent to the extent that, across multiple major platforms, listings for stolen merchandise, unlicensed pharmaceuticals, banned pesticides, and unsafe consumer products remain widely available. This disconnect between the declaration of policies and their enforcement raises serious concerns and underscores the need for greater focus on how existing compliance mechanisms will be operationalized in practice.

Clearly, illicit traders have learned how to exploit platforms' gaps in due diligence—bypassing onboarding checks, resurfacing under new seller identities and altering product descriptions—despite policies that ostensibly prohibit such behavior.

In practice, meaningful compliance mechanisms are often lacking or inconsistently applied. Platforms may publish detailed policies, but without robust verification, monitoring, and measures applied in case of violations, those policies amount to little more than window dressing. For example,

- The OECD's 2021 Product Safety Sweep found that 92% of banned or recalled items remained available on online marketplaces, and 54% of all inspected products failed to meet basic safety standards.
- AliExpress and Temu both continue to exhibit 'systemic failures' identified by the EU Commission for persistent listings of illegal, unsafe and non-compliant products despite formal platform policies.[71]

There are three critical junctures in the online sales process where platform rules, compliance checks and penalties can have the greatest impact on reducing illicit trade. These are: (i) seller onboarding and verification, (ii) proactive screening of product listings, and (iii) the use of credible deterrent penalties. If platforms strengthen controls at these junctures, they can sharply limit the flow of illegal goods online.

i. Onboarding

Onboarding is the process by which online platforms register and authorize new sellers (users in the case of social media) before allowing them to utilize their infrastructure. Onboarding serves as a crucial first step for platforms to facilitate compliance with their policies. This step typically involves conducting checks on users prior to granting them access. Onboarding also provides an opportunity for the platform and sellers to review the rules, procedures, and mutual expectations before commencing business. An effective onboarding process would involve:

- Identity and business verification: Confirming seller/user identity, contact information, business location, and valid trade licenses.
- IP rights validation: Requiring proof that sellers are authorized to distribute branded products and screening for any applicants who might have previously been banned for offering and/or selling counterfeit products.
- Regulated goods compliance: verifying licenses and product registrations for goods like pesticides, alcohol, tobacco, and pharmaceuticals.
- Health and product safety certifications: verifying that products meet minimum safety standards before they are listed.

When implemented properly, onboarding can be an effective gatekeeper, filtering out rogue sellers, and safeguarding consumers.[72] However, many platforms continue to operate with minimal onboarding controls, allowing sellers to register with limited verification requirements. This creates low barriers to entry for sellers with malicious intent, enabling the proliferation of illicit products.

Platforms already possess a wide range of tools to collect and verify information. The challenge is not the absence of information, but the inconsistent application of these capabilities. Platforms can assess patterns in product offerings,

geographic signals, shipping practices, and financial accounts linked to past violations. Doing so would significantly improve their ability to identify high-risk sellers and repeat offenders.

Strengthening platform accountability and transparency

To reduce repeat offending and anonymous illicit trade online, regulatory frameworks should require platforms to implement stronger seller verification and business licensing transparency obligations. Recent EU initiatives — including the Digital Services Act (DSA) and the EU Customs Reform Package (2023) — provide a foundation for mandating clearer traceability of sellers, improved transparency on enforcement actions, and stronger accountability for platforms that facilitate regulatory circumvention. Leveraging these frameworks can help close existing loopholes and make it more difficult for counterfeiters and other illicit sellers to operate anonymously at scale.

Indeed, several major platforms already deploy these types of capabilities. Amazon requires new sellers to undergo identity verification and provide government-issued identification, business credentials, bank statements and proof of address, which it can cross-check against internal and external databases. Its systems continue to monitor sellers after registration, including for connections to previously identified bad actors and other patterns indicative of risk. Amazon also reports analyzing seller identity, behavioral patterns, supply-chain data and network connections together to identify relationships and coordinated abuse that may not be apparent when individual signals are considered in isolation.[73]

Tokopedia has similarly demonstrated how its machine-learning systems analyze seller behavior, user feedback, product descriptions and relationships between products, while its detection systems assess indicators including keywords, brand terms and pricing. More significantly, Tokopedia has developed a graph-based "Seller Network Mapping" system to uncover links between seller accounts distributing infringing goods, enabling it to identify connected seller networks and prevent previously banned sellers from creating new accounts and returning to the marketplace.[74]

Mercado Libre likewise collects and processes a broad range of information capable of supporting risk-based enforcement, including seller identity and contact details, bank-account and payment information, transactional activity, IP addresses, device information and geolocation. Notably, Mercado Libre records links between accounts and users for fraud-prevention purposes and uses automated systems to support fraud prevention, identity validation and risk assessment. Its Brand Protection Program also uses reports from rights holders to

identify trends and patterns of intellectual-property infringement.[75]

Moreover, platforms already use comparable, and in some cases even more extensive, capabilities on the consumer side. For example, AliExpress openly acknowledges in its privacy notices that it collects and analyzes extensive information about buyers—names, contact details, shipping addresses, payment details, browsing and search histories, wish-lists, device identifiers and approximate location—in order to recommend products and personalize content.[76] Notably, this analysis covers more than 150 million active buyers worldwide, a far larger user base than the number of sellers. This raises the question of why platforms that already operate sophisticated data systems to better know consumers deploy such limited application of similar tools to monitor sellers.

Emerging platform-led seller verification practices

Amazon has developed a comparatively structured seller verification framework requiring prospective sellers to provide government-issued identification, business documentation, and proof of address, with additional requirements depending on the jurisdiction and marketplace. This process is supported by document-forgery detection, but perhaps more importantly, behavioral signal analysis, which tracks and flags the registration of sellers with suspicious patterns of behavior or connections to previously identified bad actors. Beyond this, Amazon continuously monitors changes in account information and other risk signals throughout the seller lifecycle. These measures represent one of the more advanced seller verification models currently deployed by a major online marketplace. Nonetheless, repeat offenders continue to surface across Amazon's global marketplaces, suggesting that the platform must continue to evolve and strengthen these controls.

The following are examples of limited verification practices by various platforms:

- **Walmart Marketplace reportedly weakened seller verification procedures** during its rapid expansion, relying heavily on basic identifiers such as U.S. Employer Identification Numbers (EINs) without requiring robust supporting documentation or live "know your customer" (KYC) checks. According to a CNBC investigation, illicit sellers exploited these gaps by impersonating legitimate businesses to open accounts and sell counterfeit health and beauty products at steep discounts. Notably, the platform deployed limited "category gating" (restrictions on who can sell in sensitive categories like health and beauty) and minimal requirements to prove where products were sourced from.[77]

- **Counterfeit sellers bypass AliExpress's business-license checks through impersonation and proxy accounts.** AliExpress requires sellers to present a valid business license, but counterfeit sellers can still regularly provide licenses from unrelated companies or set up accounts in the names of family members.
- **Minimal upfront verification on Facebook, Instagram, and Instagram Shopping allows sellers to evade INFORM Act thresholds.** Facebook and Instagram typically require only an email address, phone number, and an ID to open an account. With the passage of the U.S. INFORM Act, platforms are now compelled to collect banking, contact and tax-identification information—and even then, this applies only to "high-volume third-party sellers" with 200 or more transactions and at least USD 5,000 in annual sales – leading to sellers now breaking up sales volumes across multiple accounts.[78] Moreover, Instagram shopping requires only that users switch to a professional account, link a Facebook Page, verify a domain, and attest to their "trustworthiness," with no upfront KYC or KYB [know your customer (KYC) or know your business (KYB) measures] for first-time merchants.[79] In practice, Facebook and Instagram are frequently used to advertise and display suspicious offers, with transactions and negotiations then shifting to private chats or instant-messaging applications.

ii. Screening product listings

Across platforms, the existence of measures to screen product listings prior to publication is critical to determining whether platform policies and applicable regulations are applied in practice, particularly for regulated products. The form and depth of screening vary by platform model. On marketplaces, this typically involves reviewing uploaded product images and listing text to assess alignment with platform rules, relevant laws, health regulations, and safety standards. In social media environments, screening is more often applied to promoted content and product advertising, including indicators that posts or listings are being used to facilitate off-platform transactions.

Where screening is undertaken, it commonly includes scanning for keywords associated with prohibited products (for example, "ivory" or "narcotics"), checking product labeling or registration information where available, and verifying licenses or safety certifications when required by law. However, the application of these measures remains uneven across platforms and product categories, allowing illicit products to continue to appear online.

Technologies to vet, scrutinize and block illicit listings already exist. They have been deployed to detect counterfeits, with many platforms prominently reporting the effectiveness of machine-learning applications and proactive controls. Notably, Amazon reports that its "proactive controls blocked more than 99% of

suspected infringing listings before a brand ever had to report them." Although there is considerable scope to expand and refine the parameters used to prevent the listing of illicit products, existing machine-learning tools, enhanced by emerging artificial intelligence, are capable of doing much more. These tools can compare discrepancies in product images, analyze descriptive text, and cross-check regulatory data in real time.

Many platforms do not sufficiently apply these capabilities, leaving significant enforcement gaps. Listings often go live without thorough scrutiny, allowing sellers to upload products with vague descriptions, deliberate mis-categorization, purposefully altered spellings, or misleading images. For example,

- **Gaps in upfront verification of pesticide sellers and products on Mercado Libre, Alibaba, Made-in-China and eBay.** In principle, a listing for a pesticide product—which a platform should know—should be accompanied by proof of license (or authorization) to sell pesticides and product registration certificates. The absence of effective screening on these platforms leaves gaps in verifying missing documentation, evaluate the authenticity of submitted licenses and registration certificates, and subsequently block products before they appear online. This shortcoming creates opportunities for sellers to mislabel banned or expired formulations and disguise them as harmless products.[80]
- **Health products are listed with minimal compliance checks on platforms like Daraz and Facebook Marketplace.** On these platforms, sellers routinely post health products, OTC medicines, and even highly regulated prescription drugs without undergoing any pre-listing compliance checks required by national law. Before listings go live, these platforms fail to: (a) verify that the product is legally registered or authorized in the country of sale, (b) ensure the listing includes mandatory labeling, dosage details, batch/lot numbers, expiry dates, and storage conditions, and (c) confirm that the seller is licensed to retail that category of products.
- **Wildlife products are available for sale on eBay, Etsy, TikTok Shop, Snapdeal, and IndiaMART**, often with no apparent CITES (Convention on International Trade in Endangered Species of Wild Fauna and Flora) or domestic wildlife protection validation or checks prior to listing. Sellers commonly provide only generic photos and a phone number or handle, before shifting buyers to WeChat, WhatsApp, or Telegram.
- **Prescription weight-loss drugs sold online outside regulatory controls**: Meituan lists semaglutide openly for purchase, with no prescription checks or medical approval required—despite Chinese laws restricting its sales only to licensed healthcare providers. Similarly, Pinduoduo and Xiaohongshu (Little Red Book) have each been flagged by pharmaceutical companies for hosting unverified sellers of weight-loss injections and related paraphernalia. A

MarketWatch investigation demonstrated how easy it is to buy weight-loss drugs online: a reporter ordered a semaglutide injection pen via a mobile app and received it within hours, without ever providing a prescription.[81] Prescription-only medications—such as weight-loss drugs like Ozempic (semaglutide)—are widely promoted and sold outside legal frameworks across multiple platforms.[82]

- EU issues warning on illegal prescription medicines being sold online. In September 2025, the European Medicines Agency (EMA) and the Heads of Medicines Agencies (HMA) warned of a sharp rise in illegal medicines marketed as GLP-1 receptor agonists, including semaglutide, liraglutide and tirzepatide, being advertised and sold online across the EU.[83] Authorities identified hundreds of fake Facebook profiles, advertisements and e-commerce listings promoting unauthorized products, often through fraudulent websites and social media and, in many cases, from operators based outside the EU. Some advertisements and websites also misused official logos and false endorsements to give illegal products an appearance of legitimacy.[84] Separate investigations have identified illicit weight-loss medicine sellers using social-media platforms to advertise products before directing prospective customers to private channels, including Telegram and WhatsApp, where transactions can continue away from the originating platform.[85]

c. Do platforms maintain meaningful measures that deter violations?

Seller agreements and platform policies carry little weight without meaningful consequences for violations. While most platforms deploy "takedown" mechanisms to remove IP-infringing listings, these controls have been slow and cumbersome to implement and have demonstrated limited deterrent effect on offenders, who often reappear within hours using new accounts or similar listings.

Stronger stay-down mechanisms, permanent bans for repeat offenders, and meaningful financial sanctions could significantly strengthen deterrence, yet few platforms deploy these measures, and others remain inconsistently applied. Importantly, platforms' existing enforcement tools remain largely tailored to address IP violations. In cases involving counterfeits, platforms often specify clear consequences such as three-strike rules, account suspensions, and withheld payouts, but even these measures are not uniformly applied, nor are the enforcement actions taken by the platforms visible to brand owners. Notably, enforcement can vary widely across platforms and jurisdictions. When it comes to products from other high-risk categories—such as unlicensed pharmaceuticals, banned pesticides, stolen goods, or unsafe consumer products—penalties are

even fewer, frequently vague, inconsistently applied, or buried in inaccessible policy documents, leaving platforms vulnerable to persistent violations.

Takedown

Crucially, notice-and-takedown systems have become a standard feature across major platforms, particularly in response to sustained pressure from brand owners and are designed primarily to protect IPRs, enabling them to flag infringing listings without having to prove their trademark for every individual removal. When a listing violates platform rules, it is removed from the site—either after a report from rights holders, regulators, or consumers, or through the platform's own monitoring. In theory, this should deter non-compliance by cutting off access to the platform. In practice, however, takedown measures are more often only short-term disruptions rather than meaningful deterrents.

However, affected industries consistently report that enforcement remains resource-intensive and inconsistent. Over the years, Amazon has automated and simplified its reporting tools. Amazon's Project Zero, which is a self-service tool for brand owners to remove counterfeit listings, serves as one such method for brand owners to pursue takedowns, but brand owners still must actively monitor the platform and file notices. This work demands significant investments in terms of time and resources.

Moreover, many platform responses are not consistent across all the jurisdictions they operate. On other platforms—such as IndiaMart, DHgate and Pinduoduo—brands report that takedown systems often require multiple complaints and repeated follow-up correspondence to achieve action, particularly where the platform does not fully understand the perceived violation. As a result, what should function as a routine enforcement mechanism often becomes a burdensome and opaque process involving slow response times, unclear review procedures, and limited proactive monitoring.

The problem extends beyond counterfeit goods. Categories such as unregulated pharmaceuticals, agrochemicals sold without prescriptions, and wildlife products, among others, have no equivalent "takedown" removal procedures. Platforms continue to rely heavily on reactive, complaint-driven enforcement, which, in the case of stolen products or products that bypass safety regulations, leaves unaware consumers to do the policing. Brands and regulators are therefore expected to flag violations and follow opaque procedures, which could often involve locating a generic "report abuse" form and submitting extensive evidence, including high-resolution photos, sworn declarations, and, in some jurisdictions, even court orders. Requests may stay unresolved for days or weeks, with little transparency in the process.

On social media platforms, 'takedown fatigue' is further compounded by platform design. Ephemeral formats such as Instagram or Facebook Stories vanish after 24hours, creating visibility gaps for regulators and enforcement agencies. Closed or private groups—sometimes hosting hundreds of thousands of users—currently operate beyond the reach of keyword filters and external reporting tools, making it unlikely that an illicit post will ever be reviewed, let alone punished. In addition, on some social media platforms, like Facebook, for example, listings can be posted anonymously in groups, further reducing visibility, traceability, and accountability.

Even when listings are taken down successfully, these actions are often temporary and not significant enough to deter sellers from simply re-registering under new identities using fake documents, disposable phone numbers, or alternate storefront names to relist the same banned products within days. The cumulative effect is that platform enforcement of effective deterrent measures has had little success.

Examples

- Amazon has inconsistent takedown actions across its global markets. Amazon has relatively strong policies against the sale of counterfeit and illegal goods, including strict takedown mechanisms, account suspensions, inventory destruction, and withholding seller payouts. However, Amazon does not enforce these safeguards consistently, especially across its global marketplaces. While its US marketplace generally features stronger monitoring and faster removals, its Asian marketplaces remain more vulnerable, with repeat offenders quickly reappearing under new product descriptions, listings, or accounts after takedowns.
- Prohibited vape and nicotine products reappear on Instagram after removal. Sellers continue to host repeat listings for banned vapes and flavored nicotine products. Sellers simply re-upload identical product photos under new usernames, with slightly modified captions.
- Reappearance of toxic and illegal products on Shein. A 2025 Greenpeace investigation found that Shein repeatedly relists hazardous products even after earlier listings were removed for containing chemicals far above EU safety limits (Perfluoroalkyl and Polyfluoroalkyl Substances (PFAS), phthalates, lead, cadmium). Several items previously taken down reappeared on the platform in near-identical forms, sometimes from the same supplier.

Stay down

As noted, takedown controls have had little success in deterring criminals who can easily return to a platform by creating new accounts or slightly altering

product descriptions. Consequently, legitimate sellers have pressed for stronger "stay-down" measures to prevent platform access by repeat or otherwise known offenders. Most platforms now claim to have stay-down measures in their policies. However, as with takedown procedures, these are largely designed for IPR violations, where many platforms have outlined sanctions such as three-strike rules, permanent bans, account suspensions, and financial penalties like withholding payouts. Even in the case of IP violations, brand owners have limited visibility into how often these measures are applied, whether permanent bans are enforced, or whether repeat offenders are effectively identified and blocked, and platforms do not necessarily inform brands when such actions are taken, significantly weakening their deterrent effect.

Beyond the IP context, stay-down mechanisms are markedly less developed. For product categories, such as unlicensed pharmaceuticals, banned pesticides, stolen goods, or unsafe consumer products, staydown prohibitions are not clear, difficult to locate within a platform's policies or delineate vague penalties that are inconsistently described.

- Meta's policies illustrate this important discrepancy between platform policies concerning anti-counterfeiting/anti-piracy and categories of other illicit products. Meta's staydown rules related to IP infringements set out explicit consequences: "*Repeatedly posting content that infringes someone else's intellectual property rights can result in additional restrictions. Your account or profile may be disabled, or you may face limitations on your ability to post content or access certain features and functionality*".[86] However, for general commerce violations – where other illicit products would be included- the company only states, "*if you repeatedly post commerce content that violates our policies, we may take additional action on your account*".[87]

Illicit sellers have adapted accordingly. Many maintain multiple sales channels, including permanent e-commerce storefronts, social-media profiles, third-party websites, and direct-to-consumer messaging. When one of the rogue accounts is taken down, others remain fully operational since companies like Meta are not effectively linking accounts across the same platform or across different associated platforms (e.g., on Facebook or between Facebook and Instagram). Offenders often create dozens of parallel accounts in advance on a single platform, allowing them to relist banned products almost instantly.

As such, even effective stay-down measures have not been shown to present sufficient deterrence. Despite their stated commitments, online platforms still need to invest more in tracking repeat offenders or building systems to connect identities across storefronts, payment accounts, or devices.

- Counterfeit goods sellers repeatedly relist across multiple platforms, including Pinduoduo, Shopee, Bukalapak, IndiaMART, Lazada, Allegro, DHgate, and TikTok Shop. Sellers routinely return after takedowns by creating new seller accounts and reposting their same inventory with only minor modifications to their listings. Brand owners report that once a listing has been removed on one platform, the same operators often reappear within hours.
- Repeat offenders resurface on AliExpress. In 2024, the European Commission launched a formal investigation under the Digital Services Act (DSA). The Commission's preliminary findings found that the platform showed "systemic failures" in preventing illegal goods from being relisted on its site and noted that the platform "failed to properly consider these risks and identified systemic failures in its content moderation systems." Furthermore, AliExpress "fail(ed) to appropriately enforce its penalty policy concerning traders that repeatedly post illegal content." Despite removing individual listings, sellers routinely reappear under new storefronts or repost listings after slightly altering the product description.[88]
- Concerns that Temu fails to keep suspended traders off the platform. In October 2024, the European Commission opened formal DSA proceedings against Temu citing, inter alia, concerns about the effectiveness of its systems for preventing previously suspended traders known to have sold non-compliant products from resurfacing. The investigation also examined measures to prevent non-compliant goods from reappearing, with potential breaches of the DSA's risk-assessment and mitigation obligations.[89]

VIII. Conclusions and recommendations

Conclusions

Illicit activity online is undermining established rules governing commercial transactions, product safety and consumer protection. Counterfeiting and other IP infringements are only the most visible part of a much broader landscape of lawlessness that includes the sale of regulated products sold without authorizations, products that violate consumer protection laws, stolen goods, and unsafe or non-compliant goods.

Online platforms have become an important part of the infrastructure through which these activities are carried out. Vulnerabilities in seller verification, product controls, monitoring and enforcement continue to be exploited by illicit traders. Many platforms have invested significantly in policies, trust-and-safety systems, seller controls, and voluntary enforcement initiatives. Some have developed sophisticated compliance programs, implemented proactive monitoring technologies, and strengthened cooperation with rights holders and regulators. These efforts are important and should be recognized. At the same time, this report demonstrates that enforcement remains inconsistent across platforms, jurisdictions, and product categories, creating opportunities for criminal actors to exploit regulatory and operational gaps. As a result, the conduct of weaker or less compliant actors risks undermining confidence in the broader digital commerce ecosystem.

Consequently, governments have an important role to play in establishing clear statutory expectations, ensuring consistent enforcement, and creating stronger accountability frameworks for online commerce. This is particularly important where platforms exercise significant control over commercial transactions, derive direct financial benefit from those activities, and possess the technological capabilities necessary to identify and mitigate risks.

Several jurisdictions have already begun moving in this direction, including:

- **Vietnam**: Vietnam's 2025 legislative reforms represent an important example of stronger platform accountability and a broader shift in how governments are approaching illicit trade online. The reforms move beyond the traditional "notice-and-takedown" approach—which has often proven ineffective when illegal listings rapidly reappear after removal—toward a more proactive "notice-and-stay-down" model. Article 198B of the amended IP Law directly addresses this gap by requiring platforms not only to remove unlawful listings, but also to implement systems designed to prevent those same listings from resurfacing. Coupled with broader obligations introduced under Vietnam's E-commerce Law, which apply to both domestic and foreign platforms, the reforms seek to shift enforcement away from a purely reactive, case-by-case

approach toward one focused on identifying and disrupting repeat offending behavior. The framework also extends responsibilities beyond marketplaces to include logistics, payment, and infrastructure providers, recognizing that a wider ecosystem of commercial actors facilitates illicit trade online.

- **European Union**: The Digital Services Act (DSA) is a landmark regulation designed to create a safer and more transparent online environment. The DSA establishes strict obligations for online platforms to develop policies and take enforcement action against illicit and illegal content and goods. A key feature of the DSA is the introduction of due diligence requirements for platforms to prevent the sale of illicit and illegal goods via their websites, apps, and similar e-commerce channels.
- **United States**: The INFORM Consumers Act requires e-commerce platforms to collect, vet, and disclose information about certain high-volume third-party sellers. Specifically, INFORM directs online marketplaces to verify high-volume third-party sellers by authenticating the seller's government ID, tax ID, bank account information, and contact information. Further, online marketplaces must also supply a hotline to enable customers to report suspicious seller activities, for example, the posting of suspected stolen, counterfeit, or dangerous products.
- **India**: The Consumer Protection (E-Commerce) Rules of 2020, along with the Information Technology (Intermediaries Guidelines) Rules of 2011, impose due-diligence and marketplace obligations of e-commerce platforms. Furthermore, these rules require every seller to ensure the accuracy and truthfulness of their descriptions, images, and other relevant content pertaining to their goods or services listings.
- **China**: China's E-Commerce Law, which entered into force in January 2019, established strong legal accountability for online platforms and third-party sellers involved in counterfeit trade. Under the law, platforms that fail to act promptly on infringement notices supported by preliminary evidence from rights holders can be held jointly and severally liable with sellers for additional losses resulting from their inaction. Liability also extends to platforms that know or should know of IP infringements and fail to take necessary measures. Importantly, the law also establishes joint and several liability where platforms know or should know that products sold by third-party sellers fail to meet safety requirements or otherwise infringe consumers' legitimate rights and fail to intervene. Platforms must retain product, service and transaction records for at least three years and face fines of up to CNY 2 million in serious cases involving non-compliance. China further strengthened its regulatory framework in February 2026 through new regulations governing online trading platforms and livestream e-commerce. These introduce additional requirements

concerning platform governance, enforcement of trading rules, seller identification and oversight of livestream commercial activities. In July 2026, China published draft amendments to the E-Commerce Law proposing expanded regulatory coverage, stronger platform accountability, additional enforcement measures and improved coordination among regulatory authorities.

These examples demonstrate that stronger and more enforceable standards have been recognized by lawmakers as necessary. However, implementation and enforcement remain unclear, and there are few examples where the laws have achieved their intent.

The OECD's *Draft Voluntary Guidelines for Countering Illicit Trade in Counterfeit Goods on Online Marketplaces* could set standards to help governments strengthen legislation and improve oversight of e-commerce platforms. Governments are encouraged to translate these principles into non-negotiable statutory requirements that establish a duty of care, condition safe-harbor protections on compliance, and attach meaningful liability for failure to act.

Recommendations

The recommendations below set baseline standards and obligations that governments should consider incorporating into regulatory frameworks for online commerce. Instruments such as the EU Digital Services Act, U.S. INFORM Consumers Act and proposed U.S. SHOP SAFE Act offer useful templates for this work and should be viewed as a minimum standard going forward.

1. **Enact clear statutory duties** that reconcile online–offline regulatory parity for online platforms. Where a license, inspection, or labeling rule exists offline, the equivalent duty should be explicitly required and applied to commercial transactions taking place online. Moreover, governments should enforce standards for consumer protection, product safety, labeling, and market integrity equally online. They should also require that platforms operators take a proactive approach in preventing that the platforms themselves be used for all typologies of illicit trade.
2. **Impose binding enforcement controls** on platforms, including:
    a. *Seller vetting.* Platforms should verify each seller before allowing them to publish any listing. This vetting should (i) authenticate the seller's identity and (ii) confirm the seller's legal authority and eligibility to sell the relevant products (including any required licenses, permits, or registrations). Verification should be based on official, authoritative documentation (e.g., government-issued identification, business registration records, and applicable licenses/permits), be renewed at regular intervals, re-triggered

after material changes (e.g., ownership, legal name, address, payment account, or product category), and re-verified whenever risk signals arise.

b. *Pre-listing verification.* Platforms should implement pre-listing verification that assesses the legality of each individual listing before publication. For every new listing (and any material edit), they should require and validate listing-specific substantiation (including product identity, compliance markings/certifications where applicable, safety and regulatory documentation, and proof of authorization for controlled or branded goods. Validation can be done using authoritative sources (e.g., regulators' databases, accredited certification bodies, rights-holder registries, or verifiable manufacturer/brand attestations). Listings that cannot be substantiated should not be allowed to go live.

c. *Licensing and compliance checks for regulated categories.* For products subject to statutory controls (for example, pharmaceuticals, pesticides, alcohol, tobacco, etc.), platforms should confirm the existence and validity of all required licenses/permits/registrations and ensure listings meet labeling, packaging, safety, security, and other compliance obligations. Buyer-side conditions (age, prescriptions, professional certifications) should be subject to verification too.

d. *Proactive monitoring and takedown mechanisms.* Platforms should actively operate continuous, risk-based monitoring to detect illicit listings (using available technological tools, including AI-based solutions) and remove them within defined timelines. Monitoring and removal duties apply regardless of whether a notice of takedown has been created, submitted, or received.

e. *Stay-down mechanisms.* Platforms should be mandated to implement a "notice-and-stay-down" regime to ensure that listings removed for legal violations do not re-appear on their trade channels. To do so, upon removal platforms could for example generate and retain tamper-resistant identifiers of the infringing offer (including hashes/perceptual fingerprints of images, text similarity signatures, and key metadata such as brand/model, GTIN (Global Trade Item Number)/MPN (Manufacturer Part Number), and shipping/fulfilment markers) and use these to block identical re-uploads automatically at the point of submission. Platforms could also deploy near-duplicate detection to prevent re-posting through minor edits (cropping images, rewording titles, changing categories).

3. **Impose robust record-keeping and traceability obligations.** Platforms should retain seller verification files, product listings, licenses to trade, transaction logs, and takedown records for a defined period (for example,

five years) and maintain systems that facilitate the ability to trace listings to the responsible seller. Platforms should be required to provide relevant authorities with timely access to records suspect of violations.

4. **Mandate transparency, audits and public reporting.** Platforms should publish periodic transparency reports detailing the volume and type of illicit listings detected and removed, actions taken against repeat offenders, and the effectiveness of their controls. Regulators should have auditing authority over compliance systems and platforms should be required to designate domestic legal representatives and 24/7 points of contact to liaise with and assist enforcement agencies.
5. **Consumer redressal mechanisms.** Platforms should be required to be the primary contact for complaints, offering simple, multilingual channels with real-time tracking and human escalation, guarantee full refunds (including shipping/taxes) and immediate delisting when goods are illegal.

Establish a regime for platform liability

The proliferation of illicit trade across e-commerce marketplaces and social media platforms demonstrates the limitations of existing regulatory frameworks governing online commercial transactions. While some platforms have introduced voluntary measures to prevent the misuse of their services, these efforts remain fragmented, inconsistently applied and insufficient to deter illicit activity at scale. The persistence of illegal trade underscores the need for stronger government intervention, clearer legal obligations and more effective mechanisms for holding platforms accountable.

Governments should therefore adopt and enforce the standards and obligations outlined in this report, supported by *comprehensive statutory liability provisions that establish clear responsibilities for e-commerce marketplaces and social media platforms to prevent, detect and address illicit trade conducted through their services.*

Reform safe-harbor protections for illicit trade

A critical starting point is the reassessment of existing safe-harbor regimes, which were originally designed to shield online intermediaries from liability for third-party content, subject to certain conditions, including obligations to remove unlawful material upon obtaining the requisite knowledge or notification.

These protections were developed largely around the concept of passive intermediaries that merely host or transmit third-party information. However, the business models and operational capabilities of today's e-commerce marketplaces and social media platforms have evolved considerably beyond this traditional role.

Modern platforms increasingly exercise substantial control over the commercial environment in which transactions occur. They design and manage digital marketplaces; curate, rank and promote product listings; target advertising; facilitate payments; and, in many cases, coordinate warehousing, shipping and returns. Even where platforms do not directly own or operate logistics infrastructure, they establish the conditions of market access, determine fee and commission structures, and deploy algorithms that influence which products are promoted, discovered and purchased.

Where a platform actively structures commercial transactions, directs consumer traffic, facilitates sales and derives economic benefit from those activities, it can no longer reasonably be characterized as a merely passive intermediary. Rather, it has become a central participant in the commercial ecosystem, with both the operational capacity and corresponding responsibility to address illicit activity occurring within that ecosystem.

Evolving judicial recognition of platform responsibility

Courts in several jurisdictions have clarified the limits of intermediary liability protections and reinforced obligations of platforms that exercise control over unlawful commercial activity.

Notable judicial developments include:

- **European Union – *L'Oréal SA v. eBay International AG* (2011).** The Court of Justice of the European Union clarified that an online marketplace may lose liability protections where it plays an active role that gives it knowledge of or control over information relating to unlawful offers, including through assistance in optimizing their presentation or promoting them. The Court also affirmed the importance of expeditious action upon obtaining knowledge of unlawful activity and recognized the availability of injunctions requiring measures to prevent further infringements.
- **China – *Yi Nian Fashion Trading Co. v. Du & Zhejiang Taobao Network Co. Ltd.* (2011).** The court held Taobao liable in connection with its failure to take adequate measures against repeated trademark infringement after receiving notifications. The decision illustrates the potential liability of platforms that fail to respond effectively to known and recurring unlawful activity.
- **India – *IndiaMART InterMESH Ltd. v. PUMA SE (2025).*** The Delhi High Court accepted IndiaMART's characterization of its business-to-business platform as a directory-like intermediary rather than a conventional e-commerce marketplace. Nevertheless, the Court emphasized that intermediary status does not eliminate statutory due-diligence obligations. Platforms must undertake reasonable efforts to prevent unlawful listings, respond promptly to

notifications of infringement and take appropriate measures to prevent repeat listings of previously identified counterfeit products.

- **Brazil – Supreme Federal Court rulings (2025).** Brazil's Supreme Federal Court established a revised framework for determining the civil liability of digital platforms for unlawful third-party content, limiting the scope of protections previously available under the country's Internet Civil Framework. The rulings introduced differentiated responsibilities depending on the nature of the unlawful content and the platform's knowledge or conduct, including heightened obligations in certain serious categories of illegality.

Collectively, these decisions signal a growing judicial recognition that intermediary protections cannot be treated as unconditional immunity from responsibility for unlawful activities facilitated through digital platforms.

Nevertheless, judicial developments alone are insufficient to establish the comprehensive and consistent accountability needed to combat illicit trade at scale. Court decisions are often limited to particular circumstances, categories of unlawful conduct or jurisdiction-specific legal standards. Consequently, they do not necessarily establish the proactive, system-wide obligations required to transform platform governance and compliance practices.

Recommendations for governments

To strengthen platform accountability and ensure that liability frameworks reflect the operational realities of modern digital commerce, governments should incorporate clear and enforceable obligations into national regulatory frameworks.

Priority measures should include:

1. Establish conditions for excluding illicit goods from safe-harbor protections for e-commerce marketplaces and social media platforms. Review and revise intermediary liability regimes to establish clear conditions under which platforms facilitating transactions involving illicit goods may be excluded from liability protections. In particular, protections should not automatically extend to platforms that promote, facilitate or profit from unlawful commercial activity while failing to exercise reasonable due diligence or respond effectively to known risks.
2. Establish a comprehensive regime for platform liability. Governments must establish clear statutory conditions under which platforms may be held accountable for failing to exercise reasonable oversight of commercial activities conducted through their services. Such an approach would also be consistent with established regulatory principles in sectors such as financial services,

transportation and healthcare, where businesses exercising significant control over commercial activities are subject to corresponding duties of care, risk-management requirements and accountability mechanisms.

The objective is not to impose automatic liability on platforms for every unlawful act committed by a third-party seller. Rather, it is to ensure that responsibility is proportionate to the platform's knowledge, control, commercial involvement and capacity to prevent or mitigate illicit activity.

By embedding these principles into national legislation, governments can better align commercial incentives with public safety, consumer protection and market integrity. Clear liability rules, supported by meaningful enforcement, will encourage platforms to deploy their considerable technological, financial and operational capabilities to prevent, detect and disrupt illicit trade.

Ultimately, platforms that exercise significant control over digital commerce must also bear meaningful responsibility for the legality and integrity of the commercial activities they enable.

IX. REFERENCES

1 OECD and European Union Intellectual Property Office (2025). Mapping Global Trade in Fakes 2025.

2 *This chapter examines how online platforms facilitate the sale of regulated products in ways that circumvent established licensing, authorization, and eligibility requirements. The emphasis is on platform-enabled regulatory non-compliance, rather than on the intrinsic legality of the products themselves.*

3 International Alliance for Responsible Drinking. (n.d.). https://iard.org/actions/The-Global-Standards-Coalition. [online] Available at: https://iard.org/actions/The-Global-Standards-Coalition.

4 Digital Guiding Principles: Self-Regulation of Marketing Communications for Beverage Alcohol. (2014).

5 Pesticide Action Network Asia and the Pacific (PANAP), 'New Report: Banned Pesticides Sold on E-Commerce Platforms in Malaysia' (7 June 2023), unpaginated, at https://panap.net/2023/06/new-report-banned-pesticides-sold-on-e-commerce-platforms-in-malaysia/. Pesticide Action Network Asia Pacific

6 Pan Asia Pacific, 'Unboxed: Online Sales of Banned Pesticides in Malaysia' (2023), at https://panap.net/resource/unboxed-online-sales-of-banned-pesticides-in-malaysia/?ind=1686057693536&filename=Unboxed-Online-Sales-of-Banned-Pesticides-in-Malaysia.pdf&wpdmdl=5595&refresh=64d1e9200ee631691478304

7 Information received by industry stakeholders interviewed under this project.

8 Transnational Alliance to Combat Illicit Trade (TRACIT), 'Tackling the Sale of Illicit Pesticides on E-Commerce Platforms: Risks, Challenges and Solutions' (2024), at https://www.tracit.org/tackling-the-sale-of-illicit-pesticides-on-e-commerce-platforms.html

9 TRACIT, 'Tackling the Sale of Illicit Pesticides on E-Commerce Platforms' (2024) at https://www.tracit.org/uploads/1/0/2/2/102238034/tracit_illicitepesticides_ecommerce_april2024_full.pdf

10 TRACIT, 'Tackling the Sale of Illicit Pesticides on E-Commerce Platforms' (2024) at https://www.tracit.org/uploads/1/0/2/2/102238034/tracit_illicitepesticides_ecommerce_april2024_full.pdf

11 TRACIT, 'Tackling the Sale of Illicit Pesticides on E-Commerce Platforms' (2024) at https://www.tracit.org/uploads/1/0/2/2/102238034/tracit_illicitepesticides_ecommerce_april2024_full.pdf

12 [i] UNEP and GRID-Arendal, The Illegal Trade in Chemicals (2020), p. 41, at https://www.grida.no/publications/474.

13 Transnational Alliance to Combat Illicit Trade (TRACIT), Tackling the Sale of Illicit Pesticides on E-Commerce Platforms: Risks, Challenges and Solutions (2024), p. 25, at https://www.tracit.org/uploads/1/0/2/2/102238034/tracit_illicitepesticides_ecommerce_april2024_full.pdf.

14 World Health Organization, 'Substandard and Falsified Medical Products' (n.d.) at https://www.who.int/health-topics/substandard-and-falsified-medical-products

15 U.S. Food and Drug Administration, 'Warning Letter to Amazon.com, Inc. (689355)' (2025) at https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/amazoncom-inc-689355-04172025

16 The FDA warned that misuse of such anesthetic creams can cause serious medical harm due to increased absorption of anaesthetic agents through the skin, especially when used during tattooing or cosmetic procedures without medical supervision.

17 Rivkin Rounds, 'FDA Sends a Message with Two Warning Letters to Amazon' (2024) at https://www.rivkinrounds.com/2024/04/fda-sends-a-message-with-two-warning-letters-to-amazon/

18 The Guardian, 'Manchester Graduate Who Sold Viagra-Style Drugs Online Is Jailed' (2024) at https://www.theguardian.com/uk-news/article/2024/jul/02/manchester-graduate-who-sold-viagra-style-drugs-online-is-jailed

19 World Health Organization, 'Medical Product Alert No. 2/2024: Falsified Ozempic (Semaglutide)' (2024) at https://www.who.int/news/item/19-06-2024-medical-product-alert-n-2-2024--falsified-ozempic-(semaglutide)

20 Europol, 'Gym doping bust: traffickers selling steroids to influencers' (30 March 2023), unpaginated, at https://www.europol.europa.eu/media-press/newsroom/news/gym-doping-bust-traffickers-selling-steroids-to-influencers.

21 National Association of Boards of Pharmacy (NABP), 'Social Media Sites: The New Wild West for Illegal Online Pharmacies' (1 October 2018), at https://nabp.pharmacy/news/news-releases/social-media-sites-the-new-wild-west-for-illegal-online-pharmacies/

22 U.S. Drug Enforcement Administration, 'Social Media Drug Trafficking Threat Overview' (2022) at https://www.dea.gov/sites/default/files/2022-03/20220208-DEA_Social%20Media%20Drug%20Trafficking%20Threat%20Overview.pdf

23 European Commission, 'Commission Opens Formal Proceedings Against AliExpress Under the Digital Services Act' (14 March 2024), unpaginated, at https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1485.; Securing Industry, 'EU Wants Answers from AliExpress About Fake Products' (8 November 2023), unpaginated, at https://www.securingindustry.com/eu-wants-answers-from-aliexpress-about-fake-products/s112/a15769/.

24 Royal United Services Institute (RUSI), 'E-Commerce, Delivery Services and the Illicit Tobacco Trade' (2018) at https://rusi.org/explore-our-research/publications/occasional-papers/e-commerce-delivery-services-and-illicit-tobacco-trade

25 Industry testimony

26 P.D. Dobbs, E.D. Schisler and C. McCormick, '#Discreetshipping: Selling E-cigarettes on TikTok' (2024) Nicotine & Tobacco Research, available at: https://pubmed.ncbi.nlm.nih.gov/38778482/

27 Better Retailing, 'TikTok Fails to Stop Illicit Tobacco Sales' (2024) at https://www.betterretailing.com/tik-tok-fails-to-stop-illicit-tobacco-sales; ITV News, 'Vapes Being Sold on TikTok Shop to Under-18s Disguised as Stationery' (2024) at https://www.itv.com/news/2024-04-08/vapes-being-sold-on-tiktok-shop-to-under-18s-disguised-as-stationery

28 Financial Action Task Force (FATF), 'Money Laundering and Illegal Wildlife Trade' (2020) at https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-laundering-and-illegal-wildlife-trade.pdf

29 Global Initiative Against Transnational Organized Crime, 'Monitoring Online Illegal Wildlife Trade: Setting the Stage' (EcoSolve & GI-TOC, 2024) at https://globalinitiative.net/wp-content/uploads/2024/06/Monitoring-online-illegal-wildlife-trade-Setting-the-stage-EcoSolve-GI-TOC-June-2024.pdf

30 Global Initiative Against Transnational Organized Crime, 'Monitoring Online Illegal Wildlife Trade: Setting the Stage' (EcoSolve & GI-TOC, 2024) at https://globalinitiative.net/wp-content/uploads/2024/06/Monitoring-online-illegal-wildlife-trade-Setting-the-stage-EcoSolve-GI-TOC-June-2024.pdf; Animal Concerns Research and Education Society (ACRES), 'What ACRES Is Doing to Combat Wildlife Crime' (n.d.), section '2021–2023 | Illegal Wildlife Trade on Telegram', available at: https://acres.org.sg/what-acres-is-doing-to-combat-wildlife-crime/ ; Guan Jing and Xu Ling, Deadly Messaging: Illegal Ivory Trade in China's Social Media (TRAFFIC, November 2015), pp. 1–2, available at: https://www.traffic.org/site/assets/files/10442/deadly-messaging.pdf

31 CITES Secretariat, 'Alert: Bat Decorations and Illegal Wildlife Trade Risks' (2024) at https://mcusercontent.com/c9276ae78732e6b7f7bb610ad/files/6dba779a-1c2f-318d-c00a-fdc0c73838b5/00184_ALERT_Bat_decor_IWT_risks.2.pdf

32 End Wildlife Trafficking Online Coalition, 'End Wildlife Trafficking Online' (n.d.) at https://www.endwildlifetraffickingonline.org/

33 Earth.org, 'Illegal Pangolin Trade' (2023) at https://earth.org/illegal-pangolin-trade/;Popular Science, 'Social Media Is Helping Endangered Animals Get Sold' (2024) at https://www.popsci.com/environment/social-media-endangered-animals-for-sale/;Livemint, 'Wildlife Traffickers Use Facebook & Instagram to Find Black Market Buyers' (2019) at https://www.livemint.com/technology/tech-news/wildlife-traffickers-use-facebook-instagram-to-find-black-market-buyers-1562836571339.html; International Fund for Animal Welfare (IFAW), 'How a Daring Team Stops Illegal Trade of Endangered Wildlife in Indonesia' (2023) at https://www.ifaw.org/au/journal/how-a-daring-team-stops-illegal-trade-of-endangered-wildlife-in-indonesia; Madras Courier, 'Critically Endangered Pangolins Are Still Being Sold on Social Media – Will It Stop?' (2022) at https://madrascourier.com/environment/critically-endangered-pangolins-are-still-being-sold-on-social-media-will-it-stop/

34 Livemint, 'Wildlife Traffickers Use Facebook & Instagram to Find Black Market Buyers' (2019) at https://www.livemint.com/technology/tech-news/wildlife-traffickers-use-facebook-instagram-to-find-black-market-buyers-1562836571339.html

35 TRAFFIC, 'New research shows alarming levels of online illegal wildlife trade in Vietnam' (2024) at https://www.traffic.org/site/assets/files/26050/traffic_stw_online_report_en_final_compressed-1.pdf

36 CNBC, 'The Fight Against Stolen Products on Amazon and Facebook Marketplace' (2022) at https://www.cnbc.com/2022/06/17/the-fight-against-stolen-products-on-amazon-and-facebook-marketplace.html

37 Meg Moore, 'The Future of Retail: Adapting to the Evolving Threat of Organized Retail Crime', LiveView Technologies (11 December 2023), available at: https://www.lvt.com/blog/retail-adapting-to-evolving-threat-organized-retail-crime

38 Retail Industry Leaders Association (RILA), 'CEO Letter on the INFORM Consumers Act' (2021) at https://rilastagemedia.blob.core.windows.net/rila-web/rila.web/media/media/pdfs/letters%20to%20hill/2021/ceo-inform-consumers-act-final1.pdf

39 U.S. Congress, House of Representatives, Combating Organized Retail Crime Act, H.R. 2853, 119th Congress (introduced 10 April 2025), available at: https://www.govinfo.gov/app/details/BILLS-119hr2853ih; U.S. Congress, Senate, Combating Organized Retail Crime Act, S. 1404, 119th Congress (introduced 10 April 2025), available at: https://www.govinfo.gov/app/details/BILLS-119s1404is

40 Integrity, Notification, and Fairness in Online Retail Marketplaces for Consumers Act (INFORM Consumers Act), 15 U.S.C. § 45f(a)–(d), available at: https://www.govinfo.gov/link/uscode/15/45f

41 Valleau, L. (2026). Pillages : Vinted, Amazon, Leboncoin… le gouvernement réunit les plates-formes pour éviter la revente de produits volés. [online] leparisien.fr. Available at: https://www.leparisien.fr/economie/consommation/pillages-vinted-amazon-leboncoin-le-gouvernement-reunit-les-plates-formes-pour-eviter-la-revente-de-produits-voles-19-10-2026-LVHP3V6ZFJHSBOWGGMLHXCJJ5I.php.

42 Race, M. (2026). Vinted blocks French looters listing stolen goods for sale. [online] Bbc.com. Available at: https://www.bbc.com/news/articles/cm8xzrljv72ro.

43 Thibaut Déléaz (2026). Violences du 17 octobre : ce que Vinted, Leboncoin et eBay se sont engagées à faire pour éviter le recel des produits pillés. [online] Le Figaro. Available at: https://www.lefigaro.fr/conso/violences-du-17-octobre-ce-que-vinted-leboncoin-et-ebay-se-sont-engagees-a-faire-pour-eviter-le-recel-des-produits-pilles-20261020.

44 New York Post, 'eBay and Facebook Marketplace Fuel NYC's Shoplifting Economy' (2024) at https://nypost.com/2024/03/21/us-news/ebay-and-facebook-marketplace-fuel-nycs-shoplifting-economy/

45 Ernesto Lopez, Robert Boxerman and Kelsey Cundiff, 'Shoplifting Trends: What You Need to Know', Council on Criminal Justice (November 2023), unpaginated, at https://counciloncj.org/shoplifting-trends-what-you-need-to-know/.

46 The Independent, 'Shops Buying Stolen Goods from Professional Shoplifters, Retail Groups Say' (2024) at https://www.independent.co.uk/business/shops-buying-stolen-goods-from-professional-shoplifters-retail-groups-say-b2603885.html

47 Suffolk County District Attorney's Office, 'Brentwood Pawn Shop Owner and Three Associates Arrested and Charged for Running Organized Retail Theft Ring' (9 August 2022), available at: https://www.suffolkcountyda.org/brentwood-pawn-shop-owner-and-three-associates-arrested-and-charged-for-running-organized-retail-theft-ring/; Suffolk County District Attorney's Office, 'Brentwood Pawnshop Owner and Three Co-Defendants Plead Guilty to Operating an Organized Retail Theft Ring' (11 September 2023), available at: https://www.suffolkcountyda.org/brentwood-pawnshop-owner-and-three-co-defendants-plead-guilty-to-operating-an-organized-retail-theft-ring/

48 Alvarez Technology Group, 'Organized Theft' (n.d.), available at: https://www.alvareztg.com/organized-theft/

49 U.S. Department of Justice, 'Two Indicted for Buying Stolen Goods and Selling Them Online on Amazon or eBay for More Than $3 Million' (11 July 2024), available at: https://www.justice.gov/usao-wdwa/pr/two-indicted-buying-stolen-goods-and-selling-them-online-amazon-or-ebay-more-3-million

50 European Parliament and Council, 'Regulation (EC) No. 1223/2009 on Cosmetic Products' (2009) at https://eur-lex.europa.eu/eli/reg/2009/1223/oj/eng

51 UK Food Standards Agency, 'Food Crime Strategic Assessment' (2020) at https://www.food.gov.uk/sites/default/files/media/document/food-crime-strategic-assessment-2020.pdf; BBC News, 'Facebook: Home Food Businesses Concern FSA Watchdog' (24 February 2020), unpaginated, at https://www.bbc.com/news/uk-51475289.

52 Lao Động News, 'Cục An Toàn Thực Phẩm Yêu Cầu Shopee & Lazada Ngừng Bán Sản Phẩm Chưa Đăng Ký' (2025), available at: https://news.laodong.vn/suc-khoe/cuc-an-toan-thuc-pham-yeu-cau-shopee-lazada-ngung-ban-san-pham-chua-dang-ky-1513580.ldo

53 U.S. Food and Drug Administration, 'Warning Letter to Amazon.com, Inc. (689355)' (2025) at https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/amazoncom-inc-689355-04172025

54 Nicole Dunn, 'A Dupe or Just Duped?: An Analysis of the History and Policy Behind Counterfeit Cosmetics and Social Media's Role in Perpetuating its Sales' (2024), vol. 20, pp. 92–118, available at: https://bpb-us-e1.wpmucdn.com/sites.suffolk.edu/dist/e/1232/files/2025/01/12-Dunn.pdf

55 DIA Global Forum, 'Cosmetovigilance: Safeguarding Consumer Health in the Global Beauty Market' (2025) at https://globalforum.diaglobal.org/issue/february-2025/cosmetovigilance-safeguarding-consumer-health-in-the-global-beauty-market/

56 Which?, 'At Least Two-Thirds of Cosmetics We Bought from Online Marketplaces Are Likely Counterfeits' (24 July 2025), available at: https://www.which.co.uk/news/article/at-least-two-thirds-of-cosmetics-we-bought-from-online-marketplaces-are-likely-counterfeits-a6DmA3P3BjhV

57 Gabrielle Fonrouge and Paige Tortorelli, 'Walmart's Marketplace Boom: How Lax Vetting Came with Identity Theft and Fakes', CNBC (19 September 2025, updated 22 September 2025), available at: https://www.cnbc.com/2025/09/19/walmart-marketplace-fakes-scams-investigation.html

58 Tests showed PFAS in jackets at more than 3,000 times the legal limit, phthalates in children's shoes and clothing at up to 200 times the limit, and lead and cadmium in footwear exceeding EU thresholds — chemicals that can impair brain development, lower IQ, damage kidneys and reproductive organs, and accumulate in the body over time. Even a children's mermaid costume exceeded formaldehyde limits by 3.5×, exposing kids to a carcinogenic compound that can cause DNA damage and respiratory irritation. Read more at https://www.greenpeace.org/eu-unit/issues/pollution/47807/new-report-hazardous-chemicals-in-shein-clothing-continue-to-violate-eu-limits/

59 Danish Consumer Council Think Chemicals, Avoid slime toy bought outside the EU, 1 November 2024, available at: https://taenk.dk/kemi/visit-our-english-version/avoid-slime-toy-bought-outside-eu

60 By way of illustration, the EU frames product safety as serving both high levels of protection and the functioning of the internal market.

61 Organisation for Economic Co-operation and Development (OECD), Online Product Safety Sweep Report, OECD Digital Economy Papers, No. 354 (26 June 2023), available at: https://www.oecd.org/en/publications/online-product-safety-sweep-report_c1faa51e-en.html

62 Channel News Asia, 'Baby Cots, Strollers and Accessories Found Unsafe in CCS Tests; Lazada & Shopee Listings Removed' (2025), available at: https://www.channelnewsasia.com/singapore/baby-cots-strollers-accessories-unsafe-ccs-lazada-shopee-5464306

63 Which?, 'Illegal and Dangerous Plug-In Mini Heaters for Sale on Online Marketplaces' (2024) at https://www.which.co.uk/news/article/illegal-and-dangerous-plug-in-mini-heaters-for-sale-on-online-marketplaces-a8pu66r0ZAlG

64 Euroconsumers, 'Systemic Failures in Product Compliance on Temu and SHEIN' (3 November 2025), available at: https://www.euroconsumers.org/systemic-failures-in-product-compliance-on-temu-and-shein/

65 Toy Industries of Europe (TIE), '95% of Toys Bought from New Online Platform Break EU Safety Rules' (2024) at https://www.toyindustries.eu/95-of-toys-bought-from-new-online-platform-break-eu-safety-rules/

66 Euroconsumers, 'Systemic Failures in Product Compliance on Temu and SHEIN' (3 November 2025), available at: https://www.euroconsumers.org/systemic-failures-in-product-compliance-on-temu-and-shein/

67 Euroconsumers, 'Systemic Failures in Product Compliance on Temu and SHEIN' (3 November 2025), available at: https://www.euroconsumers.org/systemic-failures-in-product-compliance-on-temu-and-shein/

68 The Guadian, 'EU accuses China's AliExpress of systemic failure on illegal goods' (2025), available at https://www.theguardian.com/business/2025/jun/18/eu-accuses-china-aliexpress-of-systemic-failure-illegal-goods

69 Office for Product Safety and Standards (OPSS), 'Product Recall: Lithium-Ion Battery Charger sold via TikTok (2504-0019)' (21 May 2025) https://www.gov.uk/product-safety-alerts-reports-recalls/product-recall-lithium-ion-battery-charger-sold-via-tiktok-2504-0019

70 U.S. PIRG Education Fund, 'Trouble in Toyland 2024: Unsafe Toys That Slip Through the Border' (2024) at https://pirg.org/edfund/resources/trouble-in-toyland-2024-unsafe-toys-that-slip-through-border/

71 European Commission, 'Commission Accepts Commitments Offered by AliExpress Under the Digital Services Act and Takes Further Action on Illegal Products' (18 June 2025), pp. 1–2, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1551; Jennifer Rankin, 'EU Accuses China's AliExpress of "Systemic Failure" over Illegal Goods', The Guardian (18 June 2025), unpaginated, at https://www.theguardian.com/business/2025/jun/18/eu-accuses-china-aliexpress-of-systemic-failure-illegal-goods.

72 Office of the United States Trade Representative (USTR), 2024 Review of Notorious Markets for Counterfeiting and Piracy (8 January 2025), p. 18, available at: https://ustr.gov/sites/default/files/2024%20Review%20of%20Notorious%20Markets%20of%20Counterfeiting%20and%20Piracy%20(final).pdf

73 Amazon. (2026). Trustworthy Shopping Experience Report available at: https://trustworthyshopping.aboutamazon.com/2025-trustworthy-shopping-experience-report

74 Tokopedia, IP Protection Report H1 2023 (2023), pp. 6 and 8, available at: https://assets.tokopedia.net/asts/ipp/IP-Protection-Report-H1-2023.pdf

75 Mercado Libre. Privacy Notice and Data Confidentiality, Available at: https://www.mercadolibre.com/privacy/privacy-notice; Mercado Libre, "How we protect intellectual property at Mercado Libre". Available at: https://global-selling.mercadolibre.com/learning-center/news/check-how-we-protect-intellectual-property-on-mercado-libre

76 AliExpress. (2026). AliExpress.com Privacy Policy, effective 30 July 2026, Sections A–B Available at: https://terms.alicdn.com/legal-agreement/terms/suit_bu1_aliexpress/suit_bu1_aliexpress201909171350_82407.html; AliExpress, Terms and Conditions for Platform Transactions by EU/EEA/UK Consumers (updated 30 June 2026, effective 15 July 2026), section 6.1, 'Personalized Recommendations', available at: https://cdn.contract.alibaba.com/terms/EU_EE_UK_platform_service_agreement/20250514112355975/20250514112355975.html

77 Gabrielle Fonrouge and Paige Tortorelli, '5 Takeaways from CNBC's Investigation into Walmart Marketplace', CNBC (19 September 2025), available at: https://www.cnbc.com/2025/09/19/walmart-marketplace-fakes-scams-investigation-takeaways.html

78 Federal Trade Commission, 'Informing Businesses about the INFORM Consumers Act' (June 2023), available at: https://www.ftc.gov/business-guidance/resources/INFORMAct

79 Instagram, 'Commerce Eligibility Requirements' (n.d.), available at: https://help.instagram.com/1627591223954487

80 Transnational Alliance to Combat Illicit Trade (TRACIT), Tackling the Sale of Illicit Pesticides on E-Commerce Platforms: Risks, Challenges and Solutions (April 2024), pp. 16, 41–44 and 57–58, available at: https://www.tracit.org/uploads/1/0/2/2/102238034/tracit_illicitepesticides_ecommerce_april2024_full.pdf

81 MarketWatch, "Weight loss has become the hottest new Chinese consumer craze," 8 September 2025, available at: https://www.marketwatch.com/story/weight-loss-has-become-the-hottest-new-chinese-consumer-craze-4d9d70fb

82 Vanity Fair, "Why counterfeit Ozempic is a global-growth industry," Vanity Fair, 4 June 2024, available at: https://www.vanityfair.com/news/story/counterfeit-ozempic-global-growth-industry

83 European Medicines Agency (EMA), 'Warning About Sharp Rise in Illegal Medicines Sold in the EU' (2024) at https://www.ema.europa.eu/en/news/warning-about-sharp-rise-illegal-medicines-sold-eu

84 European Medicines Agency (EMA), 'Warning About Sharp Rise in Illegal Medicines Sold in the EU' (3 September 2025), available at: https://www.ema.europa.eu/en/news/warning-about-sharp-rise-illegal-medicines-sold-eu

85 The Guardian," TikTok influencers fuelling parallel market for unlicensed weight-loss drug" Available at: https://www.theguardian.com/money/2025/oct/11/tiktok-influencers-telegram-whatsapp-parallel-market-unlicensed-weight-loss-drug-retatrutide-uk

86 Meta Platforms, 'Intellectual Property Across Meta Platforms' (n.d.), section 'Repeat Intellectual Property Infringer Policy', available at: https://www.meta.com/en-gb/help/policies/3234337743488413/

87 Meta Platforms, 'Facebook Commerce Policies' (n.d.) at https://www.facebook.com/policies_center/commerce

88 European Commission, 'Commission Accepts Commitments Offered by AliExpress Under the Digital Services Act and Takes Further Action on Illegal Products' (18 June 2025), available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1551; Digital Policy Alert, 'European Commission Accepted AliExpress's Commitments Under Digital Services Act and Issued a Preliminary Finding That It Violates Its Obligation to Assess and Mitigate Risks Related to the Dissemination of Illegal Products' (2025) at https://digitalpolicyalert.org/event/31152-european-commission-accepted-aliexpresss-commitments-under-digital-services-act-and-issued-a-preliminary-finding-that-violates-its-obligation-to-assess-and-mitigate-risks-related-to-the-dissemination-of-illegal-products

89 European Commission, 'Commission Opens Formal Proceedings Against Temu Under the Digital Services Act' (31 October 2024), p. 1, available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_5622/IP_24_5622_EN.pdf

90 Transnational Alliance to Combat Illicit Trade (TRACIT), Exposing Supply Chain Vulnerabilities to Illicit Trade (2023), p. 167, available at: https://www.tracit.org/uploads/1/0/2/2/102238034/tracit_exposing_supply_chain_vulnerabilities_to_illicit_trade_nov2023_full_report.pdf

91 AMLEGALS, 'Counterfeiting of Products on E-Commerce Platforms' (2023) at https://amlegals.com/counterfeiting-of-products-on-e-commerce-platforms/

92 Standing Committee of the National People's Congress, E-Commerce Law of the People's Republic of China (2018), Articles 31, 38(1), 42, 45, 83, 84 and 89, available at: https://www.cac.gov.cn/2018-09/01/c_1123362506.htm

93 Transnational Alliance to Combat Illicit Trade (TRACIT), Exposing Supply Chain Vulnerabilities to Illicit Trade (2023), p. 167, available at: https://www.tracit.org/uploads/1/0/2/2/102238034/tracit_exposing_supply_chain_vulnerabilities_to_illicit_trade_nov2023_full_report.pdf

TRANSNATIONAL ALLIANCE
TO COMBAT ILLICIT TRADE
TRACIT.ORG

Transnational Alliance to Combat Illicit Trade
9 East 8th Street #201, New York, NY 10003
+1.917.815.2824 I info@TRACIT.org I TRACIT.org