ICAIE

Criminals Accelerating Global Illicit Trade by Exploiting Digital Assets, Trade Finance Fraud, and other Emerging Transaction Laundering Schemes

The Dark Side of Illicit Economies: How Digital Assets and Transaction "Value" Schemes are Being Leveraged to Finance a Global Ecosystem of Criminality and to Launder Dirty Profits across the International Trading System, Digital Markets, Hubs of Illicit Trade, Risky Free Trade Zones (FTZs) and Financial Safe Havens

John Cassara
David M. Luna

APRIL 2026

CONTENTS

Executive Summary 3

The Global Scale of Dirty Money and Value Trails 6

Digital Commerce and Transaction Laundering 10

Underground Banking and the Informal Value Transfer Systems 15

Trade-Based Money Laundering 19

M-Payments and Mirror Swaps 23

An Archipelago of Trans-Shipments, Free Trade Zones, Criminalized Ports 28

The Role of Financial Safe Havens, Complicit Power Elites, and Enablers 40

The New Frontiers: Cryptocurrency, Digital Assets, Non-Fungible Tokens (NFTs), Online Gaming, AI and Synthetic Identities, Charities 44

Case Studies: Chinese Money Laundering Networks (CMLNs) Cryptocurrencies, and Social Media 52

References and Endnotes 59

About ICAIE & Co-Authors 62

Executive Summary:
Emerging Illicit Finance Threats in 2026

Across today's global security landscapes, a global network of trade, commerce, and illicit activities is thriving where the selling and buying of legal and illicit goods and services take place through electronic and digital payouts across online connections, the global trading systems, e-commerce marketplaces, apps, social media, and encrypted channels. As such, this new global market architecture is exploited by criminals to move dirty funds in all corners of the globe through digital technologies, the internet, mobile phones, and data-driven AI, IoT, and cloud/quantum computing. Globalized trade and tariff rows have also created new arbitrage opportunities for criminal across low-tariff markets, trans-shipment points, fraudulent schemes that misuse country of origin declarations, and trade-based money laundering often using cryptocurrency for payment settlement.

As international trade and commerce are further digitized, the evolution of today's payment systems has also altered the security landscapes to detect and fight money laundering and financial crime, especially as markets shift towards digital currencies and a cashless economy where "value" becomes the operative payment method for transactions.

Criminals have seized on globalization that exploits digital commerce to finance an international ecosystem of criminality and illicit trade that is siphoning trillions of dollars from legal economies. The IMF estimates that between 2-5% of world GDP accounts for the magnitude of international money laundering (or up to $6 trillion based on the global economy – $117 trillion in GDP – in 2025).[1] Of course, it depends on what is included in the count. We don't know the IMF's dated internal calculations and methodology in deriving its estimate. But it doesn't appear, for example, tax evasion is included in the IMF estimate. Yet tax evasion is a now a predicate offense for money laundering in many countries and jurisdictions. Forms of underground financing and even capital flight are also not included. Trade-based money laundering is probably underestimated. As this report elaborates, new forms of money laundering are rapidly escalating such as those driven by artificial intelligence and crypto-currencies.

> **So, the actual magnitude of money laundering could actually be much greater than the generally accepted $6 trillion 2026 estimate that has cascading negative effects and critical domestic and international policy implications.**

The dirty monies derived from today's criminal activities are laundered across commercial markets, e-commerce platforms, free trade zones (FTZs), financial safe havens, and hubs of illicit trade that are not only reinvested in profitable industries, but also leveraged to finance greater insecurity and violence around the world.

Criminals and threat networks are connected through a global pipeline of professional enablers and service providers who exploit advances in technology, transportation and other critical infrastructure for the illicit enrichment of their clients.

> **In fact, illicit economies and threat finance systems 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.**

Illicit economies are pervasive threats that undermine democracy, corrode the rule of law, fuel impunity, imperil effective implementation of national sustainability and economic development strategies, contribute to human rights abuses and enflame violent conflicts. The lucrative multi trillion-dollar global illicit economy includes an array of cybercrimes as well as the smuggling and trafficking of narcotics, opioids, weapons, humans, fake medicines, counterfeit and pirated goods; illegal tobacco and alcohol products; illegally harvested timber, wildlife and fish; pillaged oil, diamonds, gold, natural resources and critical minerals; and other illicit commodities and contraband.

Money launderers and criminal enablers are very nimble and adaptive and are constantly finding more ways to reinvest filthy lucre into the legitimate global economy. In this regard, newer illicit finance methodologies surface in changing security landscapes and money (and value) trails in both the physical banking system and the criminal underworld as enablers disguise and launder the proceeds of their clients' illegal activities by exploiting anonymous shell companies in jurisdictions designed to be opaque, along with financial havens and multiple forms of trade-based money laundering.

Transaction laundering takes advantage of the seams and vulnerabilities in the global financial system and the digital world. In this newer reality, illicit finance trends continue to evolve including in emerging digital markets and underground banking systems through pseudo-anonymity, digital assets, and a lack of uniform regulation related to crypto and virtual currencies, Non-Fungible Tokens (NFTs), and online gaming and decentralized finance (DeFi) platforms. Crypto crimes continue to increase significantly in recent years, with illicit crypto volume reaching an all-time high of $158 billion in 2025, up nearly 145 percent from 2024 increasing use of stablecoins by illicit actors.[2] Artificial Intelligence (AI) is increasingly leveraged by criminals to further their money laundering operations by obscuring the origins of illicit funds, bypass or evade Know Your Customer (KYC) and AML monitoring and detection systems including crypto mixers and tumblers.

Moving forward, we must apply "whole-of-society" approaches, leveraging public-private partnerships to enhance information - and intelligence - sharing to better target criminals' illicit trafficking operations, their corruptive influence, and the laundering of the dirty monies.

Breaking their financial wherewithal becomes more necessary and urgent.

In these dangerous times, the International Coalition Against Illicit Economies (ICAIE) is committed to inform interested communities of the expanding dimensions of today's illicit finance harms in our digital world, and similarly, to advance more dynamic policies, action plans, and unity of effort(s) to counter illicit trade and converging market threats including criminals' filthy lucre that, if left unmitigated, will continue to erode our collective governance, prosperity, and security.

John A. Cassara
David M. Luna

The Global Scale of Dirty Money and Value Trails

Greed begets criminality; money laundering enables criminals to use their dirty profits to diversify their illicit enterprises, and to finance a greater cycle of greed crimes.

The amount of illicit money generated globally every year is staggering.

The pernicious criminal activity behind the dirty money affects the peace and security of nations, societies as a whole, and citizens' safety, as trillions of dollars that are the product of transnational crime continuously corrupts the global financial order.

The illegal funds are generated from hundreds of specified unlawful activities. The Financial Action Task Force (FATF) considers all "serious crimes" as predicate offenses for money laundering. While ranking the severity of differing types of criminal activity is subjective, a list of the top twelve transnational crimes that generate illicit proceeds that are subsequently laundered could include the following:

- the trade of counterfeit and pirated goods;
- narcotics trafficking;
- intellectual property theft;
- human trafficking;
- organ trafficking;
- wildlife trafficking;
- illegal logging;
- illegal fishing;
- illicit cigarettes and tobacco products;
- trade fraud;
- arms trafficking and WMD proliferation; and
- corruption.

While estimates of the total annual amount of illicit proceeds generated from the above predicates are subject to debate, there is generally a consensus estimate of about $5-7 trillion annually.

As underscored earlier, globalization and global trade have given rise to a transformative movement of goods, services, people, money and value across borders, and also ushered in lucrative illicit markets and services controlled by drug cartels, transnational criminal organizations, other criminal entrepreneurs and bad actors, and their professional enablers. A new digital world is now a global network of trade, commerce, and illicit activities where the selling and buying of legal and illicit goods and services take place through electronic and digital payouts across online connections, the global trading systems, e-commerce marketplaces, apps,

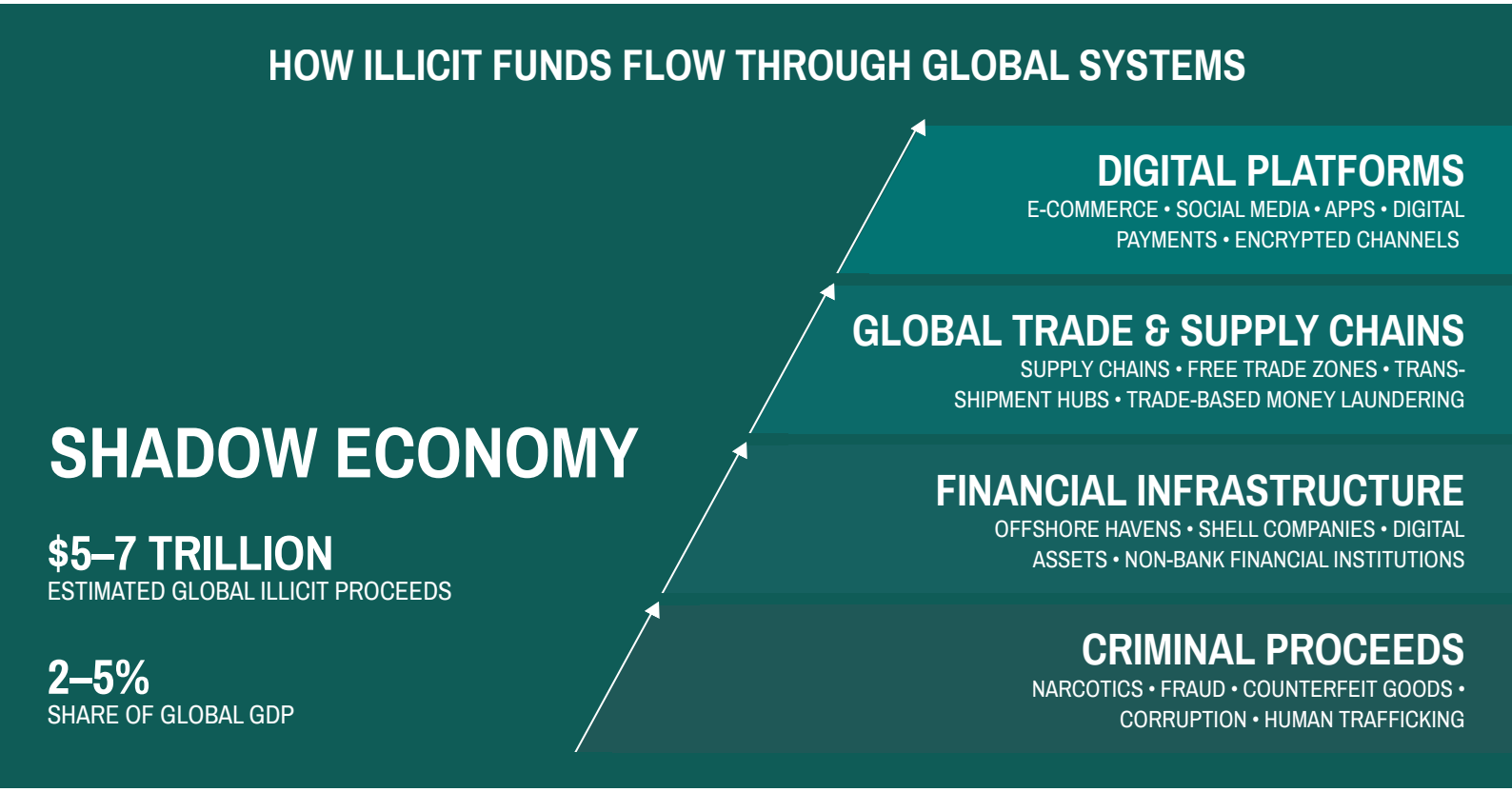
social media, and encrypted channels.

Related to transaction laundering, ICAIE has reported in the recent past on how China may be the biggest illicit finance hub in this new globalized trade world. As the biggest illicit trade syndicate in the world, the Chinese Communist Party, CCP Inc., is a leading market driver (stakeholder) in many of the transnational crime sectors noted above (as predicate offenses), China is responsible for introducing and laundering at least $2 trillion dollars of illicit proceeds into the world's economy every year as measured by Specified Unlawful Activities (SUAs) including washing the criminally-derived proceeds of the Mexican cartels and other transnational criminal organizations (TCOs).

ICAIE believes that the amount of money laundered in the United States alone is estimated to account for at least $1 trillion. Canada is also a money laundering safe haven, enabling the laundering of hundreds of billions of dollars every year for many bad actors and threat networks. Similarly, it is estimated that across Latin America, up to $400 billion is laundered every year related to corruption, drug trafficking, human trafficking, tax evasion, and other crimes.

Over the past few years, the U.S. Treasury's money laundering risk assessments have shown that fraud against government programs including false claims for federal tax refunds, Medicare and Medicaid reimbursement, Covid-19 relief fraud, and food and nutrition subsidies generate more illicit proceeds than drug trafficking. Several other cross-border crimes also yield higher profits than narcotics to transnational organized groups.

Of course, whether international or domestic, estimates of the magnitude of the problem depend on what is included in the count. For example, some countries and jurisdictions include tax evasion and illegal capital flight as predicates for money laundering.



Global regulators report[3] that in 2024 non-bank financial institutions held approximately $257 trillion in assets operating largely beyond traditional banking rules. Due to the secrecy that pervades the tax haven system, precise numbers are impossible to obtain, yet $257 trillion exceeds the combined annual GDP of every country. This hidden parked wealth is unproductive. Concealed offshore wealth also means that governments lose hundreds of billions in tax revenue every year.

And with the miracle of compound returns, the proceeds of crime are integrated into the world's economy. The tainted money multiplies over time, further polluting the world financial system.

It is apparent from news headlines that these staggering amounts of dirty money and the criminal activity behind it corrupts and debases society as a whole. Governments, institutions of all sorts, and industry are tarnished by the greed that generates dirty money.

This siphoning off of vast resources from the more transparent and beneficial legal economies have enormous costs.

Instead of being used, for example, to fund quality education, housing, medical care or investing in productive infrastructure such as roads, sanitation and water treatment plants or food security projects, dark money in secrecy havens is wasted. It is unproductive wealth.

Black money and illicit financial flows undermine the rule law and serve as drivers of endemic poverty, crushing corruption, instability, migrations and violence. It finances violent conflicts of all sorts, fuels impunity, imperils the sustainability of economic development strategies, and contributes to human rights abuses.

As ICAIE tirelessly reiterates, corruption is the great facilitator.

On the micro level, individual citizens are directly affected by the surge of criminality driven by greed. Every day, citizens are bombarded with e-commerce crime[4] reaching out to them directly via their computers and smart phones. For example, counterfeit goods and fake medicines are sold on-line. There are various types of fraudulent schemes peddled via social media. Scams of all sorts emanate from call centers located in India, Cambodia, Thailand, Nigeria, Ghana, Ukraine, Myanmar and other many other countries. Romance scams, investment frauds, and scare tactics that threaten family members target our most vulnerable – particularly the elderly. The situation is being made even worse because criminals are using AI to enhance their nefarious schemes.

Contraband and illicit supply chains are dependent on a "fixer chain" to move the products and repatriate the profits. Much of the logistics of illicit trade piggyback on overwhelmingly legitimate world trade and supply chain.

Because of the mixing of illicit with licit, it is extremely difficult for law enforcement, customs, and tax authorities to identify suspect transactions.

It is critical that we follow the money and value trails.

Unfortunately, we are failing. If we examine the "metrics that matter" in our fight against international money laundering – specifically successful forfeitures, investigations, prosecutions and convictions – total failure is "a decimal point away"[5] or less than one percent. The dismal failure rate is same in the United States and most of the world.

There are many reasons for the horrible results and they have been documented elsewhere.[6] However, what is becoming increasingly clear – and is the focus of this ICAIE Executive Brief – is the old adage of "following the money" isn't as true as it once was.

According the FATF, money laundering through financial institutions and bulk cash smuggling are still two of the top three global money laundering methodologies, other value mediums and new payment methods (nms.) are ascending such as trade goods, cyber currencies, central bank digital currencies, stored value cards, smart technologies, etc. Many countries are moving towards cashless societies.

Of particular note is trade-based money laundering (TBML) – perhaps the largest, most varied, and perverse money laundering methodology. It revolves around various forms of trade fraud and value transfer. In other words, dirty money is masked by trading in goods (and services).

According to the United Nations, global trade (goods and services) is expected to surpass $35 trillion in 2025.[7] The very volume of trade is the primary obstacle for law enforcement and customs services in identifying suspect trade transactions. There is also a lack of awareness and expertise regarding value transfer. And, for the most part, trade-based value transfer and related money laundering methodologies such as underground financial systems, avoid financial transparency reporting requirements which are our primary anti-money laundering countermeasure.

We are seeing a very active evolution in money laundering. Whereas money or value has long been transferred without actually moving, it is now being transferred via mobile payments, mirror swaps, digital assets, cryptocurrency transactions, decentralized finance (DeFi) platforms, end-to-end encryption-powered apps, and other novel digital-technological means that facilitate anonymity and underground criminality (outside of regulated financial systems and evading law enforcement).

Financial crimes investigators are often hard pressed to "follow the money" if it stays in place. Moreover, there is little – if any – financial intelligence.

In short, money is no longer money in the conventional sense of the term. And it no longer "moves" as it did in the past. The challenges are greater than ever. So is the criticality of our efforts to impede the spread of illicit funds.

Digital Commerce and Transaction Laundering

Today, illicit trade and transaction laundering – massive across e-commerce platforms, online marketplaces, and social media – are booming, as more and more criminalized digital markets become lucrative including counterfeits, pirated and stolen products, and other illicit goods and contraband that transverse borders and communities, and enter our supply chains, businesses, and homes.

Due to the recent expansion of e-commerce and e-banking operations, online sales of illicit goods and services are generating billions of dollars for criminal networks through digital payment processing systems and value-based mobile technologies

Cybercrimes across the digital world result 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.

The United States Patent and Trademark Office (USPTO) reports that IP-intensive industries account for close to $8 trillion of US GDP and over 47% of all jobs (as of 2019).[8] This helps to explain why intellectual property theft is a major illicit trade that imposes a substantial cost on not only the US economy, but the global economy as well.

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.

According to the FBI, 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.

IP crime also hurts the ingenuity, innovation, and competitiveness of leading market companies and small-and-medium sized businesses.

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.

Often, transaction laundering includes the formal financial and banking system, unregulated payment gateways, and some payment systems of e-commerce platforms. 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.

Like TBML, daigou, which translates to "buying on behalf of," is also growing problem for trade fraud and money laundering. 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 (or Asian) 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.

Approximately 15% of luxury goods consumption in China comes from daigou, with high-end fashion brands accounting for higher percentages of all total sales in mainland China. Cosmetics from top international brands account for more than half of daigou sales, followed by luxury bags, watches, and jewelry. China's gray markets and daigou schemes may be the biggest threat to luxury brands in the next five years.

Other transaction-based money laundering can occur through stolen identities, credit/value cards, or other forms of digital currencies including cryptocurrency.

According to the U.S. Department of the Treasury, the use of prepaid cards is growing rapidly. Prepaid cards (also referred to as prepaid debit cards, stored value cards, or prepaid access devices) are a type of prepaid access that enables preloading, and in some cases, reloading of funds onto physical or digital cards.

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.

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. 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.

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.

The exponential growth of social media and its role in e-commerce have also directly related to the growing threat of mobile payments and money laundering.

In 2025, over 5 billion people or an estimated 62% - 69% of the world's population were using social media.[9] The average daily usage is 2.5 hours. Worldwide, the number of social media users is projected to increase to 6 billion by 2027.

According to the Pew Research Center, 84% of adults and 81% of teens in the U.S. use social media: YouTube (84% user rate), Facebook (71% user rate), and Instagram (50% user rate) are among the most popular platforms, while TikTok increasingly being used by teens.[10] Usage of online platforms varies by factors such as age, gender and education. 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 ecommerce 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.

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. 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 ecommerce.

Simultaneously, digital platforms are also more and more susceptible to different types of fraud and illicit finance as criminals leverage speed, volume, and anonymity of online marketplaces and social networking platforms including through digital wallets, credit and value cards, and virtual banking transfers.[11] "This convenience also creates many low-friction entry points for illicit funds."[12]

Criminals exploit these features by returns and refunds, vouchers, staged purchases, and multi-account schemes to obscure the money trail. Some even use high-value goods as a store of value, and create fake e-stores that generate phantom sales.

Money Laundering Typologies Found Across E-Commerce & Social Media

- **Fake E-Commerce Store Laundering and Digital Fakes:** Money launderers create shell e-commerce sites or replicate legitimate e-commerce platforms often digital fakes solely to generate fictitious transactions. Illicit funds are processed through payment gateways to accounts that criminals control, without any actual goods or services being exchanged (sometimes called "ghost laundering").

- **Return/Refund Laundering:** Criminals purchase expensive luxury goods with illicit funds or stolen credit or value cards, then return the merchandise to obtain "clean" refunds to a legitimate bank account or card.

- **TBML Mispricing Schemes:** Transactions involve goods that are significantly overpriced or undervalued to discreetly move large sums of money. For example, a high-value item might be "sold" for a fraction of its cost to transfer value, or a cheap item might be sold for a vastly inflated price to clean money. [Learn more in TBML Section above]

- **Gift Cards/Voucher/Coupon Laundering:** Cybercriminals convert illicit cash into store credit, gift cards, or vouchers, which may be resold in the open market or transfer the "value" into legitimate accounts.

- **Arbitraging Fake Vendors:** Criminals use multiple marketplaces, currencies, and payment systems including creating fake merchants or partnering with greedy, complicit vendors to process payments to obscure the fund origin.

- **Influencer Collusion and Mule Networks:** Criminals exploit social media

influencers with large followers and sales or to promote counterfeit and fake products and then use their bank accounts to pass illicit funds and commingle them with their legitimate income. Often times, the social media influencers are often recruited as "money mules," either knowingly or unknowingly, to move money through their personal accounts in exchange for a solid percentage of the funds.

- **Account Takeover:** Criminals use networks of compromised or synthetic accounts to make numerous smaller transactions ("smurfing") and funnel payments across several legitimate accounts.

- **In-Game Currencies and NFTs:** Online gaming and e-commerce-like marketplaces for digital assets (such as NFTs) are used to convert illicit funds into virtual currencies or assets. These can be traded across different accounts and platforms before being converted back into real-world currency, adding layers of complexity and anonymity.

In addition to using these social media platforms to recruit money mules, criminals are able to launder their proceeds of crimes and disguise illicit funds through e-commerce business for goods and services as legitimate revenue through schemes like fake sales, investments, and financial scams.

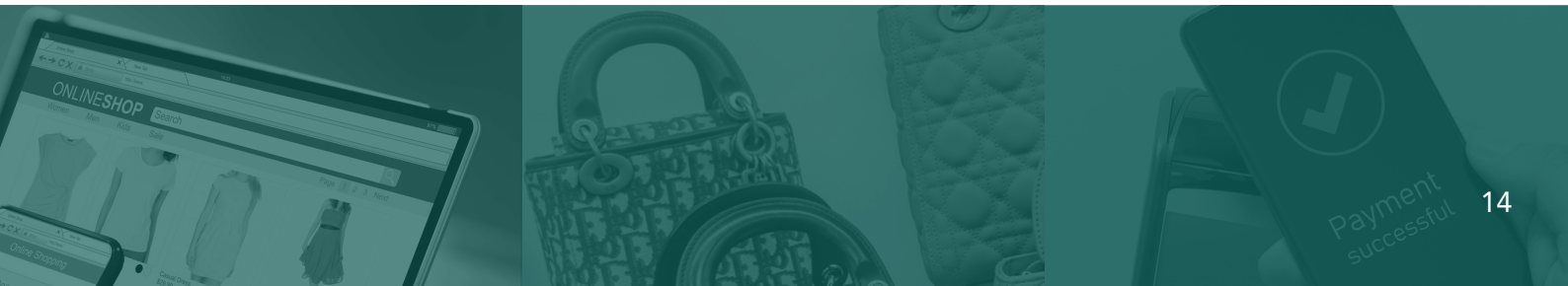
Criminals will also exploit and finance with dirty funds social media influencers, who often generate legitimate revenues, and then proceed to commingle, layer, and integrate the illicit funds into the financial system obscuring their original source.

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.



Underground Banking and the Informal Value Transfer Systems

Following the September 11 attacks, analysts and policymakers focused an immense amount of attention on an ancient system of moving money – hawala. The money transfer system is essentially a simple broker system based on trust. Many different cultures use hawala-like systems. They are often connected to ethnic groups or to specific geographic regions.

Some examples are hawala/hundi (meaning "trust" in Urdu and Hindi; it is indigenous to the Middle East, South and Central/Asia and also found today in the Americas and parts of Africa), fei-chien (meaning "flying money;" indigenous to China), padala (meaning "to send" in Tagalong; indigenous to the Philippines), and phoe kuan (meaning "message houses" indigenous to Thailand).[13]

The above systems are also sometimes called "underground banking," "parallel banking systems," and/or "informal value transfer systems" (IVTS). Today, most of these systems are used to remit wages from immigrants back to their families in "the old country."

Unfortunately, because these systems are underground, hidden, opaque and avoid anti-money laundering countermeasures, criminals and terrorists are also attracted to them. The defining trait common to all of these systems is the transfer of money or value without physically moving it.

This definition was concisely expressed during the 1998 U.S. federal trial of Iranian drug trafficker and money launderer Jafar Pour Jelil Rayhani and his associates, in which prosecutors called hawala "money transfer without money movement."

In other words, a "hawaladar" (the hawala broker) on one side of the transaction accepts money from a customer who wishes to send funds to someone else. The first broker then communicates with a second broker (either directly or indirectly or through third party hawala settlement hubs) who distributes the desired amount to the intended recipient. The delivered money is already in place. The funds do not physically move from, for example, the sender's country to the recipient's country. The equivalent amount of money is already at the destination locale. The brokers profit from customer fees.

After a series of such transfers which generally move both directions, the brokers involved must settle accounts. Somebody is running a surplus and the other a deficit. There are a wide variety of methods used to "balance the books." Some hawaladars use direct bank transfers. Depending on the location, (within Afghanistan, for example), direct cash settlements are sometimes used. But historically and culturally, trade-based value transfer is the preferred settlement method.

Value transfer is predominant in trade-based money laundering (TBML). Money laundering through the over-and-under invoicing of goods and services is a common practice around the world. The key element of this technique is the misrepresentation of the trade good in order to transfer additional value between importer and exporter. The shipment of actual goods and the accompanying documentation provide cover for the transfer of money.

For example, to move money out of a country conspirators can import goods at over- valued prices or export goods at under-valued prices. Or to move money into a country, the participants can import goods at under-valued prices or export goods at over-valued prices.

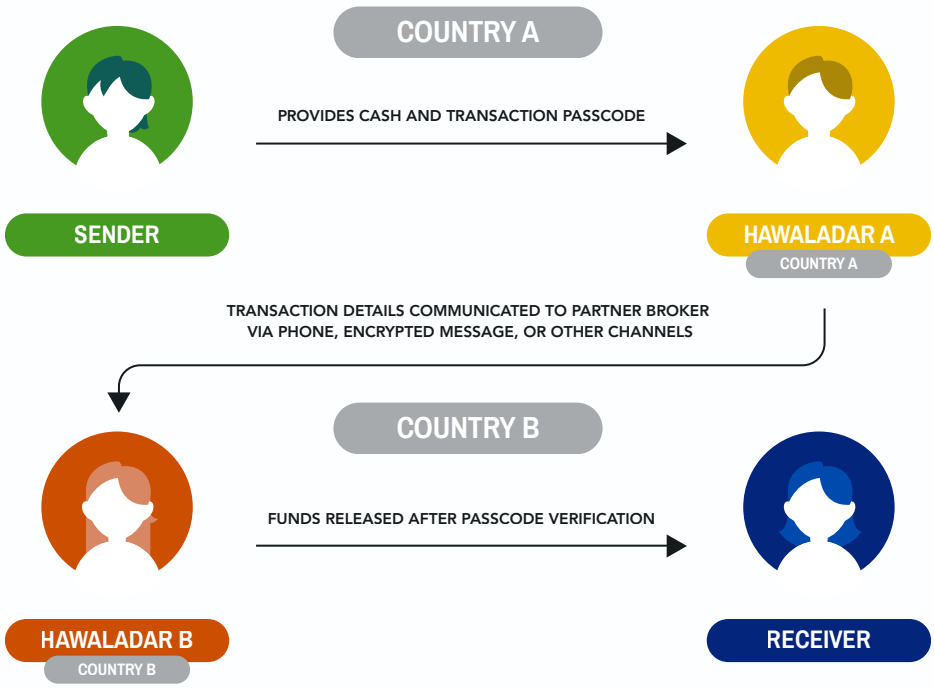
Other frequent forms of invoice manipulation in TBML include falsely described goods, multiple invoicing, short shipping (the effects are similar to over invoicing), over shipping (the effects are similar to under invoicing), and phantom shipping when no goods are actually shipped but the fraudulent documentation is used to justify payment.

Invoice fraud and manipulation have existed since the beginning of commerce. And value transfer, where money stays in place, has also existed since ancient times.

Value transfer is also frequently employed not only to launder money but, from the participants' perspective, because it is often more secure. Value transfer also generally avoids government scrutiny and often times limits or avoids taxation.

Recently, the relationship between tariffs and money laundering has received increased scrutiny. As tariff rates increase, so too does the incentive for both legitimate commercial partners as well as criminal actors to engage in customs fraud and TBML. There is a dual threat. Higher tariffs incentivize evasion schemes, while these same schemes provide a reliable method laundering illicit proceeds from other criminal activities.[14]

HAWALA TRANSFER PROCESS



Another new development is that brokers that use the ancient systems of underground finance are increasingly embracing the modern digital world.

Cryptocurrencies are more and more used in scams due to its hard-to-trace and decentralized nature and prevalence in the dark web. And once a crypto payment is made, it is usually irreversible unless the recipient chooses to send the money back.[15]

For example, some hawaladars use digital currencies to facilitate transfers. The evolving system is sometimes referred to as "hawala 2.0."[16] While traditional hawala was built on trust and a network of brokers, hawala 2.0 uses digital tools to expand its scale and operate with enhanced anonymity and speed. Hawala 2.0 no longer exclusively involves the payment or distribution of physical cash or even is dependent on personal broker interactions. Rather, digital wallets, cryptocurrencies, encrypted communication platforms, and peer-to-peer payment services are now embedded into the system.

Transactions that once relied on the payment and delivery of cash are now completed using Bitcoin, Ethereum, Monero, or privacy-focused tokens. Of course, trade-based value transfers and other traditional settlement methods continue. But hawaladars increasingly coordinate settlements using blockchain transactions, online banking, and even prepaid cards.

Digital currencies reinforce some of the traditional hawala benefits, such as speed and low costs. They simultaneously add another layer of anonymity and complexity to obscure the origin and destination of funds. In other words, they further "layer" transactions making tracking by authorities more difficult. This convergence allows for money laundering and the financing of illicit activities including terror and criminalized economies.

Today there are hybrid channels involving both traditional hawala networks and cryptocurrency exchanges.

How Does "Hawala 2.0" Work?

- Instead of cash, clients sometimes make the payment by depositing funds into a digital currency wallet or converted digital asset.
- Over time, hawala transactions are multi-directional. Accounts between hawaladars have to be settled. With hawala 2.0, a hawaladar settles the value with a counterpart abroad using digital channels.
- The local payout to the hawala client is still generally arranged in the desired local currency.

Digital currencies enhance underground financial systems such as hawala and fei-chien or the Chinese "flying money" systems because they facilitate the movement of funds outside of regulated financial systems. Digital transfers often bypass financial transparency reporting requirements, our primary anti-money laundering countermeasure.

In addition, similar to traditional hawala, digital currencies can bypass the fees and overhead of traditional banking systems. Digital currency transactions can be very fast, enhancing the efficiency of money transfers.

According to the 2022 National Money Laundering Risk Assessment by the U.S. Department of the Treasury,[17] "U.S. law enforcement agencies have detected an increase in the use of virtual assets to pay for online drugs or to launder the proceeds of drug trafficking, fraud, and cybercrime, including ransomware attacks."

Europol notes that "terrorist organizations increasingly use digital currencies and virtual assets service providers (VASPs), as these provide a higher level of anonymity for donors and recipients." Europol continues, "as regards to jihadism, ISIS and al-Qaeda and their affiliates appear to have stepped up the use of VAs (virtual assets), especially cryptocurrencies, for fundraising and the movement of funds in recent years, possibly as a result of an increased knowledge of VAs among members of jihadist terrorist groups. Right-wing extremists also resort to funding platforms operating with cryptocurrencies."[18]

Both traditional hawala, fei-chien, and other underground networks and those using digital currencies and virtual asset service providers are categorized as a money transfer business. Money service businesses (MSBs) are generally regulated and licensed in the country and jurisdiction in which they do business.

But most hawaladars and fei-chien brokers operate underground – both in the United States and around the world.

They are not registered, licensed or follow AML/CFT norms and guidelines including the filing of suspicious activity reports.

They also generally service close-knit family, tribal or clan interests that are almost impervious to law enforcement infiltration and monitoring. Unfortunately, these are some of the reasons why they attract criminals and terrorists.


Trade Based Money Laundering

Perhaps the most extensive or widespread form of global money laundering these days comes from "trade-mis-invoicing" or trade fraud. Trade fraud or customs fraud is a Specified Unlawful Activity (SUA) for money laundering.

Depending on its form, trade fraud can also be a money laundering methodology. It is also the least understood, recognized, and enforced. Most forms of trade mis-invoicing revolve around invoice fraud and manipulation.

Generally speaking, invoice fraud means the contents, description, and/or the value of goods is deliberately misrepresented. Sometimes this is done to facilitate simple customs fraud, i.e., minimize the payment of taxes and duties, avoid currency controls, or move capital or value offshore. International trade via invoice manipulation is also a very common means used by criminals and criminal organizations to illegally transfer value across international borders.

TBML is defined by the FATF 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 origins."[19] The key word in the definition is value.

Instead of following the money trail via cash or the electronic bits and bytes of a bank-to-bank wire transfer, with TBML we examine the shipments of commodities and trade goods. Their sale and transfer—real and fictitious—very effectively launders money, evades taxes and tariffs, and transfers value between cooperating parties in the transaction(s).

TBML is very broad. It includes customs fraud, tax evasion, export incentive fraud, value-added tax (VAT) fraud, capital flight or the transfer of wealth offshore, evading capital controls, barter trade, underground financial systems such as hawala and fei-chien (the Chinese "flying money" system), black market exchange systems, and even forms of commercial TBML such as trade diversion, transfer pricing, and abusive trade mis-invoicing.

For money launderers and terrorist financiers, transferring value via trade goods is particularly attractive because it generally does not trigger financial transparency reporting requirements or the filing of financial intelligence or, as it is commonly called in the U.S., "Bank Secrecy Act data."

Financial intelligence promotes a degree of financial transparency and is our primary AML/CFT countermeasure.

The most common forms of trade mis-invoicing are:

- Over and under invoice pricing
- Multiple invoicing for the same goods
- Falsely described goods
- Mis-representation of the quantity being shipped
- Mis-representation of voyage to disguise origin from sanctioned countries
- Mis-representation of shipment origin and voyage to evade customs duties

How is over and under invoicing used to transfer value and launder money? The key element of this technique is the misrepresentation of trade goods to transfer value between the importer and exporter or settle debts/balance accounts between the trading parties.

When an importer and exporter are working together, they can easily manipulate the invoice to reflect a price that does not adhere to true market value. The shipment (real or fictitious) of goods and the accompanying documentation provide cover for the transfer of money. Invoice fraud is generally considered customs fraud. And customs fraud is the primary predicate offense or specified unlawful activity in TBML cases.

What are the most common invoice scams? First, by under-invoicing goods below their fair market price, an exporter is able to transfer value to an importer while avoiding the scrutiny associated with more direct forms of money transfer. The value the importer receives when selling (directly or indirectly) the goods on the open market is considerably greater than the amount he or she paid the exporter.

For example, Company A located in China ships one million widgets worth $2 each to Company B based in Mexico. On the invoice, however, Company A lists the widgets at a price of only $1 each, and the Mexican importer pays the Chinese exporter only $1 million for them. Thus, extra value has been transferred to Mexico, where the importer can sell (directly or indirectly) the widgets on the open market for a total of $2 million.

The Mexican company then has several options:

1. It can keep the profits;
2. Transfer some of them to a bank account outside the country where the proceeds can be further laundered via layering and integration;
3. Share the proceeds with the Chinese exporter (depending on the nature of their relationship); or
4. Even transfer them to a criminal organization that may be the controlling interest behind the business transactions.

UNDER-INVOICING TBML SCHEME

To transfer value in the opposite direction, an exporter can over-invoice goods above their fair market price. In this manner, the exporter receives value from the importer because the latter's payment is higher than the goods' actual value on the open market.

Here is a simple way of looking at things:

To move money/value out:
• Import goods at overvalued prices or export goods at undervalued prices

To move money/value in:
• Import goods at undervalued prices or export goods at over-valued prices

Unfortunately, the magnitude of TBML has never been systematically examined by the FATF, international financial institutions (IFIs) —e.g., IMF or World Bank—or the U.S. government.

Trade-based value transfers are also not closely examined by many intelligence, law enforcement, and customs services. However, some academics and non-profits have done very useful work examining TBML and estimating the extent of the challenge.

In the United States, Dr. John Zdanowicz, an early pioneer in the study of TBML, conducted research that identified glaring anomalies in U.S. trade data.

For example, Dr. Zdanowicz found:
- plastic buckets from the Czech Republic imported with the declared price of $972 per bucket;
- Toilet tissue from China imported at the price of over $4,000 per kilogram;
- Bulldozers shipped to Colombia at $1.74 each;
- Why are non-industrial diamonds being exported to France for $2.32 per carat but imported from South Africa for $929,390.82 per carat?

Dr. Zdanowicz compares the declared value of the trade good or commodity against true market value. By examining 2021 U.S. trade data, Dr. Zdanowicz found that approximately $784 billion was moved into the U.S. via over-valued exports and under-valued imports. China was the trading partner for about $85 billion of the total. Approximately $640 billion was moved out of the U.S. via undervalued exports and over-valued imports. Approximately $70 billion was moved out to China via suspect trade.

Dr. Zdanowicz then compared those numbers to the overall value of U.S. imports and exports. He found (depending on import or export) approximately 14 to 17% of U.S. trade could well be tainted by customs fraud and perhaps TBML (The above has serious fiscal ramifications. Examining 2021 U.S. trade anomalies, per the above, Dr. Zdanowicz estimates that the U.S. Treasury lost about $640 billion of taxable profits due to trade-based tax evasion and TBML.[20] The same type of trade fraud revenue loss occurs in every country.)

China is the world's largest trading nation.

In 2021, according to CCP Inc.'s own numbers, even factoring in the worldwide pandemic, China's foreign trade volume hit a record high of $6.05 trillion.[21] China's total trade volume was approximately $5.87 trillion in 2023, based on figures from the General Administration of Customs (GAC).

So, if we use a very conservative estimate that only ten percent of trade is suspect, mispriced, or related to forms of trade fraud, that could mean that suspect and possibly illicit Chinese trade is approximately $600 billion a year and could very easily be much higher than that.

By its volume and sheer dominance of international trade, Chinese actors are assuredly involved with a massive amount of trade fraud. In addition, trade also masks money laundering methodologies and value transfer schemes that are instrumental in the trafficking of fentanyl and other forms of contraband.

TBML is attracting more attention due to the tariffs President Trump has enacted.

High tariffs undoubtedly encourage invoice manipulation and transshipment strategies. However, there is not yet sufficient data or enforcement action to quantify increased levels of customs fraud.

Other current events such as Iran sanctions and the Russia–Ukraine conflict have elevated TBML as a primary sanctions-evasion technique. Shadow fleets, diverted cargo routes, transshipments and disguised shipping activity have become common tools to bypass trade restrictions. Post sanctions "flag hopping" has hit an unprecedented pace. The average time between a ship being sanctioned and reflagging nearly halving in 2025. A Lloyd's List analysis of Automatic Identification System (AIS) data reveals the average time from initial sanction designation to a ship switching flags has dropped to 45 days for those sanctioned in 2025, compared to 85 days for those sanctioned in 2024.[22]

In 2025, the FATF also reports a surge in layered shipments, ship-to-ship transfers and opaque beneficial ownership structures.[23]

The Black-Market Peso Exchange (BMPE) continues to evolve. As reported years ago by ICAIE, China is now becoming the money launderer of choice for both Colombian and Mexican cartels. Chinese actors have pioneered new methods to circulate criminal proceeds through informal trade systems (see below).

TBML has also been enhanced by technology. New forms of instant payments such as Chinese mobile apps combined with virtual asset service providers enable funds to move quickly, often without clear links to underlying trade documentation. The technology enablers avoid traditional AML countermeasures making TBML significantly harder to detect.

M-Payments and Mirror Swaps

A notable outcome of the growing use of mobile payments is the increased accessibility of mobile phones and mobile money to conduct tens of billions of dollars of trade and on-line transactions every day across e-commerce and the digital world.

In fact, mobile payments transaction volume reached $8.1 trillion in 2024.[24]

M-payments' popularity stems from the wide array of secure financial services they offer, providing convenience and efficiency. For example, they allow the greater ease of purchase of products, services, the payment of bills, the transfer of money 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.

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.

M-payments have been used to foster transparency and crack down on fraud, extortion, and corruption by ensuring the responsible distribution of salaries and government benefits directly to cellular devices. Cell phones have also become the means for remittances from migrant workers to be sent back home.

The impact of M-payments extends beyond individuals, as they generate more significant revenue for small and medium enterprises (SMEs) and empower the creation of new businesses. Mobile lending is also an increasingly popular service.

But along with an array of benefits, m-payments have also given rise to higher volumes of money laundering around the world.

In recent years, through numerous investigations by U.S. law enforcement working across borders with other security counterparts, their joint operations have uncovered how Chinese money laundering networks (CMLNs) working with the Mexican cartels have pioneered the growing use of "mirror accounts" or "mirror swaps" to launder the proceeds of crime.

Mirror accounts or mirror swaps are illicit methods used to launder the proceeds of crime. They involve the creation of fraudulent financial transactions that via Chinese mobile phone apps aim to obscure the true origin and ownership of illicit funds. With "swaps," Chinese brokers often work with Chinese organized crime groups and cartels to identify Chinese/American cash-intensive businesses willing to cooperate.

How do the swaps work? The Chinese / American businessperson receives illicit proceeds from the Chinese broker working with the cartels. The broker generally has a network of businesses that cooperate, or the broker identifies customers by posting advertisements on internet bulletin boards or private WeChat forums online.

The Chinese-American business later "places" the proceeds of crime into its revenue flow and represents the drug cash as legitimate proceeds from the business. In addition, the cash could be used to assist mainland Chinese citizens that want to circumvent Chinese government capital flight restrictions and, for example, purchase U.S. property and housing, or other high-ticket goods.

Within China, there is growing dissatisfaction with the Chinese Communist Party policies, such as Covid-19 lockdowns, business crackdowns, a dangerous real estate bubble, and paltry returns on savings. Many among the Chinese elites and the growing middle class are desperate to move currency out of the country. The availability of U.S. based criminal proceeds help meet the demand through these mobile mirror swaps.

The complicit businesses are asked to transfer a designated amount of money through Chinese phone apps to accounts based in China. As discussed below, this type of layering is almost impervious to U.S. law enforcement detection and countermeasures. Using a currency converter app on a smartphone, the participants agree on the exchange rate between the U.S. dollar and the Chinese yuan. Once the money is offshore in China, the value can be used to purchase trade goods to further the black-market peso exchange or BMPE.

The purchase of trade items or other tangible goods represents the final integration stage of the money laundering cycle. Or the monetary credits can be re-routed to Mexico or elsewhere per the instructions of the cartels.

It's called a "swap" because the participating businessperson takes possession of the drug cash while simultaneously transferring the equivalent in Chinese yuan from his/her account in China to the account provided by the broker. Of course, the Chinese/American businessperson also receives a commission.

During the years of the original Colombian and Mexican BMPE, the average commission for the black-market peso broker was about 15%. The Chinese commissions average 1 to 2% on the hundreds of thousands or millions of dollars per transaction. And the speed is almost instantaneous.

For the traffickers, the big plus is that the Chinese organized crime groups involved absorb all the risk. The cartels know they will get paid. For added security and even better tradecraft, a burner or disposable phone could be used. Mirror swaps also avoid U.S. financial intelligence reporting requirements – our primary anti-money laundering countermeasure.

HOW DO MIRROR SWAPS WORK?

1

A Chinese broker collaborates with narco-traffickers and finds a willing Chinese-American businessperson.

2

The businessperson receives drug cash and uses their cash-intensive business to integrate it into the financial system.

3

In exchange for a commission, the businessperson conducts transfers of equivalent amounts through Chinese phone apps.

4

Mirror swaps occur when the businessperson acquires drug cash while simultaneously transferring the equivalent in RMB from their Chinese account.

Commonly, the communications and financial transactions between the Chinese broker and the Chinese American business person occurs on WeChat, a Chinese-developed multipurpose app by Tencent. The WeChat app contains WeChat Pay, a digital wallet similar to Zelle or Venmo that allows the user to transfer money. WeChat is very popular both in China and among overseas Chinese.

WeChat is not end-to-end encrypted. Nevertheless, U.S. law enforcement is still reportedly challenged to monitor communications and monetary transactions that occur over it. WeChat's use of a form of only partial encryption still allows Tencent and the People's Republic of China's government access to content. In other words, WeChat usage is closely monitored by Chinese intelligence entities, who are at least tacitly aware of the illicit money flows. This overt use of WeChat for criminal activity like money laundering is an indicator that Beijing is aware of what is happening.

The CCP's refusal to shut the networks down suggests authorities turn a blind eye to such criminality or may even profit from it. According to retired DEA Special Agent Cindric, "It is all happening on WeChat. The Chinese government is clearly aware of it. The launderers are not concealing themselves on WeChat."

Chinese Money Laundering Networks

Money Laundering Networks (CMLNs) that have been active in recent years in laundering tens of billions of dollars annually for the drug cartels and other TCOs including in the illegal fentanyl trade. CMLNs are also referred to as Chinese money laundering organizations (CMLOs).[25] Admiral Craig Fuller, then-commander of U.S. Southern Command, testified in Congress in 2021 that CMLNs helped to significantly underwrite the finances for an array of TCOs.[26]

The International Coalition Against Illicit Economies (ICAIE) has in recent years reported on how the Chinese Community Party (CCP) has leveraged corruption, illicit markets, and predatory trade and lending practices to become the world's largest player in almost every major sector of transnational crime including: counterfeits, trafficking in weapons, humans, wildlife, illegally-harvested timber, fish, and natural resources, theft of IP and trade secrets, illicit tobacco, organ harvesting, and other crimes.[27]

Several trillion U.S. dollars in illicit proceeds every year are generated from predicate offenses for money laundering that touch China's jurisdiction and markets, and are often used to finance China's authoritarian regime. According[28] to ICAIE, China may very well be the biggest money laundering hub in the world and the CCP and its criminal proxies may be among the most profitable transnational illicit trade syndicates.[29]

As while the Financial Action Task Force (FATF), the Eurasian Group, and the Asia-Pacific Group on Money Laundering (APG) has assessed China as largely compliant on most of the FATF Recommendations to combat money laundering and terrorist finance, China remains a jurisdiction of concern on the laundering of proceeds of crime.[30]

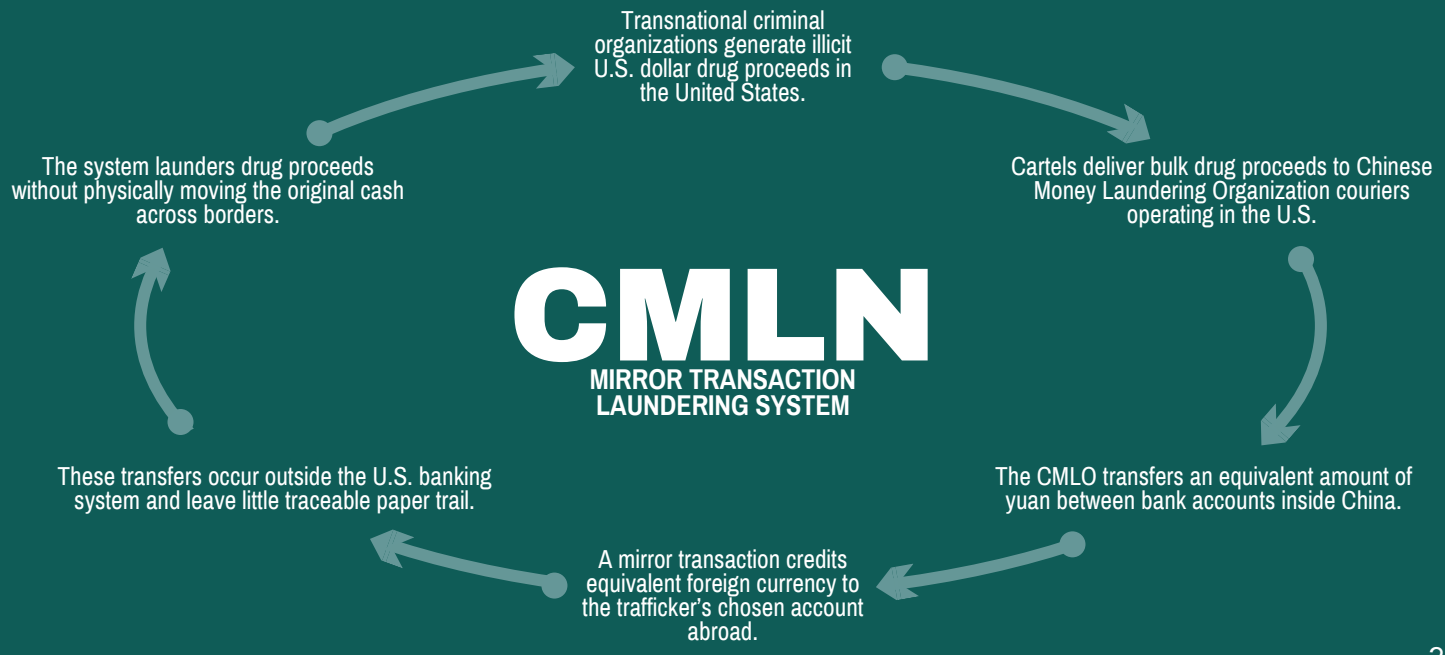
As noted below, the U.S. Financial Crimes Enforcement Network (FinCEN) in a 15-page advisory and 21-page analysis released in August 2025 sounded alarm bells in CMLNs using trade-based money laundering, mirror transaction methodologies, and

other illicit financial schemes to move and hide funds for the Jalisco New Generation Cartel (CJNG), the Sinaloa Cartel, the Gulf Cartel Mexican cartels and other Mexican-based TCOs.[31]

In the United States, CMLNs operating as unregistered money services businesses (MSBs), exploit the international banking system by serving as money brokers in the global Chinese underground banking system (CUBS), which provides Chinese citizens the ability to move funds out of China despite the PRC's currency control laws, and laundering proceeds of crime (including trafficking in illicit fentanyl, marijuana, counterfeits, humans, and other illicit goods and contraband).[32] China also allows Chinese citizens to only convert about $50,000 worth of Chinese currency into U.S. dollars annually, while restricting the direct transfer of Chinese currency abroad. Many affluent individuals in China are able to evade these currency controls by buying dollars through encrypted apps from CMLNs that exchange the U.S. currency for Chinese currency through underground informal value transfer system (IVTS) often as part of a money laundering scheme.[33]

Chinese triads and money laundering organizations also provide fei-chien ("flying money") and mirror swaps to clean not only drug profits but also for both licit goods and for illicitly-traded counterfeits and illegal goods such as Amazonian gold, wildlife, timber, critical minerals, and other natural resources.[34] More specifically, according to a senior official with DHS Homeland Security Investigations, mirror swaps work as follows:[35]

> *[I]n mirror transactions involving illicit drug proceeds, a TCO delivers the cash drug proceeds to a CMLO courier. Upon receipt of the illicit cash proceeds in the United States, the CMLO transfers a comparable amount of yuan from a bank account it controls in the PRC to another PRC-based bank account the CMLO is using to launder funds. Often, the bank account nominally is in the name of a company not otherwise affiliated with the underlying criminal activity. Once this transaction occurs, a second "mirror swap" occurs which results in a comparable sum of foreign currency being credited – almost immediately – to the drug trafficker's account of their choosing anywhere in the world. These transactions occur outside the U.S. banking system, with no paper trail that connects the criminal proceeds originally obtained in the United States with the final cash in the hands of the TCO. This method also allows TCOs to avoid the risk and cost associated with attempting to smuggle bulk cash across borders.*



An Archipelago of Trans-Shipments, Free Trade Zones, Criminalized Ports

Trans-Shipments: Evading Tariffs

In a multi-polar world of geopolitics, global trade, trans-shipment and tariffs, China and other countries under threat of higher tariffs or sanctions have been known to exploit U.S. trade laws in the recent past—including by unlawfully transshipping products through third countries into the United States—to circumvent tariffs and duties, evade customs enforcement, sanctions or obfuscate the origin of products produced in some cases, whole or in part with forced labor.

The use of transshipment to evade U.S. tariffs is a serious violation of U.S. law and undermines American economic and national security.

To evade Section 301, 232, and 201 tariffs and duties, many PRC companies ship their "Made in China" products to countries that do not face tariffs at the same level as those the United States imposes on the PRC.

Without fundamentally transforming the product, these companies then ship their "Made in China" products to the United States (EU and other markets) under the guise of being made in a country other than the PRC.

According to the US Congress,[36] an entire industry of PRC logistics companies has emerged since the imposition of Section 232 and 301 tariffs on the PRC in 2018, with logistics brokers openly advertising that they can "break [...] the barriers of international trade and antidumping to let Chinese products enter international markets successfully" and that "transshipment is the only way to avoid high tariffs and import limits:

> *These companies boast of tariff evasion by sending steel, aluminum products, clothing, and stainless-steel sinks, among other goods, through third countries to the United States, and Europe, including by obtaining false certificates of origin in third countries for goods made in the PRC.*[37]

These customs-trade fraud schemes and trans-shipments cost the U.S. government billions of dollars in lost tariff revenue annually. Many other governments around the world similarly lose tax revenue to such criminalized trade schemes including via trade-based money laundering.

As a hypothetical scenario in today's global trade rows, to avoid the tariffs, Chinese consumer goods manufacturers may re-engage in nearshoring by shifting their supply chains to countries such as Mexico, or other countries not facing as high of an American tariff imposition.

Thus, to protect margins without having to adjust supply chains, some Chinese factories would evade the threatened higher tariffs by shipping their US-bound products to neighboring countries including Vietnam, Malaysia, and other Southeast markets. Once the goods arrive in these markets, for example, they would be relabeled as Vietnamese or Malaysian exports and sent to the United States.

The Aftermath Turbulences of Tariffs and High Duties in Global Trade and Commerce[38]

A recent 2026 U.S. Trade-Tariffs Conundrum has illustrated the 2nd and 3rd order effects of the long-term impacts of higher tariffs and duties on trade and how they will continue to contribute to the expansion of the global illegal economy: Higher tariffs on imported goods or higher duties on certain goods frequently act as a catalyst for increased criminality, counterfeiting or illegal domestic manufacturing and the proliferation of cheaper, often illicit, alternatives - expanding the global illegal economy and black markets.

By raising the cost of legitimate goods, tariffs and related taxes create a price gap that criminal entrepreneurs and counterfeiters exploit, making illicit goods and black markets more attractive to cost-conscious consumers.

Numerous case studies have shown that while reducing tariffs after they have been raised does lower the cost of imported goods or taxes on excise goods, for example, it does not necessarily eliminate the growth of illicit markets which benefitted from the increased demand for cheaper, counterfeit, or illicit goods triggered by earlier tax, trade policies, and economic conditions.

Moreover, lowering tariffs or taxes to earlier rates do not eliminate the incentivized criminal behaviors, infrastructure, counterfeit operations (or illegal manufacturing) or smuggling networks that are deeply entrenched and profiting from illicit trade often with complicit state actors.

In light of a recent U.S. Supreme Court decision finding the Trump Tariffs unconstitutional, we need more evidence-based research and case studies on the following issues/questions:

1. The broader global impact of higher tariffs (duties) on the possible expansion of illicit trade and/or illicit markets internationally, including the abuse of transshipment points or Free Trade Zones (FTZs); and

2. Do global illicit markets (high criminal market penetration) remain in place when tariffs or duties are subsequently lowered as consumers get accustomed to the cheaper – including fake or counterfeit – alternatives and don't gravitate back to the earlier brands and goods that they were buying before these tax policies were instituted?

The Licit-Illicit Trade Conundrum

Around the world, higher tariffs lead to consumers paying more out-of-pocket for imported goods. There are diminishing returns on revenue as tariffs hit a certain percentage point that has collateral damage to a national economy.

In many instances, higher tariffs and duties on consumer goods also lead to an increase in illicit trade, more counterfeits, cheaper (lower quality) goods, and organized crime. But what happens in high tariffs trade policy regimes or in markets with high excise tax, once higher tariffs or duties are lowered (e.g., recent U.S. Supreme Court decision that the Trump tariffs are unconstitutional)? Or when excise taxes are lowered?

Do illicit markets remain in place as consumers have become accustomed to the cheaper – including fake or counterfeit – alternatives and don't gravitate back to the earlier brands and goods that they were buying before these tax policies were instituted?

Kine-Dynamics/Threat Convergence:
There is concern in some law enforcement communities that higher tariffs and taxes actually fuel greater illicit trade and the expansion of illicit markets, and related organized crime, illicit trafficking and smuggling, and tax evasion.

POLICY SHOCK **Higher Tariffs on Imported Goods**	Tariffs and duties increase the retail cost of legitimate imported goods for consumers.
MARKET DISTORTION **Price Gap Widens Between Legal and Illicit Goods**	As legal goods become more expensive, counterfeiters and criminal entrepreneurs exploit the price differential between licit and illicit products.
CONSUMER RESPONSE **Demand Shifts Toward Cheaper Illicit Alternatives**	Cost-sensitive consumers increasingly purchase counterfeit, smuggled, or illicitly manufactured goods that offer lower prices.
CRIMINAL EXPLOITATION **Expansion of Smuggling and Counterfeiting Networks**	Organized criminal groups scale up illicit supply chains, smuggling routes, and counterfeit production to meet rising demand.
LONG-TERM OUTCOME **Illicit Markets Persist Even After Tariffs Decline**	Even when tariffs or duties are later reduced, illicit markets often persist as criminal infrastructure and consumer behavior have already adapted.

Free Trade Zones: Conduit for Counterfeits

Many countries have developed Free Trade Zones (FTZs) to promote and accelerate economic development. FTZs are designated regions that usually lay beyond the economies' customs jurisdiction, and hence, are not subject to customs tariffs or inspections that would apply to imported products. FTZs are important in global commerce and have been used for centuries to increase trade among countries and businesses and their popularity has soared in the last 50 years. In 1975, there were only 79 FTZs in 25 countries; today, there are over 5,000 FTZs worldwide. In the past five years, at least 500 more zones have been announced, with the majority of them expected to be operational in the coming years. Today, FTZs support scores of millions of direct jobs with exports valued at approximately $3.5 trillion annually.[39]

FTZs––also known as special economic zones, free ports, or free zones––are designated transshipment areas that provide benefits such as duty and tax exemptions, simplified administrative procedures, and duty-free imports of raw materials, machinery, components, and equipment, and liberal foreign exchange regulations. All contribute to increased trade, business development, technology transfer, and foreign investment. While FTZs advance exports, foreign direct investment, and domestic employment they also offer exemptions from certain revenue, financial, and labor requirements.

Evolving in response to global economic development as governments become more dependent on them to stimulate economic growth and investment, FTZs have become synonymous with globalization. However, the standards, supervision, and regulations within these zones have not kept pace with the rapidly-changing global supply chains and "just in time" delivery strategies.

International frameworks governing FTZs currently fail to consider money laundering vulnerabilities and the risk of illegal activity. Perhaps more significantly, certain enterprises operating in FTZs are exempt from national AML legal and regulatory frameworks since their activities falls outside the scope of onshore financial industry providers. As a result, the anti-money laundering requirements, even if they do exist, do not apply to businesses within these special regions.

The sheer number of FTZs, coupled with the lack of uniform standards, complicates the mission of rationalizing their activity. Standards and rules vary significantly across the globe and even within a same country. Because they exist to facilitate large volumes of commerce, they are inherently more vulnerable to illicit activity. What the formal economy views as faults and vulnerabilities in FTZs, the criminal economy views as chances for money laundering, illicit commerce, and terrorist financing.

Through illicit commerce and the abuse of maritime containerized shipping, counterfeits, illicit goods and contraband are flooding markets across the region

through FTZs. The goods are mostly from China and other parts of Asia. Latin America remains a transit point to the U.S. of fake products, with some posing great danger to all consumers such as counterfeit medicines, vaccines, or personal protective equipment (PPE) as was the case during COVID-19 pandemic.

The FTZs of primary concern include UAE's Jebel Ali Free Zone (JAFZA), Panama's Colon Free Trade Zone, Isla Margarita in Venezuela, Maicao Special Customs Zone in Colombia, Tri-Border Area (TBA) in Ciudad del Este in Paraguay, the Aruba Free Trade Zone, Corozal Free Zone in Belize, and others. The TBA has become one of the world biggest hubs of illicit trade including narcotrafficking, cigarette smuggling, counterfeiting, money laundering, and other criminal activities worth an estimated tens of billions of dollars per year. The TBA is also a significant hub of the illicit tobacco trade in Latin America, known for its multitude of knockoffs of well-known cigarettes brands.[40] In a country that consumes about 2.5 billion cigarettes annually, at least 65 billion cigarettes are produced in Paraguay.[41]

The abuse of one FTZ in the region can cause ripple effects globally. For example, in the recent past, the Cártel del Tobaco, which has numerous business connections with the Cartel Jalisco Nueva Generación (CJNG) and Cártel del Noreste (formerly known as Los Zetas), has illegally imported illicit cigarettes from China, UAE, India, Paraguay and other countries, including through the misuse of Free Trade Zones (FTZs) in Panama and Belize. For example, in early 2020, the U.S. Department of Homeland Security (DHS) seized over 420 million smuggled U.S.- made cigarettes transiting to Mexico. At the time, this was one of the largest illicit cigarette seizures recorded in the U.S., with a total value estimated at $88 million. FTZs/bonded warehouses were instrumental in moving such contraband from the UAE and Panama into McAllen, Texas.

Across Southeast Asia a number of economic zones have thrived as hubs of illicit trade especially the Golden Triangle Special Economic Zone (GTSEZ), located along the Mekong River in the Golden Triangle area where Laos, Myanmar and Thailand meet, and the Boten Special Economic Zone along the Laos-China border. In addition to tens of billions of dollars laundered through casinos, crypto exchanges, and underground banking, Asian criminal syndicates have engaged in poly-criminality including corrupt activities, financial scams, and illicit trafficking in narcotics/synthetic drugs (e.g., meth), humans, weapons, counterfeits, fake medicines, endangered wildlife parts, illegal timber, illicit cigarettes, and other contraband. Financial crimes such as "pig butchering" romance scams and other cyber frauds have also flourished in these economic zones and other hot spots in the Southeast region. Recent reporting estimates that such scams have defrauded Americans alone of nearly $10 billion per year, and many more billions of dollars from people in other parts of the world. Tens of thousands of trafficked individuals were recruited by criminal networks to perpetrate such online fraud on a global scale.

The spread of cryptocurrencies and digital payments have helped to finance the ecosystem of criminality and corruption. "Proceeds from scams are passed through mule bank accounts, exchanged to virtual currency, moved through various crypto wallets and mixed (with tumblers) with other funds, laundered by over-the-counter brokers, and reintroduced into formal banking channels."

CLEAN FTZ Act

In April 2025, U.S. Senator Bill Cassidy, M.D. (R-LA) introduced the Containing and Limiting the Extensive Abuse Noticed in Free Trade Zones Act (CLEAN FTZ) Act to create a trade rating system based on U.S. and international standards to combat trade-based money laundering and other criminal activities in foreign free trade zones. Currently, no formal rating system for free trade zones exists making it challenging for federal enforcement authorities to address illegal trafficking of illicit narcotics, persons, weapons, tobacco, counterfeits, commodities, wildlife, and more.

"Why are we trading with countries that don't fight corruption?" said Dr. Cassidy. "We are combating the flow of illegal drugs, weapons, and more. Seems important."

The CLEAN FTZ Act:

- Creates a formal rating system with four tier classifications of countries based on compliance to U.S. and international standards.
- Gives countries an overall rating based on the performance of all free trade zones under their national jurisdiction.
- Makes the ratings publicly available and is updated annually.
- Allows the Commissioner of U.S. Customs and Border Protection to make recommendation to improve efforts to combat illicit trade to countries rated tier II, III, and IV.
- Creates a hotline for reporting of instances of illicit trading and money laundering activity.
- Provides financial penalty options for foreign persons involved in illicit international trade.

Senator Cassidy was joined by U.S. Senator Sheldon Whitehouse (D-RI) in introducing this legislation.

The CLEAN FTZ Act is supported by the International Coalition Against Illicit Economies (ICAIE), Advocacy for Transparency International U.S., the Global Financial Integrity (GFI), and other market stakeholders.

> *"We applaud Senators Cassidy and Whitehouse for their leadership in protecting our national security, American competitiveness, and the health and safety of our citizens by countering illicit trade, organized crime, and money laundering across some of today's risky free trade zones around the world," said David M. Luna, Executive Director for ICAIE. "Disrupting the increasing cross-border flows of illicit goods, contraband, and dirty monies and dismantling transnational illicit networks and their enablers from financing other criminalities and threats helps all communities to secure greater peace and security."*

Colón Free Trade Zone

The Colón Free Zone (CFZ), which is one of the world's largest free ports, is located near the Atlantic entrance of the Panama Canal. CFZ was established in 1948 and has historically served as the key commercial hub for Latin America and the Caribbean, and for trans-regional shipment of goods from other parts of the world. It began in a modest part of Colón with only ten businesses and is presently home to over 2,500 businesses and occupies an area of 1,065 hectares. Total trade (imports and exports) passing through the zone was valued at $24.7 billion in 2024, a considerable decline from the CFZ's 2012 peak, when total trade reached an astounding $30.8 billion.

Among the benefits for businesses operating in CFZ, and other free trade zones (FTZs) in Panama, are the numerous incentives and exemptions from paying import duties and re-export fees, as well exemption from income taxes on profits from foreign operations.

For decades, a lack of transparency and systemic corruption has enabled a thriving illicit trade environment in the CFZ, where goods are imported, manufactured, repackaged, and reexported, often as contraband products, to many markets across Latin America and the Caribbean, if not globally. As such, the CFZ is also known as a hub of illicit trade including counterfeit apparel, footwear, electronics, illegal alcohol products, medicines, and other fake goods and contraband. It has also become a notorious hub for smuggling illicit white cigarettes coming from China, Korea, India, UAE, Paraguay, and other countries. In recent years, Panama-based networks using shell companies have been quite active in exporting significant volumes of Chinese illicit whites "in transit" from CFZ across Latin America and the Caribbean including to Colombia, Costa Rica, Dominican Republic, Ecuador, and other nearby markets. Additionally, these cigarettes are transported to other FTZs, such as the ones, for example, in Guatemala, Trinidad and Tobago, and Chile. The reason these cigarettes and many other forms of unlawful trade pass through special economic zones such as the CFZ is to facilitate the change of their certificates of origin, a process known as origin laundering. There is often collusion between cigarette smugglers and complicit customs officers and other government officials in destination FTZs.

The CFZ has been impacted by the economic crisis in Venezuela, and over the years, escalating trade dispute between Panama and Colombia over re-exports of footwear and textiles from the zone to Colombia.

Finally, numerous international organizations and investigative exposes have highlighted Panama's notable distinguishing qualities free trade zones, particularly the integration of illicit drug trafficking and money laundering. Panama's limited banking regulations, dollarization of the economy, and historically corrupt and lax court system make it a perfect place for money laundering operations on a global scale. One of the CFZ's most widespread challenges is its proximity to the illegal cocaine trade located in Colombia, Venezuela and Ecuador.

Criminalized Ports

In any given year, cargo ships and maritime vessels transport hundreds of millions of containers, comprising close to 90% of the world's goods.

The global scale and volume of such trade create vast opportunities for criminals to hide and move illicit goods to destinations across the world. Maritime trafficking is the favored method of smuggling illicit drugs, counterfeits, and other contraband across the Americas through routes in the Atlantic, Pacific, the Caribbean Sea/Gulf of Mexico, and other oceans and seas. There is a growing consensus that escalating security threats demand a more coordinated and unified transnational strategy to enable targeted disruptions of the logistics and fixer networks of transnational organized crime, including targeting unruly spaces in FTZs and ports.

Globally, many maritime ports have become "criminalized" hubs for illicit trade, drug trafficking (including fentanyl), and money laundering by cartels, Chinese Triads, Eurasia Mafias, and other threat networks. These networks exploit supply chains across Free Trade Zones (FTZs) and other risk points, creating inter-connected "criminalized" nodes that threaten global security.

Europol has underscored how criminal networks continue to infiltrate ports across Europe to expand their illicit trafficking operations including by seeking greater control of major logistical points and other critical other infrastructure.[42]

> *Criminal networks arrange the infiltration of ports and coordinate local networks of corrupted port insiders to organise the passage of containers containing illicit goods into the EU. For this, they rely on worldwide networks of cells with trusted members, or use dedicated service providers. They work in a targeted way, by analysing insider data to select container shipments that are less likely to be inspected and that are organised by logistics companies where they have access to corrupted actors.*[43]

The EUROPOL report also noted some of the methods used by criminal networks to extract illicit goods and contraband (e.g., cocaine and synthetic drugs) from ports such as the use of misappropriated container reference codes (or so-called PIN code fraud). Corruption was another enabling factor used for criminal infiltration of European ports including through bribery and the vulnerable exploitation of port workers and personnel of shipping companies, freight forwarders/shipping agents, importers, transport companies, terminals, security companies, law enforcement and customs.[44] But criminalized ports have also become weak links and threat multipliers across global supply chain security operations.

Ports across the Americas also continue to be exploited or remain vulnerable to transnational criminal organizations that corrupt officials and strategically use

maritime shipping as logistical platforms to move tens of billions of dollars' worth of narcotics, precursor chemicals, opioids, counterfeits (electronics, apparel and footwear, tobacco products, pharmaceuticals), stolen cars, pillaged gold and other critical minerals, illegally - poached wildlife, illicitly-harvested timber; and other goods.

The urgency in the Americas is due to the fact that cartels and organized criminals have co-opted a growing number of governments at all levels. These "criminalized states" use transnational organized criminal groups as instruments of state policy rather combatting them, fundamentally realigning the purpose and objectives of the state. The paradigm of the criminalized state is Venezuela, closely followed by Nicaragua and other members of the Bolivarian Alliance of populist authoritarian regimes.

These criminal groups now control critical strategic infrastructure such as major ports and FTZs, while expanding into agriculture, mining and pharmaceuticals. There are multiple examples:

- In Mexico, the cocaine cartels and other illicit actors wield great influence over the largest seaports including Lázaro Cárdenas, Manzanillo, and Veracruz, where they control smuggling operations for an array of counterfeits good, precursor chemicals for fentanyl other illicit drugs, and a broad array of contraband. These strategic assets enable them to move illicit goods across Mexico, into the United States, and beyond.

- In the Northern Triangle of Central America – Honduras, El Salvador, and Guatemala – endemic corruption, grinding poverty and transnational gangs have generated systemic violence and impunity while creating conditions for mass migration and long-term ungovernability. The Mara Salvatrucha (MS-13) gang, along with Mexican cartels, and a complicit kleptocratic network of government officials, have created convergence centers in key ports of the deeply criminalized states of Honduras and Guatemala for multiple transnational criminal networks from China, Russia and Mexico. This in turn leads to increased trafficking of drugs, weapons, human being, and other contraband leaving many individuals, especially young adults, with the choice of joining gangs or cartels or seek to migrate.

- According to Brazilian Federal Police, the port of Santos, second largest port in Latin America after Colón in Panama, has become one of the biggest cocaine trafficking hubs in the world and biggest illicit transit points of contraband to Europe. Criminals are able to bribe government officials across the Andean region to Brazil, and onwards in other connected maritime ports in moving such narcotics. Among the biggest criminal organizations operating out of São Paulo is the First Capital Command (PCC) which has strategic partnerships with the Latin American cartels, Hezbollah, Italian mafia groups, Chinese triads, and other illicit networks.

- In Chile's Port of Iquique, weapons trafficking has increased in recent years as criminals leverage vulnerabilities in the port to commingle guns with other contraband to distribute to other parts of the region. The port is also the center of Shi'ite Islam in Chile, and Hezbollah has a strong foothold there. According to

> Chilean prosecutors, criminal organizations, including Hezbollah have been taking advantage of Chiles industrial free trade zone, its ports and its border situation to "reach other destinations, or to reach our country more easily with firearms of this caliber.

Key hubs of illicit trade in the Asia Pacific region (e.g., the Mekong region) and other transit points across Pacific Islands (Fiji, Palau) are similarly targeted by criminal networks due to limited monitoring capabilities.

The Mega Maritime Port of Chancay in Peru

The PRC's Transformative Acquisition of Chancay Port: The inauguration of operations in Chinese-controlled mega container port of Chancay, Peru on Nov. 14, 2024, likely represents a transformational moment in global supply lines and the correlation of Great Power forces in the Western Hemisphere. Its importance is perhaps matched only by the 2018 initiation of the PRC's autonomous, military control deep space station in Neuquén, Argentina, in displacing the United States' strategic influence, military power and economic interests.

The magnitude of the impact of the hemisphere's newest mega container port in the PRC's global strategy of economic and technological dominance is hard to overstate. In the strategic hemispheric and global contexts, the port will reshape global supply chains, solidify China's control of key choke points in those supply chains–particularly crucial links to the United States–while directly challenging vital U.S. hemispheric interests.

The $1.3 billion investment by PRC state owned COSCO Shipping in Chancay, with more than $2.2 billion more to be injected in the next three phases of the port construction over the next six years, is the PRC's most important strategic port acquisition in Latin America and is the crown jewel of its Belt and Road Initiative (BRI). This is part of a concerted effort by the PRC to not only expand its dominance of global trade, but is likely to become a preferred hub of illicit trade, as BRI projects, particularly ports, are noted for being hubs of criminality, trade-based money laundering, strategic corruption and malign influence operations.

ICAIE assesses that the port's operations – set to expand from the current four container berths to 15 berths (11 exclusively for container traffic and four multipurpose piers) on completion– will significantly realign the region's economic and political balance in favor of the PRC and away from the United States.

A full analysis of the impact of the completed port is not possible at this time but will become measurable when Chancay is fully operational and must include an analysis of the changing logistics of the multiple illicit economies that are likely to move operations to the same pipelines built to move legal trade.

A 2020 U.S. Treasury Department sanctions release concluded that "The Chinese enterprises behind the BRI projects have several things in common: their leadership has links to criminal networks or actors involved in illicit activities in other parts of Southeast Asia, as well as China; they have pre-existing organizations engaged in

casinos and crypto currencies; they advertise themselves online to be associated with Beijing's BRI and flaunt connections with key Chinese government agencies; and all of them have established associations that actively seek to assist Chinese nationals."

Conclusions: The port of Chancay, operating with numerous anomalies that characterize strategic Chinese investments, will likely be the catalyst for a profound realignment of South America's licit and illicit supply changes and commerce. It also signals the ascension of China as the region's primary partner of choice for economic, political and strategic development, displacing the United States, which has not matched China's recent investment and commercial activities in Latin America or globally. This realignment will have multiple collateral effects and likely create new illicit economies and ecosystems around those economies that will pose strategic national security challenges to the United States and its allies in the hemisphere and beyond, in a world of interconnected threats.

DISRUPTING ILLICIT PATHWAYS, RISKY FTZS, AND CRIMINALIZED PORTS

Free Trade Zones are generally organized around major seaports, international airports, and national frontiers—areas with significant geographic advantages for trade; the shipping industry moves almost 90% of global goods.

The Role of Financial Safe Havens, Complicit Power Elites, and Enablers

Financial safe havens, complicit power elites, and enablers play a central role in money laundering. They provide the infrastructure and services that conceal and legitimize the proceeds of crime, often by exploiting corruption, secrecy, weak regulations and lack of enforcement. Safe havens are countries and jurisdictions that offer financial secrecy and convenient pathways to launder dirty money.

Corrupt ruling elites are those individuals in power that pillage the national assets of their countries, crippling development and laundering tens of billions of dollars of their illicit wealth in offshore safe havens every year. Criminals' laundromat washers are those co-conspirators who often help launder the dirty monies for drug cartels and transnational criminal organizations, move and reinvest them in the legitimate economy. Such enablers are individuals (for example, lawyers, accountants, and real estate agents) or organizations such as anonymous shell companies and charities that use their influence and expertise to create complex and non-transparent financial structures designed to move money, layer it, and make it appear legitimate. Combined, financial safe havens, complicit power elites, and their enablers help criminals to avoid detection, hide illicit wealth, and integrate it into the legal economy.

Financial safe havens or offshores provide money launderers secrecy and anonymity by negating transparency and accountability. An offshore account is a bank account held in a country different from the account holder's country of residence. These are primarily jurisdictions that provide strong individual, bank and corporate secrecy laws, making it difficult for law enforcement to track the origin of assets. Using enablers (see below), financial safe havens allow the creation of anonymous "shell companies," Limited Liability Companies (LLCs), trusts, and other vehicles which can be used to obscure ownership and the movement of funds.

In recent years, economists have pegged the volume of illicit wealth stashed by kleptocrats at trillions of dollars in offshore centers, shell companies, and reinvested laundered dirty money in G7, EU markets, financial havens, and popular luxury-real estate, casinos, resorts, and other top travel and leisure destinations around the world.[45]

Generally speaking, shell companies do not have active business operations or significant assets. They are "hollow" or non-substantive. They may only be identifiable by a name and mailing address.

While they do sometimes have a number of legitimate uses – such as mergers, diversifying investments, accessing different currencies, or benefiting from potentially higher interest rates or tax advantages, holding assets during complex transactions and protecting trade secrets – anonymous shell companies are often

used for tax evasion, fraud, and money laundering. They are commonly used in the "layering" stage of money laundering.

Offshores help escape homegrown rules, regulations, and financial transparency. They are generally opaque, private, and non-transparent. Their most important attribute for anti-money laundering purposes is that they generally protect the beneficial owner; in other words, the real person or entity who actually enjoys the benefit or proceeds or income of the property or actually controls the trust or LLC even though the title might be in another name.

Financial safe havens and offshores attract illicit financial flows. They provide a hospitable environment for criminals to move illicit money with little fear of investigation or prosecution from their home countries.

In numerous parts of the world other bad actors such as corrupt power elites continue to "use political power to appropriate the wealth of their nation".[46] According to Oxford Dictionary, kleptocracy is defined as the "rule of thieves," or a "government by people who use their power to steal their country resources." Across today's geo-security landscapes, kleptocrats, tyrants, autocrats - and their enablers - exploit every opportunity to leverage power, and to enrich themselves through corruption, fraud, embezzlement, illicit trade, money laundering, and other forms of crime. In a complex, more dangerous world, and with democratic backsliding in some corners, kleptocracy has been increasing around the world and "most countries are failing to stop corruption".[47]

Illicit wealth through corruption and criminality acts as a threat multiplier and is financing an array of conflicts, violence, market chaos, and global instability. Kleptocracy remains a pervasive threat to democracy, corroding the rule of law, fueling impunity, imperiling effective implementation of national sustainability, undermining poverty alleviation and economic development strategies, contributing to human rights abuses, and enflaming insecurity in many regions.

Among the jurisdictions and territories that have been considered as top safe havens for money laundering in the past decade or so include: Australia, The Bahamas, British Virgin Islands, Canada, Cayman Islands (UK), China, Cyprus, Guernsey (UK), Hong Kong, Israel, Italy, Japan, Jersey (UK), Kenya, Lebanon, Luxembourg, Mexico, Panama, The Seychelles, Singapore, South Africa, Switzerland, UAE, United Kingdom, the United States, and others.

Corruption is a predicate offense for money laundering. ICAIE has often called corruption "the great enabler" for various types of criminal activity and illicit financial flows. In fact, according to research conducted by the World Bank's Stolen Asset Recovery Initiative, an analysis of 213 major corruption cases found that in 70% of them, anonymous companies were used to hide illicit funds.[48] When corrupt power elites, their families, and business associates conspire with criminals, they manipulate weak governance structures to erode judicial independence and quash anticorruption investigations and the rule of law so that democracy cannot take hold.

Professional gatekeepers and enablers have helped corrupt power elites and criminals to hide their assets and launder them across financial safe havens around the world through anonymous shell companies, opaque investments, and other legal

mechanisms. Often, these bad actors will work with enablers through offshore banking with shell companies or trusts that contain valuable real estate or other assets.

These professional facilitators and enablers include bankers, lawyers, accountants, wealth managers, art dealers, investment advisors, real estate agents, trust creators, company incorporators, gold and diamond traders, money laundering firms, and other service-based providers.

Professional enablers provide the needed expertise and services for many entrenched money laundering methodologies. For example, attorneys and accountants have played essential roles in the criminal construct and management of complex financial structures needed for laundering.

Attorneys can use their expertise and legal professional privilege and secrecy to facilitate frauds and to conceal the criminal origins of the funds of others. They can assist setting up the legal and financial structures that help money launderers avoid external scrutiny. Lawyers can help registering fictitious companies, structuring layered transactions and set up nominee directors and/or shareholders to help hide the true ownership of assets. They can advise their clients in how to establish a business or cover company with no real operations; one that exists only to assist in layering and to move illicit funds.

Accountants similarly are sometimes employed by money launderers to help prepare financial statements, tax filings, and audits. They may falsify revenue and expenses, create fictious transactions, manipulate financial records, avoid tax scrutiny and assist in justifying suspicious income. Of course, both attorneys and accounts can unknowingly assist money launderers. For example, a client may ask an accountant to wire money to and from various bank accounts without giving any explanation for it.[49]

The business models of offshores and secrecy havens vary. Generally speaking, professional enablers construct offshore registry firms that essentially are one-stop shops that for a fee will do everything from filing tax returns and annual reports to acting as the director of a client's company. Other essential services include providing proxies to serve as company directors, helping clients issue shares and find proxy shareholders, assisting in setting up bank accounts and other financial instruments, and arranging for company formation in other countries and jurisdictions owned or controlled by the client. Arrangements are often handled over the phone or Internet. Some countries and jurisdictions do not require verifiable information.

Countries, jurisdictions and states establish offshore secrecy havens and anonymous shell companies to attract investment and to obtain licensing fees. For example, in 2022, corporate license fees accounted for 14.6 percent of Delaware's state and local general revenue.[50] Delaware's corporate franchise taxes, which include LLCs and other registered companies, constitute a significant portion of its annual revenue, making up roughly 25% of the state's total budget. In 2024, this revenue source was estimated at around $1.8 billion. Professional and other services also provide employment and fosters banking and financial services growth.

The U.S. has long struggled with AML issues involving enablers. In 2001, the USA

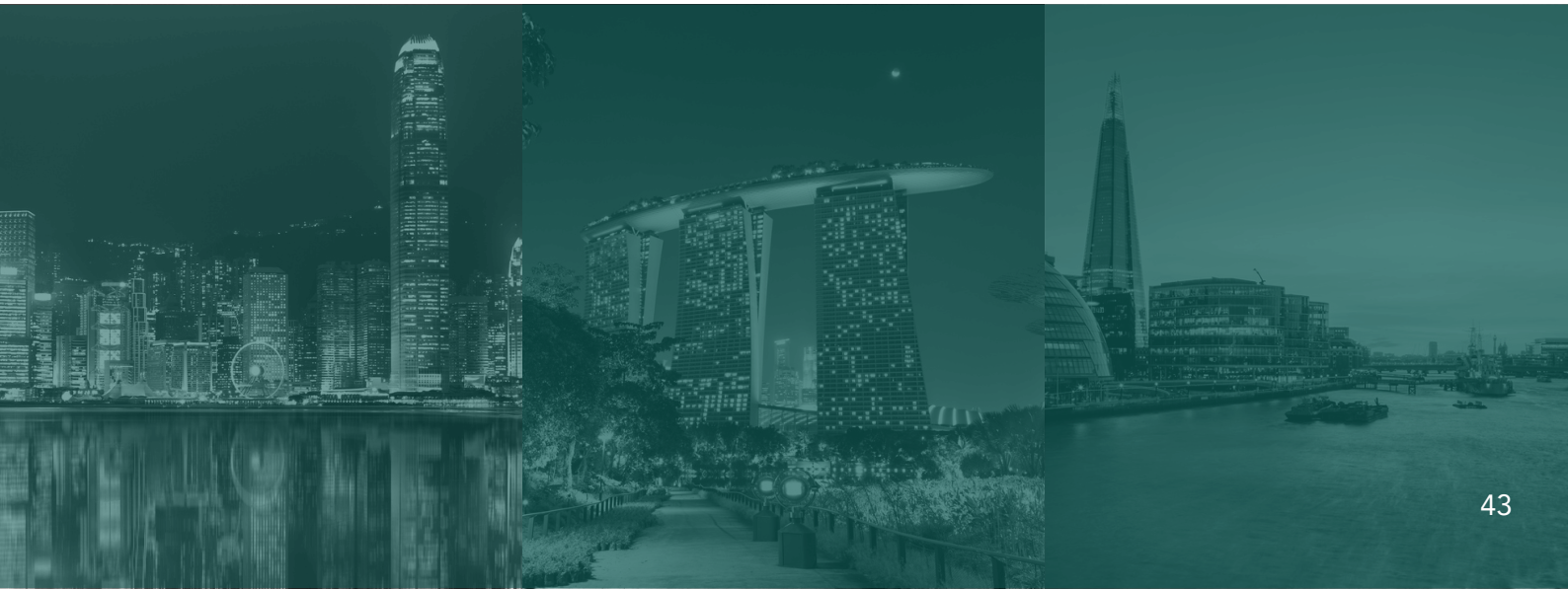
PATRIOT Act significantly expanded the scope of AML regulations under the Bank Secrecy Act (BSA) and mandated AML programs for a wide range of "financial institutions" (such as broker-dealers, investment advisors, etc.). However, the U.S. Department of the Treasury was given the authority to defer the application of these rules to other sectors, including lawyers and accountants, to allow time to study how to apply regulations appropriately.

Almost a quarter of a century later, the Department of Treasury is apparently still studying the issue. As a result, the U.S. has a "non-compliant" rating from the Financial Action Task Force (FATF) regarding anti-money laundering (AML) and counter-terrorism financing (CFT) regulations for designated non-financial businesses and professions (DNFBPs), which include lawyers and accountants. The U.S. has faced global criticism for years because its framework for these professions has been perceived as a loophole for money laundering and tax evasion, as lawyers and accountants are not required to report suspicious activity in the same way financial institutions are.

The end result is that non-transparent safe havens make it more difficult for law enforcement to trace the money. Whether negligent or complicit, enablers can facilitate money laundering by using their expertise for nefarious purposes such as failing to conduct proper due diligence or turning a blind eye to suspicious activity.

Unfortunately, there have been too many instances where enablers assist clients with investing illicit funds into the legitimate economy, sometimes through prestigious investments while safe haven provide the secrecy to prevent detection.

In just one expose, in 2016 a representative of Global Witness, a London-based NGO that promotes financial transparency and accountability, acted in an undercover capacity. He constructed a cover story that he was acting as a representative of a very wealthy West African minister that had personal control over much of his country's mineral wealth. The kleptocrat had access to large sums of money that he wanted to invest in U.S. real estate and other high-end possessions. On behalf of the fictional kleptocrat, the representative approached 16 New York City law firms seeking their guidance. The undercover approach was coordinated with CBS' News 60 Minutes in an episode called *"Anonymous, Inc."*[51] With one exception, 12 out of the 13 law firms, including 15 out of the 16 lawyers, not only heard the undercover representative out, but they suggested ways that the suspicious funds could be moved into the U.S. without compromising the minister's identity.



The New Frontiers

Cryptocurrency, Digital Assets, Non-Fungible Tokens, Online Gaming, AI and Synthetic Identities, Charities

Criminals are moving to newer forms of transaction laundering schemes to move dirty funds and value faster and anonymously. In fact, criminals are finding novel methods to exploit the seams and vulnerabilities in the increasing cashless global economy and digital world to conduct an array of illicit activities and for transaction laundering to obscure, layer, and integrate dirty monies. In this newer reality, illicit finance trends continue to evolve including in emerging online markets and underground banking systems through pseudo-anonymity, digital assets, and a lack of uniform regulation related to crypto and virtual currencies, convertible virtual currency ("CVC") kiosks, Non-Fungible Tokens (NFTs) wash trading especially in the art world, and online gaming and decentralized finance (DeFi) platforms.

Criminals often use virtual assets such as cryptocurrencies, digital value, or Central Bank Digital Currencies – and related technologies that provide anonymity including via encrypted Tor or virtual private networks (VPNs) – to launder dirty funds derived from illicit activities to swiftly transfer money and/or value around the world, thereby making harder for law enforcement to find their IP addresses or coordinates, or trace and confiscate such illegal funds.[52] Transaction laundering using digital assets and crypto can occur in both unregulated exchanges or formal ones using fake digital identities, bypassing verification processes, and other methods and schemes.[53]

The rise of anonymous digital transactions, digital assets, artificial intelligence (AI), and other frontier trends add greater challenges and complexities in fighting newer forms of money laundering as criminals become savvy in the digital age and the advancement of leap-ahead technologies.

Cryptocurrencies

Social media and the internet are regularly used by criminals including in the dark web to launder all sorts of dirty monies often using cryptocurrencies and mixers (tumblers) or peer-to-peer transactional exchanges to increase anonymity and obscure the source of funds.

Bitcoin, the first cryptocurrency, was launched in 2009. Today, more than 10,000 different cryptocurrencies have evolved and followed in Bitcoin's footsteps. Cryptocurrencies are increasingly popular around the world.

In the United States, approximately 25 percent of millennials own Bitcoin, compared to 14 percent of all U.S. adults.[54] 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 ecommerce 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. Convertible virtual currency or CVC kiosks have also populated supermarkets, shopping malls, and convenience stores that allow customers to exchange physical cash for cryptocurrencies such as Bitcoin or Ethereum.[55] These cryptocurrency ATMs are increasingly being leveraged to conduct money laundering, financial frauds and scams.

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.

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 below, 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.

Of note, these bad actors prefer the use of stablecoins such as Tether (USDT) for the stability provided. 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.

Financial Scams

Investment scams are common in many parts of the world. But scammers are also impersonating government agencies, businesses, organizations of all sorts, even dating services and "pig butchering" financial scams especially originating in Southeast Asia, where the target is often 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.

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.

Pig butchering scams are romance scams that typically take place on dating platforms or apps. In this type of scam, often by Asian criminal syndicates, 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." In reality, the funds sent by victims for these purported investments are instead funneled to cryptocurrency addresses and accounts controlled by scammers and their coconspirators.

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.[56] "Once the victim places enough trust in the scammer, the scammer brings the victim into a cryptocurrency investment scheme."[57] 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.

Non-Fungible Tokens

Generally, NFTs are unique digital identifiers on a blockchain that certify ownership and authenticity for digital or physical items such as art, music, or collectibles.[58] NFTs help to create verifiable digital assets, allowing them to be bought, sold, and traded, with ownership recorded and transferable via smart contracts in safer transaction marketplaces, acting as a digital certificate of authenticity that can't be copied, substituted, or divided, unlike fungible cryptocurrencies.[59]

Now artists and other individuals can use NFTs to transform their digital works of art, digital properties and effects. A buyer of such unique art, makes them the owner of an original digital asset that cannot be copied, substituted, or divided.

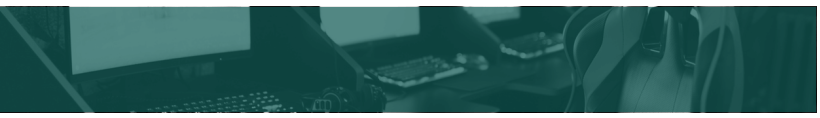
However, counterfeiters and other criminals, for example, may forge NFTs by counterfeiting expensive and rare digital art pieces or cultural artifacts, creating smart fraudulent contracts with falsifying data that possess unique properties, and selling them as forgeries in auction houses or online marketplaces.[60] Money launderers too exploit NFTs including by overpaying to another party and transferring ill-gotten gains, and giving such a transaction the appearance of legitimacy from an NFT sale. Another method includes creating one's own NFTs and selling it at inflated prices or to oneself through different digital wallets that they control and successive transactions, one's anonymous shell company, or a complicit third party.[61] Artificially created NFT certified wealth could be used to launder illicit funds.

Like other forms of illicit finance, money launderers can leverage crypto wallets and exchanges virtually anywhere in the world to sell and buy NFTs, often in anonymity or disclosing where the funds came from and making it difficult to ascertain any illicit activities.

Synthetic Identities and AI Sophisticated Deepfakes

As noted above, artificial intelligence (AI) continues to create new opportunities for criminals in the world of counterfeiting including through the creation of authentic-looking product images, videos (highly sophisticated deepfakes), and marketing materials, making it difficult for consumers and even algorithms to distinguish fakes from legitimate goods.

But criminals are also leveraging AI technologies to create convincing fake documents and synthetic identities by combining real and fabricated information to open accounts and execute transactions, bypassing standard Know Your Customer (KYC) procedures.[62]



Online E-Sport Gaming

While gambling is often associated with online gaming and is, in and of itself, a significant challenge in fight money laundering across casinos including across the digital world, a newer trend online also involves professional video electronic-sport gaming (e-sports).

E-sports include digital competitions in which different players and teams are organized and compete against one another.

In many cases, players and teams can earn virtual currencies and convertible in-game currency which can be traded with others through an exchange platform. In 2024, it generated close to $2.4 billion revenue.[63] As with other transaction laundering schemes, the use of virtual currencies and the anonymity accorded to player accounts create the perfect online conditions for the abuse by criminals.

Additionally, the ease of micro-transactions and the use of in-game currencies (like Twitch Bits or V-Bucks) in online gaming platforms make them susceptible to money laundering. Criminals can convert illicit money into virtual assets and then convert them back into "clean" real money in secondary markets. For example, criminals have exploited online games such as, for example, World of Warcraft (WoW), Fortnight, Counterstrike, and Roblox for money laundering and using stolen credit and value cards ("carding fraud") to purchase e-currency, often bitcoin or other untraceable crypto-currencies.[64] It has been reported that the unregulated environment of online video game industry has been a factor in criminals conducting cyber laundering including through loot boxes, e-currencies, and digital assets.[65]

Exploiting Charities and Non-Profits

Criminals are imaginative as ever in finding novel ways to make money illicitly and to launder their illegally-derived proceeds. In recent years, charities and Environmental, Social, and Governance (ESG) funds have also been increasingly targeted as fronts for money laundering due to their perceived legitimacy, complex financial structures, and weak oversight.[66] Criminals use these entities to cleanse illicit funds from activities like poverty alleviation, environmental crime or human trafficking to disguise the true ownership of assets and may provide fake annual reports, bribe auditors, and falsify environment impacts to validate their projects.

Central Bank Digital Currencies

Central bank digital currencies (CBDCs) are also a digital asset. Unlike cryptocurrencies, a CBDC is a digital version of a country's currency that is issued by a country's central bank/federal reserve. There are various forms of CBDCs (discussed below). They are all legal tender. They differ from cryptocurrencies and other forms of digital financial assets because they are the same as a country's traditional currency; i.e., they are centralized and a liability of the issuing central bank. CBDCs enjoy "the full faith and credit" of the issuing country's traditional national currency.

Similar to crypto currencies, a CBDC integrates blockchain technology to securely record and verify all transactions. The difference is that instead of individual users having control and being able to independently verify the veracity of a transaction, a central bank/government controls its issuance and manages the system. Most CBDCs use "permissioned" blockchain where access to the network is restricted to authorized participants only, unlike public blockchains like Bitcoin.

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.

In money laundering and other financial crimes, "cash is king." It is the most important means launderers have to ensure anonymity and finance further criminality. Depending on the model of CBDC and variables involved, over time cash would assuredly be phased out. That development, coupled with the adoption of a fully integrated CBDC, would allow investigators for the first time to more fully follow a transparent "digital money trail."

Data on all types of financial transactions would be collected, stored, analyzed and disseminated. And, in contrast to cash, a CBDC could be designed to potentially include a wealth of personal data, encapsulating transaction histories, user demographics, and behavioral patterns. Governments, working with Big Tech, would then link social scoring.

Personal data could establish a link between counterparty identities and transactions. All of this goes hand-in-hand with government mandated digital identification. Even without specific identity data, Artificial Intelligence (AI) and other analytic tools can improve understanding of trends, patterns, and flows, and help law enforcement flag anomalies similar to the good practices in, for example, unraveling trade-based money laundering.

Depending on the model, the implementation of a U.S. CBDC might also enable novel national security capabilities. For example, sanctions enforcement could be more robust with new ways to freeze assets and track foreign investments in the United States. Of course, criminals and terrorist financiers are inventive. They will assuredly find ways to work around CBDCs including trade-based value transfer and the classic, if not archaic, bartering of goods, values, and services.

Black markets will always thrive. When law enforcement puts pressure on criminal operations, they use the expression "squeezing the balloon." With the adoption of CBDCs, the criminal balloon will surely pop up elsewhere – perhaps in unexpected

ways. Nevertheless, criminal workarounds should not be of sufficient scale to overcome all enforcement measures.

In short, one can argue that the adoption of an all-inclusive CBDC model could well be a "silver bullet" for governments to more effectively mitigate the global scale of money laundering, and be able to effectively control a wide variety of financial crimes including entrenched and heretofore unsolvable problems such as corruption, embezzlement, tax evasion, sanctions evasion, capital flight, and other illicit finance threats. Perhaps CBDCs will finally unlock the closed door of financial transparency and help investigators follow the hidden money trails. Of course, at this time, the above is only theoretical in the United States and other jurisdictions until some of the CBDC system come online in places where it is being implemented or piloted to have some data to analyze or case studies to review and make a preliminary assessment. President Donald Trump formally prohibited the development of a U.S. Central Bank Digital Currency (CBDC) via an executive order signed on January 23, 2025.[67]

Case Studies

Chinese Money Laundering Networks, Cryptocurrencies, and Social Media

The following are a few recent developments, case studies, and ICAIE comments related to our on-going coverage of trend-setting money laundering methodologies and enablers.

On August 28, 2025, Treasury's Financial Crimes Enforcement (Network) issued an advisory[68] helping banks and money service businesses (MSBs) identify and report suspicious activity connected to Chinese money laundering networks (CMLNs). The focus of the report are CMLNs working with Mexican cartels. The advisory notes key financial typologies associated with CMLNs – such as mirror transactions, money mules, and trade-based money laundering, all of which have been previously reported[69] by ICAIE years ago in a number of publications including Mobile Payments and Mirror Swaps – Money Laundering Threats that Are Getting Worse.

FinCEN's Advisory and Financial Trend Analysis notes that FinCEN analyzed 137,153 Bank Secrecy Act (BSA) reports filed by financial institutions between January 2020 and December 2024 associated with suspected CMLN-related activity. There were approximately $312 billion in suspicious transactions.[70] It would be interesting to know how many actual investigations were initiated or assisted by the above SARs – very probably less than 100.

The criminal relationship between CMLNs and Mexico-based narcotics cartels is driven in part by laws passed by both the Governments of Mexico and China that restrict financial flows.[71] There is cause and effect.

In 2010, Mexico initiated more forceful restrictions to prevent large amounts of U.S. dollars from being deposited via bulk cash smuggling into Mexican financial institutions. This hindered (but did not stop) the cartels' ability to launder funds through the formal Mexican financial system. At the same time, the PRC's currency control laws attempt to limit massive capital flight. Chinese citizens can transfer abroad approximately $50,000 equivalent each year.

China leads the world in capital flight. The scale of money escaping China has overwhelmed official channels. Capital also flees China through numerous illicit methods. For example, Chinese authorities have reportedly dismantled over 100 underground money-handling operations and traced nearly $1 trillion in illegal transactions.[72]

Concurrently, in the United States CMLNs gain access to the large amounts of cash generated by narcotics trafficking and other illegal activities. Based on reports from U.S. government agencies and federal indictments, CMLNs have become the "money launderers of choice" for Mexican drug cartels. The Chinese criminal groups use cooperating Chinese-American-based cash intensive businesses and advertisements on Chinese social media apps to identify individuals willing to accept knowingly or

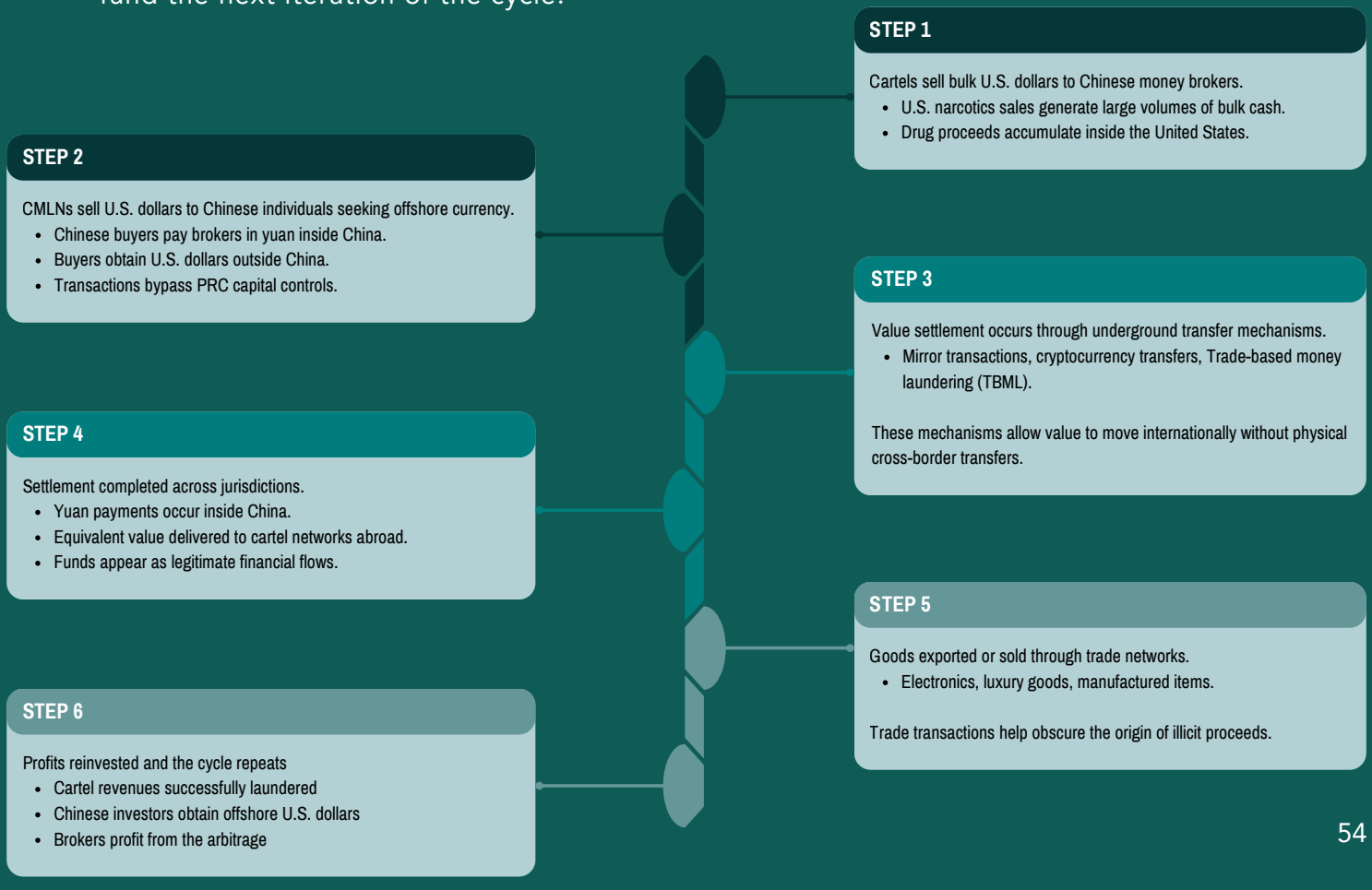
unknowingly illicit dollars. They also leverage personal networks involving Chinese citizens and/or businesses seeking to evade the PRC's currency control laws.

Ultimately, Chinese citizens' demand for large quantities of U.S. dollars and the cartels' need to launder their illicit U.S. dollar proceeds has resulted in a mutually supportive relationship wherein the cartels sell off their illicitly obtained U.S. dollars to CMLNs who, in turn, sell the U.S. dollars to Chinese citizens seeking to evade China's currency control laws. It appears there is adequate supply of illicit dollars to meet the demand for access to dollars.

The physical cash purchased by the Chinese brokers is then laundered through domestic U.S. bank accounts and made available to Chinese clients seeking to pay college tuition, purchase real estate, luxury products, vehicles, and other goods in the United States.

As described in an earlier ICAIE publication, acting with the cartels, the Chinese-Americans involved with cash intensive business "place" the proceeds of crime into the U.S. financial system. For a small commission, the Chinese-American business people transfer the equivalent amount of illicit proceeds through Chinese mobile phone apps. The "mirror transaction" or "mirror swap" in complete when yuan in China is simultaneously transferred from bank accounts owned in China by the Chinese-American business people to bank accounts designated by the Chinese money launderer working with the cartels.

Sometimes the cartels use crypto currencies sent to them by Chinese currency brokers to settle debts with suppliers. They will also use the crypto to purchase goods from Chinese manufacturers. It is a form of black-market exchange used in trade-based money laundering. The goods are then sold in local currency in Mexico and other Latin American countries generating "clean" revenues for the cartels. In turn, the Chinese manufacturers can then exchange the crypto received from the cartels for yuan with currency brokers. This completes the currency loop and provides washed currency to fund the next iteration of the cycle.



CMLNs may also use TBML schemes within the U.S. to launder funds for the cartels. The TBML schemes often involve the purchase of U.S. luxury goods, electronics and items in demand. Chinese money mules, often students and other young recruits, pay for the goods using illicit proceeds, fraudulently obtained gift cards or credit cards that are subsequently paid off by CMLNs or by a complicit business owner. FinCEN notes that once the goods are purchased, CMLNs use front companies or complicit businesses to resell or export the goods.

In some cases, a Chinese investor in the scheme to procure U.S. drug dollars will transfer an equivalent amount of Chinese currency into a designated account in China controlled by the Mexican cartel. Once transferred, the funds can be used to settle debts owed by the cartel to Chinese manufacturers. The money transfers appear legitimate. But they are also a form of trade-based money laundering operating as a black-market exchange. "The money in that account in China can legally be used to pay off legitimate debts to Chinese manufacturers who ship goods to Mexico," U.S. court filings say.[73]

The Chinese manufactured goods are shipped to Mexico where they are sold in the local market. The proceeds in pesos represent the final value of the drugs initially smuggled and sold in the United States. The loop is closed on the cartel's illicit earnings while at the same time providing the Chinese investor or those that seek to circumvent PRC capital flight controls with clean dollars to invest in U.S. assets.

TBML schemes often also incorporate daigou buyers, an arrangement popular on Chinese social media channels where buyers based outside of China purchase and import in demand luxury goods, often at a lower price, on behalf of Chinese residents. Most of the goods are popular brand-name items. Daigou means "buying on behalf of." CMLNs typically provide the daigou buyer with cash of illicit origin or send a person-to-person (P2P) transfer to their account and instruct them to purchase certain goods. The daigou buyers are then instructed to ship the purchased goods to a location in China or to a daigou broker operating within the United States that directs multiple buyers. Daigou operators typically further export the U.S. goods to China or other countries.[74]

In a recent successful case that sheds light on the above activities of CMLOs, from 2019-2023, operatives of the Sinaloa Cartel imported large quantities of narcotics, including fentanyl, cocaine, and methamphetamine, into the United States. The sales generated huge amounts of illicit cash. According to the federal indictment[75] that detailed "Operation Fortune Runner," in January 2021, the lead defendant in the case, Edgar Joel Martinez-Reyes, an individual from southern California allegedly traveled to Mexico to meet with Sinaloa Cartel members. As a result, an agreement was reached to have money remitters with links to Chinese underground banking launder drug trafficking proceeds in the United States. After the agreement, Martinez-Reyes and other co-conspirators allegedly then delivered the currency—frequently in amounts of hundreds of thousands in cash—to members of the Chinese underground money exchange and remitting organizations to be laundered. As noted above, the remitting networks possessed large amounts of illicit dollars and used some of the cash to help wealthy Chinese nationals evade China's currency controls that govern capital flight.

According to the indictment, the unregistered and unlicensed money remitters allegedly disposed of the drug proceeds by either delivering illicit cash directly to their money exchange customers or by purchasing real or personal property, including luxury goods and cars to be shipped to China – similar to the daigou explanation above. In addition, the remitters also transferred illicit drug proceeds through cryptocurrency transactions (see discussion on cryptocurrency below). They allegedly "placed" the illicit funds into

the traditional banking system by "structuring" or "smurfing" "transactions" by depositing small amounts at a time into bank accounts. In this manner, money launderers hope to avoid U.S. financial intelligence reporting requirements.

Also caught in Operation Fortune Runner was Sai Zhang, who entered the U.S. in 2010 as a student. Identifying opportunities for financial gain, Zhang began to buy the Sinaloa cartel's illicit cash dollars from the street sales of drugs at a discount. He resold them at a premium to Chinese buyers. Zhang relied on a sophisticated network of cash couriers, brokers, and money mules to keep himself insulated from street-level narcotics transactions. DEA surveillance teams tracked network Zhang's operators to numerous cash stash houses and clandestine parking lot exchanges in "pick-up" operations. Sai Zhang and other exchange students lured by the easy money and recruited through WeChat message boards, served as the primary money mules.[76]

Chinese money launderers are also increasingly using cryptocurrency in their informal shadow banking networks to facilitate rapid, pseudonymous cross-border transactions for their criminal clients.[77] In another 2025 case under "Operation Take Back America", U.S. investigators showed how CMLNs also move illicit funds through shell companies bank accounts that had been opened in the United States using fake identities to launder tens of millions of dollars in drug proceeds for the Mexican cartels.[78]

Chinese have long had a proclivity for gambling.[79] Perhaps this is one reason why cryptocurrency money laundering often takes place in both brick-and-mortar casinos and on-line gaming. Chinese organized crime or triads meld casinos and underground banking into an alternative banking system that allows criminals to launder illicit proceeds through casino accounts, betting credits, and cryptocurrency transactions. A common technique is to mix or co-mingle cryptocurrency into casino-based schemes.

In mainland China, the CCP maintains strict regulations against gambling activities within its borders. The government works to curb any potential social issues resulting from gaming practices. However, gaming is widespread in Hong Kong and Macau. Gambling junkets have expanded their reach across Southeast Asia through both physical and online casinos. Chinese money laundering via gaming is spreading around the world. For example, the Vancouver method of money laundering involves an international informal value transfer system, often using Chinese gangs, combined with casino gambling to clean illicit cash. According to the Cullen Commission findings, it was used to launder hundreds of millions of dollars through British Columbia casinos.[80] The method links a person with cash in one country to a criminal syndicate in Vancouver that needs to offload illicit cash from drug trafficking. Chinese gaming and money laundering is also taking root in a number of developing countries where China's influence is growing because of its Belt and Road initiative.

Many of these venues operate as laundering hubs, moving funds derived from drug trafficking, human trafficking, and large-scale fraud. The UN Office on Drugs and Crime states that these casino-based networks enable Chinese triads to move funds in "much bigger and more untraceable ways than in the past," making it incredibly difficult for authorities to track the money.[81]

The Financial Action Task Force (FATF) has published several reports on money laundering vulnerabilities and methodologies involving casinos, including the 2008 Guidance on the Risk-Based Approach for Casinos and the 2009 Vulnerabilities of Casinos and Gaming Sector report. Over the last 15 years, Chinese money laundering and gaming have taken FATF's concerns to a new level. Per earlier warnings, Chinese

gaming use illicit funds that are cycled through high-volume betting, often mixed with legitimate gamblers' money, and eventually withdrawn as "winnings" or declared as business income, masking their illegal origins.

Chinese gaming interests have also taken casino money laundering to a new level using crypto currency. Money launderers can deposit or "place" dirty cash or the proceeds of crime into crypto ATMs or exchanges in the U.S., convert it to Bitcoin, and send it to a Chinese network's e-wallet. Brokers can use digital assets as an intermediary value transfer to further "layer" transactions. Value transfer via blockchain is faster and more opaque than traditional methods.[82]

For example, North Korean state-sponsored hackers have stolen billions in cryptocurrency through cyber-heists and exchange hacks. To convert these stolen digital assets into usable funds for its weapons programs and other sanctioned activities, North Korea relies on Chinese underground banking networks and over-the-counter (OTC) crypto brokers.

In 2023, the U.S. indicted North Korean banker Sim Hyon Sop[83] and three OTC brokers with conspiring to launder stolen cryptocurrency. These brokers laundered the stolen crypto through numerous trading exchanges and shell companies. The process often involves using crypto currency mixers and cross-chain "bridges" to obscure the trail before the funds are cashed out by brokers. It is a modern day "layering" money laundering process. They converted crypto currencies to U.S. dollars and then purchased sanctioned goods for North Korea, including items used in North Korea's ballistic missile programs.

Crypto currencies are the payment mechanism of choice in a variety of e-commerce crimes including romance scams, "pig-butchering," and ransomware attacks. ICAIE reported on these schemes in its 2024 publication, *E-Commerce and Digital Marketplaces: The Booming Business of Cross-Border Transaction Laundering.*

Another case example of how crypto currency is increasingly used in crime is involves the Kinahan crime family.[84] The Kinahan network is relatively unknown in the U.S. However, over the last twenty years the Kinahan's have become major players in the procurement, shipment and distribution of narcotics from Latin America to Europe, Africa and Russia.

The Kinahan cartel started from humble beginnings in Dublin in the 1990s. Over the decades it became one of the primary logistics operations for the spread of narcotics throughout Europe. Concurrently, the Kinahan money laundering network grew into a sophisticated, global network used to clean billions of dollars in illicit profits from drug and firearms trafficking.

The Kinahan cartel established a significant presence in Dubai, using it as a base to run their operations and engage in business services and trade. This operation in Dubai involved setting up companies for textiles, clothing, and food, which were allegedly used to facilitate the supply of drugs and money laundering. Coordinated by the family's leadership from their base in Dubai, the scheme relies on a web of legitimate-seeming businesses.

In coordinated street operations taking place in many different countries, couriers collect vast sums of drug money. The cash is given to the Kinahan network, which in turn arranges for the equivalent in cryptocurrency to be delivered to the gang's digital

wallets. The cartel used Russian-led cryptocurrency exchange networks, such as Smart and TGR, to convert massive amounts of illicit cash into digital assets. These networks charged a fee and then provide crypto, which can be sent instantly and untraceably to drug suppliers in South America.

In 2024, international law enforcement, primarily headed by the U.K. and U.S., dismantled the networks. "Operation Destabilize"[85] led to 84 arrests and the seizure of over £20 million (more than $25 million) in cash and cryptocurrency. The arrests included cash couriers in the U.K. who were moving large sums on behalf of the networks. The crackdown exposed the links between Russian elites, state actors, cybercriminals, and Western drug gangs that were tied together by the Smart and TGR networks.

There are also direct business links between the Kinahan crime family and the terrorist group Hezbollah. The two groups have sometimes shared a criminal network for money laundering and international drug trafficking. The U.S. government has sanctioned the Kinahan cartel in part due to its business with Hezbollah.[86] In one prominent case, fundraisers linked to Hezbollah helped finance a €157 million cocaine shipment destined for Ireland in 2023. The Kinahan cartel was among the international crime groups that paid an initial €5 million for the narcotics.[87]

The above case also demonstrates the Kinahan crime family's ties with Iran. Both Iran and Hezbollah use hawala to launder illicit proceeds and fund terror. There are reports that the Kinahan group also uses the hawala informal banking system, described earlier in this paper, to transfer money across borders without leaving a paper trail.[88] This is an excellent example of how today's sophisticated criminal networks increasingly use both old and new money laundering methodologies.

[1] IMF, "World Economic Outlook (GDP)". October 2025. https://www.imf.org/external/datamapper/NGDPD@WEO/WEOWORLD.

[2] TRM Labs. "2026 Crypto Crime Report". January 28, 2026. https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report

[3] Mitch Jackson, "The Parallel Financial System: The Trillion Dollar Blind Spot Reshaping the Global Economy and Undermining Stability, Security, and Democracy," Substack, December 29, 2025; https://mitchthelawyer.substack.com/p/the-parallel-financial-system-the

[4] "E-Commerce Crime and Digital Marketing: The Booming Business of Cross-Border Transaction Laundering," International Coalition Against Illicit Economies, September, 2024; https://icaie.com/2024/09/e-commerce-and-digital-marketplaces-the-booming-business-of-cross-border-transaction-laundering/

[5] John Cassara, Money Laundering and Illicit Financial Flows, see Chapter 2 – "Sobering Statistics," KDP/Amazon, 2020

[6] John Cassara, "Modernizing AML Laws to Combat Money Laundering and Terrorist Finance," Testimony before the Senate Judiciary Committee, November 28, 2017; https://www.judiciary.senate.gov/imo/media/doc/Cassara%20Testimony.pdf

[7] U.N. Trade and Development, December 9, 2025, https://unctad.org/news/global-trade-hit-record-35-trillion-despite-slowing-momentum.

[8] USPTO, Latest USPTO report finds industries that intensively use intellectual property protection account for over 41% of U.S. gross domestic product, Press Release (2022), https://www.uspto.gov/about-us/news-updates/latest-uspto-report-finds-industries-intensively-use-intellectual-property-0.

[9] Farzouq. "Top Social Media Platforms by Users (Statistics 2025)". October 17, 2025. https://www.tekrevol.com/blogs/top-social-media-platforms-by-user-statistics/#:~:text=Global%20Social%20Media%20Usage%20in,over%2099%25%20accessing%20via%20smartphones

[10] Jeffrey Gottfriend and Eugenie Park. "Americans' Social Media Use 2025." Pew Research Center, November 20, 2025. https://www.pewresearch.org/internet/2025/11/20/americans-social-media-use-2025/#:~:text=do%20so%20daily.-,Which%20online%20platforms%20do%20Americans%20most%20commonly%20use?,up%20from%2021%25%20in%202021.

[11] AML Watcher. "How E-Commerce Money Laundering Undermines Online Retail Success". November 18 2023.

[12] Ibid.

[13] For this discussion on hawala, see John Cassara and Avi Jorisch, On the Trail of Terror Finance, What Law Enforcement and Intelligence Officers Need to Know, Chapter 7, 2010, Red Cell Intelligence Group, Washington, D.C.

[14] Jerry Harr, "Tariffs are a money launderer's best friend," The Hill, August 21, 2025; https://thehill.com/opinion/finance/5462780-the-higher-the-tariffs-the-greater-the-money-laundering/

[15] John Cassara, David M. Luna, Dr. Layla M. Hashemi, "E-Commerce and Digital Marketplaces: The Booming Business of Cross Border Transaction Laundering," International Coalition Against Illicit Economies, September, 2024; https://icaie.com/2024/09/e-commerce-and-digital-marketplaces-the-booming-business-of-cross-border-transaction-laundering/

[16] "Why Hawala 2.0 is Emerging as A Global AML Threat," Riddle Compliance, April 2, 2025; https://riddlecompliance.com/why-hawala-2-0-is-emerging-as-a-global-aml-threat/#:~:text=The%20global%20adoption%20of%20digital,banking%2C%20and%20even%20prepaid%20cards.

[17] 2022 National Money Laundering Risk Assessment by the U.S. Department of the Treasury; https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf

[18] Sara Mosqueda, "Follow the Money: How Digital Currency is Changing Crime," Security Management, August 21, 2023; https://www.asisonline.org/security-management-magazine/articles/2023/08/cryptocurrency/How-digital-currency-changes-crime/#:~:text=The%20Hawala%20system%20is%20a,to%20the%20U.S.%20Secret%20Service

[19] "Trade Based Money Laundering," the FATF, Paris, June 23, 2006, p. 1; http://www.fatfgafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf.

[20] "U.S. Tax Coffers Lose $640 billion of Taxable Profits due to TBML Evasion and Money Laundering in 2021," SEK 20 Strategies, May 4, 2022; https://www.prnewswire.com/news-releases/us-tax-coffers-lose-640-billion-of-taxableprofits-due-to-trade-based-tax-evasion-and-money-laundering-in-2021-says-sk-strategies-301539461.html.

[21] "China's foreign trade hits new high in 2021," State Council, Peoples Republic of China, Jan 14,2022; http://english.www.gov.cn/archive/statistics/20220 1/14/content_WS61e11577c6d09c94e48a3a0a.html.

[22] Bridget Diakun, "Flag hopping hits unprecedented levels among sanctioned fleet," Lloyd's List, April 25, 2025; https:// 22 www.lloydslist.com/LL1153276/Flag-hopping-hits-unprecedented-levels-among-sanctioned-fleet

[23] "How criminals exploit trade to move illicit funds," FinTech Global, November 14, 2025; https://fintech.global/2025/11/14/how-criminals-exploit-trade-to-move-illicit-funds/

[24] David Curry. "Mobile Payments App Revenue and Usage Statistics (2025)". November 18, 2025. ecommerce-money-laundering/.

[25] Financial Crimes Enforcement Network (FinCEN). "FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds". U.S. Department of The Treasury, FinCEN Advisory, August 28, 2025, https://www.fincen.gov/system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf.

[26] Admiral Craig Fuller, testimony before the Senate Armed Services Committee, March 16, 2021. "2021 Posture Statement to Congress", U.S. Southern Command,https://www.southcom..mil/Media/SpecialCoverage/SOUTHCOMs-2021-Posture- .

[27] David M. Luna. "Irregular Warfare in Strategic Competition and Gray Zones: Prosecuting Authoritarian Subversion and Exploitative Use of Corruption and Criminality to Weaken Democracy." ICAIE, August 23, 2024, https://icaie.com/2024/08/irregular-warfare-in-great-power-competition-and-gray-zones-prosecuting-authoritarian-subversion-strategic-corruption-criminality-to-weaken-democracy//

[28] John A. Cassara. "Examining Policies to Counter China." Written Testimony before the U.S. House Committee on Financial Services, February 25, 2025, https://docs.house.gov/meetings/BA/BA00/20250225/117913/HHRG-119-BA00-Wstate-CassaraJ-20250225.pdf.

[29] Luna, op. cit.

[30] Financial Action Task Force (FATF). "China's progress in strengthening measures to tackle money laundering and terrorist financing." November 28, 2022, FATF Follow-Up Analysis on China, https://www.fatf-gafi.org/en/countries/detail/China.html.

[31] Financial Crimes Enforcement Network (FinCEN). "FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds". U.S. Department of The Treasury, FinCEN Advisory, August 28, 2025, https://www.fincen.gov/system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf.

[32] Ibid.

[33] Anthony Ruggiero, testimony before House Oversight and Accountability Committee, Subcommittee on Health Care and Financial Services, April 26, 2023. "China in Our Backyard: How Chinese Money Laundering Organizations Enrich the Cartels", Foundation for Defense of Democracies, https://www.congress.gov/118/meeting/house/115810/witnesses/HHRG-118-GO27-Wstate-RuggieroA-20230426.pdf.

[34] Charles (Chip) Barber. "Organized Crime in The Amazon: A Growing Threat to the World's Greatest Tropical Rainforest, World Resources Institute, July 9, 2025, https://www.wri.org/insights/nature-crime-amazon-deforestation.

[35] Ricardo Mayoral, testimony before U.S. Senate Caucus on International Narcotics Control, "Chinese Money Laundering Organizations: Cleaning Cartel Cash", Homeland Security Investigations, Department of Homeland Security, April 30, 2025, https://www.ice.gov/doclib/news/library/speeches/240430mayoral.pdf.

[36] The Select Committee on the Strategic Competition between the United States and the Chinese Communist Party. Krishnamoorthi, Moolenaar call for Enforcement Action of Unlawful PRC Trade Practices". March 6, 2025. https://democrats-selectcommitteeontheccp.house.gov/media/press-releases/krishnamoorthi-moolenaar-call-enforcement-action-unlawful-prc-trade-practices

[37] Ibid.

[38] David M. Luna. "The Aftermath Turbulences of Tariffs and High Duties in Global Trade and Commerce". ICAIE News. February 22, 2026. https://icaie.com/2026/02/the-aftermath-turbulences-of-tariffs-and-high-duties-in-global-trade-and-commerce/.

[39] TradLinx. "The Future of Free Trade Zone: Are They Still Relevant in Global Trade?" April 1, 2025. https://blogs.tradlinx.com/the-future-of-free-trade-zones-are-they-still-relevant-in-global-trade/

[40] Rashmi Singh, Jorge Lasmar. "Underworld Crossroads: Dark Networks and Global Illicit Trade in the Tri-border Area between Argentina, Brazil, and Paraguay." August 6, 2024. El Centro, Small Wars Journal. https://smallwarsjournal.com/2024/08/06/underworld-crossroads-dark-networks-and-global-illicit-trade-tri-border-area-between/.

[41] Ibid.; Felipe Umaña. "Revisiting the Crime-Terrorism Nexus in the Tri-Border Area". The Fund for Peace.

[42] EUROPOL. "Criminal Networks in EU Ports". March 2023. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Joint-report_Criminal%20networks%20in%20EU%20ports_Public_version.pdf

[43] Ibid.

[44] Ibid.

[45] International Consortium of Investigative Journalists, Panama Papers, 2021, accessed at: https://www.icij.org/investigations/pandora papers/global-investigation-tax-havens-offshore/ .

[46] USAID, DEKLEPTIFICATION GUIDE Seizing Windows of Opportunity to Dismantle Kleptocracy, September 2022, accessible at: https://www.usaid.gov/anti-corruption/dekleptification.

[47] Transparency International, "2022 Corruption Perception Index Reveals Scant Progress Against Corruption as World Becomes More Violent", Berlin, January 31, 2023, accessible at: https://www.transparency.org/en/cpi/2022.

[48] "Beneficial Ownership Registers: Implementation Insights and Emerging Frontiers," World Bank Group, March, 2024, page 10; https://documents1.worldbank.org/curated/en/099042424121018634/pdf/P179427158716b0611a32c193533943dbc0.pdf

[49] "How do organized criminals exploit accounting professionals to launder the proceeds of their crimes and what can you do to prevent this happening in your business?" Arctic Intelligence, February 11, 2025; https://arctic-intelligence.com/insights/organised-criminals-accounting-professionals-prevention

[50] "Delaware," Urban Institute, September 2025; https://www.urban.org/policy-centers/cross-center-initiatives/state-and-local-finance-initiative/projects/state-fiscal-briefs/delaware#:~:text=Corporate%20license%20fees%20accounted%20for,national%20average%20was%200.2%20percent.

[51] Anonymous, Inc., 60 Minutes, January 31, 2016; https://www.cbsnews.com/news/anonymous-inc-60-minutes-steve-kroft-investigation/

[52] Financial Crime Academy. Money Laundering in the Digital Age: Exploring Virtual Assets Role." FCA Anti-Money Laundering. January 23, 2026. https://financialcrimeacademy.org/money-laundering-via-virtual-assets/.

[53] Financial Crime Academy. The Hidden Methods of Laundering Money with Cryptocurrencies. FCA YouTube. September 5, 2023. https://www.youtube.com/watch?v=3zxQbfJmOFc.

[54] Jeffrey M. Jones and Lydia Saad. "Cryptocurrency Still Has Limited Main Street Appeal". Gallup, July 22, 2025. https://news.gallup.com/poll/692777/cryptocurrency-limited-main-street-appeal.aspx#:~:text=Crypto%20Ownership%20Most%20Common%20Among,least%20likely%20to%20own%20crypto.

[55] Kelly A. Lenahan-Pfahlert. FinCEN's Focus on Cryptocurrency Kiosks and Financial Crime. August 25, 2025; https://www.moneylaunderingnews.com/2025/08/fincens-focus-on-cryptocurrency-kiosks-and-financial-crime/.

[56] United States Attorney's Office, Central District of California. "Justice Dept. Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes, With Over Half Seized in Los Angeles Case". USDOJ Press Release, April 3. 2023; https://www.justice.gov/usao-cdca/pr/justice-dept-seizes-over-112m-funds-linked-cryptocurrency-investment-schemes-over-half.

[57] Ibid.

[58] Rakesh Sharma. "Non-Fungible Token (NFT): What it Means? How They Work". Investopedia, December 31, 2025. https://www.investopedia.com/non-fungible-tokens-nft-5115211#:~:text=A%20non%2Dfungible%20token%20is,%2C%20property%20rights%2C%20and%20more.

[59] Ibid.

[60] Allison Owen and Isabella Chase. "NFTs: A New Frontier for Money Laundering". RUSI, December 2, 2021; https://www.rusi.org/explore-our-research/publications/commentary/nfts-new-frontier-money-laundering.

[61] LexisNexis. "Money Laundering with NFTs". November 23, 2023; https://www.lexisnexis.com/blogs/gb/b/compliance-risk-due-diligence/posts/money-laundering-with-nfts.

[62] Jack Hines. "When Fraud Stops Looking Like Fraud". Ankura Insights. February 10, 2026. https://ankura.com/insights/when-fraud-stops-looking-like-fraud

[63] Pierre Jean Benghazi and Jean-Paul Simon. "Esports: everything you need to know about this exploding digital market." Polytechnique Insights; https://www.polytechnique-insights.com/en/columns/digital/esports-everything-you-need-to-know-about-this-exploding-digital-market/#:~:text=Alongside%20the%20fast%2Dgrowing%20video,championship%20title%20or%20prize%20money.

[64] Lazaros Ioannou. "Esports and Money Laundering". The Sports Financial Literacy Academy (SFLA), June 23, 2021; https://moneysmartathlete.com/esports/e-sports-and-money-laundering/.

[65] Dan Cooke and Angus Marshall. "Money Laundering through Video Games, a criminals' playground". Forensic Science International: Digital Investigation, Vol. 50, September 2024; https://www.sciencedirect.com/science/article/pii/S2666281724001264.

[66] Eric Gagnon. How Wall Street is Using Sustainability to Fight Money Laundering". JDSupra. February 16, 2026. https://www.jdsupra.com/legalnews/how-wall-street-is-using-sustainability-2293773/.

[67] The White House. "Strengthening American Leadership in Digital Financial Technology". Executive Order. January 23, 2025. https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/.

[68] "FinCEN Issues Advisory and Financial Trend Analysis on Chinese Money Laundering Networks," FinCEN.gov; August 28, 2025; https://www.fincen.gov/news/news-releases/fincen-issues-advisory-and-financial-trend-analysis-chinese-money-laundering#:~:text=FinCEN%20is%20issuing%3A%20(1),activity%20in%20the%20United%20States.

[69] See ICAIE Board Member John A. Cassara's China – Specified Unlawful Activities: CCP/Inc., Transnational Crime and Money Laundering, 2023, Amazon Kindle Direct Publishing

[70] FinCEN Advisory, op cit.

[71] Liana W. Rosen. "Chinese Money Laundering Networks". Congressional Research Service (CRS). January 8, 2026. https://www.congress.gov/crs-product/R48786.

[72] Antonio Graceffo, "Xi Jinping: The Man Who Stopped China's Rise," The Gateway Pundit, August 25, 2025; https://www.thegatewaypundit.com/2025/08/xi-jinping-man-who-stopped-chinas-rise/.

[73] Sam Cooper, "Crime Project Sleeping Giant: Inside the Chinese Mercantile Machine Linking Beijing's Underground Banks and the Sinaloa Cartel," Todayville, 2025; https://www.todayville.com/edmonton/project-sleeping-giant-inside-the-chinese-mercantile-machine-linking-beijings-underground-banks-and-the-sinaloa-cartel/.

[74] FinCEN Advisory, op cit.

[75] "Federal Indictment Alleges Alliance Between Sinaloa Cartel and Money Launderers Linked to Chinese Underground Banking," U.S. Department of Justice, June 18, 2024; https://www.justice.gov/archives/opa/pr/federal-indictment-alleges-alliance-between-sinaloa-cartel-and-money-launderers-linked

[76] Sam Cooper, op cit.

[77] Nelson Maura, "Chinese shadow bankers using crypto casinos and online gaming for organized crime money laundering," Asia Gaming Brief, August 11, 2025;

https://agbrief.com/intel/deep-dive/11/08/2025/chinese-shadow-bankers-using-crypto-casinos-and-online-gaming-for-organized-crime-money-laundering-report/.

[78] U.S. Department of Justice. "Three Members of a Prolific Chinese Money Laundering Organization Plead Guilty to Laundering Tens of Millions of Dollars in Drug Proceeds". DOJ Office of Public Affairs. May 1, 2025. https://www.justice.gov/opa/pr/three-members-prolific-chinese-money-laundering-organization-plead-guilty-laundering-tens.

[79] Christian, "Chinese Culture and Gambling: Exploring the Historic Love of the Game," April 23, 2024; https://chinaunlimited.eu/chinese-culture-and-gambling-exploring-the-historic-love-of-the-game/.

[80] "Commission of Inquiry into Money Laundering in British Columbia" June, 2022; The Honorable Austin F. Cullen Commissioner, Final Report; https://cullencommission.ca/files/reports/CullenCommission-FinalReport-Full.pdf.

[81] Maura, op cit.

[82] Ibid.

[83] FBI Most Wanted, Sim-Hyon-Sop; https://www.fbi.gov/wanted/counterintelligence/sim-hyon-sop.

[84] There are a number of excellent references on the Kinahan Crime Family. A helpful overview is a 2024 Johnny Mitchell YouTube video, "Chasing the Kinahan Crime Family: Inside the Manhunt for Europe's MOST Powerful Drug Cartel;" https://www.youtube.com/watch?v=ns_3VnsYfy0.

[85] Dominic Casciani, "Russian criminals helped UK drug gangs launder lockdown cash," BBC, December 4, 2024; https://www.bbc.com/news/articles/c70ezyrep1go.

[86] "Treasury Sanctions Notorious Kinahan Organized Crime Group," U.S. Treasury Press Release, April 11, 2022; https://home.treasury.gov/news/press-releases/jy0713

[87] "Revealed: How Hezbollah fundraisers helped finance the €157m MV Matthew drug operation," The Journal, July 4, 2025; https://www.thejournal.ie/hezbollah-links-mv-matthew-6738529-Jul2025/

[88] Clodagh Meaney, "Spanish cops bust lucrative Hawala drug money laundering ring," Sunday World, May 15, 2025; https://www.sundayworld.com/crime/world-crime/spanish-cops-bust-lucrative-hawala-drug-money-laundering-ring/a1174560673.html

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.

David M. Luna is the Executive Director of the International Coalition Against Illicit Economies (ICAIE) / ICAIE Foundation, and co-Founder of the Illicit Shadows of the Criminal Underworld investigative docuseries.

A former U.S. diplomat and national security official, Mr. Luna is a globally-recognized strategic thought leader on criminal-threat convergence, advocate for security of humanity, and a leading voice internationally on illicit trade, transnational security threats, geopolitical risks, the changing character of war and peace, threat finance, and global illicit economies ("dark side of globalization") that fuel greater insecurity and instability around the world. Mr. Luna is also President and CEO of Luna Global Networks & Convergence Strategies LLC.

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 honorable former Chairs of the Business at OECD Anti-Illicit Trade Expert Group (AITEG), the Anti-Illicit Trade Committee (AITC), United States Council for International Business (USCIB), 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

INTERNATIONAL COALITION
AGAINST ILLICIT ECONOMIES