Institute for
Financial Integrity

EXPERT INSIGHT

Cyber-Enabled Fraud

FATF Issues Report about Illicit Financial Flows

Table of Contents

Cyber-Enabled Fraud

FATF Issues Report about Illicit Financial Flows

Cyber-enabled fraud (CEF) is growing, especially with increasing digitalization across the globe. Technological advances have enabled cyber criminals to develop and increase the scale, scope, and speed of their illicit activities, according to a recent Financial Action Task Force (FATF) report, written in partnership with the Egmont Group of financial intelligence units (FIUs) and INTERPOL. The report analyzed how the CEF landscape has evolved, its links to other crimes, such as money laundering and human trafficking, and how criminals may exploit vulnerabilities in new technologies. FATF calls on jurisdictions to respond to this threat more effectively by using initiatives to increase victim and suspicious transaction reporting, more effectively analyze information inflows from reports, and recognize that strong domestic and cross-jurisdictional coordination is needed to combat CEF. The report also includes a list of red flags and anti-fraud suggestions to help both the private and public sectors detect and prevent CEF and the money laundering that invariably accompanies these crimes.

- Several banks have told the media that they have seen a significant increase in impersonation, investment, and marketplace fraud in 2022, and that much of the activity originates online—social media platforms, online marketplaces, and dating sites and applications.
- The FBI's Internet Crime Complaint Center (IC3) reports that in 2022, Americans reported $10.3 billion in losses from internet scams—up from nearly $7 billion during the previous year.
- IC3 reports that phishing was the top CEF crime in 2022, with personal data breaches, non-payment or non-delivery of purchased goods, extortion, tech support scams, and breaches of personal data included in the list of top five crimes.
- According to the INTERPOL Global Crime Trend Report 2022, online scams are one of the cybercrime trends most frequently perceived as posing 'high' or 'very high' threats globally.

Complaints and Losses over the Last Five Years*

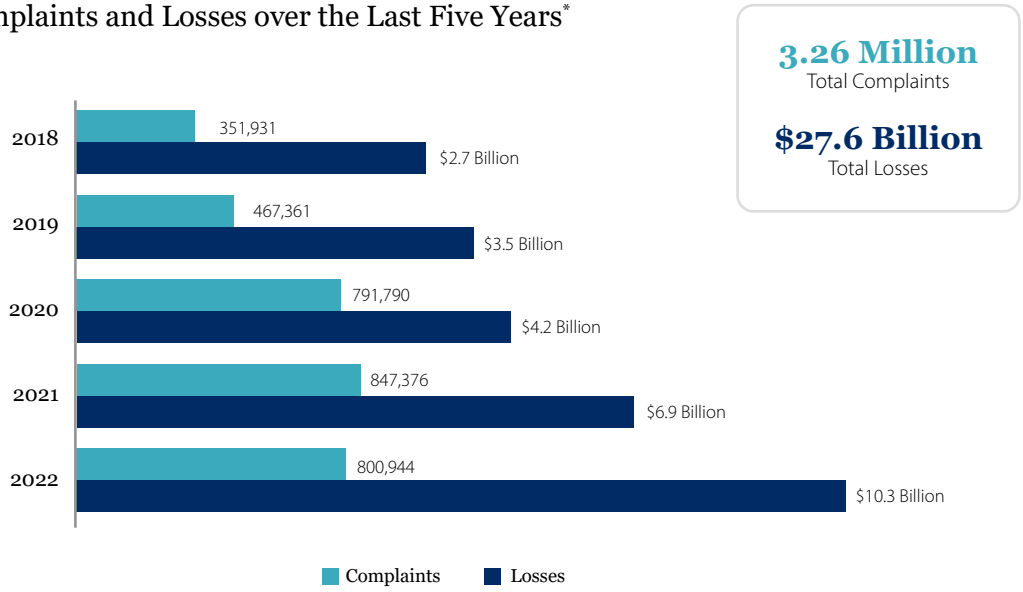


Figure 1: Courtesy of the Internet Crime Complaint Center

The FATF report focuses on illicit financing resulting from fraud that is conducted in the cyber environment, such as business email compromise (BEC) fraud, phishing fraud, social media and telecommunication impersonation fraud, online trading fraud, and online romance and employment scams.

Money laundering (ML) groups and professional enablers often operate as part of organized criminal networks that are involved in CEF, using money mules, shell companies, or even legitimate businesses to move the illicit proceeds. These ML networks also exploit different types of financial institutions (FIs), including banks, payment and remittance providers, and virtual asset service providers (VASPs). Developments in digital technologies are further enabling the laundering of the proceeds of fraud, and criminals use a combination of various traditional ML techniques, such as cash, trade-based money laundering (TBML), and unlicensed services, as well as advances in digital financial payments to move the proceeds of fraud, according to the FATF report.

The evolution of financial payments has resulted in new digital financial institutions and ways to transact, such as payment service providers (PSPs) and the issuance of e-money, buttressing the growth of CEF. Traditional FIs may have more resources at their disposal, which may result in relatively more robust controls compared to these newer digital financial institutions, making them attractive to fraudsters and their facilitators.

- FATF assesses that PSPs are approximately 200 times more risky than other financial institutions because they generally have poor identity verification and transaction monitoring, enabling illicit actors to open accounts with a stolen or fraudulent identity and check quickly if some of the open accounts are identified as fraudulent by the PSP.

- Criminals can also abuse virtual international bank account numbers (vIBANs) to help them obscure ultimate beneficial ownership information and the movement of illicit funds. vIBANs are functionally identical to conventional IBANs and can be used to send and receive payments on a global scale. A vIBAN is not matched to an account at a physical bank and can be used to deceive victims into believing that they are transferring funds into a traditional bank account.

- The COVID-19 pandemic accelerated the transition from in-person to virtual financial activities, such as online account opening, payments, and lending. As a result, fraudulent activities such as telephone and email scams; bank, elder, and healthcare fraud (e.g., related to personal protective equipment and other healthcare products) also increased after the pandemic.

- Fraudulent investment scams have significantly increased via the use of smartphones, email, and social media, as individuals seek social engagement online to minimize physical health risks. Coupled with anonymity-enhancing technologies, such as virtual private networks (VPNs), criminals have developed new and innovative methodologies to move illicit funds.

Criminal networks may rely on one or more methodologies to engage in online fraud, successfully deceiving victims into giving them money. Some fraudsters will combine elements of CEF to obtain funds and use a combination of techniques, such as those listed below, to victimize their marks.

- Information extraction (e.g., through phishing or BEC)
- Social deception or engineering, and preying on vulnerable emotions (e.g., by pretending to be another person or entity, developing "relationships" online, and using those connections as a premise to generate urgency, fear, or trust)
- False offers of investments or easy money
- Online mediums or platforms that can be used either for communication or transactions in cases of online trading fraud

Pig butchering—a combination of a romance scam and investment fraud, in which the criminal will build a "relationship" with the victim to earn their trust and convince them to invest in fraudulent cryptocurrency or other fake projects—has become a common scheme, causing billions of dollars in losses. FinCEN in September issued an alert about these scams, which are largely perpetrated by criminal enterprises based in Southeast Asia that use victims of labor trafficking to reach millions of victims around the world.

Criminals continue to evolve their methodologies and will use increasingly innovative techniques to deceive victims, and sometimes one victim numerous times. Visit the DOLFIN library to learn more about bank fraud typologies.


AML

Non-Traditional Sectors

The widespread use of social media, streaming, and gaming platforms allows users to receive donations, gifts, tokens, or credits from viewers and the public. Criminals may take advantage of the absence of AML/CFT requirements and use these platforms to launder proceeds of crime.

- Turkish authorities in early 2022 arrested 40 individuals for laundering money through Amazon's streaming platform Twitch. Scammers would use stolen credit cards to donate Bits—a proprietary Twitch currency that can be bought with real money—to small, lesser-known streamers, who would receive payouts from Twitch and return the funds to the scammer donors, keeping a portion themselves.

- Media reports this year indicated that fraudsters were using the messaging platform Telegram to recruit "walkers"—individuals who physically enter banks and cash fraudulent checks for a fee—to help them commit check fraud in which criminals steal paper checks (i.e., for pandemic relief), wash out the names of the true recipients, write in new names, and cash the checks under false identities. Telegram, in particular, has been rife with the latest tips and tricks to commit bank fraud.

Although nontraditional sectors, including social media platforms, e-commerce, and messaging platforms are not subject to AML/CFT regulations, they may possess vital digital forensic information, including IP addresses, phone numbers, and email addresses, that can help law enforcement identify illicit actors. Where fraudulent websites or advertisements are used for CEF, these sectors would also possess financial transaction and payment information linked to the criminals.

The link between CEF and human trafficking—in which victims are lured through fake job ads to call centers and forced to commit CEF on an industrial scale—is becoming more common. Forcing human-trafficking victims to participate in fraud allows CEF syndicates to increase the geographical diversity of the online victims they can target, because the trafficked victims can be exploited for their knowledge of languages and cultural insight.

- CEF center operations can become more sophisticated if skilled professionals such as IT workers or "digital sales executives" are trafficked and forced to use their skills in fraud activities. These call centers sometimes intentionally operate within the time zones of intended victims and use rental properties as temporary operations centers that allow them to quickly relocate and change IP addresses to avoid detection by law enforcement.

- Not only is cyber fraud used to recruit participants in criminal activities, sexual exploitation, and recruitment of child soldiers, but as job seekers increasingly use the Internet to find employment opportunities, they are increasingly being forced to work as cyber scammers in shuttered compounds under armed guard, according to the State Department's Trafficking in Persons Report released in June 2023.

- Criminals often recruit money mules—individuals who, at someone else's direction, receive and move funds obtained from victims of fraud—through job offers and advertisements, as well as online social media interactions, offering them incentives or fees to handle illicit funds. Money mule recruiters (aka mule "herders") recruit foreign nationals with no apparent connection to the jurisdiction and direct them to set up mule accounts, either by physical travel or through virtual account opening. Individual money mules may also be instructed to act as nominee directors for shell companies and open corporate accounts to further obscure criminal ownership.

Techniques and Typologies

Illicit actors use a variety of techniques to ensure that the proceeds of their criminal activities smoothly transit the global financial system. The money-laundering techniques used to move proceeds of CEF many times resemble those of other crimes, but criminals involved in CEF also use the Internet and digital technologies to help obscure the origins of funds and move assets.

Tests. Criminals may deposit a small amount of funds into the criminal account, so they can change the destination of the funds if the bank, PSP, or other financial institution detects the fraud.

Use of corporate accounts. In BEC fraud cases, CEF syndicates have shifted from the use of individual accounts to the use of corporate accounts to reduce the risk of detection and increase the perception of legitimacy.

Smurfing; account-hopping; conversion to other types of financial assets (e.g., (e-money). The fraudulently obtained funds move quickly through the money-laundering ecosystem via pass-through transactions, likely increasing the time necessary for FIUs and law enforcement to access the requisite financial data across borders, sectors, and institutions, to trace, secure, and recover illicit proceeds. Mules or individuals linked to CEF syndicates can also withdraw cash via ATMs, allowing them to avoid face-to-face contact with bank tellers and courier cash across borders with minimal disruptions.

Trade-based money laundering. Criminals often use false invoicing or buy high-value or readily marketable goods, such as vehicle parts, tickets, and household items with illicit proceeds. Some jurisdictions reported fraudulent wire transfers to legitimate businesses, ranging from well-known luxury or electronics brands to small local businesses for purchase of goods, which can be moved across borders and converted back into cash for further layering and integration. Commercial businesses outside of the AML/CFT regime may not have sufficient awareness or knowledge to perform identity verification or transaction monitoring – and be unwittingly exploited by criminals. The provision of overpriced or fictitious invoices for IT or consultancy services may also be part of the ML techniques adopted.

Unlicensed or unregistered remitters and VASPs. Criminal proceeds may be transferred via informal money transfer services, such as hawalas, with little or no AML/CFT controls. When moving virtual assets (VAs), syndicates may exploit VASPs based in jurisdictions with no or weak AML/CFT controls and use anonymity-enhancing techniques, such as unhosted wallets, peer-to-peer transactions, and high-risk exchanges to quickly launder CEF proceeds. Criminals are also increasingly using Bitcoin ATMs to transfer value and obscure the identity of those controlling the funds, including providing falsified or altered identification documents when depositing or withdrawing funds. They also employ obfuscating techniques, including mixers or tumbler services, as well as privacy coins, such as Monero, and decentralized finance (DeFi) services.

Technological developments are allowing CEF syndicates to quickly recruit money mules, create accounts to move fraud proceeds, and expand their cross-border reach. Criminals may steal identities using advanced technological tools and have begun using artificial intelligence to improve their phishing techniques, making them more plausible, creating synthetic identities, spoofing websites using homoglyphs to lure victims into malicious domains, and using deepfakes for account takeover.

Deepfakes can also be used in combination with social engineering techniques to trick victims into giving up their account credentials.

The FATF report provides a list of red flags or indicators that could help banks, other financial institutions, and law enforcement agencies identify possible links to CEF. The presence of these indicators should prompt further monitoring and research.

Suspicious Transaction patterns that may include activities inconsistent with normal account activities, including rapid or immediate cash withdrawals or transfers, emptying the account, transfers to and from high-risk jurisdictions, and round value amount purchases, indicating possible gift card acquisitions should prompt extra scrutiny.

Customer transaction instructions and remarks that may include poorly written instructions, variations in language and amounts that appear inconsistent with previous instructions, as well as language designating the transaction request as "Urgent," "Secret," or "Confidential" should be considered suspicious.

Suspicion in account holder's profile, in which the account holder is unwilling or unable to pass a CDD check or is unfamiliar with the source of the funds moving through their account, as well as has inadequate knowledge of the purpose or nature of the transactions in which their account is involved may indicate that the customer is acting as a money mule.

An account user's identity that includes frequent changes of contact details, efforts to conceal the user's identity by using shared, falsified, stolen, or altered identification, suspicious email addresses that do not seem compatible with the account holder's name, or abnormalities identified via online behavior should trigger further examination.

IP addresses or GPS coordinates originating from high-risk money laundering jurisdictions, use of VPNs, or other efforts to mask a user's IP address, as well as accounts operated with excessively quick keystrokes or navigation suggesting possible bot control should be eyed with suspicion.

Adverse information on the account holder, such as adverse media reports, unfavorable information provided by FIUs or law enforcement, or the presence of fraud reports from correspondent institutions or third-party fraud databases should be closely examined.

Virtual asset transactions that include sending or receiving virtual currencies to unhosted wallet addresses or addresses associated with darknet marketplaces, high-risk jurisdictions, mixing services, ransomware groups, and gambling sites should be considered suspicious.

Other red flags include mismatches of account number and name of the holder of the account, or a user captured on video as being instructed or coached during a transaction.

Detection and Deterrence

FATF identifies two key sources of detection: victim reporting and suspicious transaction or activity reports (STRs or SARs).

Given the cross-cutting nature of CEF, FATF recommends strong domestic coordination across agencies, which would help jurisdictions identify key vulnerabilities, share information, and devise holistic policy responses across the key sectors. Domestic operation coordination can also involve technical agencies to boost detection and investigation, and use technical cybercrime experts as leverage, particularly relating to network intrusions and other technical infrastructure.

Jurisdictions have also sought to collaborate with the private sector through public-private partnerships (PPPs) to help improve detection efforts, identify hidden ML networks through tactical information exchanges, and enhance operational asset recovery response. FATF also recommends information-sharing among bank officers, including best practices and common or new typologies, as well as developing collective measures to disrupt illicit activity.

Timely access to financial and banking information is crucial in accelerating the investigation and tracing CEF proceeds. Some jurisdictions have used technology to keep pace with the swift flows of CEF proceeds, often collaborating with the private sector in the process. Others rely on central registers or develop databases to streamline the information retrieval process.

Technology-enabled information retrieval. Competent authorities within a jurisdiction may agree on data fields or standardized templates that would be relevant for their investigations to enable financial institutions to quickly provide relevant information to law enforcement and file relevant reports.

Facilitating asset tracing across FIs. Developing platforms to facilitate rapid tracing and information exchange across various FIs to intercept illicit proceeds can be useful to quickly track pass-through transactions and account-hopping across multiple banks.

Using central registers. Central bank registers allow law enforcement agencies quick access to basic bank information and help speed up CEF investigations, verifying the banks in which the suspect holds accounts or the identity of the account holder.

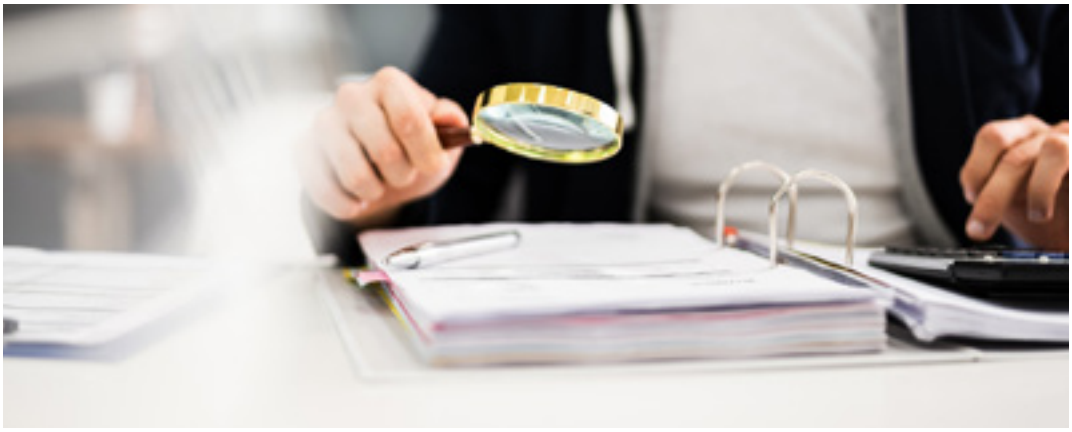
Developing databases for information sharing. Numerous mule accounts may be known or suspected to have been part of previous scams or identity takeovers used by ML syndicates. Some jurisdictions have sought to centralize data that cuts across anti-fraud and AML databases to identify deeper ML networks across various FIs.

Deterring money mules. Public education and outreach to potential money mules can help inform potential unwitting accomplices. Global social media campaigns, such as Europol's #DontbeaMule and INTERPOL's #YourAccountYourCrime, can serve as useful platforms to coordinate international awareness against money mule activities.

Real-time transaction monitoring. FATF recommends that FIs use sophisticated software and algorithms to monitor financial transactions and identify and prevent fraudulent activities in real time. By monitoring abnormal account holder information (e.g., physical, IP and email addresses, mobile numbers, etc.) and transactions in real-time, FIs can quickly identify, investigate, and report any unusual or suspicious activity.

International cooperation is critical to detecting and deterring the movement of funds obtained through CEF, but cross-jurisdictional challenges exist, especially since the jurisdiction where the CEF occurs (the location of the victim) is generally different from the jurisdiction where the proceeds are laundered. The instantaneous nature of financial transactions also presents a challenge to tracing and attributing financial transfers. Legal barriers can restrict informal information sharing, and privacy considerations between jurisdictions must be addressed. Uneven capacity and priorities also may dissuade jurisdictions from participating in joint actions.

Multilateral "rapid response" programs created by various bodies to trace and recover CEF proceeds, including INTERPOL's Global Rapid Intervention of Payments (I-GRIP), the Egmont Group's BEC Project, and the US "Financial Fraud Kill Chain," can help mitigate the challenges associated with the near-instantaneous nature of CEF financial transactions. Experience from these bodies generally shows that intervention is most effective within 24 to 72 hours of a fraudulent transaction.



Mitigation Strategies

Financial regulators have adopted anti-fraud requirements alongside AML/CFT controls, some of which target criminals' ability to register, access, and control mule accounts remotely. Rigorous Know-Your-Customer or Know-Your-Business processes, biometric features during digital on-boarding processes, and identification of one mobile or secure device to authenticate online banking transactions (others are blocked or subjected to enhanced risk mitigation measures) can help stop suspicious transactions, as can a cooling-off period for first time enrollment of online banking services or secure devices, limiting the number or value of financial transactions by the customer.

FATF also recommends developing a definition of "expected transactions," including defining the number of transactions, amounts, types of counterparties, and countries involved to help detect suspicious activity.

"Verification of payee" services allow the originator/payer/debtor of a transfer order to check that the beneficiary/payee/creditor mentioned in the payment messages matches the name of the account holder. Reducing email communications and social media with clients to general information only; adding voice recognition software and artificial intelligence support in client communications to verify identity; and requiring multi-factor authentication for customer verification can also help financial institutions detect fraud.

To authenticate the identity of the user during remote set up, financial institutions can enhance the reliability of the client identification process through "liveness" tests to ensure that a genuine human being is opening an account—although these automated tests have been shown to be vulnerable to deepfake technologies, according to media reporting, and therefore other corroborating strategies should be employed. In addition, monitoring IP addresses used to connect to online banking websites, including detecting use of Remote Access Tools, can be a useful strategy.

Financial institutions could use data that they collect and analyze about their customers, including mobile phone numbers, IP addresses, GPS coordinates, and device IDs to gain insights into possibly suspicious transactions linked to CEF, using a risk-based, real-time monitoring system to ensure that abnormal activity can be quickly detected and investigated.