

CIS BRAND BRIEFING NO. 2

Do Marketplace Counterfeits Really Threaten National Security?

Yes, and the government said so first. What it found, why marketplaces make it harder, and when a counterfeit case becomes a national security matter.

WRITTEN BY	PUBLISHED	CONTACT
Chris Anderson, Ph.D. Founder and CEO, Cyber Investigation Services	October 2026	chris@cyberinvestigationservices.com

THE SHORT ANSWER

Yes. The government said so first. In 2020 the Department of Homeland Security warned that illicit goods sold through online marketplaces “threaten public health and safety, as well as national security.”¹

Since then, Treasury has warned that illicit trade, which it defines broadly enough to cover counterfeits, is weakening national security. The border is seizing more fakes than ever. The government has suspended the package loophole that most of those fakes came through. Since the package rule, no comparable step has made it harder for a seller to hide or reappear.

WHAT THE GOVERNMENT HAS SAID

At first glance, counterfeiting looks like nothing more than lost revenue for the manufacturer, not something worth the federal government’s attention. DHS saw more: “Counterfeits threaten national security and public safety directly when introduced into government and critical infrastructure supply chains, and indirectly if used to generate revenue for transnational criminal organizations.”² The report names three kinds of risk.

- **Funding crime.** DHS described “intricate links between the sale of counterfeit goods and transnational organized crime.” It added that counterfeit proceeds “may be supporting terrorism and dictatorships throughout the world.”³

- **Supply chains.** “One of the greatest threats counterfeits pose to national security is their entry into the supply chain of America’s defense industrial base.”⁴
- **Health and safety.** DHS warned of fake prescription opioids “often laced with deadly fentanyl” and of children’s toys “laced with deadly metals like cadmium and lead.”⁵

The same report described how these sellers work. It said “listing goods on well-known platforms provides an air of legitimacy.” It said sellers abroad face “relatively little risk of criminal prosecution or civil liability.” And it found some sellers “preemptively establishing multiple virtual store-fronts.”⁶

Treasury’s 2026 money laundering risk assessment added a section on illicit trade that its 2024 edition did not have. It describes illicit trade as trafficking in “stolen, illicit, or regulated goods,” broadly enough to cover counterfeits. It says illicit trade is “weakening national security.”⁷

1 U.S. Department of Homeland Security, “Combating Trafficking in Counterfeit and Pirated Goods,” Report to the President, January 24, 2020, Foreword, p. 3. https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf

2 Same report as note 1, p. 7.

3 Same report as note 1, p. 19. The hedge is the report’s own, and DHS footnotes the terrorism sentence to the UN Office on Drugs and Crime.

4 Same report as note 1, p. 20.

5 Same report as note 1, p. 17 (opioids) and p. 18 (toys).

6 Same report as note 1, p. 20 (“air of legitimacy” and “relatively little risk”) and p. 22 (“multiple virtual store-fronts” and “little identifying information”).

7 U.S. Department of the Treasury, 2026 National Money Laundering Risk Assessment, March 2026, Section VII, “Illicit Trade,” p. 32. The quoted phrases are the assessment’s own. The section does not name counterfeits. Counterfeit goods are among the illicit goods it describes. Its 2024 edition contains no section on illicit trade. The 2026 edition adds one. <https://home.treasury.gov/system/files/246/2026-NMLRA.pdf>

WHO PROFITS FROM ILLICIT TRADE

DHS raised terrorism and dictatorships in 2020, with its own hedge. Since then, federal agencies have been more specific about who profits from illicit trade.

Transnational criminal organizations. Treasury’s 2026 assessment says illicit trade “attracts criminal organizations of all sizes and levels of sophistication.” It adds: “For TCOs, this can also be a way to diversify illicit revenue streams and expand their areas of influence.” TCOs are transnational criminal organizations. The same assessment describes “payments for counterfeit goods” that are “disguised as ordinary sales by routing them through a seemingly legitimate merchant account.”⁸

Cartels. FinCEN warned in August 2025 that Chinese money laundering networks move drug money for the Jalisco New Generation, Sinaloa and Gulf cartels partly through goods: “According to law enforcement, CMLNs may sell goods in the United States through various online marketplaces, at front companies, or at businesses complicit in their schemes.”⁹ That scheme involves genuine goods, not counterfeits.

State actors. The FBI states: “The counterintelligence and economic espionage efforts emanating from the government of China and the Chinese Communist Party are a grave threat to the economic well-being and democratic values of the United States. ... Confronting this threat is the FBI’s top counterintelligence priority.” The same page names “systematic theft of intellectual property” among the Chinese government’s methods. It also says: “To be clear, the adversary is not the Chinese people or people of Chinese descent or heritage.”¹⁰ The FBI page does not address counterfeit consumer goods. The government also publishes the

companies it has designated. Its lists cover Chinese military companies, companies tied to forced labor under the Uyghur Forced Labor Prevention Act, and people and companies under Treasury sanctions.¹¹ A claimed home country is not an indicator by itself. A name on one of those lists is.

⁸ Same assessment as note 7, p. 32 (“attracts criminal organizations” and “For TCOs”) and p. 66, on “transaction laundering”: “In a typical transaction laundering scheme, illicit payments (e.g., payments for counterfeit goods, illegal drugs, gambling, etc.) are disguised as ordinary sales by routing them through a seemingly legitimate merchant account.”

⁹ Financial Crimes Enforcement Network, “FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds,” FIN-2025-A003, August 28, 2025. CMLNs are Chinese money laundering networks. The cartels are named on p. 1. The online marketplace route is on p. 7. The advisory’s red flags for trade-based money laundering schemes are on p. 10. The scheme it describes involves genuine U.S. goods bought with illicit funds. It does not describe counterfeits. <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2025-a003>

¹⁰ Federal Bureau of Investigation, “The China Threat,” accessed October 6, 2026. <https://www.fbi.gov/investigate/counterintelligence/the-china-threat>

¹¹ Examples of the U.S. government lists meant, each accessed September 28, 2026. Department of Defense, “Notice of Availability of Designation of Chinese Military Companies,” 91 FR 35189, June 10, 2026 (the Section 1260H list), at <https://www.federalregister.gov/d/2026-11571> and the Department of Homeland Security’s UFLPA Entity List, at <https://www.dhs.gov/uflpa-entity-list> and the Treasury Office of Foreign Assets Control’s Specially Designated Nationals and Blocked Persons List, at <https://sanctionslist.ofac.treas.gov/Home/SdnList>

WHY MARKETPLACES MAKE IT HARDER

The American ecommerce marketplaces are open to exploitation in ways no single company can close alone. Three reasons matter most.

Who the seller really is. DHS found that “on at least some e-commerce platforms, little identifying information is necessary for a counterfeiter to begin selling.”⁶ One federal law now covers this, the INFORM Consumers Act, and it has gaps. Once a seller passes \$20,000 a year, shoppers are supposed to see its name and address.¹² But a seller can self-certify a returns address and show shoppers a rented warehouse dock instead of itself. A seller claiming only a home address shows nothing but a country and state.¹³ The Act puts its penalties on the marketplace, not on a seller who lies to it. The first federal INFORM case, settled in 2025, was over how seller information was shown.¹⁴

Where the product came from. A marketplace can demand that a seller prove where its product came from. The brand being copied cannot. Outside a lawsuit, it has no legal way to force a seller to show its sourcing, and no right to see what the seller showed the marketplace. The marketplace’s check can be spoofed too. An industry of fake-invoice services exists to do exactly that, and Amazon has sued six of them.¹⁵

Enforcement removes a product, not a seller. Brand protection in practice means stopping a seller from selling the one product it got caught counterfeiting. A takedown often reaches one listing, not the seller’s others. Prosecutions and lawsuits are rare. Pursuing an anonymous overseas seller is slow and costly.

None of this means marketplaces are idle. Amazon alone invested more than \$1 billion in 2024 to counter counterfeiting, fraud and other abuse.¹⁶ Still, put together, these gaps leave room for an illicit seller or an organized network to operate at scale.

¹² Integrity, Notification, and Fairness in Online Retail Marketplaces for Consumers Act, 15 U.S.C. § 45f, in force June 27, 2023. Collection and verification at 45f(a)(1) and (a)(2). The high-volume test is at 45f(f)(3). The consumer disclosure and its “\$20,000 or more in annual gross revenues” threshold are at 45f(b)(1). <https://www.law.cornell.edu/uscode/text/15/45f>

13 Same statute, 45f(b)(2)(A). Clause (ii) is the returns-address route: a seller that “certifies to the online marketplace that the seller is a business that has a physical address for product returns” may have that returns address shown in place of its own. Clause (i) is the residential route, under which the marketplace may disclose “only the country and, if applicable, the State in which such seller resides.”

14 Same statute, 45f(c)(1) (“A violation of subsection (a) or (b) by an online marketplace”) and 45f(d)(1) (a state attorney general may sue “any online marketplace”). 45f(c)(2)(B) does extend the Act’s penalties to “any person that violates subsection (a) or (b),” but the duties those subsections impose fall on the online marketplace, not on the seller, so a seller’s false certification is not itself a violation of them. Other federal law may still reach a seller who lies. *United States v. Whaleco, Inc., d/b/a Temu*, No. 1:25-cv-12466 (D. Mass.), filed September 5, 2025 by the Department of Justice on a Federal Trade Commission referral, settled for a \$2 million civil penalty. That case was about how seller information was shown, not whether it was true. The terms here are taken from the published case summary at <https://www.mcdermottlaw.com/insights/ftc-settles-first-inform-consumers-act-case-over-online-marketplace-disclosure-violations/>

15 *Amazon.com, Inc. v. Ali*, No. 2:23-cv-01062 (W.D. Wash., filed July 17, 2023), Amazon’s own complaint. An allegation, not an adjudicated finding. Amazon, “The latest updates from Amazon’s Counterfeit Crimes Unit,” entry dated June 11, 2024, accessed September 1, 2026. Amazon’s own civil suits, not government actions. <https://www.aboutamazon.com/news/policy-news-views/amazon-counterfeit-crimes-unit-latest-updates-2024>

16 Amazon, 2024 Brand Protection Report, Amazon’s own account of its spending against “counterfeit, fraud, and other forms of abuse.” <https://trustworthyshopping.aboutamazon.com/2024-brand-protection-report>

WHAT THE GOVERNMENT HAS DONE, AND THE GAP

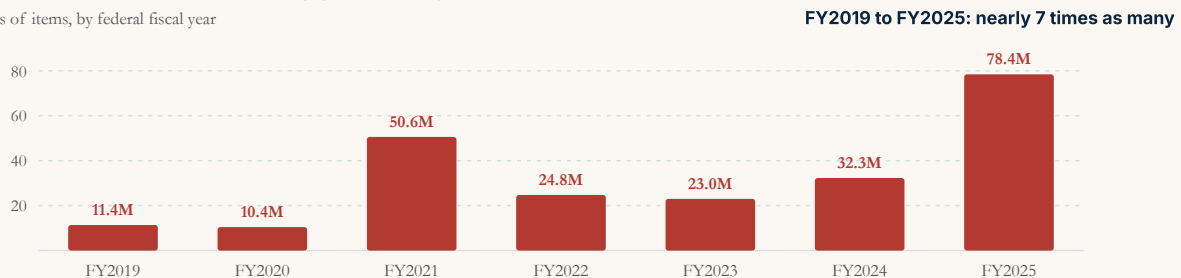
DHS warned in 2020 that sellers “spread the risk of seizure across a number of low-value packages.”¹⁷ Since then, the border has seized more counterfeit items than ever (Figure 1).

Figure 1. What the border caught

Source: U.S. Customs and Border Protection, Intellectual Property Rights Seizure Statistics. These figures show where the government looked and what it caught. They do not measure how many fakes exist.

COUNTERFEIT AND PIRATED ITEMS SEIZED BY CBP

Millions of items, by federal fiscal year



The count is not a steady climb. It spikes in fiscal 2021, falls back through fiscal 2023, then rises to its peak.

The government has moved against the package. Executive Order 14324 suspended duty-free de minimis treatment for every country effective August 29, 2025. The order itself does not mention counterfeits. Its reason is that “the risks of evasion, deception, and illicit-drug importation are particularly high for low-value articles.”¹⁸

Counterfeits were part of the picture all the same. The White House fact sheet for that order reported that de minimis shipments produced “97% of intellectual property rights seizures, totaling 31 million counterfeit items” in fiscal 2024.¹⁹ In June 2026, CBP made the suspension indefinite by interim final rule. Congress had already set its permanent end for July 1, 2027.²⁰

That action attacks the package, not the seller. The same seller can ship again under a different name, a different address, or from a domestic warehouse. That gap is where the risks DHS described remain.

17 Same report as note 1, p. 24.

18 Executive Order 14324, “Suspending Duty-Free De Minimis Treatment for All Countries,” 90 Fed. Reg. 37775 (Aug. 5, 2025), signed July 30, 2025, effective 12:01 a.m. EDT Aug. 29, 2025. The quoted phrase is the order’s own. <https://www.govinfo.gov/content/pkg/FR-2025-08-05/html/2025-14897.htm>

19 The White House, “Fact Sheet: President Donald J. Trump is Protecting the United States’ National Security and Economy by Suspending the De Minimis Exemption for Commercial Shipments Globally,” July 30, 2025. The quoted figures are the fact sheet’s own. <https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-is-protecting-the-united-states-national-security-and-economy-by-suspending-the-de-minimis-exemption-for-commercial-shipments-globally/>

20 U.S. Customs and Border Protection, interim final rules of June 24, 2026: RIN 1685-AA44, 91 Fed. Reg. 37789 (all modes other than international post, effective June 24, 2026) and RIN 1685-AA45, 91 Fed. Reg. 37801 (international postal network, effective July 24, 2026). Each rule “amends the ... regulations to implement an indefinite suspension of the de minimis administrative exemption for imports valued at \$800 or less.” The statutory end date of July 1, 2027 is from the rules’ own recital of the July 4, 2025 Act. <https://www.federalregister.gov/d/2026-12670>

21 U.S. Customs and Border Protection, Intellectual Property Rights Seizure Statistics, fiscal years 2019 through 2025. CBP reports both seizures and seizure lines, which are different units, so seizure counts are not plotted here. Quantity is. The item figures for fiscal 2019 through 2023 are from the series CBP published retrospectively in its fiscal 2023 report. <https://www.cbp.gov/trade/priority-issues/ipr/statistics>

WHEN A COUNTERFEIT CASE IS A NATIONAL SECURITY MATTER

A product buy proves counterfeiting. It does not prove a national security threat. A confirmed counterfeit case becomes a possible national security matter when the record also shows at least one of the indicators below. They are the kind investigators and the government look for, not findings about any seller. CIS supplies intelligence on who is selling, how much and where. Others investigate.

- **Ties to PRC state-linked entities.** The seller, its owner, its supplier or its importer of record is, or is owned by, a company on a U.S. government list, such as the Defense Department’s list of Chinese military companies or the UFLPA Entity List.¹¹
- **Transnational criminal organization indicators.** One operator hiding behind storefronts under different names in more than one country, nominee or shell owners, or links to people or companies named in public organized-crime cases.
- **Sanctions exposure.** A seller, owner or supplier that appears on a Treasury sanctions list.
- **Trade-based money laundering patterns.** Import or payment records that do not fit the goods sold, matching a FinCEN trade-based money laundering red flag.⁹ Fund flows are for the government to test.
- **Health and safety harm.** A confirmed counterfeit in a category where a fake can hurt someone, plus evidence of harm beyond the category itself. That means a documented injury or illness, a matching recall or safety warning, or a lab result showing a hazard.

Any one of these warrants a closer look. What the government acts on is for the government to decide.

WHAT THIS MEANS FOR A BRAND

The national security risk comes from the sellers DHS described: hard to reach, quick to open a new storefront, and selling under a real brand’s name. At CIS we fight counterfeits because they make ecommerce a consumer safety and national security problem. For a brand, the sellers who threaten your customers are the same sellers this paper is about. Finding out who is selling fakes under your name is where both problems start to get solved.

PUT YOUR BRAND ON OUR FREE WATCH LIST

If counterfeiters are selling under your brand, you should know it before your customers do. We always watch for free. When fakes put your customers at risk, we warn you and send you a CIS Consumer Safety Review: who is selling, where they ship from, and what it would take to stop them.

We package the intelligence to attract contingency attorneys to take your case. Our fee comes only from the recovery. Many counterfeiting problems can be resolved with no money out of your pocket: the attorney pays the upfront costs and takes them back from what is collected. Put your brand on our free Watch List at cyberinvestigationsservices.com/watch-list.

About the author. Chris Anderson, Ph.D., founded Cyber Investigation Services, a Florida limited liability company, in 2010 and leads it as CEO. CIS is an eCommerce consumer safety and national security intelligence firm. For 16 years Chris has built intelligence on the sellers behind counterfeit marketplace listings.