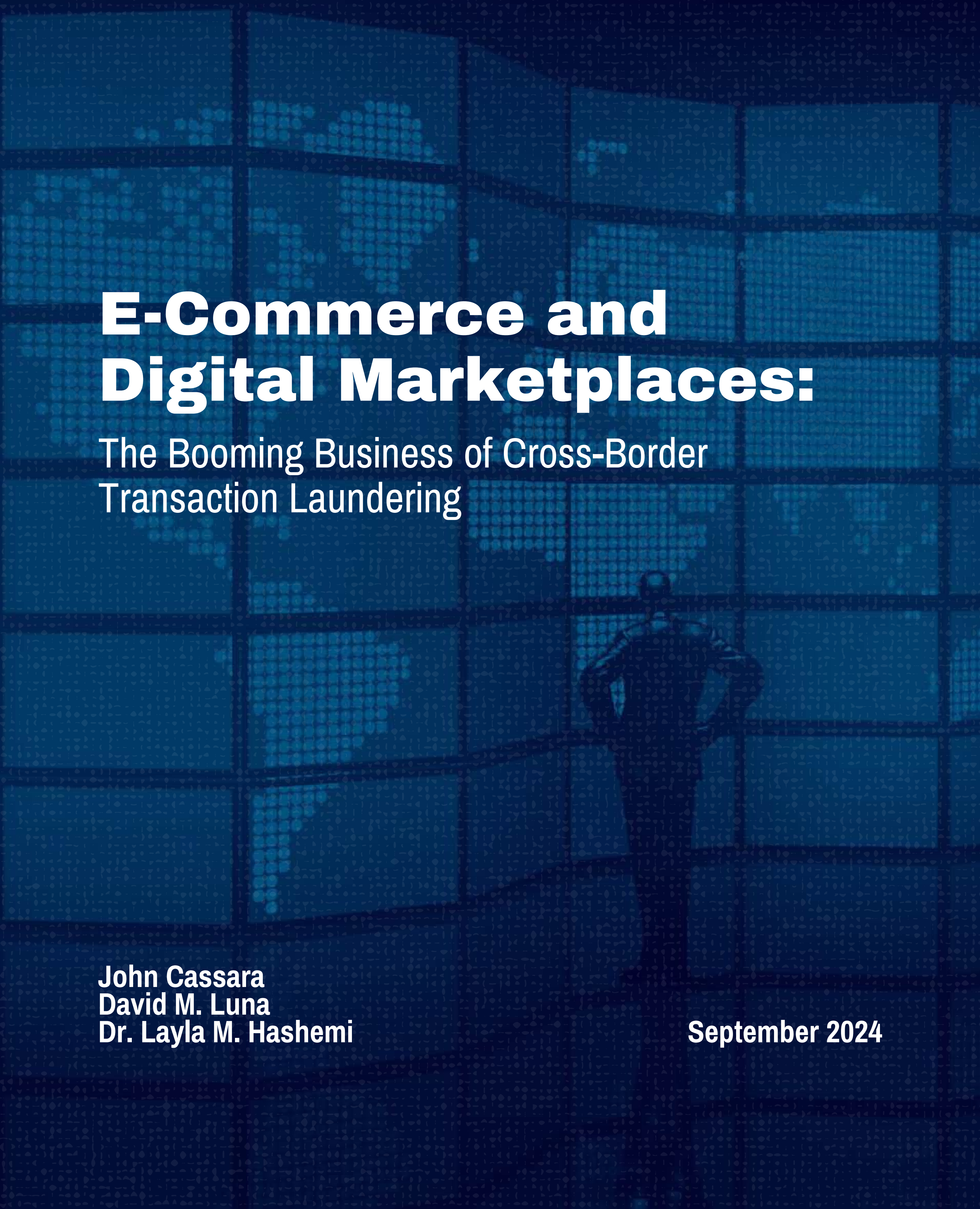


ICAIE

E-Commerce and Digital Marketplaces:

The Booming Business of Cross-Border Transaction Laundering

John Cassara
David M. Luna
Dr. Layla M. Hashemi

September 2024

Executive Summary

Criminals, counterfeiters, illicit threat networks, and money launderers are reaping hundreds of billions of dollars in profit every year from criminality across today's hubs of illicit trade, global supply chains, and e-commerce platforms. Even before the recent COVID-19 pandemic, illicit trade in the digital world and across e-commerce platforms was becoming quite lucrative. This is increasingly true due to the relative ease of gaining access to sell counterfeits and illicit goods across an array of e-commerce platforms, social media, encrypted messaging apps, online-marketplaces, and other digital shopping streams. Today, counterfeits, pirated and stolen products, and other illicit goods and contraband transverse borders and communities, and enter our supply chains, businesses, and homes.

The economic, security, social, and environmental impacts of illicit goods are serious and multi-dimensional threats. They help fuel transnational corruption and crime and greater insecurity while also endangering the health and safety of consumer-citizens around the world. Approximately 87% of consumers who bought a counterfeit product have suffered some sort of negative consequences, ranging from defective products and financial losses and, in some cases, severe illnesses and serious physical injuries.[1]

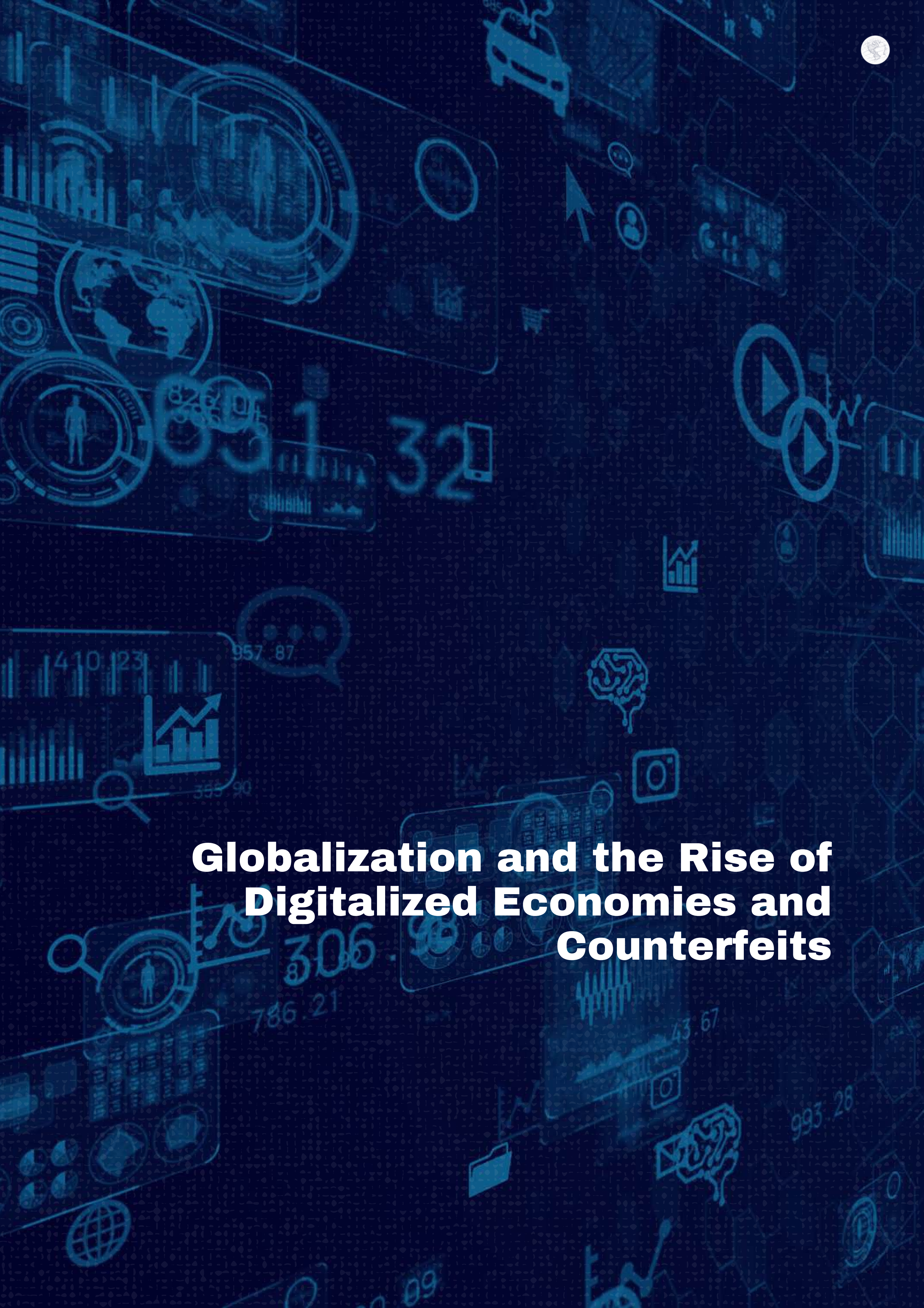
Illicit trade results in lost revenue and market share for legitimate business enterprises; theft of intellectual property, trade secrets, and critical data; job displacement for workers and business closures; increased costs of doing business overseas; and diminished brand integrity and market reputation value. According to the FBI,[2] it is estimated that China steals up to $600 billion of American intellectual property (IP) annually. It is estimated that IP theft endangers the jobs of more than 45 million Americans who work in IP-intensive industries, resulting in a loss of more than $6.5 trillion in economic output.[3]

IP crime also hurts the ingenuity, innovation, and competitiveness of leading market companies and small-and-medium sized businesses.[4] Illicit goods are often produced in unregulated spaces where criminals and criminal entrepreneurs use forced labor in dangerous, unsanitary conditions, or manufacture fake goods using pollution-creating machinery and toxic materials that harm our collective environmental and human security.

With advances in mobile devices and communications and the ease of downloading shopping apps, bad actors have shifted the trade in counterfeits, stolen and illicit goods, and related criminality away from physical retail stores to targeting digital spheres, in which payments can easily be made with digital currencies or value cards. Purchased real and fake goods arrive almost overnight through express shipping couriers or postal services.

In this ecosystem of criminality and fraud, counterfeiters and money launderers alike are similarly exploiting legal, regulatory, and law enforcement vulnerabilities to leverage anonymity in establishing online stores through the incorporation of anonymous shell companies, as well as the use of anonymous payment systems to enter e-commerce markets to transact in numerous criminalities. While counterfeiters and money launders target all aspects of the retail supply chain to traffic illicit goods, e-commerce is also increasingly used to sell illicit or stolen goods, and to launder dirty money derived from predicate crimes and cross-border illicit activities.[5] Often, transaction laundering includes the formal financial and banking system, unregulated payment gateways, and some payment systems of e-commerce platforms.[6] However, even with an array of illicit activities and transaction laundering being conducted across e-commerce platforms and digital marketplaces, one report estimates that only nine percent of retailers view e-commerce crime as a priority.[7]

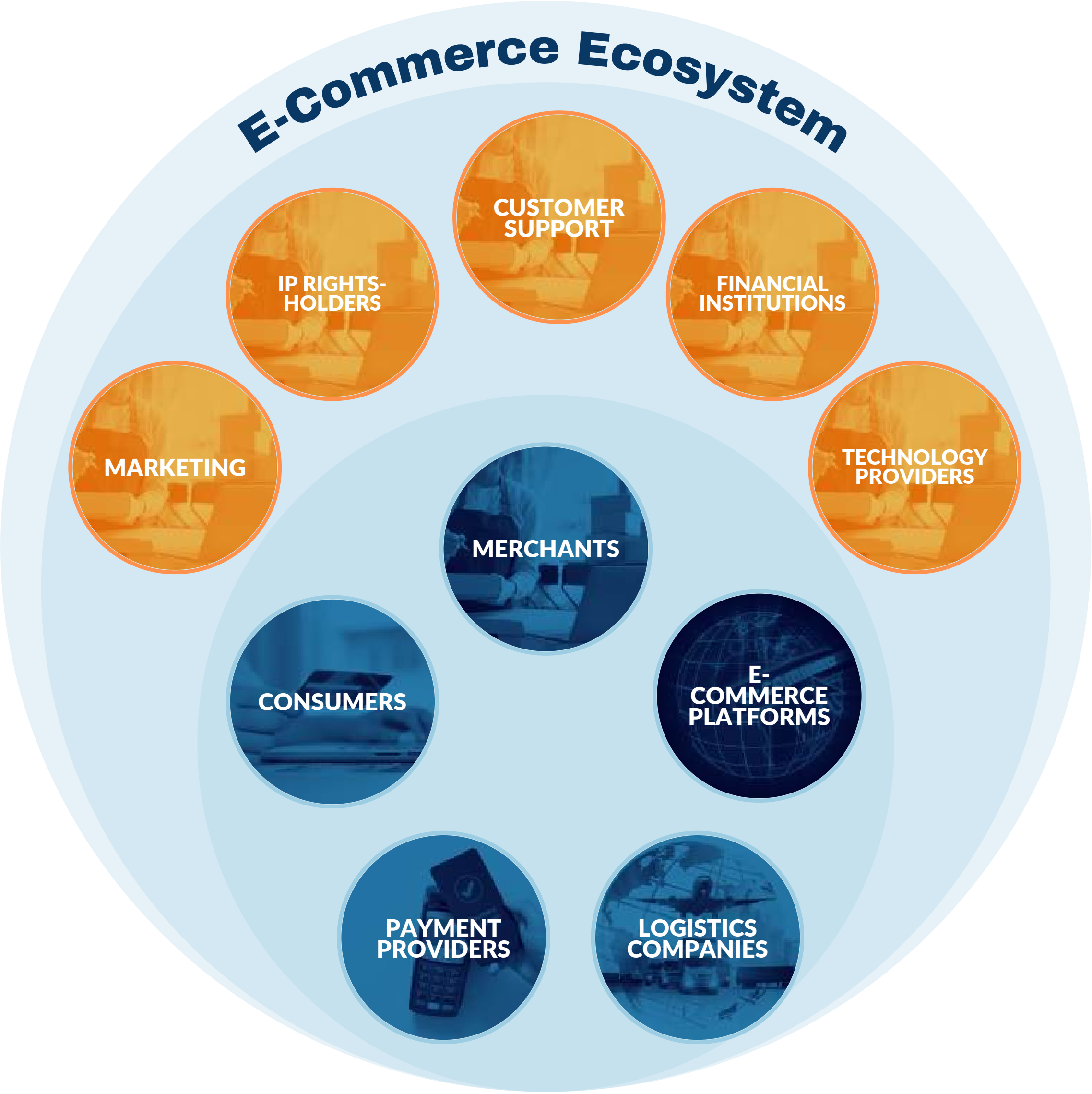
This ICAIE Fall 2024 policy brief highlights the ongoing threats related to international transaction laundering and other financial crimes related to e-commerce and the trade in counterfeits and illicit goods. These threats are significantly expanding illicit economies globally. The policy brief also provides a special focus into the trade in illicit pharmaceuticals across online pharmacies in digital marketplaces. Finally, ICAIE examines some of the new forms of money laundering in the cyber world including digital wallets, cryptocurrencies, mobile payments, and other emerging illicit finance methodologies.



Globalization and the Rise of Digitalized Economies and Counterfeits

Globalization, rapid digitalization, technological innovation, smartphone proliferation, and the rapid growth of e-commerce across the world have transformed how consumer goods and services are produced, marketed ownership titled, bought, sold, paid, distributed and conveyed around the world. The rise of business across e-commerce platforms was further accelerated during COVID-19. Consumers during forced lockdowns stayed at home for long periods and resorted to the internet and the online digital world to purchase food, medicines, apparel, and other everyday necessities and goods.

Today, the key players across e-commerce global supply chains include intellectual property (IP) rights-holders, producers, manufactures, suppliers, wholesalers, vendors, e-commerce platforms, online stores, logistics and distribution providers (warehouse and delivery), and consumer end-users. In this e-commerce ecosystem, transaction laundering provides a network of inter-connected market players in the buying and selling of goods and services. Market players in this domain become, knowingly or unknowingly, cogs in the multi-trillion money laundering global illicit economy exploited by counterfeiters and other criminals.



The global e-commerce market size in 2023 was estimated at slightly over $20 trillion in value and is forecasted to reach $50 trillion by 2030[8] with projected online retail sales of close to $10 trillion by 2030.[9] At present time, there are about 2.1 billion e-commerce shoppers, or roughly about 25 percent of the total 8 billion people globally.[10] Approximately 52% percent of all online shoppers report buying goods internationally in stores outside of their respective countries.[11]

In the United States, 79% of smartphone owners used their mobile devices to make a purchase in 2023.[12] Similarly, there were an estimated 167.8 million mobile shoppers in the U.S. in 2020 (or[13] slightly more than half of the population of 331 million people based on 2020 Census). It[14] is expected that there will be 200 million mobile shoppers in the U.S by 2025.

Today more people have smartphones than have electricity and running water. According to Statista, in 2023, including both smart and feature phones, the current number of mobile phone users is 7.33 billion.[15]

That means approximately 91% of people in the world are cell phone owners. Similarly, the use of mobile payments via cell phones has skyrocketed. Online sales using mobile phones, tablets, or computers have surged in the last 10 years alone.

In our 2023 ICAIE report "M-Payments and Mirror Swaps: Money Laundering Threats that are Getting Worse" we outlined the rapid expansion of e-commerce and mobile payments that has given rise to a surge in transaction laundering, in the process also harming online marketplaces and vendors alike.[16] It is estimated that between 2023 and 2027, online payment fraud will cause global merchant losses that will surpass $343 billion in total.[17] This underscores the urgent need for robust measures to combat this type of financial crime and protect the integrity of the financial system.

The Groupe Speciale Mobile Association (GSMA), which includes over 1,000 worldwide mobile operators and related businesses and industries, estimates that in 2023 there were 1.75 billion registered mobile money accounts processing $1.4 trillion a year.[18] Hundreds of millions of mobile accounts were added during the pandemic. By the end of 2023, there were around 435 million active mobile money accounts.

According to the GSMA, approximately $3.9 billion was transacted daily via mobile money in 2023. In addition, the number of mobile money agents grew from 12 million in 2021 to roughly 18.6 million in 2023, particularly due to the increased growth in Sub-Saharan Africa.[19]

Looking ahead, the projections for the future of the mobile payment market are equally striking. By 2030, the global mobile payment market is anticipated to reach an astounding $600 billion,[20] indicating the ongoing upward trajectory and immense potential of mobile payments as a force in the financial landscape.

As we underscore below, transaction laundering (money laundering) via credit/value cards, mobile payments, and digital currency wallets is a growing global threat across e-commerce, digital economies, and online marketplaces. Among the biggest transaction launderers are providers, sellers, vendors, and traders of counterfeit merchandise:[21]

> *But even when the goods or services in question are sold legally, falsely representing the nature of a credit [or value] card payment violates the processing merchant's agreement with its acquiring bank. Using such a scheme to sell products illegally may also violate a number of state, federal, and [Anti-Money Laundering] (AML) laws depending on the nature of the transaction.*[22]

Unfortunately, awareness of the scale of money laundering across online marketplaces is limited, especially the use of mobile payment and transaction laundering. Law enforcement efforts to disrupt, investigate, and prosecute such e-commerce crimes are also hampered by the nimbleness of criminal entrepreneurs, conflicting priorities, insufficient expertise and capacity, and the challenges presented by competing international venues and jurisdictions.

Scale of Today's Trade in Counterfeits and Stolen Goods

While the tremendous growth in e-commerce has brought many positives to the consumer shopping experience, such as the increase of selection and the ease of purchase for consumers, it has also brought significant risks,[23] challenges, and vulnerabilities. Counterfeiting is the largest criminal enterprise in the world. International sales of counterfeit and pirated goods total between an estimated $1.7 trillion and $4.5 trillion per year.[24] The proceeds of crime related to counterfeit goods are far higher than proceeds of either drugs or human trafficking.

Counterfeiting is the intellectual property infringement of copyrights, trademarks, design rights and patents. The internet and smart phones and computers, along with e-commerce platforms have fueled a boom in the sale of licit and illicit goods, including counterfeit and pirated goods.[25]

Approximately 80% of counterfeits are produced in China and Hong Kong. Other major points of origin for counterfeit goods include the United Arab Emirates, Turkey, Singapore, Thailand and India.

While counterfeit goods are found around the world – developed and developing countries alike – a significant amount of those illicit goods and products are purchased by American and European consumers. Increasingly, the high volumes of counterfeits and related illicit trade are being conducted via e-commerce platforms and digital marketplaces. The impacts are not only economic, but also societal, environmental, and political. Counterfeits also hurt the competitiveness of innovative industries and affect market share of businesses across related and online markets.

The expansion of the digital world including through social media channels for conducting commerce has also increased an array of business transactions and services between businesses (B2B), businesses to consumers (B2C), consumers to other consumers (C2C), as well as person to person (P2P) payments.

The global digital economy has also witnessed the explosion of payment processing gateways or payment service providers (PSPs) to facilitate transactional activities including to securely transmit and process payment information between the customer, the business, and the payment through credit or debit cards, digital wallets, anonymous payment systems and other e-payment methods.[26] Major digital wallets include PayPal, Apple Pay, Google Pay, and other options, in which customers finalize a transaction through an authentication process (e.g., a PIN or a biometric ID).[27]

Stolen Retail Goods and Cargo Theft Sold Online: Holding Bad Actors Accountable

Organized retail crime (ORC) is a multi-billion financial crime that provides financial and reputational harms to victimized retailers, brands, and e-commerce platforms as criminals target retail stores (e.g., "smash-and-grab") and cargo trucks for goods that they can resell to other retailers or across black markets, social media, and online marketplaces.[28] Bad actors involved in ORC aggressively attempt to exploit any possible gaps in the global retail supply chain, including stealing from manufacturers, cargo carriers, warehouses, and retailers. According to the 2021 joint report released by the Retail Industry Leaders Association (RILA) and the Buy Safe America Coalition, in 2019, nearly $70 billion in goods were stolen from retailers.[29] As staggering as this number is, it doesn't account for loss related to cargo theft nor the uptick in ORC during the COVID-19 pandemic. The abuse of these sites allows these criminal organizations to sell stolen goods at nearly 100% of their original retail value.

ORC is not shoplifting, and these crimes are not victimless. In addition to the growing number of thefts that turn violent, consumers, local communities and businesses bear the costs of rising prices.[30] These thefts are detrimental to both businesses, small and large alike, including online marketplaces, and the overall economy as they pose both societal and health risks to the community. Estimates reveal ORC costs federal and state governments nearly $15 billion in lost tax revenue, not including lost sales taxes.[31] It is estimated that the average American family will pay more than $500 annually in additional costs due to the impact of ORC. According to DHS/HSI, the most commonly targeted items for ORC are:

- Luxury Perfumes
- Pharmaceuticals
- Building Supplies
- Groceries
- Household Goods
- Electronics
- Health & Beauty Supplies
- Automobiles
- Clothing & Apparel

Organized Theft Groups (OTGs) illegally profit from systematically targeting retail establishments utilizing professional thieves known as "boosters" stealing high value goods including luxury apparel, handbags, and health and beauty products.[32] Often, boosters travel in crews throughout the country utilizing aliases, rental vehicles, and tools such as "booster bags" and illegally acquired security keys to steal high-value merchandise.[33] Although some boosters may sell the stolen goods on their own, most of the time the stolen items are being sold to a middleman known as a "fence or fencer." The fence/fencer purchases the stolen merchandise from boosters at a fraction of the retail value and will utilize several avenues to sell the stolen goods, e.g., e-commerce websites, social media, or wholesale/trading/distribution companies.[34] Often, the fence/fencer, attempts to make the items appear legitimately obtained. It is estimated that cargo theft accounts for $15-35 billion in loss annually. OTGs target cargo at the ports of entry, at truck stops, on freight trains, and anywhere else along the supply chain as the goods are in transit.[35] OTGs utilize a variety of means to steal cargo including fraudulent pick-ups, phony documentation, etc. Much of the cargo that targeted is destined for retailers and/or distribution centers.

Public-private partnerships are indispensable in fighting ORC and related cargo theft. E-commerce platforms, online marketplaces, brand owners, and other market stakeholders work across borders and supply chains with Federal, state, and local law enforcement agencies including through information-sharing and threat intelligence. Many of these partners are encouraging the U.S. Congress to pass the Combating Organized Retail Crime Act (CORCA), bipartisan legislation that would establish a coordination center between retailers, law enforcement, and other market stakeholders to fight organized retail crime and related criminality.

As discussed below, the convergence between the global digital economy and cybercrime has also given rise to money laundering. Bad actors and illicit threat networks are increasingly using e-commerce to diversify their criminality.[36] In fact, as U.S. law enforcement communities have unearthed, cybercriminals are increasingly finding novel ways to exploit vulnerabilities and regulatory gaps in online transactions to place, layer, and integrate (which are the three stages of money laundering) their dirty money.

On-Line Payment Systems

With any licit industry, criminals gravitate both to new opportunities and vulnerabilities to ply their greedy enterprises by exploiting e-commerce for profits and to launder their dirty money. Money laundering operations and illicit digital transactions across e-commerce platforms and online marketplaces are new, thriving, and expanding as e-commerce enables criminals to move their illicit proceeds faster. For example, as noted above, organized retail theft is growing rapidly in the United States. In 2022, losses to retailers and vendors totaled an estimated $125 billion.[38] Criminal organizations and market bad actors increasingly exploit the digital world as an effective means to procure and sell stolen goods through global supply chains that remain vulnerable to illicit vectors and threat networks.

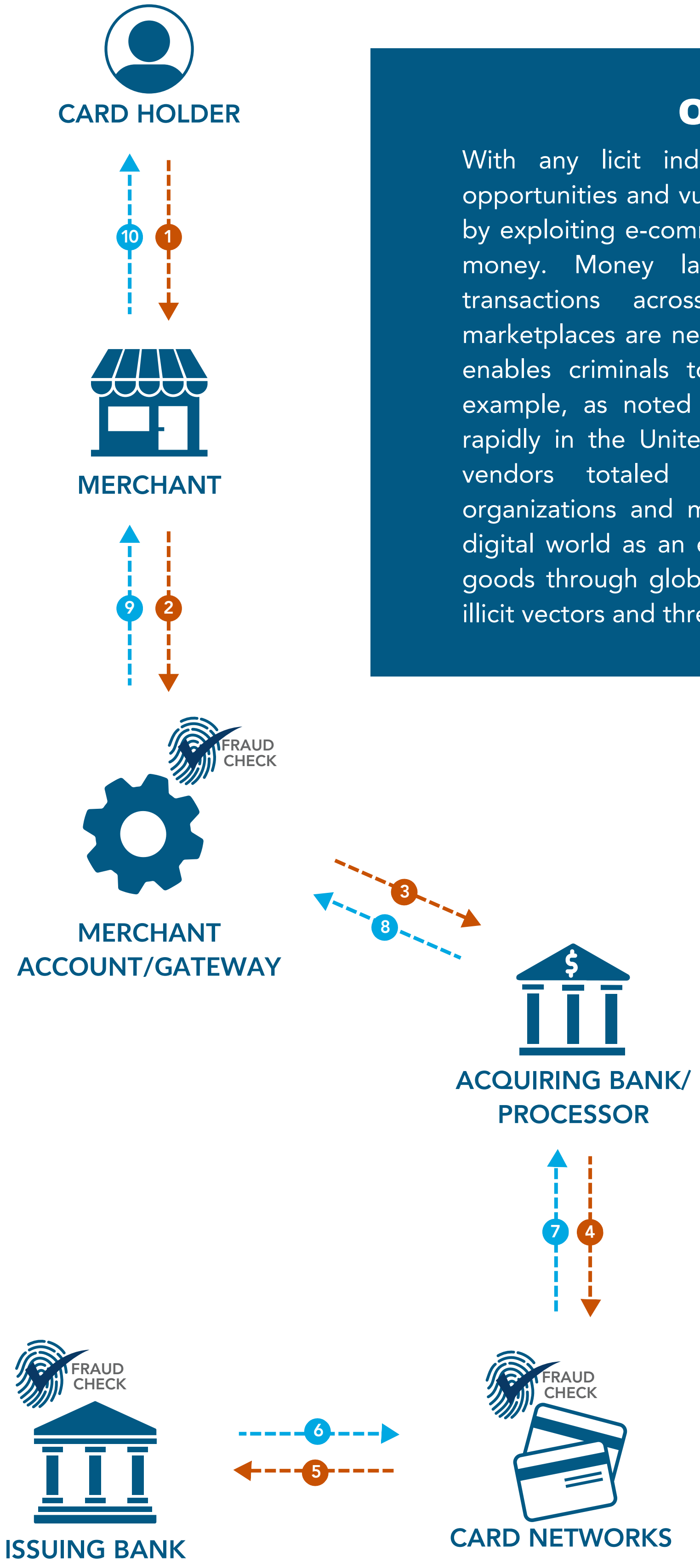
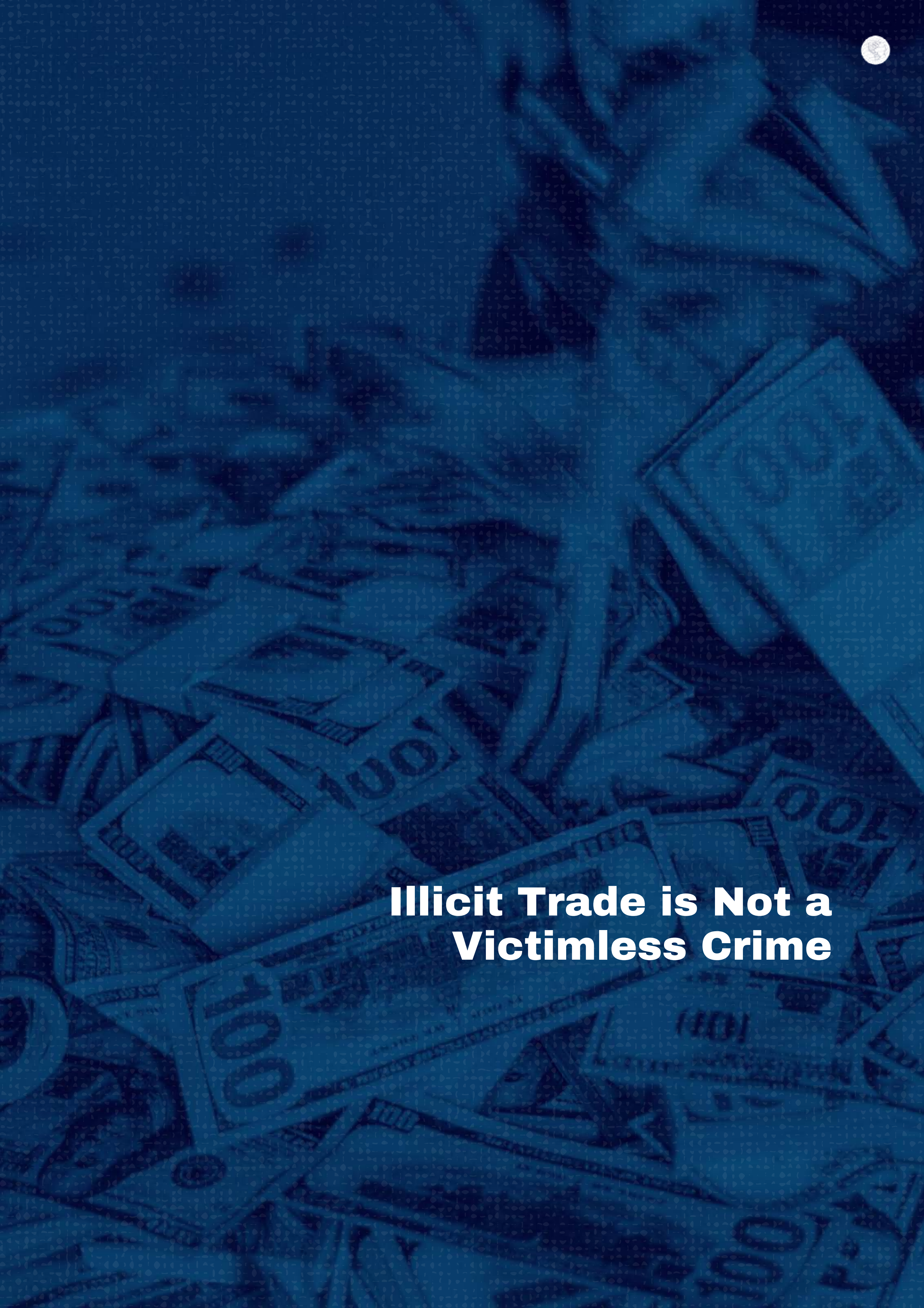


Figure 1.1. On-Line Payment Systems[37]



Illicit Trade is Not a Victimless Crime

Sometimes consumers feel it doesn't make a difference if they buy a fake rather than a genuine article. Their purchase decisions are driven by cost. And the quality of many counterfeit goods has markedly improved. The common attitude is that big business can easily afford the losses. As a result, many feel the production, distribution, and sales of counterfeit goods are a "victimless crime." This is far from true. Consumers, for the most part unwittingly, are in fact financing vicious criminal enterprises.

Illicit economies and crimes of greed have tremendous human, economic, societal and security costs and consequences to governments, markets, industries, communities, and innocent citizens.

Every year, criminalized trade and trafficking across illicit economies kill hundreds of thousands of people around the world.

From small villages in Africa and Latin America to city streets across America, Europe, and Asia, too many people are harmed by the callous criminality and disregard for human security by organized criminal enterprises, narco-cartels, threat finance syndicates, complicit corrupt officials, market profiteers, and their professional enablers.

Bad actors and threat networks are involved in the lucrative criminal activities enabling and fueling the multitrillion-dollar illicit economies include the smuggling and trafficking of narcotics, fentanyl, weapons, humans, counterfeit and pirated goods; illegal tobacco and alcohol products; illegally harvested timber, wildlife and fish; pillaged oil, diamonds, gold, natural resources and precious minerals; and other contraband commodities. Such contraband and illicit goods are sold on social media, e-commerce platforms, and on the dark web every minute of every day.

The United Nations has estimated that the dirty money laundered annually from such criminal activities constitutes up to 5 percent of global gross domestic product, or approximately $4 trillion.

In fact, the dirty monies derived from illicit trade are the lifeblood of today's bad actors, enabling kleptocrats to loot their countries, criminal organizations to co-opt states and export violence, and terrorist groups to finance their attacks against our societies.

In today's global threat environment, criminals and bad actors exploit human misery for illicit enrichment.

Collectively, these bad actors help to fuel greater insecurity and instability around the world, undermining democracy, corroding the rule of law, fueling impunity, imperiling effective implementation of national sustainability and economic development strategies, contributing to human rights abuses and enflaming violent conflicts.

By exploiting markets, supply chains of legitimate businesses, modern technologies and communication systems, and the digital world, criminals are thriving through their illicit enterprises.

Unfortunately, not enough attention is given to the magnitude and the array of harms caused to victims of the dark forces of illicit trade.

Who is Getting Hurt by Illicit Economies and Criminalized Trade?

Often it is vulnerable populations including the elderly, women and children, the poor, the sick, uninformed consumers, and others who are targeted, exploited, and abused by criminals, counterfeiters, and fraudsters. Financially-disadvantaged communities in the developing world are particularly hurt as we have witnessed during recent conflicts, the pandemic, natural disasters, and the current uneven economic recovery.

Given the size of the global e-commerce and lucrative financial rewards, counterfeiting has attracted the attention of criminal entrepreneurs and fraudsters, transnational organized crime groups, terrorist organizations, cyber bandits, and other illicit actors enabling an array of financial crimes and consumer frauds. The criminal activity endangers the integrity of commercial trade, the economic security of nations and industries, as well as the health and safety of communities and citizens.

For the criminal and terrorist organizations involved, counterfeit via e-commerce means high profit. Trafficking in counterfeit goods is generally low risk and high reward. For example, the penalties for counterfeiting are much less than those for narcotics trafficking, but the profits can be just as lucrative.

Counterfeiters and other criminals exploit e-commerce including through social apps for conducting illegal sales of illicit goods. Through the stores and apps that they operate in selling counterfeits, often they exploit the reality that online shoppers cannot physically inspect the goods that they purchase and are typically required to pay in advance of their delivery.[39] Another fraud committed by such criminals is when images of genuine products appear online but are substituted with a counterfeit good, often at bargain prices. This can have a serious health and safety impact if one looks, for example, at the effects of diverted or counterfeited baby formula which is regularly sold on fake websites and social media platforms with misappropriated product images and logos of well-known formula brands.[40]

When illicit online transactions by counterfeiters are underpinned by use of both trusted and anonymous payment systems, the challenges in detection of counterfeits or fake goods multiply. For example, the anonymity offered by digital assets and cryptocurrencies such as Bitcoin makes the financial movements connected to illegal online transactions extremely difficult to track, if not impossible.[41] Other trusted and protected payment gateways such as Paypal, Stripe, Square, and others, are exploited by more than 35 percent of counterfeiters.[42]

Weak regulatory frameworks for commercial transactions and limited online policing by the ecommerce and social platforms are the primary enabling factor for counterfeiters and illicit traffickers to exploit Internet-based platforms over traditional outlets and face-to-face commercial exchanges.

Finally, a further challenge for authorities attempting to crack down on counterfeiting is that the enormous illicit proceeds generated are laundered by the criminals and criminal organizations. Particularly for e-commerce, following the money and value trails is becoming increasingly complex.

In Focus: Online Pharmacies and Fake Medicines

In the United States, the trade in counterfeit medicines generates tens of millions of dollars and includes fake versions of Arimidex, a breast cancer treatment, Lipitor, a cholesterol drug, Diovan, a drug for high blood pressure, and other prescription medications like OxyContin, Percocet, Ritalin, Xanax, Valium, and NS Ambien. Another recent and deadly product is Xylazine, a non-opioid sedative, analgesic, and muscle relaxant which is only authorized for veterinary purposes in the United States. Also known as "traq", xylazine was first detected as an adulterant in the early 2000s by the DEA in Puerto Rico.[43] Perhaps even more alarming is the rising use of netzine, an extremely potent synthetic opioid which was developed over 60 years ago but was never released to market due to the extremely high likelihood of overdose.[44]

As a result of this flood of fake medicines onto the market, consumers are unable to get the treatment that they require and may even be further harmed by ingesting products with unknown or harmful substances, causing many to die from consuming such dangerous fakes. Alarmingly, bad actors are using online pharmacies to flood customers with dangerous illicit medicines that further compound efforts to counter illicit trade in pharmaceutical products.

According to a 2023 Office of the United States Trade Representative (USTR) Report:

> *"The manufacture and distribution of pharmaceutical products and active pharmaceutical ingredients bearing counterfeit trademarks is a growing problem that has important consequences for consumer health and safety and is exacerbated by the rapid growth of illegitimate online sales."*

Illicit online pharmacies (IOPs) facilitate the advertisement and sale of counterfeit (and often substandard) medicines and comprise a large proportion of all online pharmaceutical sales. Over 95% of pharmacies currently operating online are illicit or do not operate under the regulations or laws of the jurisdictions in which they operate,[45] [46]demonstrating the high probability that any medicine sold or purchased online is not legitimate or authorized, and potential lethal if consumed.

There are numerous documented cases in the United States and Europe in which patients have died or suffered harm due to an online purchase of counterfeit medicines. A 2023 Center for Disease Control (CDC) study found that deaths from counterfeits more than doubled from 2019 to 2021, rising from 2 to 4.7%. Deaths from counterfeit pill use tripled in western jurisdictions from 4.7% in 2019 to 14.7% in 2021.[47] Illicit fentanyl was detected in 93% of counterfeit deaths in 2021, demonstrating the fatal consequences of the rise in adulterated medicines with synthetic opioids and other dangerous chemicals and ingredients.[48]

As noted below, the Mexican cartels are also involved in producing significant amounts of counterfeit medicines often tied to the illegal fentanyl trade. For example, the cartels are pressing fentanyl into high quality counterfeit pills (Prozac, Xanax, etc.) subsequently smuggled across southern U.S.-Mexico border.[49] The pill presses used by the Mexican cartels to produce their counterfeit meds are manufactured in China and exported to the U.S. and Mexico.[50] Without these pill presses, cartels and other criminal networks would likely struggle to produce the high-quality counterfeit medicines killing hundreds of thousands throughout the world.

Counterfeiting contributes to the proliferation of substandard, unsafe medicines that do not conform to established quality standards. The United States and OECD member states are particularly concerned with the proliferation of counterfeit pharmaceuticals that are manufactured, sold, and distributed by numerous trading partners. In 2022, the top countries of origin for counterfeit pharmaceuticals seized at the U.S. border were China, India, and Turkey.

Counterfeiting is not the only illicit threat related to pharmaceuticals, the issue of diverted medicines is also a challenge. Increasingly, bad actors and transnational criminal organizations have realized that the market for trafficking in diverted medicines is extremely lucrative. The danger of diverted medicine lies in the fact that it may not be properly regulated, stored, or dispensed, potentially leading to various health risks for the individuals who consume it.[51]

Diverted medicine refers to pharmaceutical products that are distributed through unauthorized channels.[52] This can include stolen, counterfeit, expired, or improperly stored medication.

The dangers of diverted medicine include:

1. **Inefficacy:** The diverted medicine may be expired or stored improperly, leading to a decrease in potency or efficacy.
2. **Health Risks:** Consuming diverted medicine can pose serious health risks, as they may be contaminated, counterfeit, or adulterated, potentially leading to adverse reactions or even poisoning.
3. **Lack of Quality Assurance:** When medicines are diverted, there is no guarantee of their quality, authenticity, or proper manufacturing standards, which can lead to unpredictable effects on the individuals who consume them.
4. **Legal Implications:** The distribution and consumption of diverted medicine are illegal activities, and individuals involved in such practices may face legal consequences.
5. **Undermining Public Health Efforts:** Diverted medicine can undermine public health efforts to ensure the safe and effective use of medications, as it bypasses the regulatory controls and oversight put in place to protect the public.

To protect public health, it's essential to obtain medications from legitimate and regulated sources, such as licensed pharmacies and healthcare providers, and to be cautious of potentially diverted or unauthorized sources.

Greed is a primary motivator behind illicit trade. Sadly, during the COVID-19 pandemic we also saw the deadly effects of counterfeit therapeutics and medicines, pharmaceutical products, and personal protective equipment (PPE). Counterfeit PPE such as face masks and medical equipment were sold and distributed to front line health care workers and front-line defenders during the height of the pandemic. Due to sharp increased demand and limited supply, counterfeiters capitalized on the chaos of the pandemic to generate profits from counterfeit goods, illicit trade, and cybercrimes.

A National Science Foundation (NSF) funded research project run by the Terrorism, Transnational Crime and Corruption Center found that majority of counterfeit N95 respirators were sourced and manufactured in Asia and specifically China, the world's top origin country for all counterfeit products including but not limited to electronics, textiles, luxury goods, and pharmaceuticals.

The pandemic was illustrative of a known truism: When a health-related pandemic, natural disaster, or other crisis strikes communities, entrepreneurial criminals profit from human misery from causal effects.

In this report, we consider illicit online pharmacies (IOPs) to be "websites that violate regulations by selling counterfeit, adulterated or unapproved drugs or dispensing prescription drugs without a valid prescription".[53] Because the sourcing, manufacturing, and transport of these medicines and products do not follow policies and regulations put in place to protect public health and safety, they can and often do have negative effects on consumers, including but not limited to health issues or even death in case of some adulterated prescription drugs containing fentanyl, xylazine, and other deadly products.

Mexican Cartels' Diversification into Illicit Medicines

Organized criminals are raking in tens of millions of dollars from the sale of illicit medicines, especially online. In a new report by the International Coalition Against Illicit Economies (ICAIE), it is now reported that the Cártel de Jalisco Nueva Generación (CJNG) has expanded and diversified its economic profile from illegal narcotics and fentanyl to include a growing dominance in the trafficking of fake medicines and counterfeit pharmaceuticals, a multi-billion dollar illicit industry repeatedly traced back to this cartel. In Mexico, sixty percent of commercially sold pharmaceuticals are counterfeit, expired, or stolen. Pirated pharmaceuticals are most common in Guanajuato, Jalisco, Guerrero, and Michoacán. The medicines are sold online, in the informal economy, and in professional brick-and-mortar pharmacies, where CJNG liaisons force pharmacists and storekeepers to store and sell them alongside real medicine. Other criminal networks are also behind significant trafficking of counterfeit medicines in Asia, Africa, and other regions.

The market share of online pharmacies was $18.5 billion in 2022 and is expected to rise rapidly, projected to grow by 4.37% from 2024 to 2029, resulting in a market volume of US$52.88 billion in 2029. The vendor numbers also correspond to statistics which demonstrate the high demand for IOP products. For example, Americans purchased over 100 million illicit prescriptions from IOPs in 2023 alone.[54]

This section not only provides an overview of the current online market, but also examines behaviors and actions of online vendors, products advertised, associated patterns and trends, and the convergence of IOP activity with other illicit trade, including money laundering. Based on this evidence, policy actions on how to best understand, identify, and disrupt IOPs and other transnational crime are provided in the Recommended Actions section.

To properly assess the impact of IOPs, we must first understand the current state of the market and how it has evolved and rapidly expanded in the past two decades. While IOPs were a problem before 2019, the Covid-19 pandemic introduced a new client base for IOPs to exploit as more consumers began purchasing products online. Because many of these new clients often lack the knowledge or proper information to make informed buying decisions, they are much more susceptible to being duped into buying counterfeit or substandard products.

In 2017, the World Health Organization (WHO) estimated that 10.5% of medicines sold worldwide were counterfeit.[55] This means that approximately 1 in 10 medicines globally are substandard or fake, posing tremendous threats to public health, legitimate pharmaceutical and medical supply chains, and international and national security. While the global statistics on illicit medicines are alarming, the prevalence of counterfeit medicines is even more alarming in poorer nation-states, with an incidence of over 50% of low- and middle-income countries.

The types of products advertised and sold on IOPS range from vitamin supplements to cancer treatment medications. Many of these products have some sort of regulation or safeguard such as requiring a prescription from a certified doctor in most jurisdictions, but IOPs often allow customers to purchase scheduled and regulated medicines without the necessary prescription or authorization. Many products are synthetic medicines that may or may not contain fentanyl, a highly potent opioid, or other ingredients that are dangerous and regulated to prevent consumption and protect public health.

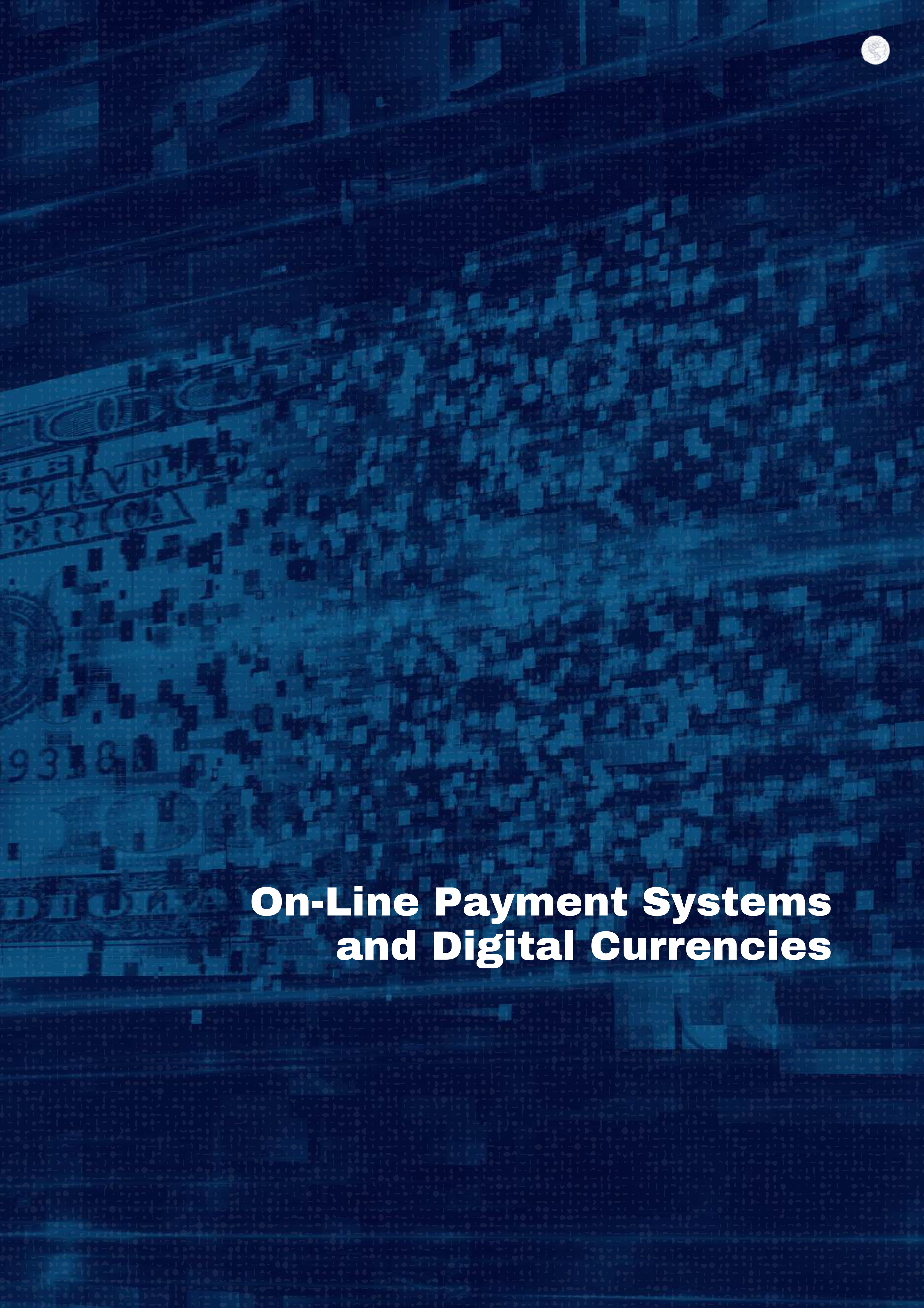
Because counterfeit pharmaceutical supply chains are often run by criminal networks (as mentioned in the previous ICAIE report cited above), the ill-gotten profits from the trade are often used to perpetuate and fund other crimes. The convergence between illicit medical supply chains and other illicit trades includes but is not limited to weapons and ammunition sales, wildlife and environmental crimes, and financial crimes such as money laundering.

Most IOPs accept multiple payment methods. This is a strategic move as the illicit activity of IOPs leave them vulnerable to account seizures and shutdowns. By accepting multiple rather than one payment method, IOPs ensure they can continue business in the event of an account being blocked or seized. The most commonly accepted IOP payment methods include credit cards, third party payment services, and cryptocurrency.

As previously discussed, IOPs often operate through transnational organized crime groups. An example of individuals joining these established criminal networks is Alaa Allawi, and Iraqi translator who was one of the top vendors on AlphaBay in 2017, one of the largest dark web marketplaces at the time. Allawi was already running a small operation selling fentanyl laced counterfeit pressed pills, but when he was introduced to the ease of purchasing pharmaceuticals ingredients on the dark web, he drastically scaled up his business. By the time he was indicted in June 2017, "investigators estimated that Allawi had made at least $14 million off his criminal activities and had sold at least 850,000 counterfeit pills in 38 states".[56] This involvement of illicit actors both facilitates the advertisement and sale of counterfeit medicines. The profits gained from these illicit sales are then used to fund other criminal activity.

These related and converging crimes demonstrate the range of activity of these transnational criminal organizations, many of which also pose threats to national and international security through funding violence, terrorism, and conflict.

As discussed in the next section of the report, IOPs also threaten legitimate financial systems through the laundering of money through banks and other financial institutions. With multiple negative consequences of IOPs, including but not limited to threats and harm to consumers, brands, the economy, and security, the rise and continuation of illicit pharmaceutical sales requires a whole-of-society approach that involves all relevant stakeholders. It is only through effective international cooperation and enforcement that the threats and harms of IOPs can be properly addressed.



On-Line Payment Systems and Digital Currencies

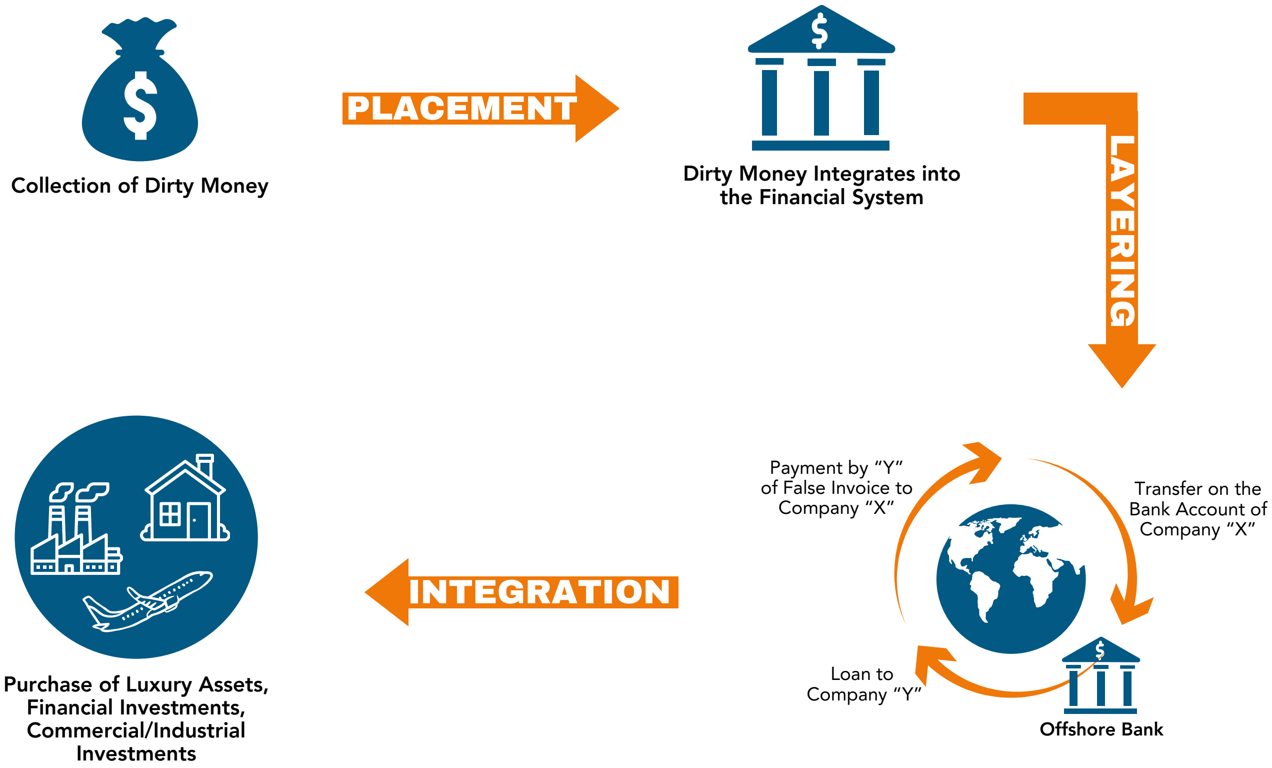
Money Laundering A Global Threat: Convergence With E-Commerce

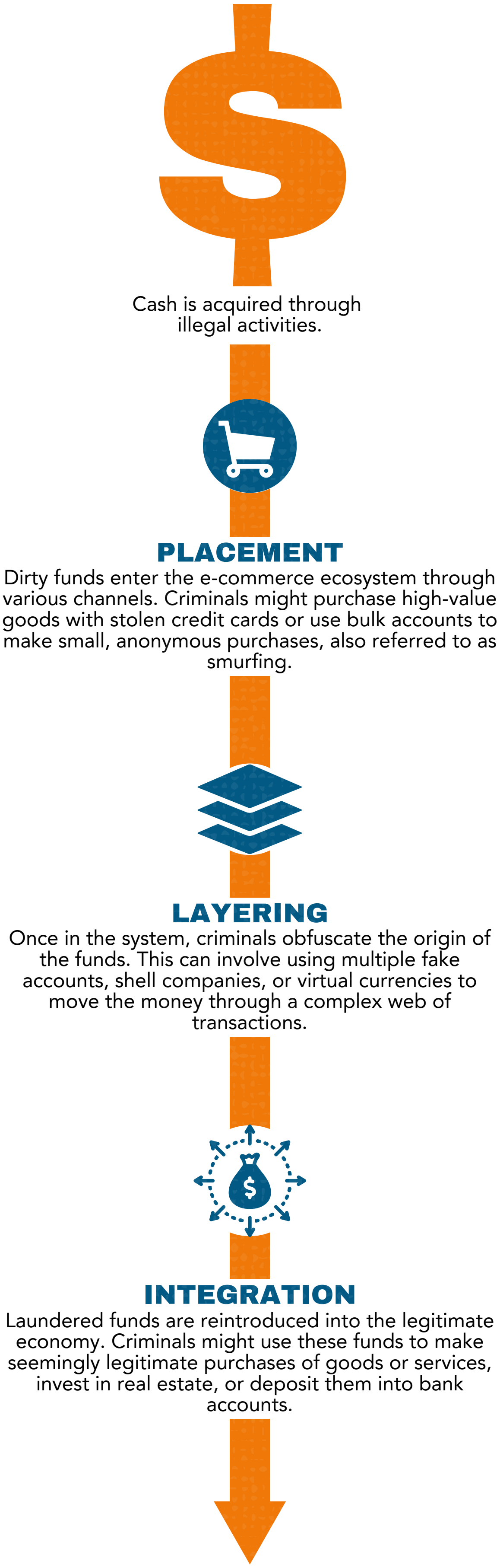
The International Monetary Fund (IMF) has estimated that the scale of global money laundering accounted for two to five percent of global gross domestic product, which surpassed $100 trillion in 2022. In other words, the scale of today's money laundering around the world is approximately $2 trillion to $5 trillion. Some experts believe the total is far higher depending what is included in the count. For example, the above estimates do not include underground financial systems nor tax evasion.

Increasingly, criminals are exploiting e-commerce platforms to launder their criminally derived funds, harming consumers and companies on many fronts that collectively present a serious threat convergence to U.S. and other developed nations' competitiveness, supply chains, brand integrity, and public health and safety.

According to the U.S. Department of the Treasury, money laundering generally involves financial transactions or value trails in which criminals, including kleptocrats, drug cartels, terrorist organizations and criminalized states, disguise, hide, and reinvest the proceeds ("dirty money"), sources, or nature of their illicit activities. Reintegrated laundered "clean" funds often include legitimate transactions, trade-based money laundering (trade fraud), investments in real estate and other sectors, purchases of consumer goods, or funds leveraged through value in stolen credit cards, ecommerce digital wallets, cryptocurrency trading, and other money laundering methodologies.

Money Laundering Cycle


Collection of Dirty Money
PLACEMENT
Dirty Money Integrates into the Financial System
LAYERING
Payment by "Y" of False Invoice to Company "X"
Transfer on the Bank Account of Company "X"
Loan to Company "Y"
Offshore Bank
INTEGRATION
Purchase of Luxury Assets, Financial Investments, Commercial/Industrial Investments



Cash is acquired through illegal activities.

PLACEMENT

Dirty funds enter the e-commerce ecosystem through various channels. Criminals might purchase high-value goods with stolen credit cards or use bulk accounts to make small, anonymous purchases, also referred to as smurfing.

LAYERING

Once in the system, criminals obfuscate the origin of the funds. This can involve using multiple fake accounts, shell companies, or virtual currencies to move the money through a complex web of transactions.

INTEGRATION

Laundered funds are reintroduced into the legitimate economy. Criminals might use these funds to make seemingly legitimate purchases of goods or services, invest in real estate, or deposit them into bank accounts.

Transaction laundering is booming in the digital world including online marketplaces which is increasingly used to clean criminal proceeds and finance other crimes such as terrorist attacks.

As criminals exploit vulnerabilities across online transactions and engage in an array of crimes to launder their dirty money derived from other crimes, they leverage the anonymity, speed, and global reach of the internet to expand their criminal illicit operations and build greater wealth.

Transaction money laundering enables illicit merchants and counterfeiters to hide their transactions by processing sales through the payment credentials of a legitimate vendor, to sell fake goods, and to clean criminally derived proceeds through reinvestment through e-commerce.

By exploiting legitimate payment channels across e-commerce, transaction launderers can evade detection and continue to engage in criminal activities and reinvest dirty money including through front companies (anonymous shell companies) or commingled legitimate and illegitimate transactions which can have serious consequences for the integrity of market, businesses, and the financial system, and pose a multitude of serious harms to consumers.[57] In many cases, they may involve the sale of counterfeits, fake goods or contraband. The value of e-commerce transactions may be over-or under-inflated, invoiced, misidentified – see trade-based money laundering (TBML) below. Or the transactions may simply be nonexistent, an illicit finance scheme sometimes referred to as "ghost laundering".[58] Finally, e-commerce often stymies criminal investigations because of issues involving venue, jurisdiction, expertise, and lack of international cooperation.

Money Laundering Exploited Across International Trade Systems and Digital Marketplaces

As noted above, among the most serious consequences of today's globalized trade and increased e-commerce transactions has been the growth of digital payments that criminals have exploited to fuel an explosion of financial illicit activities including fraud schemes, pilfering goods, funds, and information, and laundering dirty money derived from other criminality.

The Financial Action Task Force (FATF) has declared that there are three broad categories for the purpose of hiding illicit funds and introducing them into the formal economy.

The first is via the use of financial institutions; the second is physically smuggling bulk cash from one country or jurisdiction to another; and the third is the transfer of goods via trade.[59] The United States and the international community have devoted attention, countermeasures, and resources to the first two categories but methodologies related to trade have not been widely understood, or for the most part have been ignored.

A significant methodology related to big volume e-commerce transactions is trade-based money laundering (TBML).

Trade mis-invoicing is a method of moving value illicitly across borders that involves deliberately misrepresenting the value of a commercial transaction on an invoice or sale receipt by fraudulently misreporting the quantity, quality, price per unit, and/or description of a good that results in the shipment being over or under-invoiced.

TBML is defined as the "process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin." [60] In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports."[61] In many cases, TBML can also involve abuse of the financial system through fraudulent transactions involving a range of money transmission instruments, such as wire transfers. The basic techniques of trade-based money laundering include: over-and under-invoicing of goods and services; multiple invoicing of goods and services; over-and under-shipment of goods and services; and falsely described goods and services.

TBML enables criminals and counterfeiters to disguise and legitimize their dirty money by purchasing licit and illicit goods, moving merchandise across borders, falsifying product value, quality and quantity in mis-invoicing, or misrepresenting trade-related financial transactions.

The main objective of TBML is the transfer of large volumes of money or value in the form of trade goods, which the e-commerce trade transactions facilitate. TBML is very difficult to detect, track and investigate due to its transnational nature and the complexity of the international trade system, and because illicit actors strategically and carefully obfuscate their activity to avoid detection. For the most part, TBML and related schemes also successfully bypass financial intelligence reporting requirements – the primary global anti-money laundering countermeasure.

TBML is a very broad money laundering methodology that takes many and varied forms. For example, TBML is involved with customs fraud, tax evasion, export incentive fraud, VAT fraud, capital flight, evading capital controls, barter trade, mirror transactions, underground financial systems such as hawala and Chinese "flying money," black market exchanges, and even commercial trade-based schemes such as trade diversion, transfer pricing, and abusive trade mis-invoicing.

A strong argument can be made that TBML and value transfer is the largest and most pervasive money laundering methodology in the world. Conversely, it is also the least understood, recognized and enforced. The booming trade in e-commerce helps facilitate many of the above money laundering methodologies, but also complicates successful enforcement to combat these crimes. In fact, in comparison to the annual volume of tens of trillions of dollars in international general merchandise trade, successful enforcement efforts are practically non-existent.

Similarly, daigou, which translates to "buying on behalf of," is growing problem - albeit mostly unrecognized in the United States. It is much better known in the United Kingdom, Australia, and other developed countries that are popular with Chinese tourists and buyers. In daigou schemes, individual or organized groups of Chinese buyers in foreign countries purchase high demand brand-name luxury goods, smart phones, high-end computers, infant formula, and other in-demand commodities for re-sale in China. Daigou activities are generally found in grey markets; using loopholes to circumvent import tariffs and taxes imposed. In the United States, such goods purchased in the country are subsequently exported/transported to China and Hong Kong. Funds or value cards used to purchase these goods from U.S. retailers, including Apple products such as iPhones and luxury goods, are increasingly sourced from criminal activities - including drug trafficking and fraud. Collectively, these goods are consolidated by organized Chinese criminal groups operating throughout the United States (and elsewhere) and subsequently exported using express consignment shipments.

Organized groups of daigou buyers – sometimes working on behalf of the Chinese government and/or Chinese organized crime – also purchase western goods, including personal protective devices that were in high demand during the pandemic. During the Covid-19 pandemic, this illicit trade included – but was not limited to – the sale of large volumes of counterfeit respirators or facemasks globally. During the pandemic, over 30 million counterfeit N-95 respirators were seized when entering the United States alone.[62] The hoarding and stockpiling of goods often infuriates local consumers because it causes scarcities of in-demand products, disruption to the markets, and higher prices.

The Covid-19 pandemic's travel restrictions coupled with tighter government regulations severely restricted foreign daigou purchasing agents and sales within China. However, daigou sales have now almost fully recovered. Daigou brokers increasingly use e-commerce and mobile platforms in the communication and transaction process as well as livestreaming and online channels. The new forms of e-commerce platforms have proven popular because they allow daigou sellers to connect directly with customers, showcasing products in real-time. This interactive approach reportedly enhances the shopping experience for clients and also opens up avenues for personalized engagement.

Approximately 15% of luxury goods consumption in China comes from daigou.

Cosmetics from top international brands account for more than half of daigou sales, followed by luxury bags, watches, and jewelry.[63] China's gray markets and daigou schemes may be the biggest threat to luxury brands in the next five years.[64]

Other transaction-based money laundering can occur through stolen identities, credit/value cards, or other forms of digital currencies including cryptocurrency. Refund fraud is a common tactic used by fraudsters. Another type of fraud is interception, where the fraudster places an order using a valid billing and shipping address, but then attempts to intercept the goods for themselves.

Credit Cards, Pre-Paid Value Cards, M-Payments

According to the U.S. Department of the Treasury, the use of prepaid cards is growing rapidly.[65] Prepaid cards (also referred to as prepaid debit cards, stored value cards, or prepaid access devices) are a type of prepaid access that enables pre-loading, and in some cases, reloading of funds onto physical or digital cards.[66] In some cases, criminals can also steal the identity of a shopper's banking or credit card information through scam calls to pay for goods and services through digital marketplaces, or to transfer funds to other accounts or digital wallets via online payment platform (e.g., Peer-to-Peer (P2P) payments.[67] In recent years, the U.S. Department of Justice has prosecuted individuals for laundering gift cards purchased by telephone-scam fraud victims at Target stores (and other retailers) across the United States.[68]

A recent Federal Reserve Payments Study found that, on average, the number of prepaid card transactions increased by 9.6 percent per year from 2018 to 2021, and the value of prepaid card transactions grew by 20.6 percent per year, compared with 12.7 percent for debit cards and 7.0 percent for credit cards.[69] The total value of prepaid card payments was $610 billion in 2021, accounting for 6.5 percent of the value of all card payments. Globally, the prepaid card market was valued at $1.73 trillion in 2019 and is projected to reach $6.87 trillion by 2030.[70]

Credit Cards and Value Cards Used to Launder Dirty Funds often through Chinese Money Mules

In the recent years, the U.S. Department of Homeland Security (DHS) has been investigating the use of money mules involving Chinese migrants, students, and diasporic communities in the United States carrying out money laundering schemes and financial scams involving complicit individuals sending and receiving money into their bank accounts, digital wallets, or spot-market crypto trading accounts as part of their new jobs, often at the direction of Chinese criminal syndicates and Chinese Money Laundering Organizations (CMLOs).[71] These money mules are intended to disguise the beneficial owner of the funds, and are instructed to transfer illicit funds to/from multiple accounts across numerous high-risk jurisdictions.

Increasingly, CMLOs represent a serious threat to the security of markets by fueling transnational organized crime, financial fraud, cybercrime, strategic corruption, and money laundering. CMLOs are now a global threat finance network and key players in the multi-billion-dollar criminal empires run by Mexican-based cartels and other transnational criminal organizations (TCOs) and are diversifying into new criminal schemes across the United States, and globally. CMLOs operating in the United States act as foreign currency exchanges, enabling TCOs to seamlessly exchange U.S. dollars derived from criminal activity for foreign currencies.[72] By using encrypted apps to communicate with criminal associates and employing complex money laundering schemes (as discussed below), such as m-payments, mirror swaps, and other underground banking transactions, these organizations move vast sums of dirty money quickly and quietly.

CMLOs often recruit money mules for these schemes from universities or diasporic communities or workers in the hospitality or food service industry, such as a chef, cook, server, laborer, or delivery driver, when opening bank accounts at financial institutions. CMLOs are known to recruit witting and unwitting PRC nationals living in the United States to assist with the creation of bank accounts at U.S. financial institutions. These “money mules” are often enlisted by CMLOs using social media platforms, including messaging apps such as the Chinese app WeChat. Money mules may be told they are providing money transmission services for international students, or they are servicing unbanked Chinese citizens residing in the United States. Money mules are known to use counterfeit Chinese passports supplied by CMLOs to open bank accounts for the explicit purpose of moving, concealing, and laundering the proceeds of a variety of crimes, including drug trafficking, human smuggling, counterfeiting, prostitution, bank fraud, fraudulent mass marketing, and other financial fraud schemes. CMLOs are known to use encrypted messaging applications such as WeChat, QQ, and other PRC-based programs, to purchase high-quality counterfeit Chinese passports that are produced in the PRC and shipped to the United States.

Homeland Security Investigations (HSI) has testified before the U.S. Congress on some of these financial schemes, and fraudulent passports also contain counterfeit

U.S. visas as well as counterfeit entry stamps.

Chinese counterfeiters and CMLOs have also entrenched themselves in e-commerce platforms. Today, digital global commerce is dominated by third party sellers who exploit anonymity to sell fake goods and launder dirty money. Many are based in China. Some hide behind false business names, anonymous shell companies, and fictitious contact information. The sellers also have multiple accounts so that if one is removed or shut down, they simply pop back up doing business under another account. Per the above, CMLOs dispose of criminal proceeds in part via "daigou," a Chinese term that translates to "buying on behalf of."[73] Daigou operates in underground markets and will often evade Chinese laws by importing goods without paying the requisite duties and taxes, as well as not reporting the income derived from such practices, and not paying income taxes.[74]

In these schemes, CMLOs recruit mules to purchase high-value electronics and luxury goods such as handbags in retail or online marketplaces, and subsequently export the merchandise from the United States to China where it is sold for a profit. Funds generated from these goods remain offshore where they are used to replenish overseas bank accounts used to facilitate Chinese underground banking activities for predicate crimes or specified unlawful activities. For example, HSI has investigated multiple CMLOs that are using criminal proceeds to procure iPhones and other Apple products that are being exported from the United States to Hong Kong, the United Arab Emirates, and elsewhere.[75] These CMLOs have shipped thousands of parcels containing these products using express consignment companies. According to HSI agents, many of these products were determined to be stolen or otherwise fraudulently obtained by the CMLO.

Chinese criminal syndicates and CMLOs are also implicated in large retail gift card fraud ("card draining") schemes that involve removing, altering, then re-stocking gift cards at a particular retail location – using the value of such cards before the owners can spend it.[76] During the alteration process, the gift card barcodes are replaced by barcodes controlled by the CMLO. When an unwitting customer loads funds onto the altered gift card, the CMLO converts those funds to hard goods, often iPhones, through retail purchases made by CMLO mules throughout the United States.[77] The scam involves stealing hundreds or even thousands of inactivated gift cards.[78] Once the balance is added to a card, the information is given "to a different group of suspects," who purchase electronics or other expensive items such as iPhones,[79] together with devices procured with criminal proceeds purchased from TCOs, are then exported abroad for resale to complete the underground banking cycle. About 60% of retailers said they experienced an increase in gift card scams between 2022 and 2023.[80] According to the Federal Trade Commission (FTC), American consumers are losing hundreds of millions of dollars every year to card draining and other gift card scams.[81]

Mobile or M-payments have proven very popular because of the variety of secure financial services they offer. For example, they allow the greater ease of purchase of products, services, the payment of bills, the transfer of money from person-to-person (P2P), the facilitation of micro payments for low value repetitive goods such as mass transit, the settlement of utility bills, payment of taxes, school fees, health, and many other services. M-Payments also offer some transparency in helping to prevent fraud, extortion and forms of corruption. Salaries and government benefits can responsibly be credited to cellular devices. Remittances from migrant workers are sent home via the use of cell phones. Some mobile services providers offer savings accounts and over-draft protections. M-payments have also driven more revenue to small-and-medium enterprises (SMEs) and empowered new business creation. Mobile lending is an increasingly popular service.

With M-payments criminals now have a new way to place the proceeds of crime into financial networks and the global economy. For example, a professional money launderer recruits a number of smurfs or runners and gives them the proceeds of criminal activity – such as small street sales of drugs, the proceeds of stolen property, and street "taxes" (extortion or protection fees), and even suspect charitable or terror financing contributions can be laundered in this manner. The smurfs then go to M-payment establishments and use the illicit cash to load up their cell phones with money or "e-value" under the maximum threshold level. The runner will be directed to forward the mobile money credit to master accounts or other-directed transfers controlled by the money launderer. This technique has been labeled by the Asian Development Bank (ADB) as "digital smurfing." In contrast to money laundering where cash is placed into traditional financial institutions and sometimes money service businesses (MSBs), with few exceptions, financial intelligence or digital footprints are not generated. And, practically speaking, digital smurfing's evasive nature in most countries of concern is immune to law enforcement counter measures.

With M-payments, layering is taken to new levels. In most jurisdictions, mobile value can be transferred from account to account and then directed to a financial institution or MSB either in the host country or forwarded to another country or even an offshore secrecy haven. Mobile value can be credited to an online account or perhaps used to purchase virtual currencies or even gaming tokens in cyberspace. Person-to-person (P2P) transfers are simple as well as overseas remittances. A myriad of formal and informal money transfer systems such as hawala or Chinese "flying money" can also be added to the equation to further frustrate criminal investigators trying to follow the money trail using digital wallets and m-payments. M-payments can also be used in underground networks as a 21st century means of settling accounts between brokers. In short, these complex and opaque layering schemes are only limited by the criminal's imagination.

Social Media

Directly related to the growing threat of mobile payments, is the exponential growth of social media and its link with e-commerce. In 2024, more than 5 billion people or an estimated 62.3% of the world's population use social media. The average daily usage is 2 hours and 23 minutes. Worldwide, the number of social media users is projected to increase to 6 billion by 2027.[82]

According to the Pew Research Center, 69% of adults and 81% of teens in the U.S. use social media. YouTube (83% user rate) and Facebook (68% user rate) are the two most popular platforms. Usage of online platforms varies by factors such as age, gender and education.[83] In the U.S. market, both large and increasingly, small social media platforms integrate embedded shopping features. Social media is transforming how consumers discover and purchase products. Social media and e-commerce have an interdependent and synergetic relationship.

Approximately 60% of business-to-consumer (B2C) brands get their customers through social media. Companies are pioneering digital marketing techniques to engage with potential customers, build relationships, and encourage them to buy.[84] Social media connects brands and businesses to their target audiences, driving greater awareness, revenue and loyalty. In 2023, business brands spent approximately $270 billion on social media advertising.[85] The volume of e-commerce sales on social media platforms varies greatly depending on the popularity of the platform, user demographics, region, and the type of products or services being sold. In sum, social media is becoming an increasingly important boon to e-commerce.

Simultaneously, the platforms are also more and more susceptible to different types of fraud. Scams are common, innovative and evolving. Fraudsters take advantage of social media’s speed, reach, audience engagement, and lack of policing and enforcement. Making matters even worse, scammers purposefully target vulnerable populations – particularly the elderly. In addition, scammers may embed fake on-line sites, apps or links in pop-up ads, coupons and emails with malware that infects a victim’s device and harvests personal information.

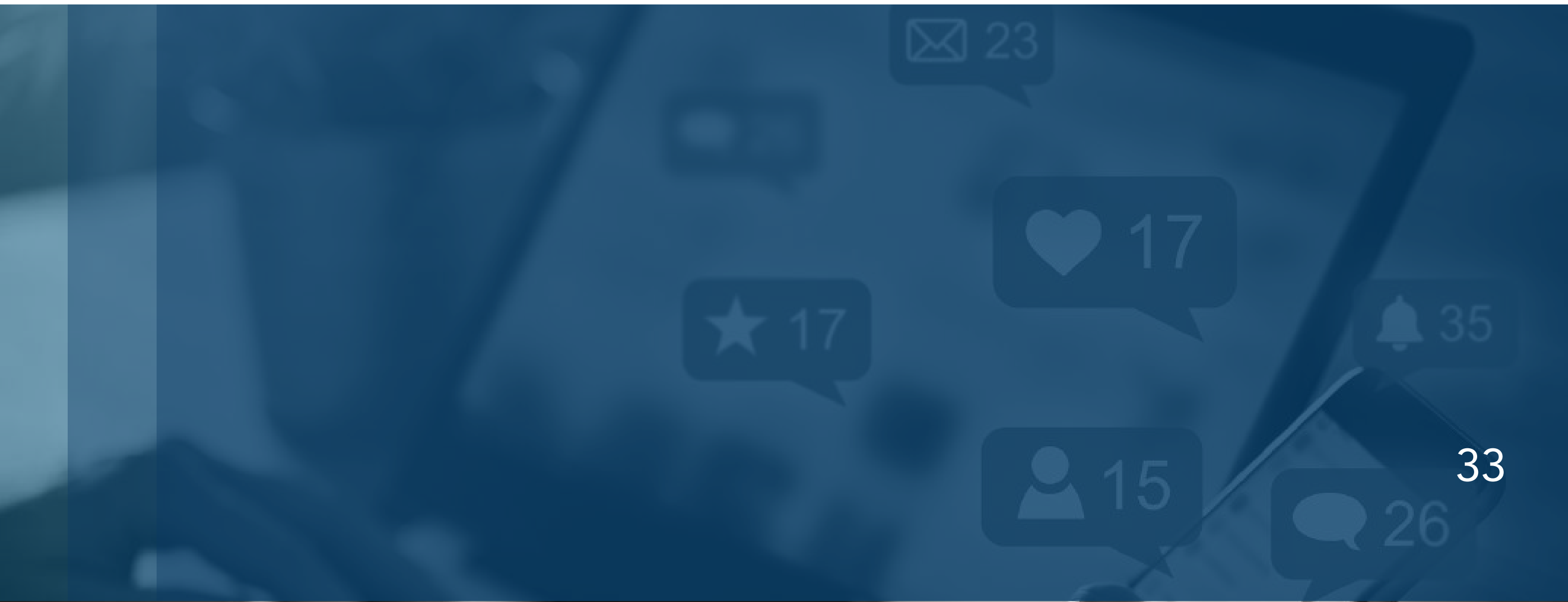
Financial losses resulting from illicit trade using social media are massive. According to the U.S. Federal Trade Commission (FCC), scams originating on social media have accounted for $2.7 billion in reported losses since 2021, more than any other method used by fraudsters to target potential victims. Frequently reported scams on social media that are reported to the FCC are buying or selling products online. Most of these reports come from people who never received the items they ordered after responding to a solicitation, for example, on Facebook or Instagram. These kinds of schemes are commonly known as non-delivery scams.

Organized social scammers are typically after three things: money, account credentials and access to the victims' social connections. Fraudsters manufacture a fake persona, or hack into an existing profile or account to get "friends" to con. Many criminals active on social-media adjust their approach by studying the personal details their victims share on social media. Fraudsters use other tactics including brand and personality impersonation, account takeover, fraudulent giveaways designed to trick social media into giving away personal and login credentials, fake product posts that take the users to a fraudulent website, targeted fake ads, etc.

Scammers also use social media to target seniors. For example, a criminal or criminal organization uses social media postings to obtain information about children in a targeted family. They contact a grandparent. The scammers might impersonate a grandchild or tell the elderly victim that they represent law enforcement and that their grandchild has been detained and needs assistance. Or the scammer tells the senior that the grandchild needs their assistance to help with an emergency such as a medical condition. Sometimes they detail an unexpected personal emergency while the grandchild is traveling overseas. The scammer uses a sense of urgency and pressures the senior to send money to assist the grandchild.

Generally speaking, the buying experience on social media is influenced by the informal nature of transactions. There is often more communication between buyers and sellers on social media sites. While the increase and ease of communication on social media of enhances the exchange of views and perhaps facilitate the shopping experience, it can also enable scams.

Direct purchases on dedicated e-commerce sites generally provide more fraud filters and practice better due diligence than being routed to a purchase site via social media. A credit card purchase on a reputable e-commerce site offers clients a variety of protection mechanisms, including guarantees, refunds, compensations, and dispute resolution procedures. E-commerce sites often feature customer reviews and ratings which combine to provide buyers with enhanced insight regarding the reputation of sellers and products.



Artificial Intelligence

Criminals and malicious actors are actively exploiting e-commerce stores across the digital world. They often deceive businesses and consumers to gain unauthorized access to sensitive data, steal confidential information, and conduct fraudulent transactions, and exploit online sales for their own purposes and profit. An increasingly important tool for cybercrime is artificial intelligence. The coming years will see AI used more and more by criminals to integrate targeting and introduce fraudulent schemes and scams into a variety of marketplaces.

Fraudsters use AI to deceive both individuals and public and private organizations. For example, AI-generated tools are used to access personal or privileged information online or on social media. An example of AI fraud in e-commerce is manipulating AI algorithms and models to create fake identities. AI is also used by fraudsters to generate false information, create phishing or spoofed emails, and conduct fraudulent transactions.

Using AI technology, scammers are able to impersonate family and friends and ask for money or personal information. Cybercriminals manipulate videos and recordings found on social media to produce realistic audio and video cloning or "deepfakes." During these scams, a victim typically receives a call from what sounds like a panicked loved one asking for money. Preying on a sense of urgency, these criminal actors carefully study and learn to exploit human behavior to increase the likelihood of a successful scam and increase profits. Other common attacks include ransomware and malware which exploit technical and human vulnerabilities to gain access to valuable information and assets.

AI has also been used by criminal organizations to create phishing emails or messages that appear to be from legitimate sources, such as financial institutions or known companies and brands. These messages can be used to create a hoax so that victims provide personal information or transfer money. AI is also used by criminals to generate phone scripts to impersonate customer service representatives and trick individuals into providing sensitive personal identifiable information (PII).

Leveraged Deepfakes and AI Threats to E-commerce Markets and Brands

As long as there is evolving technology, there will be an array of evolving fraud and criminality. The globalization of e-commerce and digital platforms, coupled with transformational financial transactions, has fueled a surge in fraudulent activities and sophisticated criminal schemes.[86] Some of the latest illicit schemes involve cybercriminals are leveraging deepfakes and AI technologies to perpetrate financial fraud, sell knockoffs from deep-faked versions of real IP-protected goods, create online market stores to sell stolen goods and counterfeits, curate false product reviews, and obtain sensitive personal and banking information.[87] A report by Signicat and Consult Hyperion show deepfakes now represent a 6.5% of total fraud attempts, marking a 2137% increase over the past three years.[88]

Furthermore, cybercrime increasingly also includes e-commerce fraud related to the sale of goods and services that are aimed to steal wealth, gain unauthorized access to PII or financial information, or conduct money laundering operations. In addition to an array of fraud schemes, criminals will use proceeds of crime, often through stolen credit or value cards, to buy physical goods and services, create e-commerce businesses to sell them or as a front to make money or e-commerce platforms exploited for laundering and moving dirty money to finance other illicit activities.[89] Through TBML, a criminal can wire crime proceeds overseas to another co-conspirator, by buying non-existent goods or services, or even legitimate ones, through an online marketplace and pay them through a payment processing gateway.[90]

According to Juniper Research, e-commerce payment fraud is expected to reach an estimated $343 billion from 2023-2027.[91] Juniper's research identified physical goods purchases through e-commerce payment fraud as the largest single source of losses and estimated it will account for 49% of cumulative online payment fraud losses globally over the next 5 years, growing by 110%. Lax address verification processes in developing markets are a major fraud risk, with fraudsters targeting physical goods specifically, due to their high resale potential.

Stolen data, PII, credit cards, and banking accounts can be purchased in specified dark web (darknet) or cybercriminal forums requires the use of unique web browsers, such as Tor, to access and affords users anonymity.[92] These black markets help to further enable licit-illicit schemes to launder money from profits derived from cybercrime, e-commerce fraud, and other illicit enterprises undertaken by criminals in the digital world and e-commerce platforms. Cybercriminals, scammers, fraudsters, hackers, and counterfeiters also using AI and deepfakes to perpetrate their illicit trade.

AI is used by fraudsters to analyze large amounts of data in order to target potential victims. For example, AI can be used to monitor social media and other online platforms to identify individuals and organizations that may be susceptible to scams. In addition, AI can examine financial transactions on e-commerce to identify patterns, methods, and trends. The AI analysis targets vulnerabilities which are then exploited for fraudulent activity.

Generative AI is technology that can produce various types of content, including text, images, audio, videos, music and synthetic data. The widespread implementation of generative AI has empowered fraudsters to accelerate their criminal schemes. Scammers are increasingly using generative AI to produce convincing deepfake content, including emails, voice recordings, images and videos. Generative AI can be used to increase the urgency in phone calls and manipulate voice-overs. They target the vulnerable by creating fraudulent websites and orchestrating online attacks. With generative AI content, seeing and hearing can no longer be synonymous with believing. Discerning truth from fiction is problematic as AI-generated content becomes indistinguishable from human generated content.

There's a growing concern that generative AI will be employed for social engineering schemes including "proof of life" scenarios using stolen identities on social media. In addition, fraudsters create synthetic or false identities that lie dormant or generate minimal activity for long periods of time. After a few years of established history, these synthetic identities become active. The created history helps fraudsters to better evade detection. Experts envision the development of digital certificates of humanity in order to distinguish real from artificial.

AI can also be a force for good in e-commerce. AI can be used by industry and security specialists to help identify and thwart fraud, flag suspicious transactions, reduce fraudulent incidents for online market merchants, and combat other illicit activities including through address verification and multi-factor authentication. Banks and companies may need to implement advanced, multilayered fraud prevention solutions that leverage AI technologies to fight real-time fraud, enhance fraud prevention, counter transaction laundering, and to develop and implement rapid response solutions to target suspicious transactions. AI is also helpful in enhancing the overall e-commerce shopping experience.

Cryptocurrencies and Scams

Bitcoin, the first cryptocurrency, was launched in 2009. Today, more than 21,000 different cryptocurrencies have evolved and followed in Bitcoin's footsteps. Cryptocurrencies are increasingly popular around the world. In the United States, approximately 26 percent of millennials own Bitcoin, compared to 14 percent of all U.S. adults.

Cryptocurrencies of all types are extremely volatile. Their values change constantly. Cryptocurrencies tend to be more volatile than more traditional investments, such as stocks and bonds. Yet they remain popular primarily as an investment vehicle.

Cryptocurrencies are also increasingly used in e-commerce. Thousands of companies and stores accept cryptocurrency payments at both physical checkout and via e-commerce platforms. For example, AT&T offers customers a payment option through BitPay. Microsoft accepts Bitcoin to pay for Xbox store credits. AMC theaters allow moviegoers to purchase tickets with Bitcoin and other cryptocurrencies. With BitPay, consumers can spend online and use cryptocurrency as payment at stores, restaurants, and to pay bills and recurring expenses.

Some consumers feel they benefit from cryptocurrency payments because they believe (sometimes mistakenly) the transactions allow for anonymous purchases by using encrypted wallet addresses. This anonymity allows purchases without consumers giving up their personal information; i.e. the belief that purchases via cryptocurrencies enhance privacy. Some consumers also use cryptocurrencies to avoid transaction fees associated with traditional banks.

Unfortunately, cryptocurrencies used in e-commerce can also enable criminal activity. For example, ransomware attacks, one of today's most pressing cyber security problems have increased in parallel with the rise of cryptocurrencies. Ransomware attacks directed against well-established businesses, organizations and even governments almost always demand payment in cryptocurrency. The dark web, a part of the internet not indexed by traditional search engines and accessed only through means like the TOR browser, uses cryptocurrencies almost exclusively as a medium of exchange. The dark web facilitates many underground and illicit markets and forums for contraband goods and illegal services. The transactions are all completed via cryptocurrencies.

E-commerce is increasingly susceptible to criminal activity via cryptocurrencies. For example, scammers on social media and other forums use their tried-and-true nefarious tactics but are more and more demanding payment in cryptocurrencies. Investment scams are common. But scammers are also impersonating government agencies, businesses, organizations of all sorts, even dating services and "pig butchering" financial scams, where the target is lured into making increasing cryptocurrency contributions. They are commonplace on social apps. Scammers might use the internet or regular mail to approach victims stating that they have embarrassing information or photos and that they will release unless they are paid in a cryptocurrency.

Pig Butchering Scam Process

1 Gaining Trust

Initial Contact:
Scammers initiate casual conversations, often pretending they received the victim's contact accidentally or through a mutual acquaintance.

Building Rapport:
Use of attractive profile images and engaging dialogue to build trust.

2 Introducing the Investment

Proposal:
Once trust is established, scammers introduce a fraudulent investment scheme, promising high returns in a short time.

Persuasion:
Use of persuasive tactics and fake investment portfolios to convince victims of the scheme's legitimacy.

3 Collecting Money

Investment Collection:
Victims are convinced to invest funds through digital payment platforms or cryptocurrencies, making it difficult to trace transactions.

4 Scammer Disappearance

Vanishing Act:
Scammers become unreachable, delete their online presence, or create new identities once they collect substantial funds or when victims attempt to withdraw their investments.

Pig butchering scams are romance scams that typically take place on dating platforms or apps. In this type of scam, often by criminal syndicates in Southeast Asia, online criminals use their knowledge of social and human behavior to target vulnerable individuals through social networking and online communications platforms, dating websites, and phone calls and text messages that are meant to appear to have been misdialed.

According to several court filings and seizure warrants in 2023 by the U.S Department of Justice related to these financial scams, fraudsters cultivate long-term, online relationships with victims, eventually enticing them to make investments in fraudulent cryptocurrency trading platforms or other "opportunities".[93] In reality, the funds sent by victims for these purported investments are instead funneled to cryptocurrency addresses and accounts controlled by scammers and their co-conspirators. Scammers control fake websites that are built to look like legitimate trading platforms, applications that victims download onto their phones, or malicious smart contracts accessed through cryptocurrency wallet software.

The victims in Pig Butchering schemes are referred to as 'pigs' by the scammers because the scammers will use elaborate storylines to 'fatten up' victims into believing they are in a romantic or otherwise close personal relationship. "Once the victim places enough trust in the scammer, the scammer brings the victim into a cryptocurrency investment scheme." Even when a victim is denied access to their funds, the fraud is often not yet over. Scammers request additional investments, taxes or fees, promising that these payments will allow victims access to their accounts. These scam operations often continue to steal from their victims and do not stop until they have deprived victims of any remaining savings.

Related illicit financial activities include money laundering, identity theft, and the use of fake financial services. Scammers operate transnationally and use sophisticated technology, such as fake personas, apps, websites to appear legitimate. These scams are often highly organized, often part of larger criminal operations that use deception and psychological manipulation to exploit their targets.

The use of digital currencies and cross-border transactions make pig butchering difficult to detect and disrupt. Law enforcement agencies and financial institutions are increasingly focused on raising awareness and improving detection methods, but victims are often left with little recourse once their funds have been stolen. These rapidly rising fraud scams have left many victims traumatized and in crippling debt and financial instability and demonstrate the increased need to educate users on how to educate themselves about investing financially online to avoid falling victim to these devastating crimes.

In early part of 2024, the FBI, OFAC, FINCEN also informed the public on how the Jalisco New Generation Cartel (CJNG) and other Mexican cartels are scamming hard-working Americans out of their financial egg nests and retirement savings by scamming even more Americans to shell out hefty sums of cash related to timeshare properties in Mexico and across the Caribbean.[94] As they diversify into other industries and criminalities including cybercrime and financial scams, the ill-gotten funds are then used to back these illicit threat networks' illicit operations and to build their illegal empires.

Find indicators to help detect, prevent, and report potential suspicious activity related to pig butchering and precautionary steps against falling victim to these financial scams,[95] here.

Scammers also impersonate well-known companies including financial institutions communicating through text, phone calls, email, or social media messages. There are countless variations on their scams but generally they tell the victim that there is fraud on the victim's account or that the victim's assets are at risk. In order to fix the problem, the victim is encouraged to buy cryptocurrency and send it to them.

The danger to consumers is compounded because cryptocurrency payments do not have legal protections. In contrast, credit and debit cards consumers have some legal recourses if something goes wrong with a transaction. For example, if a consumer uses a credit card and needs to dispute a purchase, the credit card company has a process to help recover the disputed funds. Cryptocurrency transactions do not have such protections. Also, cryptocurrency payments are not generally reversible. Once you pay with cryptocurrency, you can only get your money back if the person you paid sends it back.

For scammers active in illicit activities across the digital world and dark web, for example, these vulnerabilities make cryptocurrency the monetary medium of choice. Only scammers demand payment in cryptocurrency. As discussed above, numerous financial frauds and scams today including cybercrime, pig butchering (investment/romance schemes), condo/timeshares scams, and mass marketing fraud organizations are victimizing Americans at an unprecedented rate. Many of these frauds perpetrated by these organized criminals and illicit threat networks involve purported investments in cryptocurrencies.[96] Of note, these bad actors prefer the use of stablecoins such as Tether (USDT) for the stability provided.[97]

For vendors, one of the main benefits of using cryptocurrency for e-commerce transactions is that they can reduce transaction costs and increase efficiency. The demand for increased speed and ease of financial transactions exists for cryptocurrencies as well as other payment methods. This encourages vendors to make customer transactions with fewer barriers and maximum ease, often referred to as frictionless payment.

Cryptocurrencies in e-commerce also provide vendors secure, fast, and cost-effective payment processing with end-to-end traceability of payment transaction. Unlike traditional payment systems such as the use of credit cards or checks, cryptocurrencies often do not require intermediary third-party processors and associated fees to facilitate transactions. In addition, cryptocurrencies promote access to an expanded customer base.

Cryptocurrency accounts are not backed by governments. For example, in the United States cryptocurrency held in accounts is not insured as the FDIC does with bank accounts. If something untoward happens to a crypto account or cryptocurrency funds — for example, the company that provides storage for a crypto wallet goes out of business or is hacked — the U.S. government has no obligation to intervene.

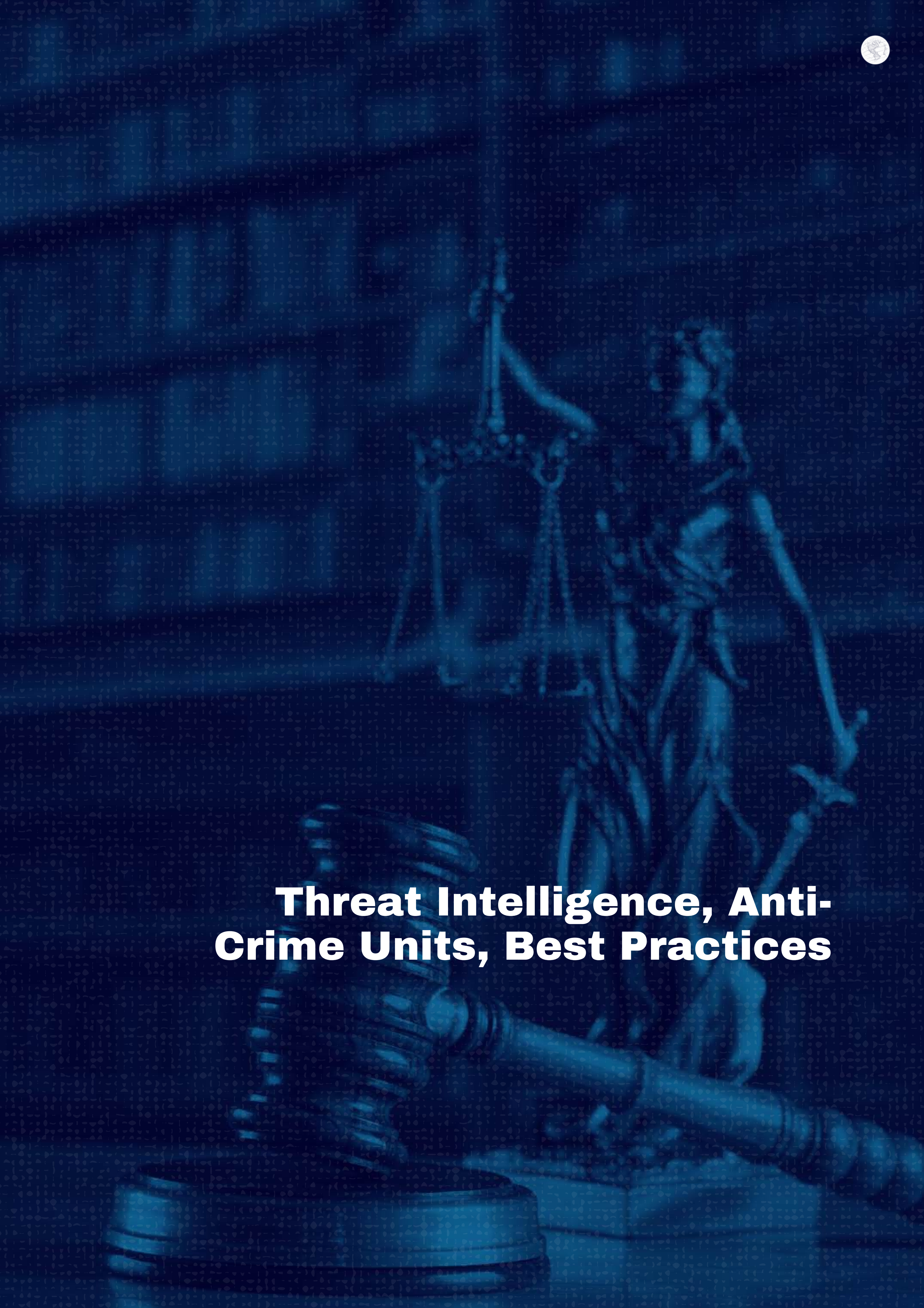
Central bank digital currencies (CBDCs) are on the horizon. Approximately 130 countries representing 98% of the global economy are now exploring digital versions of their currencies. Some have already launched or are in advanced development. It appears an unspoken goal of many of those backing CBDCs is the eradication of private cryptocurrencies. The introduction of CBDCs will upend the discussion of crypto-currencies and e-commerce described above.

There are various CBDC country models that vary in large part on the amount of government control. For example, China has the world's second largest economy. China is in the process of introducing digital yuan to become its CBDC. The China CBDC model is also designed to intertwine social control and influence behavior.

Tracking capital flight, tax collection, and following dirty money trails will be much easier for the governments and other stakeholders involved. Unfortunately, it is also an easy process for the government to “demonetize” undesirables and control citizenry. Human rights and civil liberty concerns will be threatened where the China CBDC model is adopted.

Demonetizing those out of favor with authorities can easily be done with a flip of a switch. The Chinese Communist Party (CCP) CBDC model appeals to authoritarian regimes and many global elites. Other projected types of CBDCs include retail, wholesale, and hybrid. Retail CBDCs are the most widely acknowledged CBDCs and are intended for use by the general public. Retail will directly affect e-commerce, allowing users to make everyday payments and transactions quickly and easily, often with a simple click of a button. Wholesale CBDCs are primarily intended to settle accounts between financial institutions. Hybrid CBDCs, as the name implies, are more adaptable. They can be used by both the general public - primarily for large purchases - as well as by financial institutions.

There are various policy level debates about the adoption of CBDCs in the United States and around the world. Important issues need to be resolved including interoperability between systems, civil liberty and privacy concerns, and the future of fiat currency. Will the traditional paper dollar still be allowed to exist? In short, there are few issues that will affect general populations and commercial concerns more than the adoption of CBDCs.



Threat Intelligence, Anti-Crime Units, Best Practices

Best Practices And Public-Private Partnerships To Fight The Trade In Counterfeits Across E-Commerce

In recent years, the **Working Party on Countering Illicit Trade of the Organization on Economic Cooperation and Development (OECD)**, in partnership with the EU Intellectual Property Office (EUIPO) and Business at OECD (BIAC), has been conducting evidence-based research and data analytics on various aspects of illicit trade including the cross-border seizures of counterfeits and fake goods, and threat intelligence on the key drivers of such criminality in online marketplaces.

The results have been published in a set of factual reports, starting with Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact (2016).[98] The results have been deepened, expanded and updated in subsequent reports, including Misuse of Small Parcels for Trade in Counterfeit Goods: Facts and Trends (2018), Trends in Trade in Counterfeit and Pirated Goods (2019) [99] and E-Commerce Challenges in Illicit Trade: Governance Frameworks and Best Practices (2021).[100]

Throughout the OECD reports, the global threats posed by illicit trade and the abuses of e-commerce by networks of trade in counterfeit goods were constantly present, illuminating the damaging effects on governance, innovation, and ultimately, economic growth. The misuse of the online environment has become particularly worrying during the COVID-19 pandemic, with law enforcement detecting increasing volumes of various e-crimes. The OECD and BIAC are working on best practices and a draft OECD "Guidelines for Countering Illicit Trade in Counterfeit Goods on Online Marketplaces") aimed at developing support for a final set of voluntary codes of conduct and anti-counterfeiting best practices for online marketplaces.

United to Safeguard America from Illegal Trade (USA-IT) is a public and private sector partnership, which launched in June 2021, designed to combat black-market trade. Supported by a coalition of national and state brand enforcement experts, law enforcement agencies, and leading business organizations, USA-IT is working across numerous cities and states facing critical illegal trade issues to empower local officials, law enforcement, and other leaders with information and training programs, and raising public awareness of the depth and severity of these crimes.

USA-IT continues to bring together national and state brand enforcement experts, law enforcement agencies, and leading business organizations dedicated to fighting illegal trade. The coalition is engaging on the ground across the U.S., advocating for new policies to be embraced to combat the growing threats posed by illegal trade—including counterfeiting, smuggling, organized retail theft, and other trafficking crimes including humans, drugs, wildlife, natural resources, and predicates to money laundering.

Additionally, coalition members have sponsored several state and nationwide dialogues featuring subject matter experts from large and small companies, law enforcement, and policy to examine how illegal trade funds transnational organized crime, including terrorism; new challenges confronting law enforcement; and the vital role public-private partnerships can play to reduce illegal trade.

Amazon Counterfeit Crimes Unit (CCU) [101] is a pioneering in-house investigatory hub that works with brands, law enforcement, and customs across the globe to stop bad actors and hold them accountable. CCU has an effective track record in stopping counterfeits from entering global supply chains and reaching customers, while surfacing bad actors and working with law enforcement communities to hold criminals accountable, no matter where they operate, be it online or offline.

CCU works through coalitions and business networks to defend the rights of brand owners, protect customers and consumers from counterfeit products, and helps share threat intelligence to detect and address illicit trade through public-private partnerships in order to make it more difficult for counterfeiters to move from one online marketplace to another.

In 2023, Amazon identified, seized, and appropriately disposed of more than 7 million counterfeit products worldwide, preventing them from harming customers or being resold elsewhere in the retain supply chain. Amazon works to diligently detect counterfeit and IP infringing products in their e-commerce store and takes proactive security measures to identify vulnerabilities that can be exploited by criminals, scammers, and fraudsters, referring cases to law enforcement, and pursuing litigation to seize counterfeit products and get justice for rightful owners.

Red Flags

Avoid Buying Counterfeits

Don’t Buy into Fraud: Online Marketplaces and Social Media

Buy products from online marketplaces and third-party sellers that put a premium on quality assurance and protecting customers, brands, and sellers alike but especially “customers trust” and a commitment to ensuring customers receive authentic goods when they shop at their stores.

Know the “real deal”: Conduct due diligence and engage in good online shopping practices before making a purchase, and understand the hallmarks of legitimate goods:

- Buy from reputable marketplaces and sellers that guarantee a product’s authenticity, have hotlines for reporting fraud, or investigate counterfeiting claims and take potential IP infringement seriously.
- Be suspicious of any account without a professional, domain-based email address or a functioning e-commerce website and has no information.
- Examine pictures of a product of interest; often pictures are photo-shopped and do not match the specific descriptions, colors, or specifications.
- Read consumer reviews of products bought at online stores.
- Beware of excessive discounts and prices that are less than in verified stores (e.g., buying Nike shoes from the brand itself or authorized dealers v. unknown third party sellers or questionable smaller e-commerce vendors).
- Inspect packaging of bought goods for material authenticity, quality, logo, spellings, and other brand characteristics.
- Examine shipping logistics and how long it takes to receive a product door-to-door.
- Pay with a credit card that has two-step verification processes.
- Be a part of the anti-illicit trade solution, and not a part of the problems.

Money Laundering Awareness and AML Risk Monitoring, Mitigation, and Compliance

Learn to identify money laundering and threat finance and ensure that criminals and other bad actors are not exploiting legitimate e-commerce payment systems to disguise sources of funds or layering through numerous transactions and multiple accounts across the digital world, e-commerce platforms, and social media including in high-risk jurisdictions, and through credit/value cards, cryptocurrency, and virtual assets.[102] Strengthening risk-based AML due diligence, detection and prevent controls, compliance program, and monitoring are importance good practices.

- Know Your Customer (KYC): Verify identities and mitigate financial risks and fraudulent activities including information about nature and purpose of its business or information on its incorporation or business location.
- Be aware that payment processing gateways doing business with banks in the U.S. and around the world could also become conduits through international correspondent accounts for dirty money flowing into online marketplaces and the global financial system,
- Avoid third-party sellers and online marketplaces that demand payment through anonymity, non-traceable and difficult to track transactions such as value or gift cards, cryptocurrency, wire transfers, or other novel m-payment or e-wallets.
- Flag suspicious and large financial transactions and purchases including buying products frequently through multiple or foreign accounts.
- Block buyers or sellers that use suspicious identification documents or trade names that cannot be readily verified and emails or business telephone that are not operable.
- Watch for financial fraudsters or scammers who take buyers' payments without delivering the "purchased" goods or products.
- Monitor transactions to detect purchasing patterns and anomalies related to illicit behaviors and suspicious activities including screenings of concern against global watchlists and databases.
- Scrutinize large volume of credit transactions from e-commerce platforms for sale of stolen goods; and large and frequent deposits from online payments systems which have no apparent online, brick and mortar, or auction business.
- Customers purchasing several pre-paid cards with purchases are not commensurate with normal business activities.
- Customers using mixers, privacy coins, cryptocurrency, or private wallets to further mask their identity.
- Customers repeatedly use bank locations that are geographically distant from the customers' physical locations without logical business purpose.
- Online search indicates that buyer and seller have identical addresses with the same individuals as registered agents.

Steps Forward: Recommended Actions

Steps Forward: Recommended Actions

The following recommended actions are advanced by ICAIE to encourage serious policy discussions of possible next steps on the development of effective countermeasures and authorities to confront the growing threat of transaction laundering across e-commerce platforms. Private sector stakeholders can also play an important role in uncovering illicit trade, transaction laundering, and other financial frauds and scams through the digital world and formal commerce and banking sectors.

The actions below include not only policy recommendations, new legislative authorities, and national TBML strategies, but also public-private partnerships and collective action initiatives to counter these cross-borders and e-commerce threats and financial fraud activities including leveraging data analytics, generative AI, federated machine learning, information-sharing, public-private partnerships, and public awareness campaigns.

1. Develop Reasonable Legislation to Combat the Sale of Counterfeits in E-Commerce

Reasonable bipartisan legislation is needed to help reduce the sale of counterfeit goods online. We encourage policymakers to engage with stakeholders as they consider current legislation, such as the Stopping Harmful Offers on Platforms by Screening Against Fakes in E-Commerce (SHOP SAFE) Act,[103] as a legislative solution to reduce the availability of counterfeit goods and increase greater transparency and accountability across e-commerce.

2. Encourage E-Commerce Platforms, Marketplaces, and Payment Processing Gateways to Make AML a Higher Priority

When it comes to AML/CFT, payment processing gateways need to be more responsible in ensuring the integrity of e-markets and making sure that bad actors and networks are not exploiting vulnerabilities to ply their criminality and launder their dirty money. In fact, all market stakeholders must become active and be part of effective AML solutions including securing online marketplaces and e-commerce transactions and payments to ensure that they are not being exploited for money laundering or other illicit activities. Banks, financial institutions, payment providers association groups and e-commerce platforms should be at the forefront of an energized movement that emphasizes AML's best practices across today’s e-commerce platforms. Some retailers/online marketplaces do not fall under the BSA/USA PATRIOT Act definition of a “financial institution”. As such, ICAIE recommends that such entities should consider implementing robust voluntary AML programs in recognition of the emerging and evolving transaction laundering and financial crime risks.

The industry should adopt a uniform and rigorous AML compliance program which includes procedures, policies, and controls that help to identify, assess, and mitigate financial crime and fraud risks, including money laundering, counterfeiting, and other cybercrimes. For those carriers that operate in multiple countries and jurisdictions, rigorous AML compliance must be standard in all locations.

AML controls must involve the development of an effective customer due diligence (CDD) and know your customer (KYC) process to detect illicit and suspicious activities, which includes the collection of data for third-party vendors and unscrupulous customers alike, risk profiling, and ongoing monitoring of sales, purchases, and transaction laundering.

Customer and third-party vendor identity verifications are essential. In addition, AML programs should include sanctions screening, transaction monitoring, and suspicious transaction reporting mechanisms as well as robust liaison with law enforcement and/or the country's financial intelligence unit. Payment processing gateways, e-commerce platforms, and companies doing business online should also provide AML training to their employees to raise awareness about financial crime and fraud risks and the importance of AML compliance. There should be regular internal audits and assessments to make sure the AML compliance program is functioning as intended and to identify any weaknesses.

3. Establish a Public-Private Partnership and Working Group to Combat Cross-Border Illicit Trade/TBML across E-Commerce and the Digital World

The security challenges surrounding e-commerce fraud and transaction laundering of illicit funds across digital platforms are increasing every year. In addition to elevating these cross-border security threats as national priorities, ICAIE aims to work with interested partners across sectors and industries to launch a public-private partnership and to convene quarterly meetings of an AML-Illicit Trade (AML-IT) experts' working group to share threat intelligence and strategic information and data to combat the illicit trade harms that are proliferating across the digital world and online marketplaces including examining numerous money laundering methodologies and trends such as M-Payments, mirror swaps, TBML, and other financial fraud schemes and scams.

Launching innovative public-private partnerships and a dialogue forum will help to improve the quality and availability of data, threat intelligence, and evidence-based research on illicit economies and share best practices and case studies in order to better understand the convergence of threats and harms posed by transaction laundering across e-commerce and online marketplaces. This includes analyzing emerging trends, data analytics, and field research that helps to inform enforcement and judicial actions to counter transnational organized crime, scammers, and fraudsters, and to disrupt threat finance and investigate and prosecute bad actors.

ICAIE will work with interested partners to convene a group of industry leaders and well-respected organizations and think tanks to launch an open dialogue forum in Fall/Winter 2024.

4. Encourage Congress to Pass "The Combating Cross-Border Financial Crime Act of 2023" that would create a Cross-Border Financial Crime Center and Expand the Trade Transparency Units (TTUs)

The U.S. Congress must also have a shared responsibility in ensuring open testimony and discussions on the current law enforcement and regulatory limitations and policy shortcomings which must be corrected in order to address the threats posed by M-payments and other newer forms of money laundering in the digital world.

In November 2024, Senators Sheldon Whitehouse (D-RI), Bill Cassidy (R-LA), and Angus King (I-ME), introduced Senate bill (S.3384), Combating Cross-Border Financial Crime Act of 2023,[104] and referred it to the U.S. Senate Committee on Banking, Housing, and Urban Affairs. S.3384 aims to combat cross-border financial activity and to improve the Trade Transparency Unit program of the U.S. Homeland Security Investigations (DHS/HSI), and for other purposes. ICAIE calls on the U.S. Congress to include S.3384 as an amendment to the National Defense Authorization Act for Fiscal Year 2025 (NDAA), pass the NDAA, and have it signed into law by the President of the United States.

S.3384 requires the FINCEN Director, in coordination with other relevant USG agencies to reach out to "private sector entities in the United States in order to exchange information, in real-time or as soon as practicable, with respect to tactics and trends being used to conduct illicit cross-border financial activity".[105] This would include such activity that involves corruption, international commercial trade and counterfeits products, bulk cash smuggling, the illicit use of digital assets or digital currencies and the dark web,[106] and financial institutions and designated non-financial businesses and professions.

S.3384 also internationalizes the fight to combat cross-border financial crime by instructing that the Secretary of State, acting through the Assistant Secretary of State for International Narcotics and Law Enforcement Affairs, shall coordinate [with other relevant USG agencies] "to facilitate capacity building and perform outreach to law enforcement agencies of countries that are partners of the United States and foreign private industry stakeholders by developing and providing specialized training and information-sharing opportunities regarding illicit cross-border financial activity". This would include activity that involves corruption, international commercial trade and counterfeit products, bulk cash smuggling, the illicit use of digital assets or digital currencies and the dark web,[107] and financial institutions and designated nonfinancial businesses and professions."

Encourage the State Department's Bureau of International Narcotics and Law Enforcement Affairs (INL) to work with the U.S. Trade Transparency Unit within DHS/HSI to determine how to improve and expand the international partnership of trade transparency units (TTUs). The initiative should include determining technical capacities, including support and training, for partner governments that are already involved with TTU initiatives as well as other customs services qualified to join the TTU program. The conversation between ICE and INL should include estimates regarding funding, staffing, and the collection and sharing of data and technology.

ICAIE also calls on the U.S. Congress to establish an Anti-Illicit Trade Caucus. We need to elevate the fight against illicit economies and crime convergence in Congress as a national security and foreign policy priority, including through a strong bi-partisan Congressional caucus and/or an Advisory Commission. Such a platform can send a strong and united message to bad actors and illicit threat networks, and others that the United States will robustly prosecute the fight against criminalized trade globally. ICAIE also urges the U.S. Government and committed partners to internationalize the fight against illicit trade across borders through collective action and high visibility to shut down illicit markets including across e-commerce platforms and online marketplaces, investigate and prosecute corrupt and criminal actors and their complicit facilitators, and to confiscate their dirty money.

5. Develop a U.S. TBML National Security Strategy

We must develop a national security strategy to combat trade-based money laundering (TBML) and to confiscate criminally-derived proceeds; promote information-sharing, coordinate actionable intelligence across borders; leverage blockchain, AI, and innovative technologies; and to develop more innovative and smarter global supply chain solutions to combat illicit pathways and illicit financial flows.

ICAIE urges the full implementation of the Biden administration's designation of corruption as a core national security interest in order to maintain the fight against illicit threat networks, illicit finance, and illicit economies as national security priorities. This includes the development of specific implementation strategies to prevent and combat illicit trade, identify and recover stolen assets and illicitly acquired funds and impede the effects of illicit financial flows on sustainable development strategies.

6. Fight Counterfeits en route to Free Trade Zones and Hubs of Illicit Trade

Encourage public-private partnerships across global supply chains including with brand holders, couriers, cargo services, freight shipping services, international shipping, and money service businesses, to combat corruption, money laundering, and illicit trade in FTZs, ports, and hubs of illicit trade overseas. Invest in more evidence-based research that examines the inter-connection of numerous criminal threats from one FTZ or Hub to another and find commonalities to counter cross-border illicit trade. Internationalize the fight across multilateral organizations including the Organization for Economic Cooperation and Development (OECD), World Customs Organization (WCO), INTERPOL, EUROPOL, United Nations Office on Drugs and Crime (UNODC), Organization of American States (OAS), the Asia Pacific Economic Cooperation (APEC) Forum, the Association for Southeast Asian Nations (ASEAN), and other relevant international and region diplomatic fora.

7. Innovate ideas to leverage generative AI and big data to combat Transaction Laundering and Deepfakes

Promote the appropriate utilization of artificial intelligence (AI), machine- and federated-learning, and other innovative technologies by law enforcement and security agencies to interrogate data and fight crimes associated with kleptocracy, illicit trade, money laundering and TBML.

Advanced analytics can be applied. For example, current fraud frameworks and security intelligence platforms are agile and can be adapted to various architectures and use cases. They are currently being used by both global banks and telecom companies for financial crime detection, public security, and regulatory purposes. Technology enables identity management capabilities and risk scoring using rules, predictive models, anomaly detection, as well as link and association analysis. In short, "red flags" can be engineered into M-payment systems that could automatically trigger alerts, suspend suspect transactions, and generate the filing of financial intelligence reports with the host country's FIU. There are currently some M-Payment AML software providers. While these developments are welcome, more can be done.

8. Call for a new FATF Recommendation on Trade-Based Money Laundering

Given that TBML schemes have evolved since FATF's 2006 study and their 2008 best practices paper, encourage the Financial Action Task Force (FATF) to work with cooperating member countries' customs services as well as the World Customs Organization (WCO) to determine what tools, data, analytic systems and regulatory and investigative authorities' customs services are needed to better detect trade fraud and trade-based money laundering (TBML) including related to Chinese Money Laundering Organizations (CMLOs), and other threat finance networks. The findings should be incorporated into the creation of FATF Recommendation 41 that will specifically focus on countering TBML.

The new recommendation will also encourage financial institutions, non-bank financial institutions, designated non-financial businesses and professions (DNFBPs), and money service businesses (MSBs) to include all forms of TBML in their standard due diligence, record keeping, and financial intelligence reporting. FATF Recommendation 41 should also encourage the above reporting entities to focus on service-based money laundering (SBML) in their AML/CFT due diligence, record keeping, and reporting obligations.

9. Promote Public Awareness Campaigns

Increase public awareness through dialogue, infographics, and evidence-based research on how the convergence of illicit economies impact public health and safety, legal economic actors, and the stability of governments, markets, and global supply chains.

Provide resources to protect investigative journalists, civil society activists and academic researchers who are exposing corruption, violent organized criminal activities, terrorist-financed campaigns, malign foreign influence, and the expansion of illicit economies.

Promote and facilitate technical assistance and training to enable law enforcement to effectively prevent and combat predicate crimes associated with money laundering, TBML and illicit economies, addressing the specific challenges and needs of developing countries.

10. Encourage a Threat Convergence Approach to Address the Global Digitalization Environment to Fight Cross-Border Crime and Transaction Laundering.

Increasingly, criminals and malign adversarial nation states are exploiting licit-illicit pathways across digital commerce including through cybercrimes, financial frauds, and transaction laundering. In response, law enforcement, intelligence, defense, and multilateral cooperative communities (e.g., the FBI, DHS, DOJ, DOD, CIA, NSA FVEYs, EUROPOL, NATO) must implement full spectrum capabilities to disrupt the booming illicit economies and criminality in the shadows of the digital world. This includes more investigative resources that examine threat convergence and leveraged criminality through proxies across social networking platforms, the darknet, encrypted apps, and newer forms of e-banking and use of private digital currencies. In addition to enabling anonymity, insecurity, and new criminal opportunities, bad actors and illicit threat networks are creating new black-market niches to sell illicit goods and contraband, increase recruitment, and to launder dirty monies and value.

Threat convergence partnerships are critical to enhance proactive and robust real-time exchange of information including between trusted government agencies, private sector e-commerce platforms, social-network sites, high technology sector/encryption systems, financial banking companies and online payment systems to disrupt illicit trade across digital spheres, and mitigate today's and evolving cross-border security threats to our nation(s). More investments in digital technologies and solutions are also needed in artificial intelligence (AI), blockchain, and quantum computing. Additionally, other innovations are needed to combat the growth in cyber-enabled organized crime and malign influence operations across digital markets, global supply chains, and open trade landscapes.

1 Zach Tozyński, "The Dangers of Counterfeiting", BeSafeBuyReal. https://besafebuyreal.ul.org/resource/dangers-counterfeiting.

2 Federal Bureau of Investigation (FBI). China: The Risk to Corporate America. FBI. https://curtis.house.gov/uploadedfiles/china-executive-summary-risk-to-corporate-america-2019.pdf.

3 Frank Cullen. "Congress should investigate Chinese IP theft". The Hill, February 23, 2023. https://thehill.com/opinion/congress-blog/3871875-congress-should-investigate-chinese-ip-theft/.

4 Bruce Crumley, "Scammers Target Small Business Websites with Fake Sales and Counterfeit Goods", Inc. June 10, 2024. https://www.inc.com/bruce-crumley/scammers-target-small-business-websites-with-fake-sales-counterfeit-goods.html.

5 ACAMS. Detecting and Reporting the Illicit Financial Flows Tied to Organized Theft Groups (OTG) and Organized Retail Crime (ORC). ACAMS/HSI. https://www.acams.org/en/media/document/29436.

6 Ibid.

7 SecurityTags. Retail Theft Statistics in 2021. Security Tag. Com. May 2021. https://securitytags.com/retail-theft-statistics-2021/.

8 Bob Koigi, "Global e-commerce market to reach $47.7 trillion by 2030", Marketing Report, January 18, 2024. https://marketingreport.one/retail/global-e-commerce-market-to-reach-47.7-trillion-by-2030-report.html.

9 RetailCustomerExperience.com, "Global online retail market will hit $9.93T by 2030", OMNI Channel, October 4, 2023. https://www.retailcustomerexperience.com/news/global-online-retail-market-will-hit-993t-by-2030/.

10 Ibid.

11 Kristy Snyder, "35 e-commerce statistics for 2024", Forbes Advisor (Business), May 28, 2024. https://www.forbes.com/advisor/business/ecommerce-statistics/.

12 Jack Flynn, "25 Must-Know Mobile Commerce Statistics [2023]: Facts About M-Commerce in the U.S.", February 26, 2023, Zippia. https://www.zippia.com/advice/mobile-commerce-statistics/.

13 Ibid.

14 United States Census Bureau, 2020 Census. https://www.census.gov/programs-surveys/decennial-census/decade/2020/2020-census-main.html.

15 Petroc Taylor, "Forecast number of mobile users worldwide from 2020 to 2025", Statista, November 18, 2023. https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/.

16 John Cassara, M-Payments and Mirror Swaps: Money Laundering Threats that are Getting Worse", ICAIE News, July 2023. https://icaie.com/wp-content/uploads/2023/07/Mobile-Payments-and-Mirror-Swaps-Print-Version.pdf.

17 Louis Colombo, "E-Commerce fraud to cost $48 billion globally this year as attacks skyrocket, report says", Old National, October 17, 2023. https://www.oldnational.com/resources/insights/e-commerce-fraud-to-cost-48-billion-globally-this-year-as-attacks-skyrocket-report-says/#:~:text=E%2Dcommerce%20losses%20attributable%20to,2027%20will%20exceed%20%24343%20billion.

18 Groupe Speciale Mobile Association, "State of Industry Report on Mobile Money", GSMA, 2024. https://www.gsma.com/sotir/#download.

19 Ibid.

20 Ibid.

21 Thomson Reuters, "The growing threat of transaction laundering: What banks and processors need to know to safeguard the payment system – and themselves". https://store.legal.thomsonreuters.com/law-products/solutions/clear-investigation-software/anti-money-laundering/the-growing-threat-of-transaction-laund ering.

22 Ibid.

23 OECD/EUIPO (2021), "Misuse of E-Commerce for Trade in Counterfeits, Illicit Trade", OECD Publishing, Paris, https://doi.org/10.1787/1c04a64e-en.

24 The U.S. Patent and Trademark Office (USPTO), U.S. Intellectual Property and Counterfeit Goods—Landscape Review of Existing/Emerging Research (uspto.gov)

25 U.S. Department of Homeland Security (DHS), Combating Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States. DHS Office of Policy, Strategy & Plans. January 24, 2020. https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf.

26 Check-out.com, "A Guide to Marketplace Payments", June 29, 2023. https://www.checkout.com/blog/a-guide-to-marketplace-payments.

27 Ibid.

28 Siddharth Cavale, "Explainer: 'Organized' retail crime: a 'multi-billion dollar problem'. Reuters, June 29, 2023. https://www.reuters.com/business/retail-consumer/organized-retail-crime-multi-billion-dollar-problem-2023-06-29/.

29 Retail Industry Leaders Association (RILA). Study: Retail Theft Balloons to Over $68 Billion. RILA, November 18, 2021. https://www.rila.org/focus-areas/public-policy/study-retail-theft-balloons-to-over-68-billion.

30 Homeland Security Investigations (HSI), Operation Boiling Point. DHS News, Insider Point. https://www.dhs.gov/hsi/insider/op-boiling-point.

31 Ibid.

32 ACAMS, op. cit.

33 Ibid.

34 Ibid.

35 Ibid.

36 Drini Vula, "How is e-commerce used for money laundering?", Pideeco, April 2024. https://pideeco.be/articles/ecommerce-compliance-aml-financial-crime/.

37 Yan Anderson, "What is the Best Way to Process Payments on a Marketplace", May 6, 2021, CS Cart. https://www.cs-cart.com/blog/what-is-the-best-way-to-process-payments-on-a-marketplace/.

38 Diving Beyond Boosters into Organized Retail Crime Rings (asisonline.org)

39 Transnational Alliance to Counter Illicit Trade (TRACIT), "Exposing Supply Chain Vulnerabilities to Illicit Trade: A Global Report on Dynamics, Hotspots, and Responses across 10 Sectors", TRACIT, November 8, 2023. https://www.tracit.org/uploads/1/0/2/2/102238034/tracit_exposing_supply_chain_vulnerabilities_to_illicit_trade_nov2023_full_report.pdf.

40 Federal Trade Commission (FTC). "Not enough baby formula means plenty of scammers". FTC Consumer Advice, May 18, 2022. https://consumer.ftc.gov/consumer-alerts/2022/05/not-enough-baby-formula-means-plenty-scammers.

41 Ibid.

42 Ibid.

43 DEA Joint Intelligence Report. "The Growing Threat of Xylazine and Its Mixture with Illicit Drugs," October 2022. https://www.dea.gov/sites/default/files/2022-12/The%20Growing%20Threat%20of%20Xylazine%20and%20its%20Mixture%20with%20Illicit%20Drugs. pdf.

44 ADF. "Nitazenes - Alcohol and Drug Foundation," July 10, 2024. https://adf.org.au/drug-facts/nitazenes/.

45 Williams, Ryan. "How Registrars Can Stop Illicit Internet Pharmacies." LegitScript, February 14, 2022. https://www.legitscript.com/2022/02/14/help-stop-illicit-pharmacies/.

46 Limbu, Yam B., and Bruce A. Huhmann. "Illicit Online Pharmacies: A Scoping Review." *International Journal of Environmental Research and Public Health* 20, no. 9 (May 8, 2023): 5748. https://doi.org/10.3390/ijerph20095748.

47 O'Donnell, Julie. "Drug Overdose Deaths with Evidence of Counterfeit Pill Use — United States, July 2019–December 2021." *MMWR. Morbidity and Mortality Weekly Report* 72 (2023). https://doi.org/10.15585/mmwr.mm7235a3.

48 Sartain, Marie. "CDC: Overdose Deaths from Counterfeit Drugs on the Rise." American Pharmacists Association, September 5, 2023. https://www.pharmacist.com/Pharmacy-News/.

49 UCLA. "Counterfeit pills sold in Mexican pharmacies found to contain fentanyl, heroin, and methamphetamine". UCLA Health, February 2, 2023. https://www.uclahealth.org/news/release/counterfeit-pills-sold-mexican-pharmacies-found-contain.

50 Drug Enforcement Administration (DEA). National Drug Threat Assessment 2024. DEA Strategic Intelligence Section, 2024. https://www.dea.gov/sites/default/files/2024-05/NDTA_2024.pdf.

51 U.S. Department of Health and Human Services, "Drug Diversion: What Is a Prescriber's Role in Preventing the Diversion of Prescription Drugs?". HHS February 2016. https://www.hhs.gov/guidance/sites/default/files/hhs-guidance-documents/DrugDiversionFS022316.pdf.

52 Ibid.

53 Limbu, Yam B., and Bruce A. Huhmann. “Illicit Online Pharmacies: A Scoping Review.” *International Journal of Environmental Research and Public Health* 20, no. 9 (May 8, 2023): 5748. https://doi.org/10.3390/ijerph20095748.

54 Fiore, Kristina. “100 Million Scripts Came Through Illegal Online Pharmacies Last Year,” May 8, 2024. https://www.medpagetoday.com/special-reports/features/110030.

55 Pathak, Ranjana, Vaibhav Gaur, Himanshu Sankrityayan, and Jaideep Gogtay. “Tackling Counterfeit Drugs: The Challenges and Possibilities.” *Pharmaceutical Medicine*, May 15, 2023, 1–10. https://doi.org/10.1007/s40290-023-00468-w.

56 Morenne, Benoît. “On the Trail of the Fentanyl King.” *Wired*, March 9, 2023. https://www.wired.com/story/on-the-trail-of-the-fentanyl-king/.

57 Drini Vula, Op. cit.

58 Michael Schidlow, “Ghost Laundering (Part 1): Transaction Laundering’s Online Twin Grows in Popularity,” Thomson Reuters, September 25, 2018. https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/ghost-laundering/.

59 FATF; Trade Based Money Laundering (Paris: FATF, June 23, 2006). http://www.fatfgafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf

60 FATF. “Trade-Based Money Laundering.” https://www.fatf-gafi.org/en/publications/Methodsandtrends/Trade-basedmoneylaundering.html.

61 Ibid.

62 Layla Hashemi , Edward Huang & Louise Shelley, “Counterfeit PPE: Substandard Respirators and their Entry into Supply Chains in Major Cities” (a TraCCC Study), Urban Crime - An International Journal Vol. 3-No 2-September 2022. https://traccc.gmu.edu/wp-content/uploads/2022/09/4.Hashemi_Huang_Shelley_Covid-19-and-Urban-Safety.pdf.

63 Daxue Consulting, “Navigating China’s Daigou landscape: resilience, challenges, and novel avenues in post-pandemic luxury markets,”, January 3, 2024. China's Daigou industry: resilience, challenges, and novel avenues (daxueconsulting.com).

64 Lisa Nan. Is there a Solution to China’s $81B “Daigou” Gray Market. Jing Daily. October 17, 2023. https://jingdaily.com/posts/is-there-a-solution-to-china-81-billion-daigou-gray-market.

65 U.S. Department of the Treasury, “2024 National Money Laundering Risk Assessment”, February 2024. https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf.

66 Ibid.

67 KPMG, Rising Financial Crime Risks in Digital Payments. Advisory online. https://kpmg.com/us/en/articles/2023/rising-financial-crime-risks-digital-payments.html.

68 U.S. Department of Justice. Los Angeles Trio Sentenced for Laundering Gift Cards Purchased by Victims of Telephone Scams. DOJ Office of Public Affairs, March 26, 2024. https://www.justice.gov/opa/pr/los-angeles-trio-sentenced-laundering-gift-cards-purchased-victims-telephone-scams.

69 Federal Reserve, “The Federal Reserve Payments Study: 2022 Triennial Initial Data Release”, Table 1. https://www.federalreserve.gov/paymentsystems/fr-payments-study.htm.

70 Allied research, Prepaid Card Market Research 2023. https://www.alliedmarketresearch.com/prepaid-card-market.
Credit Cards and Value Cards Used to Launder Dirty Funds often through Chinese Money Mules
22

71 U.S. Department of Homeland Security (DHS). Statement of Ricardo Mayor, Assistant Director for Countering Transnational Organized Crime, Homeland Security Investigations (HSI), “Chinese Money Laundering Organizations: Cleaning Cartel Cash” before the U.S. Senate Caucus on International Narcotics Control. https://www.ice.gov/doclib/news/library/speeches/240430mayoral.pdf.

72 Ibid.

73 National Crime Agency (NCA). Chinese Underground Banking and ‘Daigou’. NCA Crown Copyright. October 2019. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/445-chinese-underground-banking/file.

74 Ibid.

75 Homeland Security Investigations (HSI). “Chinese Nationals Arrested for Alleged $12.3 Million Fraud Involving Return of Counterfeit iPhones, Other Devices” DHS, June 3, 2024. https://www.dhs.gov/hsi/news/2024/06/03/chinese-nationals-arrested-alleged-123-million-fraud-involving-counterfeit-devices.

76 Craig Silverman and Peter Elkind. “Propublica: Chinese Organized Crime Latest U.S. Target: Gift Cards”. TickletheWireNews. May 2023. https://ticklethewire.com/propublica-chinese-organized-crimes-latest-u-s-target-gift-cards/.

77 HSI, Op. cit.

78 Tony Schinella. “Concord Police, HSI Bust Multi-Million Dollar Gift Card Scam Operation”. Patch, March 25, 2024. https://patch.com/new-hampshire/concord-nh/did-concord-police-help-bust-multi-million-gift-card-scam-operation.

79 Ibid.

80 National Retail Federation. National Retail Security Survey 2023. https://nrf.com/research/national-retail-security-survey-2023.

81 Federal Trade Commission (FTC). “Scammer prefer gift cards, but not just any card will do”. FTC Consumer Protection: Data Spotlight. December 8, 2021. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2021/12/scammers-prefer-gift-cards-not-just-any-card-will-do.

82 Chaffey, Dave. “Global Social Media Statistics Research Summary 2024 [May 2024].” Smart Insights, May 1, 2024. https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/.

83 Gottfried, Jeffrey. “Americans’ Social Media Use.” Pew Research Center (blog), January 31, 2024. https://www.pewresearch.org/internet/2024/01/31/americans-social-media-use/.

84 Manish. “The Most Important Social Selling Statistics for 2024,” January 11, 2024. https://optinmonster.com/social-selling-statistics/.

85 Ibid.

86 Kennedy Meda, “Identity theft is being fueled by AI and cyber attack”. Thomson Reuters, May 3, 2024. https://www.thomsonreuters.com/en-us/posts/government/identity-theft-drivers/.

87 Jurica Dujmovic, “Financial scammers have a new weapon to steal your money: AI”. MarketWatch, April 13, 2024. https://www.marketwatch.com/story/financial-scammers-have-a-new-weapon-to-steal-your-money-ai-744eb000.

88 Kristian McMann, “AI in Financial Fraud: Deepfake Attacks Soar by over 2000%”. AI Magazine, June 1, 2024. https://aimagazine.com/articles/ai-in-financial-fraud-deepfake-attacks-soar-by-over-2000

89 Anton Moiseienko. Understanding Financial Crime Risk in E-Commerce. Royal United Services Institute. https://static.rusi.org/20191312_e_commerce_risks_moiseienko_final.pdf.

90 Ibid.

91 Juniper Research. Online Payment Fraud Losses to Exceed $343 Billion Globally Over the Next 5 Years. July 2022. https://www.juniperresearch.com/press/online-payment-fraud-losses-to-exceed-343bn/.

92 Moiseienko, op. cit.

93 U.S. Department of Justice, “Justice Dept. Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes, With Over Half Seized in Los Angeles Case”. U.S. Attorney’s Office, Central District of California, April 3l 2023. https://www.justice.gov/usao-cdca/pr/justice-dept-seizes-over-112m-funds-linked-cryptocurrency-investment-schemes-over-half

94 U.S. Department of The Treasury, “FinCEN, OFAC, and FBI Joint Notice on Timeshare Fraud Associated with Mexico-Based Transnational Criminal Organizations”. FIN-2024-NTC2. July 16, 2024. https://www.fincen.gov/sites/default/files/shared/FinCEN-Joint-Notice-Timeshare-Mexico-508C-FINAL.pdf.

95 U.S. Department of Treasury, FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as “Pig Butchering”. FINCEN-2023-Alert005. September 8, 2023. https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf.

96 Timothy Shen. “United Nations Identifies USDT as prominent choice for fraud in Southeast Asia”. The Block, January 15, 2024. https://www.theblock.co/post/272568/usdt-fraud-southeast-asia-united-nations

97 L. Kelly, C. Quinn, E. Robinson, “Tether takes fire as UN says stablecoin is ‘preferred choice’ for $17bn in Asian crime rackets”. DL News, January 18, 2024. https://www.dlnews.com/articles/defi/tether-takes-fire-as-un-says-usdt-is-used-in-asia-crime/.

[98] OECD. Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact 2016. https://www.oecd.org/en/publications/trade-in-counterfeit-and-pirated-goods_9789264252653-en.html.

[99] OECD. Trends in Trade in Counterfeit and Pirated Goods. 2019. https://www.oecd.org/en/publications/2019/03/trends-in-trade-in-counterfeit-and-pirated-goods_g1g9f533.html.

[100] OECD. E-Commerce Challenges in Illicit Trade: Governance Frameworks and Best Practices. 2021. https://www.oecd.org/en/publications/e-commerce-challenges-in-illicit-trade-in-fakes_40522de9-en.html.

[101] Amazon Counterfeit Crimes Unit. https://brandservices.amazon.com/counterfeitcrimesunit

[102] FATF, FATF Report on Virtual Assets and Red Flag Indicators of Money Laundering and Terrorist Financing. September 2020. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf.

[103] Stopping Harmful Offers on Platforms by Screening Against Fakes in E-Commerce (SHOP SAFE) Act. https://www.congress.gov/bill/118th-congress/senate-bill/2934/all-actions.

[104] 118th Congress (2023-2024). S.3384 – Combating Cross-Border Financial Crime Act of 2023. https://www.congress.gov/bill/118th-congress/senate-bill/3384/all-actions.

[105] Ibid.

[106] Ibid.

[107] Ibid.

The **International Coalition Against Illicit Economies (ICAIE)** is a national security-centric NGO based in Washington DC that brings together committed champions across sectors and communities, including former members of the public sector, companies and prominent organizations from the private sector and civil society to mobilize collective action to combat cross-border illicit threats. ICAIE advances innovative energies through public-private partnerships, policy dialogues, and transformative threat intelligence and risk management solutions to counter illicit economies.

With an eye towards full-spectrum investigations, our ICAIE team bridges the gap between private industries and the government public sector. ICAIE Labs generate deeper investigation and supports judicial action. We leverage communications, financial, geospatial, artificial intelligence, federated learning, and other advanced analytics and technologies to investigate suspicious behavior and map networks. Ultimately, we use counter threat network operations to provide actionable intelligence, forensics, and enhanced security across the globe

John Cassara, an ICAIE Senior Advisor, is a retired federal government intelligence and law enforcement officer with a 26-year career. He is considered an expert in anti-money laundering and terrorist financing, with particular expertise in the areas of money laundering in the Middle East and the growing threat of alternative remittance systems and forms of trade-based money laundering and value transfer. He invented the concept of international "Trade Transparency Units," an innovative countermeasure to entrenched forms of trade-based money laundering and terrorist financing.

A large part of his career was spent overseas. John is one of the very few to have been both a clandestine operations officer in the U.S. intelligence community and a Special Agent for the Department of Treasury. His last position was as a Special Agent detailee to the Department of Treasury's Office of Terrorism Finance and Financial Intelligence (TFI). His parent Treasury agency was the Financial Crimes Enforcement Network (FinCEN), the U.S. Financial Intelligence Unit (FIU). He worked at FinCEN from 1996-2002. From 2002-2004, John was detailed to the U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL) Anti-Money Laundering Section to help coordinate U.S. interagency international antiterrorist finance training and technical assistance efforts

Since his retirement, he has lectured in the United States and around the world on a variety transnational crime issues. John has consulted for government and industry. He has testified seven times before Congressional committees on matters dealing with money laundering, threat finance, and transnational crime. John is on the Board of Directors of Global Financial Integrity (GFI) and the International Coalition Against Illicit Economies (ICAIE). He is a fellow at George Mason University's Terrorism, Transnational Crime and Corruption Center (TraCCC). John has authored or co-authored several articles and books.

Dr. Layla M. Hashemi is the Director of Programs and Partnerships at Women In International Security (WIIS). Previously, she was a postdoctoral researcher and data analyst at the Terrorism, Transnational Crime and Corruption Center (TraCCC) focusing on international supply chains, cybercrime and illicit trade, Program Director of Organized Crime and Corruption at C4ADS, and part time faculty at Montgomery College's History and Political Science Department for over ten years. Dr. Hashemi earned her PhD in Public Policy at George Mason University's Schar School and her Masters in International Relations and Comparative Politics at New York University with a concentration in Middle Eastern and Islamic Studies.

Dr. Hashemi has held positions at governmental and non-governmental organizations including Forum 2000 and the Journal of Civil Society where she is currently Managing Editor. Her volunteer work includes moderating the Anti-Corruption Advocacy Network (ACAN), board member and research manager at the Security, Gender and Development Institute (SGDI) and Political Economy Project (PEP) coordinator at the Arab Studies Institute (ASI).

Dr. Hashemi has presented her research — among other places — at NATO, the United Nations and professional conferences. Her work has been published in the Washington Post, academic journals and other outlets. She co-edited the Routledge volume Antiquities Smuggling in the Real and Virtual World (2022) and published a solo authored book which was released in 2024 which used social media data to analyze social networks and transnational feminist connections. Based in Washington DC, Dr. Hashemi teaches a course at George Washington University on transnational organized crime and provides lectures, trainings, and speeches on transnational crime for universities, organizations, and at international and local conferences.

David M. Luna is the Founder and Executive Director of the International Coalition Against Illicit Economies (ICAIE) working across sectors to advance public-private partnerships to tackle hubs of illicit and threat convergence vectors around the world. A former US diplomat and national security official, David is a globally-recognized strategic thought leader, advocate for security of humanity, and a leading voice internationally on cross-border security threats, international affairs, geopolitical risks, illicit trade, organized crime, terrorism, threat finance, and illicit economies ("dark side of globalization") that fuel greater insecurity and instability around the globe.

David held numerous senior positions with the U.S. Department of State, Bureau of International Narcotics and Law Enforcement Affairs (INL), including directorships for national security, transnational crime, and anti-corruption and good governance; and advisor to the Secretary's Coordinator for the Rule of Law. David also served as an Assistant Counsel to the President, Office of the Counsel to the President, The White House; and other positions with the U.S. Department of Labor and U.S. Senate. David is currently the Chair of the Business at OECD Anti-Illicit Trade Expert Group (AITEG); Chair of the Anti-Illicit Trade Committee (AITC), United States Council for International Business (USCIB); Chair of the Peace & Security Committee, United Nations Association of the USA – National Capitol Area (UNA-NCA); Member of the Business Twenty (B20/G20); Advisory Council Member, Transparency International US, and Chair of a Summit for Democracy (S4D) Kleptocracy and Illicit Finance Working Group.

David is a Senior Fellow for National Security and Founder/co-Director of the Anti-Illicit Trade Institute (AITI) at the Terrorism, Transnational Crime, and Corruption Center (TraCCC), Schar School of Policy and Government, George Mason University. David is a graduate (M.S.S.) of the U.S. Army War College, and received his B.A. from the University of Pennsylvania, J.D. from The Columbus School of Law, The Catholic University of America, and awarded numerous certificates from the Harvard Business School (HBS).

ICAIE

ICAIE.COM