FATF

FATF Paper

Cyber-Enabled Fraud

Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks

February 2026

Background

This paper is part of the FATF's ongoing work to assess the risks arising from digitalisation, to raise awareness of emerging and high-priority threats or risks, to consider where further action may be required, and to provide forward-looking perspectives of current and potential cyber-enabled fraud (CEF)-related risks and trends. It forms part of the FATF's staged approach to emerging technologies to identify and explain ongoing risks and vulnerabilities associated with fraud through the lens of Anti-Money Laundering, Countering the Financing of Terrorism, and Countering the Financing of Proliferation (AML/CFT/CPF).

The paper is designed to raise awareness among national authorities, financial institutions (FIs), Virtual Asset Service Providers (VASPs), Designated Non-financial Businesses and Professions (DNFBPs), and other stakeholders, and also to encourage and support the development of effective regulatory and operational responses within the global AML/CFT/CPF framework. It explores the intersection of CEF with some of the FATF Recommendations and demonstrate the FATF's commitment to stimulate discussion on new topics and to promote forward-looking engagements on this evolving issue.

Introduction

Cyber-enabled fraud has become one of the most widespread and damaging forms of profit-motivated crime globally, generating large volumes of illicit proceeds through the exploitation of victims around the world. Rapid adoption of digital technological innovations during and after the COVID pandemic has accelerated fraud by enabling faster funds movement as well as increasingly sophisticated social engineering schemes. These technologies continue to transform economies and financial systems globally, bringing substantial benefits in efficiency, innovation, and financial inclusion. At the same time, digital technological innovations have significantly expanded the scale, speed, and complexity of fraud, increasingly enabling criminal actors to operate across borders and exploit digital platforms, instant payment systems, and emerging technologies.

Part I: The Growing Threat and Impact from Cyber-enabled Fraud

Fraud in Figures: A Rapidly Growing Threat

As part of FATF's ongoing risk assessment activities, officials from law enforcement agencies, financial intelligence units, policymaking bodies, and other illicit finance experts continue to discuss fraud, sharing case studies and data illustrating both the scale and the evolving nature of cyber-enabled fraud in their jurisdictions. Taken together, these contributions paint a sobering picture of how cyber-enabled fraud has escalated and adapted across regions.

One-hundred and fifty-six jurisdictions, or 90% of assessed jurisdictions[1], explicitly identify fraud as a major money-laundering risk. The rate of fraud is growing – for example, in Singapore alone, the number of cyber-enabled fraud (scam) cases has increased **61%** in two years.[2] In the United Kingdom, fraud now accounts for more than **40%** of all crimes. Several countries estimate up to **15%** of their adult population has fallen victim to a successful cyber-enabled fraud attempt, underscoring the widespread and growing nature of this threat. While the total estimate of fraud losses including against individuals, businesses and to the detriment of public finances is impossible to quantify, it reaches at least into the tens of billions of dollars a year in the United States alone.

Enablers of Cyber-enabled Fraud

Technological innovation has been a driver for economic and social progress, but that same innovation has brought to market enablers of cyber-enabled fraud that have lowered barriers to entry, expanded reach, and enabled fraudsters to scale operations. Many financial and non-financial services expanded swiftly into the online environment during the COVID-19 pandemic.

As highlighted in the FATF, Egmont Group and INTERPOL's joint 2023 publication on Illicit Financial Flows from Cyber-enabled Fraud, crimes such as cyber-enabled fraud are experiencing explosive growth, driven by emerging technologies like AI and AI-enabled deepfakes. These technologies enhance criminals' abilities to use phishing emails, fake websites, social media advertising, messaging applications and other cyber-enabled means to perpetrate scams remotely and at mass scale.

Financial infrastructure developments have equally contributed to the difficulties in combating fraud. The increasing use of virtual assets, as well as instant and cross-border payment channels with insufficient dedicated mitigation measures, enable proceeds to be transferred before detection or intervention unless AML-obliged entities and competent authorities can detect and intervene in a very short time period.

These cross-border dynamics compound due to challenges in information sharing and international co-operation, as competent authorities and private sector stakeholders must operate within legal, procedural and jurisdictional constraints while criminals act in real time. For example, criminals increasingly request payment directly in virtual assets or rapidly convert fiat proceeds into virtual assets to evade recovery, while tracing takes time and resources.

In many cases, large-scale cyber-enabled fraud schemes are conducted or facilitated by transnational organised crime groups and operated through dedicated "scam centres" (or

[1] 176 published and reviewed countries at the time of analysis conducted in June 2025.

[2] Singapore's *Annual Scams and Cybercrime Brief 2024*.

compounds). These hubs are often embedded within broader criminal ecosystems, converging with other illicit activities such as professional money-laundering services, human trafficking and related human-rights abuses, drug trafficking, and other serious offences.[3]

Countries observe that a growing number of cyber-enabled fraud schemes integrate money laundering mechanisms from the outset, relying on nominee accounts, money mule networks, the trade in bank and exchange accounts, and rapid fund movements through fintech platforms, thereby blurring the lines between fraud, illegal financial services, and money laundering.

[3] Source: U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia | U.S. Department of the Treasury .

Part II: Leveraging FATF Standards to Combat Cyber-enabled Fraud

The FATF Fight Against Cyber-enabled Fraud

Since FATF's 2023 report on Illicit Financial Flows from Cyber-enabled Fraud sounded the alarm that cyber-enabled fraud has grown exponentially in recent years, the volume of frauds reported and their geographical concentration have spread. In working to combat this spread, FATF has taken significant actions to assist countries in more effectively combating fraud.

Over the last few years, the FATF has taken the following steps, which can assist countries and financial institutions to trace and prohibit the generation and transfer of fraud proceeds.

Payment Transparency

The FATF also continues efforts to deal with evolving ML infrastructure, such as peer-to-peer transactions and decentralised finance, through improving transparency in payments which is critical to improving the traceability of fraud proceeds (i.e. through "confirmation of payee" mechanisms) and reducing criminals' ability to move funds anonymously or through unregulated intermediaries.

Importantly, public–private, private-private, and public-public partnerships play a critical role, enabling timely information exchange, typology development, early detection of emerging fraud patterns, and prompt response to the evolving ML threats.

Asset Recovery Standards Improvements

Over the past decade, the FATF has prioritised strengthening asset recovery frameworks globally, recognising their importance in disrupting profit-motivated crime and compensating victims of fraud.[4]

The revised FATF Standards require countries to establish rapid payment-suspension and freezing mechanisms to prevent cyber-enabled fraud proceeds from being transferred abroad. They also require non-conviction-based confiscation regimes and stronger international co-operation, including faster and more effective informal co-ordination.

Together, these measures enhance countries' ability to detect, disrupt, and recover the proceeds of fraud and other financial crimes.

Regulation of Virtual Assets

As increased adoption of digital and faster payment methods has provided greater opportunities for fraudsters to victimise consumers, the FATF's environmental scanning for emerging risks has proven vital.

In 2019, the FATF introduced global standards on virtual assets and issued guidance to regulate Virtual Asset Service Providers (VASPs) with AML/CFT controls, including customer identification and transaction tracing requirements to ensure consistency of information required in payment messages.

[4] See 2025 Guidance on Asset Recovery here: https://www.fatf-gafi.org/en/publications/Methodsandtrends/asset-recovery-guidance-best-practices-2025.html

Since that time, the FATF has focused on jurisdictions' implementation of these requirements, particularly for jurisdictions with materially important VASP sectors, in part to mitigate the opportunity for virtual assets to be used for cyber-enabled fraud, and ensure such misuses are addressed through criminal justice measures when such cases occur.

As criminals exploit gaps and differences in jurisdictions' implementation of the FATF Standards, the FATF will emphasise accelerating global compliance to ensure countries are appropriately mitigating these risks.

Unmasking Beneficial Ownership

Professionalised fraud actors use shell companies to hide criminal proceeds and property. The FATF is the global leader in ensuring that countries implement international standards on beneficial ownership (BO) of these types of legal structures.

In March 2022, the FATF revised its standards on beneficial ownership to require countries to take a risk-based and multi-pronged approach to collecting and using BO information for legal persons.

Domestic and International Partnerships

Domestic co-ordination and collaboration mechanisms have sprung from a need to share information more quickly, work across the public/private sector towards a common goal and to respond to the growing cyber-enabled fraud epidemic. National anti-fraud centres share many of the attributes, powers and constituents of national AML co-ordination centres/regimes.

In addition to domestic co-ordination, national authorities have also shown their willingness to work with international partners to identify fraud perpetrators abroad, as well as trace and recover proceeds of crime. Effective inter-agency cooperation across borders can significantly enhance the detection, disruption, and investigation of transnational fraud and scam networks.

Employing Advanced Technology

Given the sheer scale of fraudulent transactions, manual processes are not always well-suited to address the current environment's scale and complexity. Accordingly, countries are also investing in technology-driven solutions to get ahead of cyber-enabled fraud.

Some financial intelligence units (FIUs) and banks have deployed machine learning models on transaction datasets to detect anomalies associated with fraud and other forms of financial crime. Others have built risk-scoring systems for payments (flagging high-risk payments in real time based on attributes matching known fraud patterns).

FATF's recent changes in requirements for payment transparency encourages anti-fraud verification in payment processes.

Conclusion

Cyber-enabled fraud has expanded in scope, in scale, and now touches virtually every person on earth. Recognising these evolving threats, FATF has committed to focusing on fraud over the next few years. This includes through continuing to analyse emerging developments, such as the rise of scam centres and the proliferation of these compounds across the world and identifying measures to strengthen countries' abilities to respond to the fraud epidemic by mobilising the FATF toolkit.

The FATF also continues to support a strong, coherent global response to cyber-enabled fraud. Through the Global Network, over 200 jurisdictions apply AML/CFT tools that prevent money from reaching fraudsters' hands and can recover it when it does.

Continuing to meet the cyber-enabled fraud challenges of today requires sustained international commitment. The FATF has a crucial role in supporting stronger implementation of global standards that will advance international efforts to tackle fraud, including through international cooperation and asset recovery, sharing information quickly with national and international partners, continuing to adapt to the dynamic cyber-enabled fraud risk environment and intensifying our collective resolve and action.

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.

Citing reference:

FATF – (2026), Cyber-enabled fraud - Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks, FATF, Paris, France,

www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/cyber-enabled-fraud-digitalisation-ml-tf-pf-risks.html