FATF

100 YEARS · ANS · AÑOS · سنة 1923 - 2023

INTERPOL

EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

Illicit Financial Flows from Cyber-Enabled Fraud

November 2023

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard. For more information about the FATF, please visit **www.fatf-gafi.org.** This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

The goal of the Egmont Group of Financial Intelligence Units (Egmont Group) is to provide a forum for financial intelligence units (FIUs) around the world to improve co-operation in the fight against money laundering and the financing of terrorism and to foster the implementation of domestic programs in this field. For more information about the Egmont Group, please visit the website: www.egmontgroup.org.

INTERPOL's role is to enable police in our 195 member countries to work together to fight transnational crime and make the world a safer place. We maintain global databases containing police information on criminals and crime, and we provide operational and forensic support, analysis services and training. These policing capabilities are delivered worldwide and support four global programmes: financial crime and corruption; counter-terrorism; cybercrime; and organized and emerging crime.

Citing reference:

FATF – Interpol - Egmont Group (2023), *Illicit Financial Flows from Cyber-Enabled Fraud*, FATF, Paris, France, www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/iIllicit-financial-flows-cyber-enabled-fraud.html

Photo credits cover photo ©Getty Images

Table of Contents

List of Acronyms

AML/CFT	Anti-money laundering/Countering the financing of terrorism
ATM	Automated teller machine
BEC	Business email compromise
CDD	Customer due diligence
CEF	Cyber-enabled fraud
DNFBP	Designated non-financial businesses and professions
FI	Financial Institution
FIU	Financial Intelligence Unit
IBAN	International Bank Account Number
IP	Internet protocol
LEA	Law enforcement agency
ML	Money Laundering
MLA	Mutual legal assistance
PSP	Payment service provider
PPP	Public-private partnership
STR	Suspicious Transaction report
TF	Terrorist financing
TBML	Trade-based money laundering
VA	Virtual asset
VASP	Virtual Asset Service Provider
vIBAN	Virtual International Bank Account Number
VPN	Virtual private network
VoIP	Voice over Internet Protocol

Executive Summary

Cyber-enabled fraud (CEF) is a growing transnational organised crime. CEF criminal syndicates are often well structured into distinct sub-groups with specialised areas of criminal expertise, including money laundering. These sub-groups may also be loosely organised and de-centralised across different jurisdictions, which further complicate efforts to investigate CEF activity. CEF syndicates are also found to be linked to other types of criminality, notably human trafficking and forced labour in CEF call centres as well as proliferation financing linked to illicit cyber activities from the Democratic People's Republic of Korea (DPRK).

Money laundering groups and professional enablers are involved in the CEF-ML process. The ML network of accounts typically involves money mules but can also include shell companies or legitimate businesses. ML networks also feature different types of financial institutions (FIs), including banks, payment and remittance providers, and virtual asset service providers (VASPs). To further conceal the financial trail of their ill-gotten gains, criminals use a combination of various ML techniques, such as the use of cash, trade-based money laundering (TBML), and unlicensed services.

Aided by digitalisation, technology has allowed CEF criminals to develop and increase the scale, scope, and speed of their illicit activities. They use various tools and techniques to deceive victims or prey on their psychological state and emotions to extract as much funds as possible. CEF syndicates are exploiting technological developments to make it easier and faster to launder the proceeds of their crimes. Virtual services, such as remote online account opening, also allow criminals to easily set up foreign accounts and launder proceeds abroad, with financial transactions being executed at near-instantaneous speeds. Criminals are taking advantage of social media and messaging platforms to recruit money mules across borders at scale. Criminals are also quick to exploit vulnerabilities that emerge through new digital financial institutions and products, as well as non-traditional sectors such as e-commerce and social media and streaming platforms.

Jurisdictions need to respond more effectively. They need to:

- employ initiatives to increase victim reporting and enhance suspicious transaction reporting;
- effectively analyse voluminous information inflows to tackle CEF; and
- given the cross-cutting nature of CEF, strong domestic co-ordination mechanisms are required to holistically combat and prevent CEF and related ML.

The location where CEF predicate offences occur tends to be different from where the ML process occurs. Proceeds can be laundered quickly through a network of accounts, which often span across multiple jurisdictions and financial institutions. Jurisdictions must collaborate multi-laterally to effectively and expeditiously intercept CEF proceeds that are laundered across borders. To do so, jurisdictions should leverage and support existing (and any future) multi-lateral mechanisms (such as INTERPOL's I-GRIP and the Egmont Group BEC Project) for rapid international co-operation and information exchange to more effectively combat CEF.

Lastly, the report includes a list of risk indicators, as well as useful anti-fraud requirements and controls, that may be useful for public and private sector entities to detect and prevent CEF and related ML.

1. Introduction

1. Online fraud and scams have dominated the cyber-enabled crime landscape. Left unchecked, they will only grow in sophistication and pose a greater threat and risk as more organised crime groups engage in this illicit activity and take advantage of opportunities presented by new technologies, such as generative artificial intelligence.[1]

2. Under the Singaporean Presidency, the FATF started a new initiative to focus on countering illicit financial flows from cyber-enabled fraud. This report is the result of a joint project between the Egmont Group, FATF and INTERPOL, the first project that these three organisations have undertaken jointly, and reflects a strong collective commitment to tackling transnational organised criminals and their networks.

1.1. Focus and scope

3. This report focuses on illicit financing arising from fraud that is enabled through or conducted in the cyber environment and that (i) involves transnational criminality such as transnational actors and funds flows and (ii) involves deceptive social engineering techniques (i.e., manipulating victims to obtain access to confidential or personal information). Recognising the many variations of such fraud, this report focuses on the following types of criminal activity (referred to collectively as *cyber-enabled fraud* (CEF)):

- **Business Email Compromise (BEC) fraud:** Victims receive email instructions that purport to be from their clients or suppliers' asking victims to transfer funds to new payments accounts.
- **Phishing fraud:** Victims are deceived into revealing sensitive information such as personal data, banking details or account login credentials. The criminal will then use the information to drain the victims' money from their payments accounts, open new payment accounts or make fraudulent transactions.
- **Social media and telecommunication impersonation fraud:** This includes scenarios where victims are contacted via mobile or social media applications by criminals pretending to be government officials, relatives or friends, and prey on the victims' emotions to induce payment or hand over control of payments accounts or to carry out financial activities such as a loan application or an account opening to receive criminal proceeds.
- **Online trading/ trading platform fraud:** Victims are deluded by fake advertisements or advisors online to non-existent or fake (fraudulent) platforms for trading or investment related to both fiat and virtual assets.
- **Online romance fraud:** Victims are duped into sending money to criminals after being convinced that they are in a romantic relationship.
- **Employment scams:** Fake job offers on social media platforms trick victims to pay scammers upon various excuses including advanced payment for

[1] See also International Monetary Fund (August 2023) *Fintech Note: Generative Artificial Intelligence in Finance: Risk Considerations*.

purchasing commodities to boost sales of a trading platform or a guarantee fee to secure employment.

4. Illicit financing related to ransomware and other malware-enabled crimes are not within the scope of this report. Readers should refer to the FATF's report on *Countering Ransomware Financing* (March 2023) for more information on ransomware, as well as information on laundering through virtual asset (VA) and virtual asset service providers (VASPs), as well as challenges and good practices for risk mitigation. This information is relevant as VAs and VASPs are sometimes exploited to launder the proceeds of CEF.

1.2. Objectives and structure

5. This report aims to enhance competent authorities' risk understanding of the threat posed by CEF. The report builds upon existing work already done by the FATF and other international bodies (including the Egmont Group, Europol, and INTERPOL), and looks to identify significant and emerging developments which are relevant for enhanced risk understanding.

   - **Chapters 2 and 3** of the report discuss the current operating risk environment vis-à-vis CEF and provide insights on the risks, techniques, and trends on CEF and related money laundering (ML), including the impact and vulnerabilities of digitalisation and new technologies.

   - **Chapters 4 and 5** of the report identify good practices and operational solutions used by jurisdictions to overcome challenges to tackle and disrupt CEF and related ML, including mechanisms for international co-operation and asset recovery.

1.3. Methodology

6. Experts from Singapore (on behalf of the FATF), FIU Hong Kong China (on behalf of the Egmont Group) and INTERPOL, co-led this project. In addition, the following jurisdictions and entities contributed to the work as part of the project team: Azerbaijan, Brazil, Belgium, Canada, China, the Council of Europe, the European Commission, Europol, Germany, the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA), India, Italy, Israel, Japan, Malaysia, Mexico, the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), Pakistan, Portugal, Saudi Arabia, Togo, the United Kingdom, and the United States.

7. The findings in the report are based on:

   - A review of existing literature and open-source material on this topic. This includes data and research done by the Egmont Group and INTERPOL.

   - A request to the FATF's Global Network and the Egmont Group of over 200 jurisdictions and 170 FIUs respectively, for information on risks, enforcement frameworks and strategies, as well as domestic and international co-operation and co-ordination mechanisms. In total, the project team received inputs from more than 80 delegations.

- Discussions and insights shared at the FATF's Joint Experts Meeting (April 2023) and the Private Sector Consultative Forum (May 2023), including a targeted engagement with the private sector.

2. Risk environment: Cyber-enabled Fraud

2.1. Rising money laundering (ML) threat

8. CEF has increased significantly internationally. While there is no complete estimate of the global magnitude and scale of CEF, many jurisdictions report consistent growth in recent years. Illicit proceeds from CEF are often transferred to foreign jurisdictions. These proceeds may then be further laundered through the financial systems of other third-party jurisdictions.

9. According to the INTERPOL Global Crime Trend Report 2022[2], online scams are one of the cybercrime trends most frequently perceived as posing 'high' or 'very high' threats globally. Most jurisdictions that provided information for this project recognise the ML risks arising from CEF within their national risk assessments. Regions that are highly cashless and digital-based (e.g., where the bulk of financial intermediation is done via online services) are expectedly more vulnerable to the ML risks associated with this crime, although the transnational nature of CEF means that criminals can easily target victims regardless of international borders. The box below pulls together various sources of information[3] to provide a regional overview of the CEF threat landscape.

Box 1. Increased ML threats: regional CEF trends

Africa: In Africa, the rapidly digitalized financial sector has opened up a multitude of opportunities to criminals to perpetrate CEF causing a sharp increase in online banking fraud, including phishing, identity theft and virtual asset scams. The rise in financial losses through such crimes poses an increased ML threat. For example, in West Africa, CEF is reportedly considered as a major source of proceeds of crime.

Americas: CEF has been identified as an increasing or emerging risk. One jurisdiction noted how CEF reports have risen year-on-year, and noted that related ML risk would correspondingly increase. Another reported that investment fraud in virtual assets increased over 180 percent between 2021 and 2022, with criminals taking advantage of the hype and publicity around virtual assets.

Asia-Pacific: Jurisdictions have cited CEF as a high or significant ML risk. For example, one jurisdiction cited that the majority of fraud reports contain some form of CEF and had observed an increase in ML linked to CEF. Another jurisdiction highlighted the role of transnational actors in defrauding victims through a plethora of illegal investment apps. The COVID-19 pandemic accelerated the digitalization of the services and behaviours of private citizens, governments, and businesses in the region.

[2] See INTERPOL (2022) *Global Crime Trend Summary Report*

[3] Includes information and data provided by jurisdictions, as well as reports from INTERPOL and Europol.

Consequently, CEF and associated ML have escalated and are expected to continue to escalate.

Caribbean: The region is highly susceptible to CEF and related laundering, with an increase in overall fraud related to CEF over the past five years. The growing VA sector in the Caribbean Basin also creates vulnerabilities, including from the presence of VASPs, including mixers, that may be misused to launder illicit funds back to organised crime groups, including CEF.

Europe: CEF is generally assessed as posing a ML risk. Many jurisdictions noted a large increase in this activity, with CEF perceived to pose high threats. The use of VA is commonly observed to launder CEF-proceeds (particularly relating to online trading fraud relating to VAs, e.g., fraudulent initial coin offerings).

Middle East and North Africa (MENA): Consistent with trends in other regions of the world, the MENA saw digitalization rates accelerate during the pandemic as governments, businesses and citizens massively shifted activities online. Online financial frauds, including phishing, impersonation fraud, and online scams are ranked as high threats. The MENA region is also vulnerable to ML as the GCC member countries, in particular, serve as important transhipment hubs for global trade and financial activities.

10. Digitalisation and the development of new technologies serve as key drivers underpinning the growth of CEF. Digital services are now integral to daily life and public functions. As a result, more citizens (including vulnerable groups) are participating in online activity. At the same time, digitalisation means jurisdictions are becoming increasingly connected with information and funds moving swiftly across borders. These two factors have fundamentally altered the criminal landscape and created an environment of increased threats from CEF.

11. The COVID-19 pandemic accelerated the transition from in-person financial activities to online account opening, payments and lending. Fraudulent activities such as telephone and email scams; bank, elder and healthcare fraud (e.g., related to personal protective equipment and other healthcare products) and fraudulent investment scams have significantly increased via the Internet through the use of smartphones, email and social media. These changing financial behaviours have also impacted the ML landscape, including increased use of digital banking and payments platforms and remote transactions (see also section ‘Impact of digitalisation and new technologies on page 24).[4]

12. The increasingly prevalent use of smartphones, technology (with ever evolving new tools and applications), as well as remote financial transactions, have massively increased the vulnerability of users. Coupled with anonymity-enhancing

[4] See FATF (May 2020) *COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses* and (December 2020) *Update: COVID-19-Related Money Laundering and Terrorist Financing Risks*.

technology, such as Virtual Private Networks (VPNs) and 'The Onion Router'[5], this can provide criminals with a cloak of anonymity for their illicit activities. Leveraging technology, criminals can increase the scale, scope, and speed of their criminal activities. Criminals are further observed to be adopting a "Crime-as-a-Service" model[6], which also significantly lowers the barriers to entry for CEF syndicates, with an increased specialisation on different aspects of CEF distributed across different sub-groups (see Section 2.2 below).[7]

13. In many instances, organised criminal groups have expanded or adapted their activities to incorporate CEF, by using existing techniques to launder their other unlawfully obtained funds.

Box 2. Common criminal ML network used for CEF and other crimes

A ML network runs online gambling and CEF operations at its company's building in Country A's Special Economic Zone (SEZ). The complex houses around ten companies that operate online gambling and CEF operations themselves or have rented the space to others to do so. The network includes purported legitimate businesses in the border regions of neighbouring Country B. The network is led by nationals of Country B that use bank accounts in Country B's currency to facilitate the movement of money from the SEZ to Country C, where the company's major investors are based. U.S. dollars from the SEZ are laundered through money exchanges in Country B, where the money is converted into Country B's currency and then transported to Country C. On the Country C side of the border, money is then transferred to the company's investors.

Source: Transnational Organized Crime, Casinos and Money Laundering in Southeast Asia: A Threat Analysis (UNODC, 2022)

2.2. Criminal characteristics of CEF

Elements of CEF

14. Based on jurisdictions' experience, CEF criminals may rely on one or more of the following elements to successfully deceive victims into making a fraudulent transfer. Different variants of CEF can combine the elements above in different ways.

- Information extraction (e.g., through phishing);
- Social deception or engineering, and preying on vulnerable emotions (e.g., by pretending to be another person or entity and using that as a premise to

[5] Also known as TOR, this is an open-source software that allows users to surf the Internet anonymously.

[6] This is where division of labour occurs, with criminal groups developing and offering niched criminal capabilities, skills and expertise to others.

[7] See Europol (July 2023) *Internet Organised Crime Threat Assessment (IOCTA) 2023*; and INTERPOL (2022) *Financial and cybercrimes top global police concerns, say new INTERPOL report*

generate urgency, fear or trust; or by offering false claims to earn money easily); and

- Online medium or platform (that can be either used for communication or for victims to transact on in cases on online trading fraud).

15. A victim may not fall for just one type of CEF; ultimately, the goal is to induce a funds transfer, and criminals will use a variety of techniques to achieve this. Criminals are creative and may engage or transition to other types of CEF if the initial deception begins to fail. For example, a phishing or social media impersonation fraud victim could be convinced and directed to an investment fraud scheme by the same criminal by leveraging on the "trust" already built through the initial fraud scheme.

Box 3. Same victims, multiple offences

Pig butchering is a combination of romance scam and investment fraud. With this modus operandi, criminals build a trust relationship with the victim and convince them to invest savings in fraudulent cryptocurrency trading platforms. The scam is perpetrated over time, resulting in the loss of large amounts of money.

Following the realisation of the fraud, criminals often contact their victims posing as lawyers or law enforcement agents offering help to retrieve their funds, in exchange for a fee.

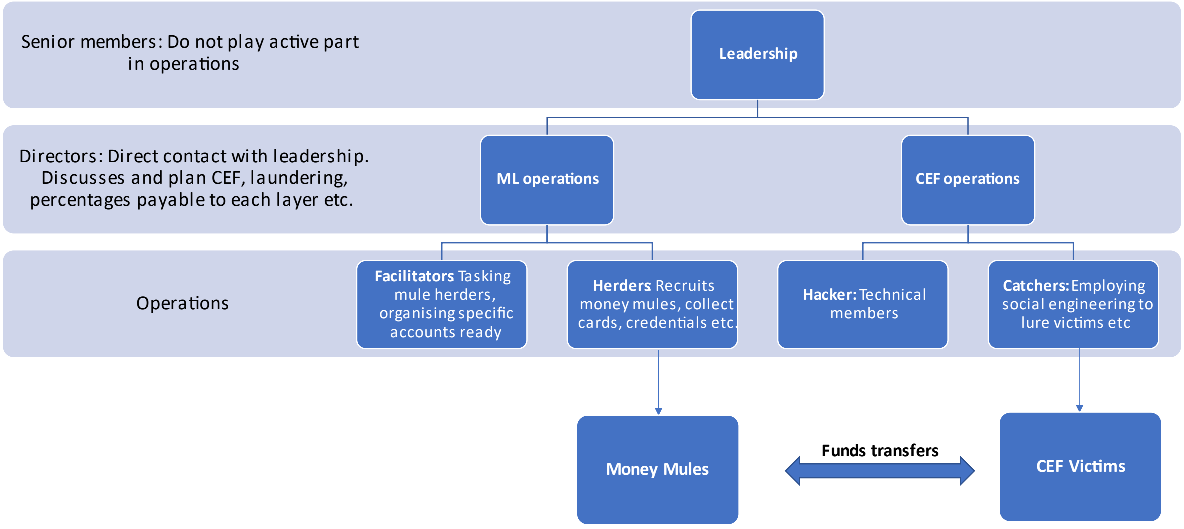
Source: Europol (2023), Internet Organised Crime Threat Assessment (IOCTA) 2023

Organised criminal structure

16. CEF and related ML are often executed by transnational organised criminal groups or syndicates. While their structures may vary, CEF syndicates often operate as hierarchical organisations (see example in Figure 1). They may also be loosely organised to retain flexibility, with members joining and leaving as needed. These syndicates may also be organised around distinct sub-groups with specialised areas of criminal expertise (e.g., in line with the elements of CEF above (information extraction, social deception; or other technical expertise like creation of an online platform or ML). In many instances, these CEF syndicates are de-centralised and have never communicated in person (e.g., through online encrypted channels), making it difficult for authorities to investigate them.

17. Furthermore, CEF syndicates are regularly composed of well-educated and technically competent professionals. This has resulted in an increasingly sophisticated approach to CEF and the laundering of illicit profits. Jurisdictions noted how CEF syndicates may intentionally recruit individuals working in professional sectors (including FIs), who may be leveraged as sources of data and information to successfully execute CEF and facilitate ML. For more information on how CEF syndicates structure and operate for ML, please see section 2.3 below.

Figure 1. Example of CEF criminal structure


Senior members: Do not play active part in operations
Leadership
Directors: Direct contact with leadership. Discusses and plan CEF, laundering, percentages payable to each layer etc.
ML operations
CEF operations
Operations
Facilitators Tasking mule herders, organising specific accounts ready
Herders Recruits money mules, collect cards, credentials etc.
Hacker: Technical members
Catchers: Employing social engineering to lure victims etc
Money Mules
Funds transfers
CEF Victims

Source: FATF

Links to other criminality

18. In addition to ML, CEF syndicates may be linked to other forms of criminality. Common crimes include activities associated or necessary to carry out CEF, including cybercrime activities such as hacking to obtain personal information, the development and sale of criminal software; document forgery, etc. Part of the criminal proceeds can be self-laundered by CEF syndicates into the purchase of new equipment and development of even more advanced technological tools.

Box 4. Operation Falcon

Three suspects were arrested in Lagos, Nigeria in 2020 following a joint INTERPOL-Group-IB and Nigeria Police Force cybercrime investigation. The Nigerian nationals were believed to be members of a wider organised crime group responsible for distributing malware, carrying out phishing campaigns and extensive Business Email Compromise scams. The suspects were alleged to have developed phishing links, domains, and mass mailing campaigns in which they impersonated representatives of organisations. They then used these campaigns to disseminate 26 malware programmes, spyware and remote access tools.

These programmes were used to infiltrate and monitor the systems of victim organisations and individuals, before launching scams and syphoning funds. According to Group-IB, the prolific gang was believed to have compromised government and private sector companies in more than 150 countries since 2017. Group-IB was also able to establish that the gang is divided into subgroups with a number of individuals still at large.

Parallel ML investigations revealed that the suspects also used foreign bank and VA accounts in the United Kingdom, the United States and Thailand to receive payments from victims. The three suspects have been charged for their unlawful activities, including for fraud and money laundering. A luxury vehicle has been confiscated & suspects' accounts have been frozen and undergoing forfeiture in court.

Source: Nigeria

19. There is also a rising link between CEF and human trafficking, where victims are lured through fake job ads to online call centres and forced to commit CEF on an industrial scale. This allows CEF syndicates to increase the geographical diversity of the online victims that they can target (as the trafficked victims can be exploited for their knowledge of languages and cultural insight). It can also increase the sophistication of CEF centres by trafficking skilled professionals such as information technology workers or "digital sales executives".[8] These call centres sometimes intentionally operated within the time zones of intended victims, and used rental properties for temporary criminal operations, which allowed them to quickly re-locate and change IP addresses to avoid law enforcement detection.[9]

[8] See INTERPOL, (June 2023) *INTERPOL issues global warning on human trafficking-fueled fraud*

[9] See INTERPOL (July 2023) *Operational Analysis Online Scams and Human Trafficking in South East Asia / Update 2 – From Regional to Global Threat*; only available to national law enforcement authorities.

Box 5. Operational Storm Makers

Operation Storm Makers saw authorities carry out enforcement actions against organised crime groups believed to be facilitating the travel of Asian men, women and children across borders for exploitation and/or profit. The operation triggered 121 arrests across 25 countries, prompting 193 new investigations.

Through Operation Storm Makers, police in Malaysia and Cambodia worked closely on a case involving 15 men and one woman lured to Cambodia on the promise of a lucrative salary to work in a call centre. On arrival, however, they were locked up and forced to work 14-hour days as scammers.

Note: For more details, see INTERPOL (May 2022) *121 arrests in operation against migrant smuggling and human trafficking*

Source: INTERPOL

20. Most jurisdictions have not seen substantial evidence of terrorist financing activities linked to CEF. However, there have been some observations where elements of terrorist activities and financing were associated with CEF criminal actors. For example, suspicious transaction reports (STRs) from one jurisdiction suggest that CEF proceeds were being transferred in some cases to specific conflict areas/jurisdictions known for terror related activities.

21. There are also links to proliferation financing, with cybercrime reported as a major source of illicit income generation for the Democratic People's Republic of Korea (DPRK). Illicit cyber activities include the sale of harvested personal information, or the provision of hacking and phishing tools and services, which may be used to by other criminals to commit CEF.[10]

[10] See also United Nations Security Council (March 2023) *S/2023/171 Letter dated 3 March 2023 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council*

Box 6. Use of DRPK phishing tools for CEF to fund weapons programmes

According to information provided by to the United Nations Panel of Experts, information technology (IT) workers of the Democratic People's Republic of Korea linked to the Munitions Industry Department have been earning foreign currency by selling voice phishing hacking applications and operating multiple overseas servers and Internet Protocol addresses.

In July 2020, four Republic of Korea (ROK) nationals were arrested by the authorities in China and extradited back to ROK. One testified that criminal groups had purchased personal information of ROK nationals as well as voice phishing hacking applications from a DPRK IT worker.

The criminal groups had fooled victims to download these developed tools to steal more information from them. They subsequently posed as FI employees to trick victims into sending money.

Note: For more details, see United Nations Security Council (September 2022) *S/2022/668 Letter dated 2 September 2022 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council*

Source: Panel of Experts of the United Nations and South Korea

2.3. ML techniques and typologies

Structure of ML networks

22. When laundering proceeds generated from various types of CEF, criminals need to be quick and efficient. Jurisdictions have observed the involvement of professional ML groups as well as third-party professional enablers including lawyers, accountants, tax advisors, company secretaries and bankers. The professional ML groups may be part of the CEF criminal syndicate, or a separate de-centralised organisation that provides ML services under the "crime-as-a-service" model (professional ML networks).

Box 7. QQAAZZ Network

The QQAAZZ advertised its services as a "global, complicit bank drops service" on Russian-speaking online cybercriminal forums, where cybercriminals gather to offer or seek specialised skills or services needed to engage in a variety of cybercriminal activities. The QQAAZZ network had opened and maintained hundreds of shell company and personal bank accounts at financial institutions throughout the world, which were used to receive money from CEF cybercriminals. The funds were then transferred to other QQAAZZ controlled bank accounts and, sometimes converted to cryptocurrency using "tumbling" services designed to hide the original source of the funds. After taking a fee of up to 50 percent, QQAAZZ returned the balance of the stolen funds to their criminal clientele.

In November 2020, an international law enforcement operation involving 16 countries resulted in the arrest of 20 individuals suspected of belonging to the QQAAZZ criminal network, which attempted to launder tens of millions of euros on behalf of the world's foremost cybercriminals. Some 40 house searches were carried out in Latvia, Bulgaria, the United Kingdom, Spain, and Italy, with criminal proceedings initiated against those arrested by the United States, Portugal, the United Kingdom and Spain.

Source: Portugal and Europol

23. Typically, CEF-proceeds are rapidly laundered through a network of accounts. Case studies show that these networks can be complex by extending across multiple borders and financial institutions, although this may vary based on the criminal group's level of sophistication.[11]

24. CEF-related ML networks of accounts typically involve individuals as well as legal entities.

- **Individual money mules** are often recruited by criminals via various means, including through job offers and advertisements, as well as online social media interactions. Money mule recruiters are also known as mule 'herders.' Money mules may be knowingly complicit in the laundering of funds or work unwittingly (through deception), or negligently, and may also be offered incentives or fees to handle the illicit funds. It is challenging to identify the mule's controller (i.e., mule herder), who recruit both witting and unwitting participants, or determine the origin of fraudulent funds. Some jurisdictions noted instances of the recruitment of foreign nationals with no apparent connection to the jurisdiction, with these individuals directed to set up mule accounts, either by physical travel or through virtual account opening.

[11] For more information on the use of mules in professional money launderers and networks, see FATF (July 2018) *Professional Money Laundering*

Box 8. Mule recruitment: Job Offer

Ms. RS is a sari-sari store owner who was recruited by a certain Mr. O into what she thought was a legitimate job offer. Mr. O is a Nigerian national who was arrested in 2019 for allegedly operating a multimillion online romance scam, resulting in more than PHP 8 million (about EUR 129 000) of losses.

Mr. O had promised Ms. RS a portion for every bank transaction that she handled. In all, Ms. RS handled 83 transactions amounting to PHP 3.6 million (about EUR 58 000) over a six-month period. All transactions were cash-based (i.e., cash deposits, ATM and over-the-counter withdrawals). Mr. O was finally arrested through the collaboration of Ms RS via an entrapment operation.

Source: Philippines

- **Shell companies** are under the control of CEF criminals, typically through strawmen or nominee directors. Individual money mules recruited may also be instructed to act as such strawmen, and open corporate accounts in a bid to further obscure criminal ownership. Some jurisdictions noted that shell companies used virtual business addresses[12] to further obfuscate their criminal activities. In cases of online trading fraud, criminals may also use these shell companies to open virtual point-of-sale accounts with merchant services companies to process payments and transfers from victims.

[12] Virtual business addresses are real physical addresses offered by some service providers that allows businesses to receive postal mail and packages.

Box 9. Shell companies in online trading platform fraud

A number of STRs were filed to Türkiye's FIU relating to an online trading platform fraud scheme where victims were approached to make foreign exchange investments via phone or social media. Underpinning this scheme was a network of 209 companies, that had laundered proceeds amongst each other. The companies had mutual accountants and were mostly established on the same date and were liquidated after a short period.

Analysis by Türkiye's FIU revealed that the shell companies also acted in three distinct sub-groups, based on the funds transfers and 3rd party individual accomplices associated with them. A total of approximately TRY 10 billion (about EUR 336.7 million) was found to have been fraudulently acquired and laundered.

- One hundred thirty-five companies received TRY 9.6 billion (about EUR 323.2 million) of fraud proceeds through payment companies. To facilitate receipt of transactions from victims, these companies established virtual point-of-sale accounts. TRY 100 million (about EUR 3.4 million) was withdrawn in cash and about TRY 6 billion (about EUR 202 million) was transferred to a gold company.
- Fifty-nine companies received TRY 700 million (about EUR 23.6 million) of fraud proceeds. TRY 200 million (about EUR 6.7 million) was withdrawn in cash, and the others were transferred to VASPs after being laundered through accounts maintained by 3rd party individual accomplices.
- Twenty-three companies received TRY 875 million (about EUR 29.5 million) of fraud proceeds. TRY 220 million (about EUR 7.4 million) was withdrawn in cash, with the others were transferred to VASPs after being laundered through accounts maintained by 3rd party individual accomplices.

Source: Türkiye

- **Legitimate companies**, similar to individual money mules, may also be tricked into receiving CEF-proceeds (e.g., as an investment or business opportunity) and asked to either re-direct the funds or be refunded into a separate criminally controlled account. In some cases, legitimate companies were observed to willingly accept such "business opportunities" particularly in times of economic distress. The involvement of legitimate companies provides an additional façade to mask illicit activities from detection.

25. There are similarities in how money mules in ML networks are established for CEF and other types of crimes. However, jurisdictions have observed some differences that may be more relevant for CEF-related mules.

- **Method of recruitment**: CEF money mules are more likely to be recruited online, including through job advertisements from fake companies or through spam emails. Criminals may also exploit economic conditions and mask this as a legitimate job opportunity for "easy money". Victims of CEF (e.g., through romance fraud) can often be tricked into acting as money mules. In some instances, victims of human trafficking (such as illegal migrants or workers) are also used to open such accounts.

- **Usage of accounts**: Money mules linked to CEF are used for their accounts with financial institutions as fraudulent funds can be received and sent quickly via electronic payment methods, as opposed to physical transfers or deposits of cash. This is likely due to how victims are defrauded (i.e., through funds transfers). Given the convenience that digital banking services offer in the movement of funds, individuals targeted for CEF-related mules likely have some basic level of knowledge or proficiency in computers and technology.

Box 10. Romance fraud victim turned mule

Between April and May 2022, an elderly woman who opened her bank account originally for receiving her pension received two payments in a higher amount. One of the remittances was from a domestic bank account while the second one was from reported victim from abroad.

Subsequent investigation by Slovakian authorities revealed that the woman communicated with an individual via social media and fell prey to a romance fraud. The elderly woman provided her internet banking credentials to the fraudster and her bank account was then used to launder other crime proceeds. Part of the received money was exchanged to a crypto currency via a foreign VASP platform.

Source: Slovakia

ML typologies and techniques

26. The location in which the CEF occurs (i.e., where the victim is) is frequently different from the location where the laundering of CEF-proceeds takes place, and money mule networks may span across multiple jurisdictions. CEF syndicates realise that FIs or competent authorities may have already identified accounts for fraudulent activity prior to laundering, which could result in the interception of their criminal proceeds before they can reach the criminals' accounts. To enhance their success, criminals may perform "tests" by carrying out small value transactions so that they can change the destination of the funds if the tests fail.

27. The type of first layer account used to receive CEF-proceeds typically depends on the type of CEF to continue the façade of legitimacy. Changes over time have also been observed in the first layer account type. For example, in BEC fraud cases, CEF syndicates have shifted from the use of accounts of individual persons to the use of accounts of corporates to reduce the risk of detection.

Table 1. Relationship between type of CEF and first layer account

Type of CEF	Type of first layer account
BEC fraud	Corporate (e.g., shell or newly registered companies)
Phishing fraud	Individual money mules
Social media telecommunication impersonation fraud	Individual money mules
Online trading/ trading platform fraud	Corporate (e.g., shell or newly registered companies)
Online romance fraud	Individual money mules
Employment scams	Individual money mules

Note: This table attempts to distil some general trends based on jurisdictions' experience on the types of first layer accounts encountered for the type of CEF. However, this may not apply to all cases.

28. Once an account is established by the CEF syndicate, the fraudulently acquired funds are quickly processed to enter the ML network. Funds are thereafter rapidly layered through a series of "pass-through" transactions via domestic or foreign accounts that are controlled by the mule/strawmen themselves or by the CEF syndicate. In the latter case, money mules would surrender banking credentials, cards, and tokens, or provide power of attorney to the CEF syndicate to allow them direct control over the accounts. The involvement of professional enablers in the process, such as during the creation of a power of attorney, lends the transactions an air of legitimacy and facilitates the obfuscation of the crime.

29. To further evade detection and remain anonymous, CEF syndicates employ various techniques and mechanisms: e.g., smurfing; hopping through accounts across different financial, remittance or payment service providers; and conversion to other types of financial assets (e.g., electronic money (e-money),[13] pre-paid cards, VAs). This may increase the time necessary for FIUs and law enforcement to access the requisite financial data across borders, sectors, and institutions, in order to trace, secure and finally recover illicit proceeds. Some money mules might also only allow their accounts to be used for a specific and limited period of time. The limited time period, together with legitimate onboarding procedures, make it relatively difficult for institutions to detect abnormal activities.

[13] E-money is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency, i.e., it electronically transfers value that has legal tender status; FATF (June 2014) *Virtual Currencies key Definitions and Potential AML/CFT Risks*

Box 11. Shell companies, bank accounts and virtual assets

Multiple complaints were filed with the Indian Police that a mobile application was being used to defraud people in the guise of an investment platform for mining of crypto currency. The app promised a share in the profits earned from such investment. The company had lured the victims to invest more in the scheme and thereafter withdrawals/payments were stopped. The website and the app became inaccessible, and the operators of the app stopped responding to the investors. Multiple LEAs pursuing investigations into complaints filed by customers in different parts of country requested for information from the Indian FIU in this case. Analysis by the Indian FIU identified two entities operating the app on Google Play Store, which were subsequently deleted from Google Play Store. Another 34 entities were identified to be linked to these two entities. Out of the 36 entities, 28 entities had foreign nationals as directors.

India's Enforcement Directorate (ED) also initiated parallel ML investigations, which revealed a large-scale criminal conspiracy and involvement of several shell entities in operation of similar fraudulent apps/website to cheat the gullible people and siphoning of proceeds of crime. On physical verification, the entities could not be found at the registered address. Following the financial trail, several of these entities were also found to be involved in operating illegal betting and loan apps and were also cheating the public in the guise of these apps too. Illicit monies collected from victims were moved to accounts of various shell entities and part of the proceeds of crime was also eventually converted to virtual assets. Proceeds of crime in the form of balances available in the bank accounts held by various shell entities to the tune of INR 865 million (EUR 9.9 million) were found and frozen.

Source: India

30. Jurisdictions further reported the use of other types of ML techniques, intended to obfuscate the link between the different criminal CEF and ML groups.

- **Cash:** Multiple case studies in this report feature the withdrawal of cash by mules and CEF syndicates. The movement of cash outside of FIs can be difficult to track. Cash may be withdrawn via ATMs after being laundered across a ML network, which allows criminals to avoid face-to-face contact with FIs. These funds may be couriered across borders by cash couriers and be deposited for further laundering. Criminal proceeds may also be used to purchase valuables and instruments which can be later resold for cash, such as prepaid cards or precious metals.

Box 12. Withdrawal of cash and purchasing of gold and fuel cards

In March 2023, an accountant of a Chinese company fell prey to a bank impersonation fraud. He was added into a group on a messaging app on the grounds that an annual inspection of the company's account had to be conducted.

Criminals in the messaging group later impersonated the company's legal representatives and shareholders and requested the victim to transfer RMB 7.8 million (about EUR 996 000) to two designated corporate accounts under the control of the criminal group. Police investigations showed that the funds were transferred into 26 secondary bank accounts, and then withdrawn in cash over the bank counters or via ATM, transferred to third-party payment platforms, as well as used to buy gold and fuel cards.

Source: China

- **Trade/service-based ML:** There are various trade/service-based ML techniques that criminals may employ to move proceeds of crime across borders.[14] For CEF-proceeds, some jurisdictions have observed that criminals use trade-based money laundering (TBML) techniques such as fictitious or false invoicing, as well as using illicit proceeds to purchase high value or readily marketable goods (e.g., vehicle parts, tickets, household items etc.). For example, 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. These goods 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.

[14] See also FATF – Egmont Group (December 2020) *Trade-based Money Laundering: Trends and Developments*; and FATF (July 2018) *Professional Money Laundering*

Box 13. CEF, mules and TBML

Irish authorities arrested a key individual, Person MS, in a scheme to launder romance and BEC proceeds from Ireland to Nigeria through TBML. Investigations are still ongoing. Thus far, authorities believe that the laundering scheme involves at least 60 names and 64 bank accounts.

In this scheme, proceeds of such fraud are first transferred into Irish mules' bank accounts. Funds are then withdrawn in cash and transferred into Irish accounts directly linked or owned by Person MS. Many of the accounts linked to Person MS were found to be opened under false identities.

A Nigerian company (controlled by a Nigerian believed to be based in the United States) orders goods from legitimate European or Chinese companies. These legitimate companies dealt with goods that can be purchased and shipped for resale, including alcohol, clothing, electronics, and pharmaceuticals. Person MS' Irish accounts would make payment for the relevant invoices, with the goods finally shipped to the accomplice company in Nigeria.

In one instance, a German pharmaceutical company received funds of more than EUR 1.7 million to pay for goods purchased by the Nigerian company. These funds were directly traced to BEC and romance fraud proceeds across Europe and the US, and came from various accounts either linked or owned by Person MS, or directly from victims. These goods were finally shipped to Nigeria.

Source: Ireland

- **Unlicensed or unregistered remitters and VASPs:** Criminal proceeds may be transferred out of jurisdiction using underground money remitters or hawala services with little or no AML/CFT controls. Where VAs are involved, syndicates may exploit VASPs based in jurisdictions with no or weak AML/CFT controls.
- **VA anonymity-enhancing techniques:**[15] The use of unhosted wallets, peer-to-peer transactions, peel chains, and high-risk exchanges are the preferred methods to quickly launder VA-related CEF-proceeds out of a jurisdiction, and are often used in combination. 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 such as different identifiers, phone numbers or dates of birth when depositing or withdrawing funds. They also employ obfuscating techniques, including using mixers or tumbler services as well as anonymity-enhanced VAs (also called privacy coins, e.g., Monero) and decentralised finance (DeFi) services.

[15] These techniques are explored at length in FATF (March 2023) *Countering Ransomware Financing*

Box 14. Complex ML across multiple sectors

A foreign romance scam syndicate targeted approximately 70 Japanese victims. Funds of USD 3 million were transferred to various money mule bank accounts in Japan. A Japanese man, who acted as the local mule herder, laundered the funds into Ghana, where the scam syndicate was based. The Japanese man was eventually arrested through the co-operation of Ghana via INTERPOL.

Funds from the mule accounts were subsequently transferred into the Japanese mule herder's account. STR analysis found that the funds were laundered through three channels by the Japanese mule herder:

- Wire transfers were made to a bank account held by the Japanese mule herder in Ghana. The funds were then physically withdrawn in cash in Ghana and hand delivered to the leader of the syndicate, who is still at-large. In making the wire transfers, the Japanese man presented fictitious invoices to his Japanese bank, and falsely declared them to be for a legitimate business activity (purchase of cacao beans).
- Some funds were exchanged into VAs through a VASP in Japan.
- Funds were also transferred to Ghana through an underground bank linked to the Ghanaian community in Japan.

Source: Japan

Impact of digitalisation and new technologies on ML

31. New technologies have provided new benefits and opportunities for consumers. There is a profound shift towards digitalisation of financial services, which accelerated during the COVID-19 pandemic. The reduction in cash usage and increased online activity have resulted in new innovative tools and processes. The financial payments chain is also growing increasingly dynamic and fragmented, with increased diversity in service providers offering payment and transaction services (see also section 3.1 below).

32. However, technological development can also be an advantage to criminal groups, who exploit these opportunities to drastically improve their ML techniques. Financial transactions are increasingly executed at near-instantaneous speeds, driven in part by consumer expectations for a frictionless experience. As mentioned earlier, coupled with digital anonymising techniques such as VPNs, this makes it difficult for authorities to identify the ultimate criminals performing these ML transactions in quick succession.

33. Digitalisation has increased the ease and speed at which accounts can be created for ML and expands CEF syndicates' cross-border reach. Some jurisdictions noted the increase in remote virtual processes in two areas: opening of accounts and the creation of companies. Such remote virtual processes negate the need to physically travel. Criminals can exploit these opportunities for ML.

Box 15. Scaling through digitalisation

FIU analysis found an extensive network consisting of 147 individuals and 276 bank accounts from eight banks. These individuals had relinquished their national digital identity, meant for user identification on government and other online platforms, to criminal syndicates. The syndicates then used the digital identity to open bank accounts remotely and exert direct control over these mule accounts to launder CEF proceeds. The FIU detected the network by identifying commonalities such as common banking transactions, data points (foreign contact information and device ID), as well as contact details (mailing, email, telephone).

The intelligence was referred to the Anti-Scam Command (ASCom), Singapore's dedicated unit to combat CEF and related ML under the Singapore Police Force. ASCom's investigations ultimately resulted in the arrest of 6 subjects and the prosecution of 3 individuals for their role in the criminal scheme.

Source: Singapore

34. Criminals can rapidly expand the (often transnational) magnitude of a money mule network by leveraging digital tools to scale up mule recruitment across borders. Social media and Voice over Internet Protocol (VoIP) applications have also been identified to be preferred mediums in the mule recruitment process. Traditionally, there may be a degree of friction in laundering through mule networks, with time needed for mules to receive and comply with instructions provided by other criminal syndicates. Such time lapses have been significantly reduced through instant messaging platforms usage by CEF syndicates.

35. Increasingly, criminals may steal identities through various techniques and technological tools, including phishing, purchasing, or deceiving someone to voluntarily hand over their identity. At times, they may use falsified identities and synthetic identities, which involve the combination of real and fake identity information to fraudulently create accounts. Criminals then directly set up and control accounts using these stolen or falsified identities. This makes it more difficult to trace ML activities as the account holders may not even be aware of their involvement.

36. One delegation flagged the risks of deepfakes being potentially used for account takeover fraud. With the help of machine learning algorithms, a fraudster might create a deepfake of someone's voice or video, which can then be used to impersonate that person over the phone or in biometric authentication systems. Deepfakes can also be used in combination with social engineering techniques to trick victims into giving up their account credentials. Deepfake technology is still relatively new, meaning the risk of deepfake-based account takeover fraud may be somewhat limited at present. However, it may pose a significant risk in the future if the technology continues to develop and becomes more widely available.

Box 16. Remote identity theft for direct control

In a series of phishing-related fraud, victims were tricked by criminals to install remote access tools onto their computers. In many of the cases, accounts were created with VASPs in the victim's name, without their knowledge. The criminals did this by using data stolen through the remote access tools. The criminals are also suspected to have guided victims through the online verification account opening process, by using the remote access tools to hide the actual interfaces.

Victims were finally tricked to transfer funds into these VASP accounts. The criminals were able to directly use these VASP accounts for subsequent laundering. In total, victims were estimated to have lost over EUR 600 000 through this series.

Source: Austria

3. Other emerging ML vulnerabilities

37. The preventive measures required for FIs, DNFBPs and VASPs under the FATF Standards (Recommendations 9 to 23) provide a foundation to prevent CEF proceeds from entering the financial and other sectors. This section focuses on emerging ML vulnerabilities that could be exploited by CEF syndicates.

3.1. Risks arising from digital financial institutions[16]

38. The evolution of financial payments has resulted in new digital financial institutions, such as payment service providers (PSPs), the issuance of e-money etc. Traditional FIs may have more resources at their disposal, which may result in relatively more robust controls compared to these newer digital financial institutions. This may lead to displacement, where criminals seek to exploit vulnerabilities in these alternative financial providers to launder funds.

39. The payments network can also be fragmented. There can be various nested financial relationships between these institutions, e.g., with various payments institutions transacting with one another or providing accounts to smaller providers, who in turn provide other types of financial services (see also box 17 below). This fragmentation can also intensify the difficulties in tracing transactions across various types of institutions in the "payment chain". This may also pose challenges in ensuring the immediate availability of basic information on the originator and beneficiary of transfers across the payment chain[17].

40. In line with FATF Standards, there should be robust regulatory supervision over newer financial institutions, including proper licensing or registration, and preventing criminals or their associates from controlling these entities. Regulatory authorities should ensure that all transacting institutions have sufficient oversight over their respective perimeter – all institutions have a responsibility to conduct or ensure proper customer due diligence (CDD) and transaction monitoring on the ordering and beneficiary nodes.

[16] This report also acknowledges the ML risks emanating from VAs and VASPs. For more information on regulatory risks and challenges relating to VASPs, please see FATF (March 2023) *Countering Ransomware Financing* as well as (June 2023) *Virtual Assets: Targeted Update on the Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers.*

[17] The FATF is also considering potential revisions to Recommendation 16 (on wire transfers) to take account of the recent and upcoming developments in the architecture of payments systems.

Box 17. PSP sector abuse

Analysis by the French supervisory authorities in the first half of 2021 identified main PSPs used to receive fraudulent wire transfers. These main PSPs were typically found to offer "banking as a service", with some having a branch in France for the sole purpose of offering French IBANs, with a minimal physical presence.

Analysis found that these main PSPs were approximately 200 times more risky than other institutions. Most of these PSPs had poor identity verification and transaction monitoring. Criminals had opened accounts with a misused identity and can check quickly if some of the open accounts are identified as fraudulent by the PSP, by trying first to carry out transactions of small amounts and change the funds destination if necessary. They then transfer fraudulently acquired funds quickly to one or several accounts. Splitting the amounts between several accounts enables criminals to circumvent restrictions imposed by the PSP regarding their services such as cash withdrawal limits or remaining under operations monitoring threshold defined internally by the PSP.

Source: France

3.2. Virtual IBAN abuse[18]

41. Another example of how financial innovation can be exploited for CEF purposes is the use of virtual International Bank Account Numbers (vIBANs). There are various institutions that issue vIBANs to clients, including banks and PSPs. While vIBANs are used in many different legitimate ways, such as facilitating and categorising payments from multiple parties, several jurisdictions have flagged the abuse of vIBANs as a tool used for CEF-related ML.

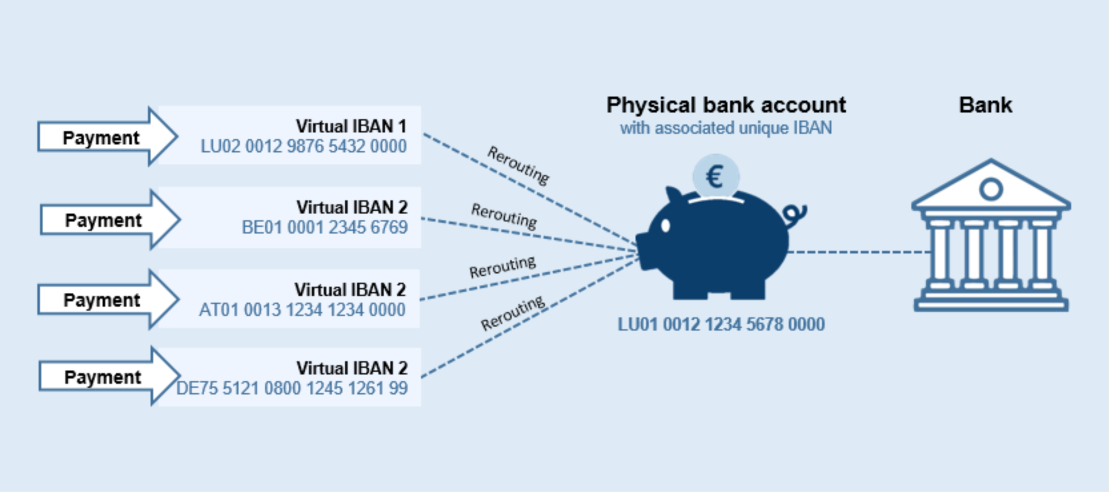
[18] For more information on the risks and challenges associated with vIBANs, see: (June 2023) *Europol Financial Intelligence Public Private Partnership (EFIPPP) Threat Intelligence Information on Virtual IBANs (available only to EFIPPP members).*

Box 18. What is a vIBAN?

vIBANs, are functionally identical to conventional IBANs in that they can be used to send and receive payments on a global scale. They even look the same as their traditional counterpart and are also composed of up to 34 alphanumeric characters. Hence, functionally and visually, they are indistinguishable from regular IBANs.

The key difference between regular and virtual IBANs lies in account matching. A regular IBAN is matched 1:1 with a bank account, meaning that there is only one single physical bank account linked to each individual IBAN number. Therefore, if a person uses an IBAN to make a payment, the funds will automatically end up in the bank account to which the IBAN is linked.

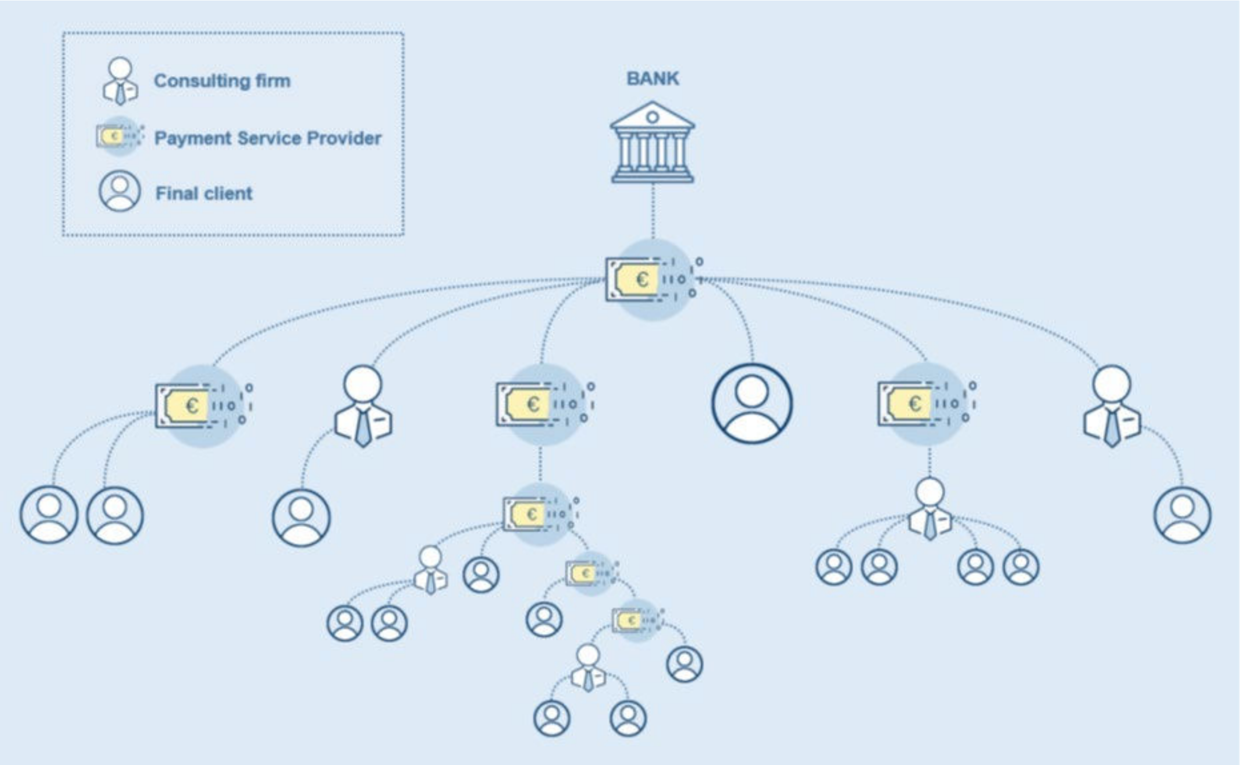
By contrast, a virtual IBAN is a virtual number that is not matched to an account in a physical bank. They are bank-issued reference numbers that enable incoming payments to be rerouted to a physical IBAN, which is itself linked to a physical bank account. They cannot hold any funds, and their balance is constantly zero. vIBAN holders can also have several unique virtual IBANs, which reroute and centralise all payments into a single physical bank account, as seen in Figure 3.



Source: Europol Financial Intelligence Public Private Partnership

42. Since IBANs and vIBANs are optically identical, criminals use them to trick victims into thinking that they are transferring funds into a bank account, when instead for example, it could be a vIBAN used for the purpose of crediting an e-wallet. To further complicate matters, vIBANs can be reissued by a financial institution's client, particularly if the client is another financial institution. This makes it difficult to identify the country of origin for the vIBAN, and the location of the master account.

Figure 2. Cascading net of vIBAN providers issuing and re-issuing vIBANs



Source: Europol Financial Intelligence Public Privâtes Partnership

43. In short, criminals can abuse vIBANs to mask ultimate beneficial ownership information and obscure the movement of illicit monies. This can make it difficult to identify where the true master account is and the issuer financial institution, as well as to ensure proper transaction monitoring. Ultimately, this results in challenges faced by competent authorities to locate the physical accounts and freeze the funds (since vIBANs are merely bank-issued reference numbers and not actual accounts that hold physical balances). As a good practice, some jurisdictions have worked with banks issuing vIBANs to quickly identify the payment institution linked to such master accounts when CEF has been identified.

Box 19. vIBANs abused for CEF

Between February and March 2023, FIU Luxembourg received several reports of so-called "Hi Mum" Scams, where victims received WhatsApp messages from an unknown but local phone number from fraudsters pretending to be their child. The victims received text messages in Luxembourgish via Luxembourg mobile phone numbers, with the inclusion of a Luxembourg IBAN.

During the investigation of this case, FIU Luxembourg discovered that the IBANs provided by the fraudsters were vIBANs. These vIBANs were issued by a Luxembourg banking institution to a Luxembourg based payment service provider who offers prepaid credit cards to European customers. These prepaid credit cards can be loaded by transferring money to the virtual IBANs, which the criminals intended to use for further laundering.

Of the six identified vIBANs used in the scam, FIU Luxembourg was able to block or recall EUR 40 000 out of EUR 55 000 defrauded funds. FIU Luxembourg's action was facilitated by the co-operation between the FIU and the bank issuing the vIBANs, which made it possible to quickly identify the payment institution holding the underlying account of the end customer.

Source: Luxembourg

3.3. Non-traditional sectors

44. Many jurisdictions highlighted the relevance of working with non-traditional sectors, including social media platforms, e-commerce, telecommunication and internet service providers in combating CEF-related ML. While these non-traditional sectors are not regulated for AML/CFT, they possess useful information that can help advance ML investigations, particularly when they are used to perpetrate CEF and recruit mules. Social media platforms, as well as telecommunication and internet service providers, can provide vital digital forensic information, including IP addresses, phone numbers, email addresses etc., which can help identify the ultimate criminal perpetrators. Where fraudulent websites or advertisements are used for CEF, these sectors would also possess financial transaction and payment information linked to the criminals (e.g., payment details for hosting of websites, advertisements).

45. Experience and case studies from jurisdictions have also shown how e-commerce or social media, streaming or gaming platforms can be abused as a conduit to launder CEF-proceeds. The widespread use of social media, streaming or 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 such platforms to launder proceeds of crime.

Box 20. Phishing proceeds laundered through social media and streaming platform

Nineteen bank accounts were discovered to have suffered losses through a phishing attack aimed at customers of certain banks. Analysis by the German FIU revealed that transactions from these bank accounts were conducted through payment accounts owned by two users. These funds were subsequently sent to a social media and streaming platform. The funds were used to recharge user accounts held at the streaming platform with "coins" (serving as a type of native currency among users of the platform) that can be used to purchase virtual gifts. Those gifts can be transferred to content creators who can convert these coins into regular currency and withdraw the equivalent monetary value.

Investigations are ongoing. IP address data showed that the fraudulent transactions were performed via the same login IP addresses. FIU analysis suggests that a common criminal is laundering large parts of the phishing proceeds through the social media and streaming platform in order to subsequently cash out later.

Source: Germany

4. National operational responses and strategies

46. This Chapter first discusses key sources of information that jurisdictions rely on to detect and investigate CEF. It then explores domestic co-ordination and co-operation structures, and how jurisdictions leverage these structures to investigate and prevent CEF and related ML.

4.1. Key sources of detection

47. Based on jurisdictions' experience and case studies, there are two primary sources of information for detecting and investigating CEF-related ML: victim reporting and suspicious transaction reports (STRs).

48. Jurisdictions also have various initiatives to enhance reporting to maximise the full amount of information they can have access to for effective enforcement. Using this information and data, competent authorities leverage digital strategies and tools to analyse and identify criminal clusters for more effective and targeted enforcement.[19]

Victim reporting

49. Victim reporting is an important source of information for detecting and investigating CEF-related illicit proceeds. In certain frauds such as BEC fraud and phishing, victims usually discover relatively quickly that they have been defrauded (e.g., where their legitimate counterparty begins requesting missed payments). In other types of CEF cases, such as investment scams, romance fraud or phishing, the victims may only realise they were defrauded after some time.

50. Timely victim reporting is important to enable competent authorities to act quickly to trace illicit proceeds and may increase the likelihood of successful enforcement outcomes. Victims may report suspected crimes to law enforcement agencies, including dedicated units that handle fraud reports. Victims may also notify their financial institutions, payments providers and VASPs, of suspected fraudulent transactions in their accounts. Other jurisdictions noted that victims may also approach financial consumer protection bodies instead of law enforcement.

51. However, CEF is likely under-reported by victims, especially where they had only suffered negligible loss. Coupled with emotional factors, including embarrassment or fear, victims may decide against coming forward.

52. As a good practice to increase victim reporting, some jurisdictions have created dedicated platforms for victims to report CEF, including online portals. The platforms can provide a structured reporting format to standardise data capturing, which facilitates cluster analysis of victim reports and can help identify criminal trends and patterns. The platforms can also include useful resources for CEF prevention and victim assistance.

[19] For more information on how FIUs and LEAs can leverage digital transformation for effective AML/CFT analysis and investigative capabilities, see Confidential Reports on Digital Transformation of AML/CFT for Operational Authorities: Egmont Group-FATF (October 2021) *Detection of Suspicious Activities and Analysis of Financial Intelligence (Phase 1);* and FATF (May 2022) *Law Enforcement Authorities and Information Exchange (Phase 2).*

Box 21. United Kingdom Action Fraud

The Action Fraud is the United Kingdom's national report centre for fraud and cybercrime. It provides a central point of contact for fraud and financially motivated internet crime and is run by the City of London Police, alongside with the National Fraud Intelligence Bureau (NFIB). The Action Fraud website provides various public outreach resources for crime prevention as well as victim protection and support.

The Action Fraud also runs an online 24/7 live reporting portal for victims. Action Fraud reports are passed to the NFIB, who assesses and analyses across different parts of the country to identify the ultimate perpetrators. These reports are then sent to the appropriate local police forces within the United Kingdom for investigations. The NFIB also uses these reports to take down bank accounts, websites and phone numbers used by fraudsters.

Source: United Kingdom

Suspicious Transaction Reports

53. Given the possibility of victim under-reporting, STRs are a vital independent source of detection for CEF-related financial flows.

54. Based on data gathered from FIUs, most CEF-related STRs were filed by the banking sector. Nevertheless, banks should continue to strengthen their capabilities to detect CEF and related ML, as CEF syndicates continuously evolve their modus operandi. The data also revealed that money value transfer services (MVTS) and VASPs submit fewer STRs. The latter could be due to the fact that in some jurisdictions, the VASP sector is not fully regulated in line with the FATF Standards.[20]

55. It is important to ensure a timely analysis of CEF-related STRs, given the possible dissipation of the CEF proceeds. Some FIUs deploy a prioritisation system to sift through the high volume of STRs and focus on the higher-risk ones, which includes CEF-related STRs. Others train officers in their FIUs on ML risks related to CEF, enabling them to screen and categorise incoming STRs relating to CEF. All these measures facilitate the timely FIU analysis, allowing law enforcement to follow up swiftly on CEF incidents.

[20] See also FATF (June 2023) *Virtual Assets: Targeted Update on the Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*.

Box 22. Prioritisation and clustering of CEF-related STRs

FIU Chile received more than 1,500 STRs from 2021 to 2022 relating to an online trading platform fraud scheme. To deal with this volume, FIU Chile applied clustering techniques for analysis and certain patterns were discovered across these STRs.

The FIU applied a text mining tool, using key words and known phrases detected. Geographical clusters were subsequently identified, which allowed for a targeted and combined referral to the Public Prosecutor's Office. The clustering allowed investigations to discover that the funds were later withdrawn through ATMs, then passed to a person of a higher hierarchy level in the organised crime group.

Source: Chile

56. Beyond detection, jurisdictions have also sought to raise awareness and improve further reporting. Many jurisdictions have issued some form of CEF-related guidelines or organised educational seminars for personnel of banks and other sectors to promote industry-wide awareness of the latest CEF trends and ML typologies. Please also see Annex A for a compilation of risk indicators that may help enhance detection of CEF. Other jurisdictions' FIUs have developed strategic analysis papers on CEF. These initiatives aim to enhance detection and prevention of CEF crime and ML activities by frontline bank staff, etc.

Box 23. Strategic analysis on CEF-related mules

A strategic analysis by the Spanish FIU focused on understanding a discovered money mule profile: bank accounts opened by a single individual at three or more financial institutions within 20 days. Drawing on information between December 2020 and February 2022 from the Bank Account Registry (BAR), the study found nearly 40 000 other bank accounts linked to about 10 000 individuals. 15% of the identified bank accounts had hits in the Spanish FIU databases. These accounts were classified as high risk, and a pilot study was launched in collaboration with four financial institutions to strengthen risk profile understanding based on these accounts.

The pilot aimed to prevent CEF and other possible fraud as well as to improve co-operation with the private sector. The pilot also aimed to strengthen financial institutions' ability to detect gaps in their systems, and to obtain further information on CEF to detect and prevent further criminality. Ultimately, the pilot also resulted in the implementation of a cross-checking system leveraging the BAR to proactively detect CEF-related ML networks.

Source: Spain

4.2. Domestic co-ordination and collaboration

Co-ordination amongst competent authorities

57. Given the cross-cutting nature of CEF, there is a clear need for strong domestic co-ordination across agencies. Some jurisdictions have approached co-ordination through a whole-of-government strategic approach that guides a jurisdiction's CEF-related policies. This involves an overarching cross-functional body, comprised of key ministries across judicial, enforcement, regulatory and info-communications sectors. The co-ordinated approach allows jurisdictions to identify key vulnerabilities and devise holistic policy responses across the key sectors.

58. Domestic operation co-ordination can also involve technical agencies to boost detection and investigation. This includes:

- Developing communication channels among FIUs, police, and prosecutors to ensure centralised reporting, streamlined information and evidence exchange, as well as instructions to freeze and seize assets. This may also include the use of automated data triage to assist in identifying possible matters of interest and quickly identify an appropriate LEA for investigation. Such co-ordination also mitigates duplicity of law enforcement efforts as CEF criminals can target victims across various parts of a jurisdiction (see section on Proper delineation of responsibility below).

- Leveraging technical cybercrime experts, particularly relating to network intrusions and other technical infrastructure crimes as well as privacy protection agencies. This reflects the multi-faceted nature of CEF, and the relevance of digital forensic evidence (such as IP addresses, identifiers linked to internet domains etc.) in identifying CEF syndicates and furthering ML investigations.

Box 24. Joint Policing Cybercrime Co-ordination Centre

The Australian Federal Police (AFP) lead the Joint Policing Cybercrime Co-ordination Centre (JPC3). Membership of the JPC3 includes federal and state law enforcement, government analysts including AUSTRAC, and industry partners, such as analysts from Australian banks. The JPC3:

- Coordinates Australia's policing response to high harm high volume cybercrime to maximise impact on the criminal environment;

- Enhances intelligence sharing and target development across Commonwealth, State and Territory police and Industry;

- Coordinates joint taskforces with police and industry partners to counter priority cybercrime threats;

- Provides national coordination of capability uplift via cross skilling, joint training and collaborative tool development; and

- Communicates nationally consistent prevention, awareness raising and media activities to industry and the public.

The JPC3 has a prevention capability that works with industry and the public domain on combatting cybercrime. To effectively support the JPC3, AUSTRAC also has a financial cybercrime team, which specifically focus on providing financial intelligence regarding cyber-enabled and cyber-dependent crime with a financial nexus, which includes ML of cyber-enabled fraud.

In January 2020, the AFP established Operation DOLOS which, is an AFP-led, multi-agency taskforce[1] which counters transnational cybercriminals conducting or facilitating BEC. Operation DOLOS works with individual Australians and small to medium businesses that have been targeted by BEC and disrupts the flow of proceeds to and from BEC syndicates. Since the commencement of Operation DOLOS, the taskforce developed new techniques leading to reduced harm to Australians and enterprises. Between 1 July 2022 and 30 June 2023, Operation DOLOS has prevented more than AUD30.6million from being lost from Australian and international victims by disrupting the financial operating model used by criminals.

Source: Australia

[1] The taskforce includes various state and territory police, intelligence and cyber-security agencies, the FIU, as well as the financial sector.

Operational partnerships with the private sector

59. Jurisdictions have also sought to collaborate with the private sector through public-private partnerships (PPPs). These PPPs can help improve detection efforts, identify hidden ML networks through tactical information exchange, and enhance operational asset recovery response.

Box 25. Project: Rapid Actions to Prevent Scams

FIU Sri Lanka has launched a project, called Rapid Actions to Prevent Scams (RAPS), to act immediately once a victim reports potential CEF. The objective is to disrupt scams in the Sri Lankan financial system, including CEF, by bringing together the FIU and compliance officers of the FIs to rapidly detect illicit account activities used by criminals and their accomplices.

The mechanism involves identifying the credentials of the scammers based on the public complaints received, and the credentials of such fraudsters are shared with the compliance officers of the FIs. Based on this information, the FIs monitor the account activities of potential fraudsters and take appropriate actions to disrupt the use of the financial system to prevent any fraud. Additionally, the fraudsters' information is shared with Sri Lanka Police to conduct investigations on the subjects.

Source: Sri Lanka

60. In view of the noticeable increase of CEF as well as the associated ML risk, many jurisdictions have established centralised response centres in LEAs or regulators to step up actions against CEF and enhance public awareness (see also section on dedicated anti-CEF units below). As a good practice, representatives of FIs and VASPs could be co-located within such centralised response centres, providing near-real time access of financial data and tracing across various financial entities and sectors, and accelerate competent authorities' ability to intercept and freeze funds.

Box 26. Co-location of bank officers

Saudi Arabia established a Joint Operations Room (JOR) for banks. The JOR is tasked with following up and monitoring cases of financial fraud that bank customers may be exposed to. The JOR brings together all banks and related financial institutions under one umbrella to tackle confirmed cases of financial fraud.

The JOR is hosted by banks in Saudi Arabia to facilitate join efforts for the stability of the banking sector. The JOR operates 24/7 and aims to provide quick and effective co-operation and integration between all Saudi banks to limit the development of fraud cases, as well as to provide a swift response to fraud complaints and where possible to take immediate actions to avoid fraudulent acts.

Source: Saudi Arabia

61. These partnerships also provide a useful platform to exchange best practices, and common typologies and co-develop recommended measures to disrupt illicit activity.

Box 27. Europol Financial Intelligence Public Private Partnership

The Europol Financial Intelligence Public Private Partnership (EFIPPP) is the first transnational information sharing public-private mechanism for AML/CFT. EFIPPP brings together law enforcement, FIUs and private entities across various EU and non-EU countries.

The Threats and Typologies Working Group within EFIPPP has dedicated work streams on various topics on/related to CEF and their different modus operandi, including BEC, investment fraud, mule accounts, virtual IBANs and crypto assets. Although the aim of EFIPPP is to create strategic typology reports, it also provides a platform to discuss the facilitation of operational co-operation between its members.

Source: Europol

62. Composition of the PPPs can vary. Many jurisdictions remain focused on traditional stakeholders (particularly banks and other financial institutions), but there is an increasing involvement of DNFBPs, VASPs and other non-traditional sectors (e.g., telecommunications business operators, and internet service providers). The specific composition will depend on the aims and objectives of the PPP.

Box 28. Co-operation with telecommunications sector

In recent years, China has continued to promote the strengthening of combating and managing telecommunications network fraud, and on December 1, 2022, officially implemented the "Anti-Telecommunication Network Fraud Law of the People's Republic of China", which has provided strong rule of law safeguards to combat and curb criminal activities of telecommunications network fraud, and related criminal acts have been effectively curbed.

The law brings together public sector authorities (including law enforcement, financial, telecommunications and Internet information agencies), as well as FIs (banks and non-bank payment service providers), telecommunications business operators and Internet Service Providers to establish an early warning and dissuasion system. This system identifies potential victims by providing an early warning, allowing appropriate and timely dissuasive measures to be taken.

FIs can also use this system when opening bank accounts, payment accounts, and provide payment and settlement services. The system is used to enhance customer due diligence processes and allows the FIs to take risk mitigation measures to prevent bank and payment accounts etc. to be used for fraudulent activities.

Source: China

4.3. Useful domestic enforcement strategies

63. This section explores some good practices and useful enforcement strategies that have been employed by jurisdictions. In general, these strategies leverage the sources of information discussed in section 4.1 above, to identify, investigate and prevent CEF and related ML more effectively.

64. These useful enforcement strategies typically involve multiple agencies and private sector entities. This means that strong domestic co-ordination and co-operation is typically required to implement these strategies (as discussed in section 4.2 above).

Proper delineation of responsibility

65. Many jurisdictions have reported an increase in the quantum of losses and the volume of CEF cases in the past few years. While some individual cases may involve small losses, the volume of such scams means that the total proceeds of crime accumulated by each syndicate is potentially large.

66. Several jurisdictions indicated that the large volume of CEF reports makes delineation of investigative responsibility a necessity. As a good practice, jurisdictions with various anti-fraud or cybercrime agencies with oversight over CEF cases have sought to identify the competent authority or authorities to handle them. Other jurisdictions introduced legislation to consolidate complex investigations involving multiple victims of the same syndicate, such that a single competent authority has oversight over the entire investigation. These initiatives prevent duplication of efforts by different competent authorities and prevent cases from "falling through the cracks", as well as to address the transnational nature of the crime.

Box 29. Using technology to delineate investigative responsibility

The Hong Kong Police Force (HKPF) established the e-Crime Processing and Analysis Hub (e-Hub) in September 2022 with the aim of enhancing the efficacy in handling technology crime and deception-related reports. The e-Hub uses enhanced computer system to perform correlation analysis against common types of cyber-enabled fraud cases and identifies case clusters.

In 2022, the number of deception cases increased by 45.1% to 27 923 cases, accounting for almost 40% of the overall number of crimes. Nearly 80% of the deception cases were CEF related. More people are reporting CEF online and most of the e-reported cases are correlated, such as from the same criminal group. The correlated cases are assigned to one single investigation team for consolidated investigation so that resources could be better coordinated.

By using clustering algorithms, e-HUB can identify patterns and similarities in the data that might not be immediately apparent to gain a deeper understanding of the scope and nature of cases. This includes common types of criminal digital tools and money mules accounts used, and how CEF is planned, executed, and concealed.

Source: Hong Kong China

Dedicated anti-CEF and related ML units

67. With a view to strengthening the AML/CFT capabilities in the face of the evolving criminal landscape, many jurisdictions set up a specific unit or taskforce to investigate CEF and related ML. These jurisdictions allocated extra resources to strengthen capabilities in financial investigation, intelligence gathering, and training for LEAs and capacity building for the private sector. These centralised units consolidate anti-CEF expertise across law enforcement and make them better able to disrupt CEF operations, trace laundered funds and recover related proceeds.

68. Jurisdictions have shared that the benefits to such an outfit are multi-fold. The consolidation of all CEF cases by a single enforcement unit enables better analysis, deployment of data analytics and network link analysis to identify syndicates. It can further serve as a singular point of contact for private sector stakeholders and foreign counterparts, and helps develop strategic relationships in the longer run.

This enhances law enforcement's intervention efforts, such as the disruption of phone lines, the removal of suspicious online monikers and advertisements, and improve asset recovery outcomes.

Box 30. National Scam Response Centre

Malaysia's National Scam Response Centre (NSRC) is a multi-faceted response that brings together a diverse range of resources and expertise from the National Anti-Financial Crime Centre, Royal Malaysia Police (RMP), the Central Bank and other public and private sector entities.

The NSRC serves as a hub for fraud information received from various sources and leverages network analysis to identify mule and laundering networks. Private sector entities, including financial institutions, will trace the funds from one layer to another layer and subsequently withhold the mule accounts. The RMP will further investigate the case and take enforcement action such as issuing freezing order to the accounts.

Source: Malaysia

Enhancing access to financial information

69. Due to the voluminous and instantaneous effect of CEF cases, timely access to financial and banking information is crucial in accelerating the investigation and tracing of CEF proceeds. Some jurisdictions have employed 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. These good practices usually rely on the creation of a centralised platform that brings together multiple stakeholders for faster information exchange.

- **Technology-enabled information retrieval:** To enable financial institutions to expeditiously provide relevant information to law enforcement, it can be useful for competent authorities within a jurisdiction to agree on data fields that would be relevant for their investigations. Issuing varied requests that each requires a customised response from the relevant financial institution can be time-consuming for the private sector to process. As a good practice, law enforcement in some jurisdictions have developed a standardised template comprising pre-agreed data fields that they require from financial institutions. The requests can then be aggregated, sent to financial institutions in batches and be in machine-readable form. Financial institutions may also provide responses to lawful requests digitally to law enforcement, enabling more efficient analysis of data.

Box 31. Leveraging robotic process automation to speed up access to financial records held by financial institutions

Timely access to banking and financial information is critical for effective interception and asset recovery. Singapore is leveraging robotic process automation (RPA) to obtain banking information at a fraction of the time it previously took. Orders are now served electronically on banks via a standardised template. Banks automate the financial information retrieval process and then send it back to LEAs electronically. The electronic data can also be used immediately for LEA analysis.

The process has improved turnaround time by up to 97%, leading to more efficient investigations. Information is now provided in a digital format, which is ready for analyses. As for the banks, this initiative has resulted in significant cost savings by eliminating manual workflows. Similarly, it has enabled data mining for the banks through its automated processes, which can be used to further detect hidden ML networks.

Source: Singapore

- **Facilitating asset tracing across FIs**: Pass-through transactions and account hopping across multiple FIs increases law enforcement tracing efforts as time is required to gather information from the respective FIs; to peel through layers of transactions and to identify the origin and ultimate destination of funds. This can be challenging, given the speed of transactions. Good practices include developing platforms to facilitate rapid tracing and information exchange across different FIs to intercept illicit proceeds.

Box 32. Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)

The CFCFRMS is an online system developed by the Indian Cyber Crime Coordination Centre for quick reporting of financial cyber frauds and preventing the flow of fraud proceeds across the financial sectors. The system has integrated LEAs across the country and Financial Entities (i.e., Bank, wallets, Payment Aggregators, Payment Gateways, E-commerce platforms etc.) together to work in tandem and take immediate action on the complaints reported on CFCFRMS. At present all State and Union Territory LEAs and 243 Financial Entities are on boarded on the module.

Once a victim reports a fraud to the LEA, details of the beneficiary of the fraudulent transaction is recorded and submitted to the CFCFRMS system in a form of a ticket. This ticket is escalated to the concerned Financial Entity (bank, payment wallet etc.), which will see the ticket on its system's dashboard. The Entity will check if the defrauded monies are still in the account and puts it on hold. If the monies have been dissipated to another Entity, the ticket is escalated to that next Entity-layer. The process is repeated until the money is intercepted. If the money is withdrawn, the details of withdrawal are filled by FIs for further action of LEAs.

The system has been highly effective in preventing fraudulent transactions from going into the hands of fraudsters. Since its inception in April 2021, the system has been able to intercept more than INR 6.02 billion (about EUR 66.1 million).

Source: India

- **Leveraging central registers** Central bank registers allow law enforcement agencies quick access to basic bank information and help speed up CEF investigations. The information allows law enforcement agencies to verify the banks in which the suspect holds accounts, or the identity of the account holder. This helps to streamline the information retrieval process by allowing law enforcement agencies to scope their investigations early and focus only on the financial institutions in which the suspect maintains accounts.

Box 33. Identifying hidden mule accounts

In Malta, a STR was filed against a suspected money mule after a series of suspicious transactions to different beneficiaries. Funds were being transferred to various local and international banks linked to a suspected romance fraud.

Searches through the national Central Bank Account Registry allowed the FIU to immediately identify another active account owned by the suspected mule at a different bank. The FIU was able to quickly establish a holistic picture and scope additional financial analysis required. This ultimately helped the FIU to quickly identify commonalities of further laundering to other foreign individuals.

Source: Malta

- **Developing databases for private-private information sharing:** In cases of professional ML networks, many mule accounts may be known or suspected as part of previous scams (e.g., romance, lottery and employment) or identity takeover activities. There are also similar overlaps in the data and processes used to identify fraud and those for identifying mule networks. As a good practice, some jurisdictions have sought to centralise data that cuts across anti-fraud and AML databases to identify deeper ML networks across various FIs in order to prevent fraud and foster asset recovery.

Box 34. Centralised private-private database

Brazil has recently approved a Resolution making mandatory a database that centralises information regarding fraud (including attempts) by all financial and payment institutions. This database is enforced by the Banco Central do Brasil (BCB) and is forecasted to start operating in November 2023.

The Resolution institutes that sharing information about frauds (including attempts) are compulsory for institutions and defines minimum information that must be shared. This includes identification of the persons involved in the commitment of fraud (including money mules), the financial institution(s) involved, and the account(s) used. The system aims to facilitate information sharing between private sector, with the objective to prevent and combat fraud, as well as recover illicit fraud proceeds.

Source: Brazil

Deterring money mules

70. As discussed earlier, money mules serve an important role in CEF-related ML networks. Mules are recruited through a myriad of techniques. Depending on how they are recruited and whether they have been unwittingly tricked or exploited, they can have varying levels of knowledge of and involvement in the underlying CEF scheme (see section 2.3 above).

71. Consequently, competent authorities may experience challenges in bringing ML charges. It can be difficult to develop sufficient evidence to prove the mule's criminal intent for ML (i.e., level of awareness in their participation in the laundering process). To address this problem, some jurisdictions have introduced legislation to lower the *mens rea* required in the ML offence, such as from "knowledge" to "suspicion".

Box 35. Article 9(3) of the Council of Europe Warsaw Convention

One of the underlying issues in effective prosecution of ML offence is a need to prove *mens rea* – i.e., that the money launderer knew that the proceeds he/she dealt with were proceeds of crime. In complex ML cases where professional money launderers are involved, a defendant commonly denies that they had a firm knowledge that the funds he/she dealt with, were proceeds of crime. Consequently, demonstrating that the "mental element" of the defendant has reached the relevant threshold is one of the most challenging tasks in proving the ML offence.

Mindful of difficulties in proving *mens rea*, the drafters of the Warsaw Convention introduced new elements in its Article 9, where the ML offence is set out. Apart from the elements already embedded in Vienna and Palermo Conventions, Article 9 of the Warsaw Convention, in its paragraph 3, goes a step further establishing that the ML offence occurs even when the offender only suspected or ought to have assumed that the proceeds were generated by crime.

Source: MONEYVAL

72. Other jurisdictions have approached the challenge presented by money mules generally through public education and outreach to potential mules. Global campaigns on social media, such as the #*DontbeaMule* supported by Europol and INTERPOL's #YourAccountYourCrime, can serve as useful platforms to co-ordinate international awareness against money mule activities, especially when funds can be easily laundered by mules across borders. Collaboration with the private sector can maximise the effect and results of such outreach efforts. Authorities may also leverage existing detection mechanisms (STRs and victim reports) to identify potential money mules that may have handled CEF-proceeds. Targeted outreach and warnings can advise such potential mules to refrain from repeating such behaviour in the future. Records of past outreach or warnings can be leveraged as useful evidence in determining criminal ML intent in the event of recidivism.

4.4. Prevention and disruption

73. Given how fast funds are dissipated, many jurisdictions have worked to explore initiatives to prevent CEF and related ML from happening. Such an approach reduces the overall profitability of CEF syndicates and significantly mitigates downstream resource dedication, from investigation to victim management.

Public education and outreach

74. A preventive approach can be adopted by educating the public and increasing vigilance against exploitation, including national awareness campaigns advocating for cyber literacy. To support this objective, some jurisdictions have leveraged technology to roll out information campaigns for citizens to help them detect fraudulent operations, raise awareness of tell-tale signs and encourage victim reporting.

Box 36. Leveraging technology for public education on CEF

The Hong Kong Police Force ("HKPF") launched the one-stop scam and pitfall search engine, namely "Scameter" in September 2022. The application aims to help the public identify frauds and online pitfalls.

When the public encounters suspicious calls and online sellers, unsolicited friend requests, arbitrary recruitment messages, suspected fraudulent investment websites, and the like, they can enter on Scameter the account name or number, payment account number, phone number, email address, URL, etc. of suspected fraudsters to assess the risk of fraud and cyber security.

The data and rating of the Scameter come from various reliable sources, including public reports to the police, information provided by organisations, suspicious phone number database, as well as the database and real-time analysis from information security companies.

Source: Hong Kong China

Anti-fraud security and controls for AML/CFT outcomes

75. Experiences from the public and private sectors begin to show that anti-fraud and AML processes are complementary. This includes leveraging technology to help users automatically reject the reception of fraudulent messages, working with private sector for horizon scanning to proactively mitigate emerging fraud trends, creating account security features, controls and rules, as well as warning messages in anti-virus software for potential phishing sites (see Annex B which compiles good examples of how financial regulators have adopted anti-fraud requirements alongside AML/CFT controls).

76. Another good practice is encouraging FIs to adopt real-time transaction monitoring to identify and prevent fraudulent or illicit 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.

77. Real-time transaction monitoring, which involves the use of sophisticated software and algorithms to monitor financial transactions, is considered useful for detecting and preventing CEF. Given the overflow of information caused by digitalisation, CEF might be difficult to detect through manual processes. Real-time transaction monitoring can help FIs identify and investigate patterns of suspicious activity across multiple accounts or transactions, even if those accounts or transactions are not directly linked, preventing future criminality.[21]

Removing criminal instrumentalities

78. As CEF can also be perpetrated through non-traditional sectors (see section 3.3. above), some jurisdictions have strengthened anti-fraud prevention and controls in such non-traditional sectors. This includes targeting the instrumentalities of CEF

[21] For more information on how technology can be used for AML/CFT, please also see FATF (July 2021) *Opportunities and Challenges of New Technologies for AML/CFT*

such as shutting down the mobile lines and fraudulent webpages used by criminals, filtering of phishing messages and malicious weblinks, etc.

Box 37. Removing suspicious websites and phishing campaigns

In Saudi Arabia, law enforcement agencies and regulatory authorities take a collaborative approach with telecommunications providers to significantly enhance its ability to predict, prevent, detect, and respond to fraudulent events effectively. To combat criminal instrumentalities, the National Cyber Security Authority in Saudi Arabia has imposed stringent brand protection requirements focusing on countering clone websites and phishing messages on social platforms. Additionally, the Saudi Central Bank (SAMA) has established a robust cyber security and counter-fraud frameworks respectively, outlining mandatory baseline control requirements for regulated entities. This framework aims to proactively protect against emerging fraud threats, thus ensuring the stability and safeguarding of the kingdom's financial sector.

A crucial aspect of these national and regulatory requirements is the proactive monitoring of criminal instrumentalities by the organisations. This involves continuous surveillance of potential fraud activities, such as suspicious websites and phishing campaigns through sophisticated technologies and brand protection measures implemented by the organisations. When detected, these activities are promptly reported to the relevant authorities. Timely reporting ensures swift action to investigate and shut down criminal operations, preventing further harm and reducing the impact of fraudulent events.

Source: Saudi Arabia

Preventing asset dissipation

79. Many jurisdictions have found that one of the most challenging aspects of CEF investigations is the rapid speed at which CEF proceeds can be laundered. There is consensus that it is crucial for competent authorities to be able to intervene swiftly to reach the CEF proceeds before they dissipate from the various bank accounts. Jurisdictions have implemented varying measures to more effectively recover assets linked to CEF (see section 5.1 below).

80. There may also be benefits to engage key financial private sector representatives to facilitate and encourage their proactive interception of illicit funds once a notice of fraud is received from a victimised client, before they have been contacted by competent authorities. This includes information exchanges between domestic and foreign FIs or VASPs (see also box 41 below).

Box 38. Egmont Group Bulletin on BEC fraud

In July 2019, the Egmont Group issued a bulletin to alert member FIUs and their jurisdictions of the increasing threat posed by BEC fraud through the sharing of key scenarios and risk indicators linked to BEC. The bulletin further identified how financial institutions (FIs) can play an important role in identifying, preventing and reporting BEC fraud by promoting greater communication and collaboration among their internal AML, business, fraud prevention, and cybersecurity units.

To assist in the investigation of BEC incidents and recovery of victim funds, beneficiary FIs that received information that a fraudulent transfer was executed to one of its customers' accounts (e.g., SWIFT recall message) were advised to not carry out any transactions that could lead to the loss of funds and contact law enforcement or the FIU to assess the validity of the received transaction.

Source: Egmont Group

5. International co-operation and asset recovery

81. As earlier discussed, the jurisdiction where the CEF occurs (i.e., where the victim is generally located) tends to be different from the jurisdiction where the proceeds are laundered. This can lead to challenges in cross-border investigations and effective international co-operation to successfully obtain information and evidence, dismantle CEF syndicates, and recover illicit proceeds. For example, a jurisdiction where CEF-related proceeds have been laundered, may have difficulties identifying every victim associated with a ML account as they can be spread out across multiple jurisdictions.

82. The de-centralised nature of CEF adds further complexity. There may be mismatches in jurisdictions' respective international co-operation priorities, for example, in cases where Jurisdiction A's victims are transferring monies to Jurisdiction B, but Jurisdiction B's victims are in Jurisdiction C (i.e., meaning A may prioritise collaboration with B, but B may prioritise co-operation with C). The need to involve multiple stakeholders and partners, both public and private, abroad also makes it challenging to identify and trace illegal funds.

- CEF syndicates use various financial services and assets classes. Transactions can be made almost instantaneously across borders between different providers and sectors. This makes funds transfers difficult to trace and attribute.

- Relevant digital forensic evidence is also likely to be distributed across different jurisdictions, which makes it difficult to piece together a complete picture of how criminal syndicates operate and launder proceeds. This is further complicated by the volatile characteristics of digital forensic evidence, which can be easily dissipated if not quickly preserved.

83. Formal co-operation, including mutual legal assistance, typically takes a long time. Given the rapid nature of digital crimes and associated ML activities (where evidence could be quickly dissipated if not preserved), relying on formal co-operation may therefore be significantly less effective. To remain nimble in rendering cross-border assistance to successfully curb CEF criminal activity, competent authorities are increasingly relying on informal co-operation mechanisms by sharing information directly with their foreign counterparts. This can occur at a law enforcement or FIU level through various channels, including the Egmont Secure Web, INTERPOL's I-24/7 as well as other informal networks such as the Camden Asset Recovery Inter-Agency Network (CARIN) and regional Asset Recovery Inter-Agency Networks (ARINs).

Box 39. Interception of CEF proceeds through informal multi-lateral networks

To combat the rise in CEF, French investigative authorities actively use informal networks, among which is the European Asset Recovery Offices (AROs) sub-network of the Camden Asset Recovery Inter-agency Network (CARIN) for effective international co-operation and related asset recovery. The French ARO works closely with members of these two networks, which allow information to be exchanged rapidly across multiple jurisdictions between LEA and FIU counterparts specialising in tracing, seizing and confiscating criminal assets, especially in cases of emergencies where requests are answered within 8 hours. Such co-operation enables funds to be quickly preserved in the initially identified destination account, and all other subsequent layered accounts.

In 2022, for example, the French ARO contacted the Slovak ARO involving a fraudulent bank transfer for € 1 875 000 to the detriment of a French victim company and requested that the funds be frozen in the beneficiary bank account in Slovakia. Exchanges between the two ARO offices resulted in the funds being frozen, and allowed the Slovak authorities to obtain all the information required to draw up and execute a judicial freeze request. In the end, the sum of GBP 1 874,907 was frozen and subsequently returned to the victim company.

Source: France

84. To maximise effectiveness in investigating CEF-related ML and recovering proceeds, co-operation should have a multi-lateral focus rather than bi-lateral. This section explores challenges and good practices vis-à-vis international co-operation through two operational outcomes: (i) asset recovery and (ii) enforcement and prosecution.

5.1. Asset recovery

85. A key challenge in CEF asset recovery is the rapid pace of laundering. To mitigate this challenge, there are multi-lateral "rapid response" programmes created by various bodies to trace and recover CEF proceeds, including the INTERPOL's Global Rapid Intervention of Payments (I-GRIP), the Egmont Group's BEC Project and the U.S.' Financial Fraud Kill Chain. Experience from these bodies generally show that intervention is most effective within 24 to 72 hours of a fraudulent transaction. Such good practices mitigate the risk of funds dissipating into multiple subsequent layers, which drastically narrow the scope of ML investigation and facilitate the recovery of illicit proceeds.

Box 40. Financial Fraud Kill Chain and Recovery Asset Team

The Financial Fraud Kill Chain (FFKC) was created by the FBI and Financial Crimes Enforcement Network (U.S. FIU) in 2016 in response to the rise in business e-mail compromise schemes. The FFKC attempts to aid in the recovery of international wire transfers sent pursuant to fraud schemes by leveraging FinCEN's relationships with the Egmont Group of Financial Intelligence Units. This process can only be implemented if the fraudulent wire transfer meets the following criteria: (1) the wire transfer is USD 50 000 or above; (2) the wire transfer is international; (3) a SWIFT recall notice has been initiated; and (4) the wire transfer has occurred within the last 72 hours.

In 2018, the FBI's Internet Crime Complaint Center (IC3) established the Recovery Asset Team (RAT) in order to address vulnerabilities in domestic wire transfers. The RAT streamlines communication with financial institutions and assists FBI field offices with the freezing of funds for domestic transfers made under fraudulent pretences. The RAT has experienced a number of notable successes, freezing 73% of funds reported to be fraudulent to the IC3 (USD 433.3 million of USD 590.62 million) to-date. According to a U.S. case example, this program can in some instances quickly identify the second-hop accounts and freeze the funds, making a full recovery possible.

Source: United States

86. Primarily, these multi-lateral programmes aim to do two things: collect the minimum level of information required for law enforcement action and pass that information into the "correct hands". To ensure effective cross-border response, all nodes of the multi-lateral networks also agree on governance rules and procedures. While such multi-lateral networks are usually global in nature, regional initiatives may also be useful to mitigate challenges by building upon already established regional collaboration.

Box 41. Multi-jurisdictional Anti-Fraud Project

Given the cross-border nature of fraud, a regional initiative within the Financial Intelligence Consultative Group (FICG)[1] called the Multi-jurisdictional Anti-Fraud Project was developed. This initiative is co-led by the FIUs of Malaysia, Indonesia and Singapore, and aims to detect, trace and recover funds for the victims.

A response mechanism was built that involves cross-border transactions between FICG member countries. This project will help FICG members share financial intelligence information quickly and easily, thus supporting swift actions by authorities to combat fraud and recover stolen money.

Source: Malaysia

[1] The FICG is a regional body of FIUs from Southeast Asia, New Zealand and Australia.

Cross-border information collection and exchange: "collect minimum level of information"

87. Where CEF is considered a serious crime under domestic law it is required to be criminalised as a predicate offence for ML under FATF Recommendation 3. In addition, unlike traditional forms of fraud committed between acquaintances where it is difficult to distinguish fraud from potential civil debtor-creditor disputes, it is relatively easier to establish prima facie criminality in CEF cases, where the fraud is typically between non-acquaintances. This mitigates the need for a lengthy request for assistance to articulate and define the criminal nexus, as is typically required for other types of crimes (that are not universally recognised as a predicate offence).

88. As a good practice, the various rapid response programmes use templates to accelerate the collection and exchange of information. Templates allow the quick collection of a minimum level of information required to establish criminality. It helps focus ground response units' efforts on the vital types of evidence or information to secure at the initial stages of a criminal complaint. Such templates also mitigate challenges in the quality of information exchanged, and improve cross-border law enforcement response.

89. In addition to a summary to describe the CEF crime, templates generally seek to secure basic data necessary to advance funds tracing efforts. The standardisation of requests allows requested jurisdictions to quickly process any incoming requests, accelerating law enforcement ability to intercept illicit funds that have entered their jurisdiction.

90. Data fields in templates may include originator and beneficiary account information and transaction information (date, time, amounts transferred). To further enhance effectiveness, templates could also include information on the next destination of funds if the funds have already been transferred out of the beneficiary account. It may also be useful to minimise any restrictions on jurisdictions to disseminate any information being exchanged with relevant competent authorities domestically on receipt.

Box 42. INTERPOL I-GRIP

INTERPOL developed INTERPOL Global Rapid Intervention of Payments (I-GRIP), which is a global stop-payment mechanism to enable member countries to submit and handle requests to follow, intercept or provisionally freeze the illegal proceeds of CEF. Known as the I-GRIP, the mechanism was originally piloted as the Anti-Money Laundering Rapid Response Protocol (ARRP) in 2022 and officially launched in November 2022 thanks to many stop-payment success cases during the pilot phase.

I-GRIP facilitates rapid communication between INTERPOL National Central Bureaus (NCBs) to prevent suspected illicit assets from being transferred between member countries. Requests submitted via I-GRIP should include sufficient details upon which the receiving NCB can act, such as – Date of transaction, currency and amount, account numbers and financial institution names of the beneficiary and remitter accounts.

Source: INTERPOL

91. In addition, standardised data fields in templates allow international organisations with centralised capabilities to easily analyse the data and maximise investigative and asset recovery efforts. For example, INTERPOL leverages information exchanged through its channels to create an internal database, the Financial Criminal Analytical File (FINCAF), to facilitate analysis of intelligence with a transnational dimension on various forms of financial crimes and to identify links between the cross-border cases and investigations, threats, crime trends and criminal networks (see also box 45 below).

92. To further accelerate asset recovery actions, some jurisdictions have enabled foreign victims to file a CEF complaint directly with their LEAs, including through their online reporting platform to directly capture requisite data fields for enforcement action (see section on Victim Reporting above). This eliminates an additional layer of communication and allows competent authorities to swiftly take any available measures against suspicious transactions made to beneficiary accounts in their jurisdictions.

Necessary powers to act: “the Correct Hands”

93. As speed is of the essence, any information collected should ideally be directly handed to authorities that are already equipped with the proper power and expertise for asset tracing and recovery. This allows provisional measures to be immediately taken upon receipt of a request to prevent further laundering or dissipation of assets. This provides law enforcement with the vital time needed to continue their investigations, develop and gather evidence and follow up with formal MLA requests.

Box 43. Request of postponement from obliged entity

FIU Italy received a request of postponement from an obliged entity about four suspicious wire transfers amounting to EUR 490 000. The transactions were being ordered by an Italian clothing wholesale trade company in favour of various firms in a far eastern Asian country.

The obliged entity had deemed the four transactions suspicious as the funds originated from incoming transfers that were being recalled by the ordering bank on the basis that the funds were sent due to a "CEO fraud" from a western European victim company. FIU Italy had also received a spontaneous international information exchange from the said western European country's FIU. The Italian company was further reported to the FIU for possible connection to VAT fraud schemes involving the said Asian country through a separate eastern European country, which provided further indication of links between CEF and other types of organised crime.

The transactions were successfully postponed. This allowed for the foreign authorities to issue a foreign order of seizure to recover the funds in Italy.

Source: Italy

94. However, such direct interfacing may encounter challenges due to the differences in legislative and enforcement frameworks across jurisdictions. Some good practices to mitigate these challenges include establishing domestic co-ordination mechanisms to facilitate requests transmission to the correct authorities, as well as leveraging public-private collaboration channels and FIs' ability to voluntarily take provisional measures once they are informed of suspicious transactions by competent authorities.

Governance & Rules: "the Collective Agreement"

95. Governance and rules for multi-lateral frameworks provides assurances and commitment to mutually recognise criminal activity and act quickly on receipt of information. This helps to overcome the challenge where there may be a mismatch of priorities amongst international agencies, as the conditions to accede and render assistance have been agreed in advance. As a good practice, these rules and criteria should be clear and easily understood.

96. The above principles apply to informal but also to formal international co-operation mechanisms. As a good example, Regulation (EU) 2018/1805 of the European Parliament and of the Council, allows the mutual recognition of foreign freezing and confiscation orders. This mechanism for direct enforcement allows swift cross-border intervention.

97. Accelerated information sharing should not be at the expense of data protection and confidentiality. To ensure the security of information transmitted, multi-lateral frameworks usually leverage on existing secure channels of communication, such as those provided by INTERPOL, Europol and the Egmont Group. These existing

secure communication channels also allow these multi-lateral frameworks to expand easily, as it circumvents the need to develop bilateral communication channels.

Box 44. The Egmont BEC Project Team

To address the increasing and serious threat posed by BEC to financial institutions and their customers, 11 FIUs launched the "Egmont BEC Project Team", which focused on analysing BEC trends, indicators, and methodologies, as well as to share key findings with FIUs. Common BEC financial typologies and case studies show that a prompt reaction to stop and follow the wire transfers is the most effective way to tackle this type of crime.

As such, the Project Team[1] establish protocols between law enforcement and FIUs, and between international FIUs to follow and freeze BEC proceeds.

- On receipt of an STR relating to suspected cross-border BEC flows, the originator FIU develops a "rapid response" request to the destination FIU.
- The request should contain agreed upon basic data and information needed to be exchanged for enforcement action.
- The destination FIU is requested to take (where possible) immediate action to suspend and recover the illicit proceeds, ideally within 72 hours after the crime has occurred.

The BEC Project leverages on the Egmont Group's secured platform for communications to exchange the "rapid response" requests.

Source: The Egmont Group

[1] The Project team members currently consist of: AUSTRAC (Australia), BFIU (Bangladesh), CTIF-CFI (Belgium), TRACFIN (France), GHFIU (Ghana), HFIU (Hungary), IMPA (Israel), SIC (Lebanon), FIU Luxembourg, UPWBNM (Malaysia), FinCEN (USA), and Europol.

5.2. Enforcement and prosecution

98. Beyond asset recovery, the transnational nature of CEF has also resulted in difficulties throughout the enforcement process, from gathering intelligence and investigation, to the collection of evidence for prosecution. The evolution of technology has increased the speed of transactions and facilitated fragmented operations across borders. It has also increased the time and effort necessary for law enforcement to trace and identify them.

Digital evidence collection

99. While not exclusively related to ML, digital forensic evidence can provide critical clues to direct law enforcement to further their ML investigations. The widespread

availability and ease of use of identity-concealment services, such as VPN, further complicates efforts to locate the ultimate perpetrators of CEF.

100. Unfortunately, there is currently no single global regime that governs the duration of digital data retention, including relating to technical service providers. Several jurisdictions highlighted the significant risk of digital evidence dissipation. Delays in formal co-operation mechanisms would also pose a challenge in swiftly securing digital evidence.

101. There are several good practices that can mitigate these challenges.

- **Leveraging informal channels** to first gather and secure intelligence. Formal co-operation channels are thereafter used to obtain the necessary evidence and statements for preparation of judicial proceedings.
- **Conventions and investigative tools** such as the Convention on Cybercrime, also known as the Budapest Convention, allows for expeditious preservation of electronic data and transmission of spontaneous information, which helps accelerate identification of the ultimate CEF perpetrators. The Budapest Convention also establishes a 24/7 network that ensure immediate investigative assistance for the provision of technical advice, collection of evidence, preservation of data etc.
- **Direct co-operation** with foreign service providers to obtain the necessary forensic evidence such as subscriber information without going through the MLA process. According to one jurisdiction, direct voluntary co-operation from a foreign service provider is the most effective mechanism to gather relevant digital evidence.[22]

[22] See also Council of Europe (July 2020) *The Budapest Convention on Cybercrime: benefits and impact in practice* for more information on voluntary co-operation with foreign service providers.

Box 45. The Budapest Convention

The Budapest Convention sets out procedural powers for: expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data. The Convention also provides a fast and effective regime of international co-operation.

Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence also provides a legal basis for disclosure of domain name registration information and for direct co-operation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection safeguards.

Source: Council of Europe

Joint Enforcement Action

102. Cross-border Joint Investigation Teams (JITs) involve a legal agreement between competent authorities of two or more jurisdictions for the purpose of carrying out criminal investigations. These may facilitate information sharing and cross-border financial tracing. Information sharing is typically leveraged through various frameworks and agreements (e.g., Eurojust, Joint Cybercrime Action Taskforce supported by Europol).

103. JITs also provide an important point of co-ordination for multi-lateral enforcement action against CEF, given its transnational and de-centralised operations. With the lowered barriers of criminal operations, CEF syndicates can easily relocate and set up new digital centres of operations remotely. Hence, co-ordination action is necessary to simultaneously uproot the various sub-groups (that can be working across multiple jurisdictions).

Box 46. Joint action against large-scale investment fraud[1]

Serbia, together with Austria, Bulgaria and Germany and with the support of Eurojust – participated in successful operations against two organised crime groups suspected of large-scale investment fraud in cyber-trading. The Serbian authorities arrested five suspects and searched nine locations, seizing five apartments, three cars, a considerable amount of cash, and IT equipment. More than 30 Serbian bank accounts were also put under surveillance. In addition, four suspects were arrested in Bulgaria, while EUR 2.5 million were frozen in the bank account of a company involved in the fraud scheme in Germany.

Based on the information gathered during the operation, authorities quickly engaged in another operation against a company in Belgrade 2 days later, arresting one suspect and seizing servers, other IT equipment, and documents.

In this case, the Serbian authorities, inter alia, made use of Article 26 Budapest Convention (Spontaneous information) to share information with other partners. Eurojust further assisted the investigations by funding a joint investigation team (JIT), as well as organising both a coordination meeting at its premises in The Hague and a videoconference.

Source: Serbia; Council of Europe (July 2020) The Budapest Convention on Cybercrime: benefits and impact in practice

[1] For more information, see also Eurojust (April 2020) press release, available at: www.eurojust.europa.eu/news/action-against-large-scale-investment-fraud-several-countries

104. That said, there are also challenges associated with joint enforcement action.

- **Legal barriers** may restrict informal information sharing even within joint investigation teams. One jurisdiction shared the need to still rely on MLA requests to allow exchange of information, which may hamper effectiveness and involvement. There may also be limits to the information that can be shared, particularly relating to granularity of financial transaction information.
- **Uneven capacity and priorities** may also dissuade jurisdictions from participating in joint action. As discussed earlier, internal domestic priorities may not align with joint action and jurisdictions may face a difficult decision in balancing these interests in the face of resource constraints despite the rise in CEF.

105. In addition to JITs, joint operations organised by multi-lateral organisations such as INTERPOL also provide an important point of co-ordination for multi-lateral enforcement action against CEF. While such operations may be more informal than JITs in the absence of formal legal agreements, they can still provide an important platform for relevant jurisdictions to jointly fight CEF.

Box 47. INTERPOL Operation HAECHI

Since 2020, INTERPOL conducts a yearly operation named HAECHI that targets cyber-enabled financial crimes and associated ML, which supports the information exchange between participating jurisdictions. Under the recent HAECHI III (2022), participated by 30 jurisdictions, almost 1 000 suspects were arrested and 2 800 bank and virtual-asset accounts linked to the illicit proceeds of USD 130 million were blocked. Through HAECHI III, INTEPROL has co-ordinated numerous cases between member countries to jointly combat CEF.

Operation HAECHI also served as the platform for FINCAF which gathers information from different sources and identifies links between ongoing investigations in different member countries. The FINCAF is structured to include data and other items of information relating to any types of financial crime and offences with a transnational dimension. INTERPOL uses FINCAF to work with member countries to strengthen the overall tactical response to international organised crime such as CEF. The FINCAF is an important tool that provides better insights into criminal activities across borders, criminal organisations, their group structures, individual roles and key persons, modi operandi, and fraudulent financial transactions.

Source: INTERPOL

Public-private collaboration

106. Public-private collaboration can extend beyond national borders, which can harness greater results given CEF's transnational reach. Like domestic PPPs, such collaboration can cover typologies or strategic sharing as well as operational co-ordination. Composition of such partnerships would also be dependent on the objectives and could include relevant traditional AML/CFT and non-traditional sectors.

Box 48. European Money Mule Action

The European Money Mule Action is an international operation built upon public-private information sharing to fight complex modern crimes.

In 2022, with the continuing coordination of the European Banking Federation, around 1,800 banks and financial institutions supported law enforcement in this action, alongside online money transfer services, cryptocurrency exchanges, Fintech and KYC companies, and multinational computer technology corporations.

The operation consisted of law enforcement from 25 jurisdictions[1], and was further supported by Europol, Eurojust, and INTERPOL. 8,755 money mules were identified alongside 222 money mule recruiters. In all, EUR 17.5 million of funds were intercepted, with 2,469 money mules arrested.

Source: Europol

[1] Australia, Austria, Bulgaria, Colombia, Cyprus, Czech Republic, Estonia, Greece, Hungary, Singapore, Hong Kong (China), Ireland, Italy, Moldova, Netherlands, Poland, Portugal, Romania, Slovak Republic, Slovenia, Sweden, Switzerland, Spain, United Kingdom, and United States.

6. Conclusion and priority areas

107. CEF is perpetrated by transnational, organised crime syndicates. The scale and magnitude of CEF is expected to grow with the rising trend of digitalisation and virtual services across the globe. Jurisdictions should also be aware of the additional vulnerabilities across various sectors, including digital financial institutions and non-traditional sectors, that criminals may exploit to enhance CEF and ML techniques through growing digitalisation.

108. Jurisdictions need to focus on breaking down siloes to accelerate and enhance collaboration between various sectors and entities, both on a domestic and international level. Due to the de-centralised nature of CEF and related laundering, vital financial information and evidence are often fragmented in different locations. This complicates efforts to investigate and dismantle CEF syndicates, and trace and recover CEF-proceeds.

109. CEF can have significant and crippling financial impact on victims. But the impact is not limited to monetary losses; it can have devastating social and economic implications. The conclusions of this report indicate three priority areas in which jurisdictions should act to tackle CEF and related ML more effectively: enhancing domestic co-ordination; supporting multi-lateral collaboration; and strengthening detection and prevention.

Priority areas to effectively counter CEF and related ML

Enhancing domestic co-ordination across public and private sectors

- Jurisdictions should develop co-ordination mechanisms to bring together relevant competent authorities to tackle CEF and the laundering of related proceeds holistically. This includes technical cybercrime experts as well as non-traditional sectors such as social media platforms, e-commerce, telecommunication and internet service providers. Jurisdictions should also leverage public-private partnerships to improve detection and investigations, and accelerate operational asset recovery responses.
- A good practice involves the creation of a dedicated centralised unit that can harness relevant information and co-ordinate actions across various public and private sectors, including investigations, asset recovery and fraud prevention.

Supporting multi-lateral international collaboration

- To enhance asset recovery outcomes and avoid dissipation of CEF-related proceeds, jurisdictions should work together to intercept CEF-proceeds expeditiously. Operational experience shows that intervention is generally most effective within 24 to 72 hours of a CEF incident. A global united approach is required to effectively trace and recover CEF-proceeds, which are being laundered and distributed across multiple jurisdictions.
- To do so, jurisdictions should leverage and support existing (and any future) multi-lateral mechanisms (such as INTERPOL's I-GRIP and the Egmont Group BEC Project) for rapid international co-operation and information exchange to combat CEF. Such multi-lateral mechanisms also allow jurisdictions to collaborate and collectively dismantle transnational CEF syndicates.

Strengthening detection and prevention

- To enhance detection, jurisdictions should ensure ease of victim reporting, for example, through dedicated platforms that allow streamlined reporting. Jurisdictions should also work with the private sector to improve suspicious transaction reporting.
- Jurisdictions should promote awareness and vigilance against CEF through public education, including to share tell-tale signs of CEF and enhancing cyber literacy. Prevention plays a key role in reducing the overall profitability for CEF syndicates. Jurisdictions can also collaborate with the private sector to support CEF prevention strategies, such as consumer protection and removal of criminal instrumentalities.

Annex A: Risk indicators for CEF

The following potential risk indicators draw from the experience and data received from jurisdictions across the FATF Global Network, the Egmont Group, and the private sector. These indicators aim to enhance the detection of suspicious transactions relating to CEF. The list is further categorised into various perspectives from account opening to transaction monitoring. The indicators can be relevant to regulated entities, including FIs, VASPs, DNFBPs and other financial and payment institutions.

The existence of a single indicator in relation to a customer or transaction may not alone warrant suspicion of a CEF offence, nor will a single indicator necessarily provide a clear indication of such an activity. However, it could prompt further monitoring and examination as appropriate.

Transaction patterns

- Rapid or immediate, high or low value transactions after opening of an account, inconsistent with the purpose of the account
- Rapid or immediate cash withdrawals or transfers of large amounts following the receipt of a funds transfer in order to empty the account
- Frequent and large transactions, which are inconsistent with the account holder's economic profile (e.g., sudden international transfers, withdrawals of cash performed through payment cards at foreign ATMs, large purchases of VA or goods to be exported abroad, or payments in favour of unlicensed foreign MVTS)
- Transfers of funds to and from high-risk money laundering jurisdictions
- Large frequent transactions with recently established companies and/or whose main activities are not consistent with the activities carried out by the beneficiary or have a general purpose
- Small payment to a beneficiary, which once successfully completed, is rapidly followed by larger value payments to the same beneficiary
- Round value amount purchases that are frequent and/or in large amounts, which can indicate gift card purchases

Customer transaction instructions and remarks

- A customer transaction requests for additional payments immediately following a successful payment to an account not previously used by the customer to pay its suppliers/vendors. Such behaviour may be consistent with a criminal attempting to issue additional unauthorised payments upon learning that a fraudulent payment was successful
- A customer's seemingly legitimate transaction instructions contain a different language vernacular, timing, and amounts than previously verified transaction instructions.
- Transaction instructions include markings, assertions, or language designating the transaction request as "Urgent", "Secret" or "Confidential"

- A customer presents poorly formatted messages / emails (spelling and/or grammar mistakes) as justification of a transaction.
- Transaction instructions direct payment to a known beneficiary; however, the beneficiary's account information is different from what was previously used
- The intended beneficiary in the transaction description and the name of the account holder known to the beneficiary bank are inconsistent
- Transfers ordered by natural persons (alleged investors) with no financial experience and expertise, in favour of companies (in many cases established in high-risk jurisdictions) with reasons for payments related to investments and financial products
- Counterparties incommensurate with the business/company name of the account might suggest which may provide cover for the movement of large amounts of funds internationally (e.g., the company reported as a furniture company made multiple large transfer to a company named as petroleum trading company)
- Transactions conducted with device time zone mismatch

Suspicion in account holder's profile

- Account holder is unwilling or unable to pass CDD checks
- Account holder is unfamiliar with the source of the funds moving through their account or claiming they are transacting for someone else
- Frequent changes of legal entities'/sole proprietorships' names using foreign expressions and terminology
- The customer shows to have inadequate knowledge on the nature, object, amount or purpose of the transaction/s or relationship or provides non-realistic, confusing or inconsistent explanations, which drive to the suspicion that the customer is acting as a mule.

Suspicion in account user's identity

- The user is attempting to conceal their identity by using shared, falsified, stolen or altered identification (address, telephone number, email)
- Frequent changes of contact details, phone numbers, email addresses after opening of the account
- E-mail addresses that do not seem compatible with the name of the account holder, or a pattern of similar email addresses seen across multiple accounts
- Irregularities in customer profile particulars, such as shared credentials (e.g., shared by two or more users) with other accounts
- Abnormalities identified via online behaviour, such as hesitation inputting data, keystroke delays, signs of automation, multiple failed login attempts, etc
- Accounts relating to entities who could be expected that they are no longer active in the jurisdiction (e.g., overseas students' account sold when completed study)

- IP addresses or GPS coordinates originating from high-risk money laundering jurisdictions
- Use of virtual private networks (VPNs), compromised devices (such as IOT devices), and hosting companies that may mask a user's IP address
- Multiple IP addresses or electronic devices associated with a single online account
- Single static IP address or electronic device associated with multiple accounts of various account holders
- Remote desktop connection access to an account through computer ports used by applications such as TeamViewer etc. which prevents the true device and location to be seen
- Accounts operated with excessively quick keystrokes or navigation suggesting possible bot control

Adverse information on the account holder

- Presence of material relevant and verifiable negative news on customer or counterparties, e.g., account held by a known or suspected previous victim of scam, mule, or identity takeover activity
- Fraud report or recall from a correspondence institution, or other 3rd party fraud databases
- Presence of wire transfers' recall requests
- Presence of adverse information provided by FIUs or LEAs about persons involved in a transaction

VA transactions

- Sending/receiving large volumes or high frequency low amounts worth of VAs to unhosted wallet addresses; or addresses associated with darknet marketplaces, child sexual abuse material platforms, cyber exploit marketplaces, ransomware groups, mixing/tumbling services, high-risk jurisdictions, gambling sites, and scammers
- Maxing out daily funding limits at Bitcoin ATMs
- No documents proving the origin of VA or of the money converted in crypto-assets
- Transfers of VAs to wallets linked to illegal activities on the dark web (e.g., terrorism, child pornography, narcotics, etc)
- Transactions involving more than one type of VAs, particularly those that provide higher anonymity
- Abnormal transaction activity of VAs from peer-to-peer platform associated wallets with no logical business explanation

Other

- Mismatch of account number and name of the holder of the account

- The user is seen on the phone or accompanied by an individual through Closed Circuit Television (CCTV) and being instructed or coached during the transaction
- Beneficiary companies manage Internet Web Sites providing trading/investment services, in many cases not authorised or listed by the domestic Supervisory Authority

Annex B: Harnessing synergies between anti-fraud and AML/CFT controls

This Annex compiles some good examples of how 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. These include varying measures related to customer verification and transaction monitoring.

These controls may be useful for FIs, VASPs and other financial and payment institutions.

- Putting in place rigorous Know-Your-Customer (KYC) or Know-Your-Business processes, biometric features during digital on-boarding process etc, and identification of one mobile or secure device to authenticate online banking transactions (others are blocked or subjected to enhanced risk mitigation measures).
- A cooling-off period for first time enrolment of online banking services or secure devices (i.e., full suite of banking services is not immediately available on opening), limiting the number or value of financial transactions of the customer.
- Developing a definition of expected transactions (number of transactions, amounts, types of counterparties, countries involved) to help detect suspicious transactions as well as tightening of fraud detection rules and triggers to pre-emptively block illicit transactions.
- Using "verification of payee" services, which 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 any communication via email and social media with clients to general information only, explicitly stating that no identification or personal data should be exchanged with the FI/VASP via email.
- Adding voice recognition software and artificial intelligence support in the communication with the clients to ensure their true identity.
- Requiring multi-factor authentication mechanisms for customer verification and for performing financial transactions, adding or activating beneficiaries using different channels.
- To authenticate the identity of the user during remote set up and to prevent criminals gaining access to multiple accounts using money mules' or victims' account information by:
    - Enhancing the reliability of client identification process through liveness tests (i.e., ensuring live and genuine human being), including if an individual is being socially engineered during the liveness checks; or
    - Monitoring IP addresses used to connect to on-line banking websites, etc., including detecting use of Remote Access Tools and "Man-in-the-Browser" attack.

- Extending the types of data that reporting entities collect and analyse about customers, including e.g., mobile phone numbers, IP addresses, GPS coordinates, device ID etc. For fraud prevention purposes, FIs could repeat such identification using a risk-based approach (e.g., conduct these checks when anomalous behaviour is detected).
- Implementing a risk-based real-time transactions monitoring system to ensure that any abnormal activity can be swiftly detected, investigated and where relevant, reported through the filing of a suspicious transaction report. The sophistry of the monitoring system should be commensurate with the volume and nature of transactions handled by the FI.

www.egmontgroup.org | www.interpol.int | www.fatf-gafi.org

November 2023

Illicit Financial Flows from Cyber-Enabled Fraud

This report analyses the methods used for cyber-enabled fraud, its links to other crimes and how criminals may exploit vulnerabilities in new technologies. It highlights examples of national operational responses and strategies that have proven successful in tackling cyber-enabled fraud. The report also identifies risk indicators and useful anti-fraud requirements and controls, that may help public and private sector entities detect and prevent cyber-enabled fraud and related money laundering.