

The Bangkok Blueprint

for Fraud-Resilient
Financial Services



WORLD BANK GROUP

The Bangkok Blueprint for Fraud-Resilient Financial Services

Prepared by Ben Aldersey, Marianne Bechara, Carine Chartouni, Gabriela Conde, Dorothee Delort, Erik Feyen, Guillermo Alfonso Galicia Rabadan, Dirk Jan Grolleman, Tanai Khiaonarong, Michelle Morales, Anca Paduraru, Nadine Schwarz, Puja Singh, and Indulekha Thomas

Authorized for distribution by Tobias Adrian and Yan Liu (for the IMF) and Pablo Saavedra (for the World Bank Group)

The authors gratefully acknowledge the valuable feedback and insightful comments provided by Marina Moretti, Sophie Sirtaine, and Harish Natarajan and World Bank Group peer reviewers Lalita Moorthy, Ravi Shankar Chaturvedi, and Jennifer Chien, and thank Marie-Bernadette Amand de Mendieta for her excellent editorial support.

The views expressed are those of the staff of these institutions and do not necessarily represent those of their Executive Boards, management, or member country governments. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent. The World Bank does not guarantee the accuracy, completeness, or currency of the data included in this work and does not assume responsibility for any errors, omissions, or discrepancies in the information, or liability with respect to the use of or failure to use the information, methods, processes, or conclusions set forth. The boundaries, colors, denominations, links/footnotes, and other information shown in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries. The citation of works authored by others does not mean The World Bank endorses the views expressed by those authors or the content of their works. Nothing herein shall constitute or be construed or considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, all of which are specifically reserved.

Recommended citation:

International Monetary Fund and World Bank Group. 2026. "The Bangkok Blueprint for Fraud-Resilient Financial Services." International Monetary Fund, Washington, DC.

Cover design:

Rana Al-Gazzaz, International Monetary Fund

Please send orders to:

International Monetary Fund, Publication Services

PO Box 92780

Washington, DC 20090, USA

T. +(1) 202.623.7430 | F. +(1) 202.623.7201

publications@IMF.org | eLibrary.IMF.org

Contents

Abbreviations	1
Executive Summary	2
I. Introduction	5
A. The Evolution of Cyber-Enabled Fraud	6
B. Foundations of Fraud-Resilient Financial Services	7
II. Framework and Scope	9
A. The Fraud Life Cycle	12
B. The Mitigation Life Cycle	13
III. Key Considerations	14
A. Establish Strategic and Legal Foundations	15
B. Strengthen the Fraud-Mitigation Life Cycle	19
C. Leverage Existing Risk Mitigation and Enforcement Frameworks	24
D. Expand Domestic and Cross-Border Coordination and Cooperation	29
E. Promote Consumer Protection and Resilience	31
Annex 1. Cyber-Enabled Fraud Definition and Lexicon	34
Annex 2. Measuring Cyber-Enabled Fraud	36
References	38
Boxes	
Box 1. Main Characteristics of Cyber-Enabled Fraud	9
Box 2. Cyber-Enabled Fraud's Relationship with Cyber Incidents and Money Laundering	11
Box 3. Digital Finance and Cyber-Enabled fraud: Examples of Trade-Offs	16
Figures	
Figure 1. Cyber-Enabled Fraud Typologies Targeting Retail Financial Services	11
Figure 2. The Cyber-Enabled Fraud and Mitigation Life Cycles	12
Figure 3. The Bangkok Blueprint to Address Cyber-Enabled Fraud	14

Abbreviations

AI	Artificial intelligence
AML	Anti-money laundering
CERT	Computer Emergency Response Team
CFT	Combating financing of terrorism
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
GASA	Global Anti-Scam Alliance
ICT	Information and communication technology
IMF	International Monetary Fund
ISAC	Information Sharing and Analysis Center
KC	Key consideration
KPI	Key performance indicator
PET	Privacy enhancing technology
UNODC	United Nations Office on Drugs and Crime
WBG	World Bank Group

Executive Summary

Rising cyber-enabled fraud¹ and potential operational and cyber vulnerabilities across increasingly interconnected digital ecosystems threaten safe and inclusive digital financial services. Cyber-enabled fraud spans both unauthorized transactions, where funds move without the customer's consent, and, increasingly, authorized transactions, where victims are manipulated into initiating transactions themselves. As scams become more sophisticated and industrialized, large-scale operations—often linked to transnational organized crime—are now generating losses significant enough to affect households and businesses and potentially undermine trust in the financial system, a foundation for both inclusion and stability. These threats can erode confidence in digital financial systems and services, dampening the development gains—financial inclusion, resilience, job creation, and economic growth—that they are meant to deliver.

Since the 2018 IMF-WBG Bali Fintech Agenda, which established policy considerations for harnessing digital financial services while managing the risks, the digitalization of finance has increased innovation and efficiency while broadening access to financial services. At the same time, it has expanded the scale, speed, and sophistication with which fraud can be perpetrated. As a result, cyber-enabled fraud in financial services has emerged as a systemic policy challenge rather than a series of isolated criminal acts, requiring coordinated action across the financial sector and beyond.

To safeguard trust in the financial system and support financial inclusion, consumer protection, integrity, and stability, this paper sets out 12 key considerations (KCs) to address cyber-enabled fraud in financial services. These KCs are intended as a high-level blueprint with a focus on the financial sector—titled the Bangkok Blueprint, and launched during the 2026 IMF-WBG Annual Meetings in Thailand—to guide national policymakers, regulators, financial institutions, financial infrastructures, and other stakeholders in identifying vulnerabilities and in designing and implementing comprehensive mitigation approaches.

The Blueprint emphasizes the need for clear strategies, fit-for-purpose legal, regulatory, and supervisory frameworks, and strong cooperation and coordination arrangements to ensure swift action. Effective fraud mitigation is ideally embedded in financial services and supported by real-time intelligence, operational capacity, and adequately protected and empowered consumers while maintaining a balance between innovation, inclusion, and risk. Its distinctive contribution is to frame cyber-enabled fraud as a financial sector policy challenge organized around five pillars: establish strategic and legal foundations; strengthen the fraud-mitigation life cycle; leverage existing risk mitigation and enforcement frameworks; expand domestic and cross-border cooperation; and promote consumer protection and resilience.

Because fraud frequently originates outside the financial sector—on social media, digital platforms, e-commerce sites, and telecommunications networks—financial sector measures are necessary but not sufficient, and effective mitigation requires a whole-of-ecosystem response. This entails strong coordination and accountability across public sector actors, including central banks, supervisory authorities, data protection authorities, finance ministries, financial intelligence units, law enforcement, and relevant sectoral

¹ See Annex 1 for an overview of fraud definitions. In the context of the blueprint, cyber-enabled fraud refers to the use of digital technologies and psychological manipulation of victims (mostly individual consumers) to obtain illicit gains, whether through authorized or unauthorized transactions, and involving actors within or outside the financial sector.

authorities, as well as with private stakeholders such as financial institutions, financial infrastructures, telecommunications providers, and digital platforms.

In applying the KCs, national authorities are encouraged to tailor their approach to domestic conditions. Such an approach acknowledges differences in institutional, legal, and regulatory frameworks, the risk profile of cyber-enabled fraud, and the structure of digital financial ecosystems across jurisdictions. The KCs are all important and mutually reinforcing, and are not presented in order of priority. In practice, however, countries may wish to begin by conducting a risks and gaps assessment and establishing a national strategy and the necessary legal and institutional foundations, which provide the basis for sequencing the remaining measures.

The blueprint is a nonprescriptive framework, not formal IMF and WBG policy guidance. It offers considerations to address cyber-enabled fraud and aims to provide a foundation for further international engagement to ensure safe and inclusive digital finance. In developing the framework, the IMF and WBG built on the work of standard-setting bodies, members' emerging practices, and engagements with private sector stakeholders. Within their respective mandates, the Blueprint will also help IMF and WBG staff develop their work on cyber-enabled fraud, inform their dialogue with national authorities, and shape their contributions to standard-setting bodies and other relevant international institutions.

Establish Strategic and Legal Foundations:

- **KC1—Establish a Comprehensive National Strategy for Fraud-Resilient Digital Finance.** Establish a comprehensive national strategy to address cyber-enabled fraud, grounded in the current and evolving risk environment and backed by high-level ownership, accountability, and a clearly designated lead entity. The strategy sets out clear goals and measurable objectives and aligns with broader public policy objectives and strategies. It outlines governance and collaboration arrangements, an action plan, and clearly assigned responsibilities supported by adequate legal mandates. In addition, it includes public communication, monitoring, and evaluation mechanisms.
- **KC2—Establish a Sound Legal, Regulatory, and Supervisory Framework to Address Cyber-Enabled Fraud.** Establish a robust legal, regulatory, and supervisory framework for cyber-enabled fraud that equips authorities with the powers needed to allocate liability, protect financial consumers, share information quickly, and freeze and recover fraud proceeds, while applying a risk-based, proportionate, and adaptable approach.

Strengthen the Fraud-Mitigation Cycle:

- **KC3—Build Cyber-Enabled Fraud Resilience in Financial Services Design.** Mitigate cyber-enabled fraud through accessible, proportionate, and continuously adaptive safeguards embedded in the design of digital financial services.
- **KC4—Implement Collaborative and Adaptive Fraud Prevention.** Implement prevention as a preemptive, coordinated, and financial system-wide function that identifies vulnerabilities early, adapts to emerging threats, and actively disrupts fraud actors and networks.
- **KC5—Build a System-Wide Fraud-Detection Architecture.** Build a system-wide detection architecture for cyber-enabled fraud, combining institution- and ecosystem-level monitoring through enabling protocols, structured data sharing, and collaborative analytics.
- **KC6—Operationalize Coordinated Response and Recovery Mechanisms.** Ensure that cyber-enabled fraud incidents are contained rapidly and their impacts limited through effective response and

recovery, supported by strong coordination, preparedness, escalation planning, investigation, and standardized incident reporting across relevant institutions, financial infrastructures, and authorities.

Leverage Existing Risk Mitigation and Enforcement Frameworks:

- **KC7–Strengthen Financial Sector Cyber Resilience.** Strengthen cyber resilience across the digital financial ecosystem to protect service providers, infrastructures, and users of financial services from cyber-enabled fraud by ensuring effective cybersecurity regulatory, supervisory, and risk-management frameworks.
- **KC8–Leverage the Existing Anti-Money Laundering/Combating the Financing of Terrorism Framework to Address Cyber-Enabled Fraud.** Leverage anti-money laundering measures to complement fraud-mitigation measures, bolstering the prevention and detection of cyber-enabled fraud, depriving fraudsters of illegal gains, and disrupting those actors, including transnational organized crime groups.
- **KC9–Deter Cyber-Enabled Fraud through Effective Law Enforcement and Criminal Sanctions.** Deter criminals from committing cyber-enabled fraud and related money laundering through effective law enforcement responses, proportionate and dissuasive sanctions, and the recovery of criminal proceeds. Publicizing successful law enforcement actions can strengthen deterrence and demonstrate to the broader public that criminals involved in fraud are being held to account.

Expand Domestic and Cross-Border Cooperation and Coordination:

- **KC10–Promote Domestic Collaboration for Cyber-Enabled Fraud Mitigation.** Promote systematic, risk-based collaboration between public and private stakeholders that strengthens fraud mitigation in the financial sector, addresses vulnerabilities originating outside it, and enables rapid coordinated action across the fraud-mitigation life cycle.
- **KC11–Harness Cross-Border Cooperation, Coordination, and Information-Sharing Frameworks.** Ensure that cross-border cooperation, coordination, and information-sharing arrangements prevent and mitigate cyber-enabled fraud across jurisdictions.

Promote Consumer Protection and Resilience:

- **KC12–Strengthen Consumer Protection, Empowerment, and Awareness against Cyber-Enabled Fraud.** Strengthen existing financial consumer protection frameworks to ensure they are fit for purpose. Ensure that consumers understand cyber-enabled fraud risks, their rights and protections, and how liability, redress, and remediation arrangements apply when fraud occurs.

I. Introduction

Cyber-enabled fraud undermines public trust in digital financial services and the vision of safe and inclusive digital finance. It encompasses fraud carried out both through unauthorized transactions, where funds move without the customer's consent (for example, through account takeover, stolen credentials, or system compromise), and, increasingly, through authorized transactions, where victims are manipulated into initiating payments themselves (for example, through impersonation, investment, or romance scams). Cyber-enabled fraud has reached significant scale around the world and poses financial integrity, consumer protection, cybersecurity, and macrofinancial risks, and it could stall the adoption of digital financial services, thereby undermining the universal financial access agenda (World Bank 2021). It also reduces financial institutions' resources and shock-absorbing capacity and affects trust in the financial system, potentially contributing to financial instability (BCBS 2023).

Resilience to cyber-enabled fraud is also a precondition for confidence in the broader digital economy and for promoting and sustaining the development gains that it enables. Digital financial services are increasingly the gateway through which individuals and businesses receive income, make payments, save, borrow, insure against shocks, access public transfers, and participate in the broader digital economy. When cyber-enabled fraud erodes trust, users may reduce participation in or abandon digital services and systems, limiting their benefits for financial inclusion and resilience for households and micro, small, and medium enterprises, as well as their contribution to job creation and economic growth.

To address these systemic challenges, this paper proposes a framework consisting of 12 key considerations (KCs) for a comprehensive national strategy to combat cyber-enabled fraud. It builds on the IMF-WBG Bali Fintech Agenda (IMF and WBG 2018), which established policy considerations for harnessing digital financial services while managing the risks, including safeguarding financial integrity and fostering international cooperation. Launched at the 2026 IMF-WBG Annual Meetings in Thailand, the framework—titled the Bangkok Blueprint—deepens that agenda, building on existing international standards and frameworks and emerging country practices (BOT and PIER 2026) to establish the foundations for building fraud-resilient finance. Within their respective mandates, the blueprint will also help IMF and WBG staff develop their work on cyber-enabled fraud, inform their dialogue with national authorities, and shape their contributions to standard-setting bodies and other relevant international institutions.

Although these KCs are directed primarily at the financial sector, the challenges they address are inherently broader. Cyber-enabled fraud frequently originates outside the financial sector, on social media, digital platforms, e-commerce sites, and telecommunications networks, where victims are first targeted, deceived, or recruited before any transaction reaches the financial system. Financial sector measures alone are therefore necessary but not sufficient. Effective mitigation requires a whole-of-ecosystem response that engages nonfinancial actors—relevant authorities, platform operators, and telecommunications providers—so that prevention, detection, and response extend across the full chain through which fraud is perpetrated. The blueprint focuses mostly on financial sector stakeholders, with the understanding that they are part of a wider ecosystem.

A. The Evolution of Cyber-Enabled Fraud

Digital transformation is reshaping financial services in ways that benefit consumers, firms, and regulators alike. For consumers and businesses, it reduces costs, improves efficiency, increases competition and transparency, and expands access, especially for low-income and underserved groups.² For financial regulators, it enables more data-driven, real-time, and risk-sensitive approaches to supervision and oversight. Policymakers therefore continue to embrace and promote digitalization of the financial sector as a driver of economic growth, financial inclusion, and development.

Digital transformation has also fueled cyber-enabled fraud in financial services, which has evolved into a global concern. Over the past decade, cyber events in the financial sector accounted for about 10 percent of total global cyber events and have grown tenfold, whereas cyber-enabled fraud (also referred to as online scams or digital fraud) cases have nearly tripled (Khiaonarong and Zheng 2026). These trends are underestimated as reporting systems are often rudimentary, and underreporting is significant. Despite these data limitations, various global and national estimates point to substantial and growing losses.³ In most countries, credit transfer and card scams remain dominant, whereas crypto-related fraud is on the rise. Industry studies also suggest that scam losses represent a higher share of gross domestic product in developing economies, whereas advanced economies tend to incur higher individual losses (UNDP 2026).

Recent national assessments of money laundering risk consistently identify fraud, often cyber-enabled, as a major source of illicit proceeds. A recent Financial Action Task Force (FATF) analysis highlighted that 90 percent of 165 assessed jurisdictions consider fraud a major money laundering threat (FATF 2026a). In addition, 85 percent of regulators in 60 jurisdictions report it as a top risk facing consumers (OECD 2026).

Cyber-enabled fraud has emerged as a systemic policy challenge: its cross-sector and cross-border nature exposes the fragmentation of policy and regulatory frameworks, whereas rapid technological change makes it increasingly potent. Fraud spans several sectors, from banking, payments, insurance, and investments to telecoms, social media, and e-commerce, yet oversight remains largely siloed, reactive, and insufficient. Because fraud proceeds can move across accounts and borders within minutes, swift, coordinated action is essential to trace and recover funds and freeze fraud-related accounts. As scam operations adjust and relocate to evade law enforcement, countries with weaker legal, regulatory, and supervisory frameworks face growing exposure, underscoring the need for coordinated and consistent cross-border policy responses. Three features stand out:

- *Fraud is now one of the world's most severe and rapidly evolving transnational crimes, which is inextricably linked to organized crime and professional money laundering networks* (FATF, INTERPOL, and Egmont Group 2023; UNODC 2025; INTERPOL 2026). Criminal groups operating from one country target fraud victims in other countries and may move the proceeds of their fraudulent activities to yet another country. Fraud is also increasingly linked to other serious crimes, such as human trafficking and slavery (to sustain scam centers where victims are forced to commit fraud), drug smuggling, and terrorism (APG 2026). The response to these threats has often been piecemeal and inconsistent, with protections

² The latest World Bank Findex data show that the share of adults with a transaction account in low- and middle-income countries rose from 41 percent in 2011 to 75 percent in 2025, and 62 percent made or received digital payments, an increase of 27 percentage points since 2014.

³ For example, the US National Money Laundering Risk Assessment estimates the actual consumer fraud losses over 2024 at \$195.9 billion compared to only \$12.7 billion reported fraud losses for the United States alone (US Department of the Treasury 2026). The Global Anti-Scam Alliance estimated global fraud-related losses at almost half a trillion dollars in 2025 (GASA and Feedzai 2025).

siloes within specific sectors and fraud receiving less than 1 percent of total police resources in major jurisdictions (UK Government 2023).

- *Emerging technologies have acted as force multipliers for cybercrime networks, lowering barriers to entry and increasing the sophistication of cyber-enabled fraud.* Recently, frontier artificial intelligence (AI) models have obtained powerful capabilities to detect and exploit cyber vulnerabilities at speed and scale. AI, including deepfake technology, enables the creation of convincing synthetic voices and images that can impersonate family members, corporate executives, government officials, or celebrities. Automation through bots and “phishing-as-a-service” platforms allows criminals to launch millions of attacks with greater sophistication as well as to scale and conceal their proceeds. Agentic AI and the new financial service models and consumer interfaces they enable may expose new fraud vulnerabilities. At the same time, AI and other new technologies can also be used to combat fraud, for example, for dynamic alert systems for consumers and to analyze multiple data points and patterns across the fraud-mitigation life cycle. When used effectively, AI can help identify potential and materialized instances of fraud more quickly and enable rapid intervention. Nevertheless, its use varies, and institutions still face challenges in adopting AI, including difficulties modernizing data infrastructure and challenges with AI models themselves, such as bias, lack of transparency, and data privacy.
- *The nature of the threat has shifted from unauthorized to authorized fraud* (GASA and Feedzai 2025). In authorized fraud, like authorized push payment and investment fraud, criminals use psychological manipulation and coercion to trick or force victims into initiating and approving transactions themselves. Scammers exploit communication channels, targeting victims through calls, texts, or emails with increasing frequency, and this manipulation is heavily facilitated by digital infrastructure, where numerous cases originate on social media platforms and smishing (SMS phishing).

The ubiquity of the threat is reflected in wide-ranging victim demographics, which challenge the common misconception that only the elderly or vulnerable people are targeted. Evidence shows that approximately 50 to 70 percent of adults globally have experienced some form of online scam or fraud attempt, and this exposure to cyber-enabled fraud is common across all age groups. Although older adults may lose more money per incident, individuals between the ages of 29 and 60 are among the most likely to be victimized. Furthermore, victims often experience profound harms beyond financial loss, including debilitating stress, shame, and a loss of confidence in digital life that leads to further exclusion. Businesses are also increasingly vulnerable to fraud, with business email compromise prevalent across most regions (GASA and Feedzai 2025).

B. Foundations of Fraud-Resilient Financial Services

Building on international standards and frameworks, the blueprint aims to support the establishment of the foundations for fraud-resilient digital finance and integrating the fraud-mitigation life cycle—from prevention and detection to response and recovery—into a “whole-of-ecosystem” paradigm rooted in the following main components (see Figure 3):

- **Establishing Strategic and Legal Foundations.** Given the system-wide reach and impact of cyber-enabled fraud, an effective response requires a comprehensive, well-governed national approach, aligned with broader policy objectives and supported by clear responsibilities and coordination arrangements across stakeholders. This needs to be anchored in a robust legal, regulatory, and

supervisory framework that equips authorities with the powers and resources to ensure effective oversight and adequate financial consumer protection, allocate costs and liability across financial and nonfinancial entities, enable information sharing, and support the timely freezing and recovery of fraud proceeds, using a risk-based approach.

- **Strengthening the Fraud-Mitigation Life Cycle.** This cycle comprises prevention, detection, response, and recovery. Robust prevention starts with a focus on fraud-resilient design and proactive prevention embedded across the financial ecosystem. This design-based approach is reinforced by system-wide, intelligence-led prevention supported by real-time information sharing, advanced technologies, and coordinated analytical capabilities across stakeholders. Effective detection depends on a system-wide architecture that combines institutional-level monitoring with shared, real-time intelligence to identify and escalate fraud as it emerges. This needs to be complemented by coordinated response and recovery arrangements that enable rapid containment, structured investigation, and effective remediation and asset recovery for affected users.
- **Leveraging Existing Risk Mitigation and Enforcement Frameworks.** The national strategy can build on preexisting frameworks, like those for cybersecurity and AML/CFT. Although these may not be uniquely or specifically dedicated to addressing fraud, they include requirements and approaches that protect the financial system from being exploited by criminals, including fraudsters. For example, the AML/CFT framework provides a comprehensive approach to prevent, detect, and sanction financial crime. It notably imposes a range of so-called preventive measures (such as customer identification) on key private sector actors. It also provides tools for law enforcement that are key to effectively deter fraud, disrupt criminal networks, and remove the financial incentives that sustain fraud activity across the system.
- **Expanding Domestic and Cross-Border Cooperation and Coordination.** Existing financial sector cross-sector collaboration will need to be expanded beyond traditional boundaries, enabling shared intelligence, aligned responsibilities, and coordinated intervention across public and private stakeholders, including through public-private partnerships on fraud-related controls and information sharing. To address the transnational nature of cyber-enabled fraud, structured and operational cross-border cooperation and information sharing are also essential to enable coordinated prevention, detection, response, recovery, and enforcement across jurisdictions.
- **Promoting Consumer Protection and Resilience.** Authorities can build on existing financial consumer protection rules, supervisory tools, complaints mechanisms, redress arrangements, and conduct expectations while reviewing and updating or clarifying them where needed so they are fit for purpose for cyber-enabled fraud. Consumer empowerment and awareness are also central to help users understand fraud risks, their rights, and available safeguards—including how liability, redress, and remediation mechanisms apply—and take effective action when fraud occurs (Boeddu and others 2021) (World Bank 2017).

By operationalizing these components, national authorities can move from a reactive posture toward a proactive resilience model. The aim is to make fraud harder to execute, both nationally and across borders, less financially rewarding, and more likely to result in prosecution and sanction, thereby preserving trust in digital financial services and safeguarding citizens' economic prosperity. Where it occurs, nevertheless, the aim is to minimize losses and other damages, especially to retail consumers.

II. Framework and Scope

The Bangkok Blueprint offers key considerations (KCs) to support jurisdictions in strengthening their response to cyber-enabled fraud. The KCs form a nonprescriptive framework and are intended to guide national policymakers, regulators, financial institutions, financial infrastructures,⁴ and other stakeholders in identifying vulnerabilities within the digital financial ecosystem and in designing comprehensive mitigation strategies. Rather than focusing on individual fraud typologies, the KCs adopt a holistic perspective that examines the drivers and enabling conditions that allow cyber-enabled fraud to grow and evolve. Understanding what distinguishes cyber-enabled fraud from traditional fraud is essential for identifying systemic vulnerabilities and informing the development of effective prevention, detection, and response and recovery mechanisms (Box 1).

BOX 1. Main Characteristics of Cyber-Enabled Fraud

- **Adaptive and agile**—Continuously evolving tactics and techniques, combined with speed and operational flexibility, which allow fraudsters to bypass emerging defenses, regulatory controls, and institutional safeguards.
- **Cross-border**—Exploiting jurisdictional gaps and differences in regulatory frameworks to operate across multiple countries and move funds internationally.
- **Cross-sector**—Exploiting institutional gaps across sectors including financial services, telecommunications, commerce, and digital services.
- **Convergence with other serious crimes**—Cyber-enabled fraud networks frequently converge with other forms of serious and organized crime, including drug trafficking, human trafficking, and other predicate offenses, often sharing infrastructure, actors, and laundering channels (see Box 2).
- **Multichannel**—Blending digital and physical vectors such as SIM swaps, social media impersonation, phishing campaigns, call center scams, and the use of cash-out agents.
- **Scalable**—Organized, automated, and mass-oriented attacks capable of targeting large numbers of victims simultaneously.
- **Real-time**—Exploiting instant and 24/7 financial infrastructures to minimize detection windows and accelerate the movement of funds, assets, and the theft of personal and sensitive information.
- **Facilitated by interconnectedness**—Leveraging interconnected financial systems, platforms, and institution-hopping strategies to accelerate fraud execution and obscure transaction traces.
- **Technologically driven**—Using advanced tools such as bots, artificial intelligence, malware, spoofing kits, and automated scripts to enhance reach and sophistication.

⁴ For this report, the term “financial infrastructure” refers to the set of institutional, legal, operational, and technical arrangements that support the provision of financial services, including financial market infrastructures and payment systems. This broader concept is used to distinguish it from the established CPMI-IOSCO definition of a financial market infrastructure.

- **Data-driven**—Relying on leaked, stolen, or purchased data to identify victims, personalize attacks, and increase the likelihood of success.
- **Commercialized**—Fraud infrastructure, services, and tools are available for purchase and hire (for example, Fraud as a Service—FaaS), enabling the assembly of fraud operations ranging from one-person rudimentary plans to highly sophisticated operations run by transnational organized crime networks or automated systems.

Source: Authors

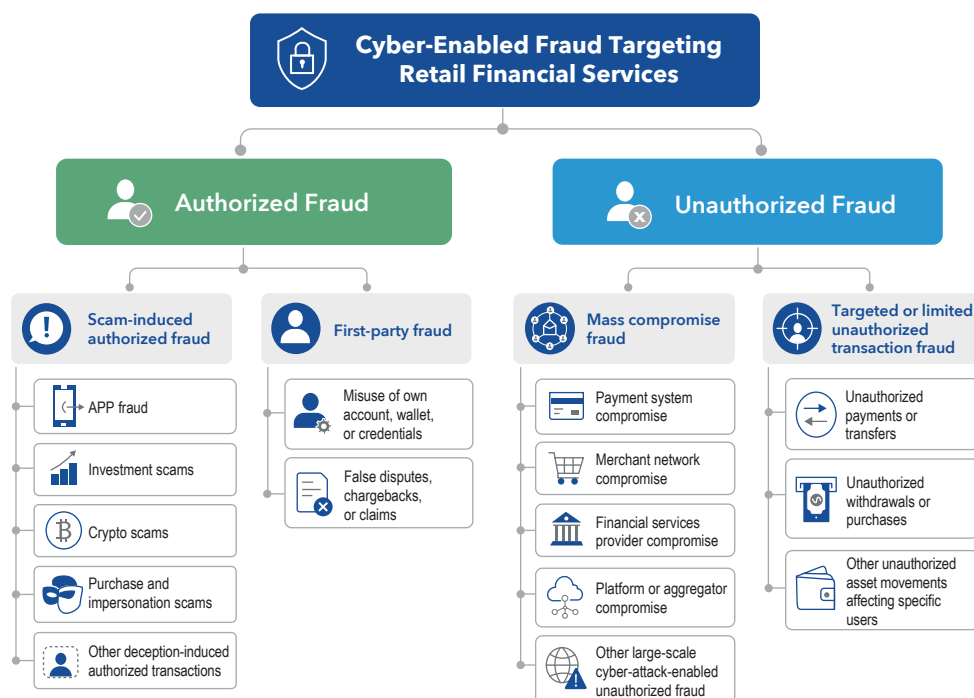
The scope of the KCs addresses a range of cyber-enabled fraud activities across the domestic and cross-border financial ecosystem. The KCs focus on fraud plans targeting users of retail financial services, including individuals and businesses, as well as financial assets accessible through digital financial services such as bank deposits, e-money balances, crypto assets, and other instruments. These plans span a wide range of transaction values and time horizons, from high-frequency, low-value attacks conducted at large scale to plans targeting smaller groups or individuals involving larger amounts. They frequently rely on a combination of digital interfaces and physical access points such as ATMs, agent networks, and intermediaries to extract and disperse funds and assets, obtain personal and other sensitive data, or launder the proceeds of fraud through the financial system.

Cyber-enabled fraud targeting retail financial services can be classified into two broad categories: authorized fraud and unauthorized fraud (Figure 1). Authorized fraud includes cases where the user or legitimate account holder formally authorizes the transaction or financial action, including scam-induced authorized fraud and first-party fraud. Unauthorized fraud covers cases where the user or legitimate account holder did not authorize the transaction or financial action, including mass compromise fraud and targeted or limited unauthorized transaction fraud. The typology is intended to clarify the scope of the KCs while recognizing that specific techniques such as phishing, credential compromise, malware, SIM swaps, social engineering, or account takeover may operate as enabling methods across different fraud types.

The KCs recognize the interlinkages between cyber-enabled fraud, cyber incidents, and money laundering, as well as the central role of financial consumer protection, awareness, and empowerment since fraud directly targets and harms users. Cyber-enabled fraud centers on the manipulation or deception of users of financial services to extract funds, assets, and personal or other sensitive data from victims. Its distinct technological, institutional, and operational characteristics, and involvement of transnational criminal organizations in some cases, allow cyber-enabled fraud plans to evolve rapidly and operate across sectors and countries. Cybersecurity incidents typically focus on system or data compromise, whereas money laundering focuses on the legitimization of criminal proceeds, including cyber-enabled fraud (Box 2).

The KCs are designed to cover both institutional and functional perspectives and to capture the typical stages of a cyber-enabled fraud incident from the fraudster's and the fraud-mitigation angles (Figure 2). The "fraud life cycle" describes how fraudulent plans are carried out and where opportunities for intervention exist to prevent, disrupt, or limit financial harm. The "mitigation life cycle" helps authorities, financial institutions, and other stakeholders address risks across the fraud life cycle, from reducing exposure and fraud attempts to containing harm once fraud has occurred.

Figure 1. Cyber-Enabled Fraud Typologies Targeting Retail Financial Services



Source: Authors

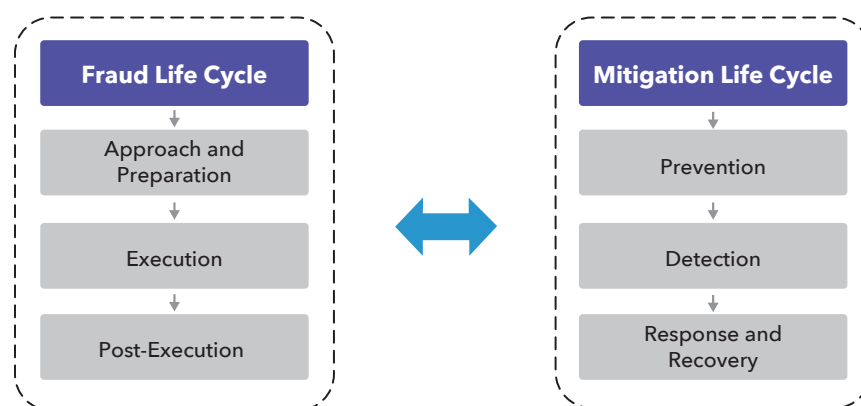
BOX 2. Cyber-Enabled Fraud's Relationship with Cyber Incidents and Money Laundering

- Cyber Incident.** Cyber-enabled fraud may stem from a cyber incident that adversely affects the cybersecurity of an information system or the information the system processes, stores, or transmits, whether resulting from malicious activity or not. Cyber incidents may enable the unauthorized extraction of funds or support fraud preparation through the exposure of sensitive data, with breaches resulting in compromised credentials, account takeover, or manipulation of authentication processes that may lead to fraudulent transactions. In other cases, exposed personal or financial information such as email addresses, phone numbers, or account details can later be used for targeted social engineering or credential harvesting. As a result, weaknesses in cyber hygiene can facilitate both the preparation and execution of cyber-enabled fraud.
- Money Laundering.** Most proceeds of fraud and related criminal activities are laundered, that is, their criminal origin is concealed. Considering that fraud has become one of the dominant proceeds-generating predicate offenses globally, fraud-related money laundering is a critical threat; a broad set of anti-money laundering/combating the financing of terrorism measures, set out by the Financial Action Task Force Standards, should therefore be implemented to prevent it. This includes measures imposed on private sector entities (notably financial institutions) such as customer due diligence, payment transparency requirements, or transaction monitoring that

aim at preventing financial crimes, notably by shedding light on whose behalf a transaction is made or received and why. It also includes requiring transparency over the beneficial owners of legal persons and arrangements and introducing alignment-check obligations for cross-border payments. In addition, rapid payment-suspension and freezing mechanisms are necessary to intercept fraud proceeds before they disperse. All anti-money laundering/combating the financing of terrorism measures are essential to an effective preventive framework. Although primarily aimed at preventing and combating money laundering and terrorist financing, they assist in the prevention of any financial crime, including fraud. For example, when appropriately implemented, they enable suspicious activities and transactions to be identified and stopped, whereas when they are not properly implemented, it becomes easier for criminals to commit crimes, including fraud (for example, by enabling the creation or use of mule accounts or front companies) and rapidly move stolen funds across institutions or jurisdictions to escape law enforcement action.

Source: Authors

Figure 2. The Cyber-Enabled Fraud and Mitigation Life Cycles



Source: Authors

A. The Fraud Life Cycle

- **Approach and Preparation.** Fraudsters form the intent to commit fraud and establish the conditions for execution prior to the initiation of any financial transaction or personal and sensitive data theft. This phase involves activities aimed at enabling future fraud by gathering information, compromising access, or positioning the attacker to execute fraudulent actions, even though no funds have yet been moved.
- **Execution.** Fraudsters attempt or carry out a fraudulent transaction, resulting in the initiation or transfer of funds or assets within the financial system. This phase may include unsuccessful attempts that are detected or interrupted, as well as transactions that are fully executed.
- **Post-Execution.** If the fraud is successful, fraudsters may instantly withdraw the proceeds or seek to conceal them (for example, transfers across multiple accounts, institutions, and jurisdictions, including through the use of intermediaries such as money mules), including through complex money laundering

plans, or convert the funds into other assets (for example, real estate, crypto assets, and so on). The immediate fraud-mitigation priority is to block the proceeds before they can be extracted or laundered through the financial system.

B. The Mitigation Life Cycle

- **Prevention.** Authorities, financial institutions, financial infrastructure operators, digital platforms, telecommunications operators, and other stakeholders take measures aimed at reducing exposure to fraud and lowering the likelihood that fraudulent activity can be initiated, executed, or perpetrated at scale. This includes ensuring that only authorized financial service providers can provide, promote, or distribute financial services to the public, including through third parties such as advertising platforms, social media platforms, app stores, affiliates, influencers, and AI agents. This stage includes actions to strengthen protections across access points and products, public information campaigns, including financial literacy efforts, as well as efforts to disrupt known fraud networks, patterns, and enabling structures before harm occurs. It includes AML/CFT as well as anti-fraud measures.
- **Detection.** Continuous surveillance is necessary to identify suspicious financial activity across the entire fraud life cycle. Detection may occur (i) before the execution stage, through identification of preparatory signals such as anomalous access or behavior; (ii) during execution, through real-time monitoring of transaction initiation; or (iii) post-execution, through system-level alerts or user reporting when unauthorized transactions are discovered.
- **Response and Recovery.** Stakeholders need to take immediate action after the detection of a fraud event—suspected or confirmed—to contain harm, address financial exposure, support investigation, enable remediation and recovery, resolve consumer redress and liability outcomes, and initiate law enforcement action, including investigation, prosecution, and asset recovery.

III. Key Considerations

The Blueprint does not establish a prescribed sequence or priority order for implementing the key considerations (KCs). Its five pillars and KCs are all important and mutually reinforcing (Figure 3). In practice, however, countries may wish to begin by conducting a risks and gaps assessment regarding the nature and scale of cyber-enabled fraud risks, existing institutional mandates and capabilities, gaps across the fraud-mitigation life cycle, and the roles of financial and nonfinancial actors. This assessment could inform the establishment of a national strategy and the necessary legal and institutional foundations, which provide the basis for assigning responsibilities, prioritizing reforms, and sequencing the remaining measures.

In implementing the KCs, national authorities are encouraged to adopt a contextual approach that accounts for local conditions. This is important because institutional, legal, and regulatory frameworks, the risk and extent of cyber-enabled fraud, and the structure of the digital financial ecosystem typically differ across countries. Consequently, high-level commitment and leadership are essential to coordinate across mandates spanning financial stability, financial and market integrity, financial inclusion, consumer protection, and public safety, and collectively identify and address gaps, for example, through a national-level committee.

Figure 3. The Bangkok Blueprint to Address Cyber-Enabled Fraud



Source: Authors

A. Establish Strategic and Legal Foundations

KC1—Establish a Comprehensive National Strategy for Fraud-Resilient Digital Finance

Establish a comprehensive national strategy to address cyber-enabled fraud, grounded in the current and evolving risk environment and backed by high-level ownership, accountability, and a clearly designated lead entity. The strategy sets out clear goals and measurable objectives, and aligns with broader public policy objectives and strategies. It outlines governance and collaboration arrangements, an action plan, and clearly assigned responsibilities supported by adequate legal mandates. In addition, it includes public communication, monitoring, and evaluation mechanisms.

Reflect cyber-enabled fraud risks across the ecosystem and align the strategy with broader public policy objectives. An effective strategy sets out clear goals, relies on evidence-based analysis—underpinned by robust data collection (Annex 2), including statistics, incident reporting, and intra- and inter-sector-wide information sharing (for example, between telecommunication companies and financial institutions). It needs to be supported by regular assessments of the level and nature of cyber-enabled fraud risk. High-level ownership of the strategy and accountability for its implementation require measurable objectives, recognition of potential trade-offs among policy goals (Box 3), specifying the acceptable level of fraud risk, and mechanisms for tracking progress over time.

Align the strategy with broader policy objectives. This includes alignment with policy objectives for preserving financial integrity and stability, maintaining trust in the currency and digital payments, supporting innovation and efficiency in payments, protecting consumers, and promoting financial inclusion. To ensure policy coherence, these objectives should be reflected in and coordinated with national strategies and action plans addressing crime, anti-money laundering/combating the financing of terrorism (AML/CFT), cybersecurity, economic growth, and digital innovation.

Incorporate governance arrangements and a collaborative multistakeholder approach with a clearly designated lead entity. Effective governance arrangements define roles and responsibilities for prevention, detection, response, and recovery. Given the intra- and inter-sector-wide and multistakeholder nature of fraud and scam mitigation, a clearly designated lead entity should coordinate the development, implementation, and monitoring of the national strategy, ensuring accountability and alignment across stakeholders. Senior representation from all relevant public and private sector organizations—supervisors, financial intelligence units, data protection agencies, telecommunications operators, public and private sector associations, financial infrastructure operators, and financial institutions—can help ensure delivery of the strategy and promote cooperation between private and public stakeholders domestically and across borders. This includes efforts to reduce incentives for criminals to commit fraudulent acts, including by recovering the illicit proceeds.

Set strategic expectations for coordinated action and data and information sharing across agencies, sectors, and jurisdictions to help avoid a fragmented approach. The strategy applies to all financial institutions, both regulated and nonregulated, proportionally. The responsibilities of digital platforms, including social media, telecommunications operators, and other relevant nonfinancial entities, also need to be clearly articulated across the prevention, detection, and response continuum. Where comprehensive governance arrangements are not yet established, individual stakeholders may nevertheless incorporate relevant good practices and implement appropriate prevention, detection, response, and recovery measures within their respective mandates while broader coordination mechanisms are being developed.

Set out a dedicated action plan and identify the key tools and resources needed to tackle cyber-enabled fraud. Equally important is a dedicated action plan, with clear stakeholder accountability and a timeline for review and progress assessment, as well as a framework for monitoring and evaluation to periodically track progress against measurable objectives. To enable the execution of the action plan, the strategy identifies tools and resources, including risk-management frameworks, crisis management playbooks, intelligence-sharing systems, transaction-monitoring capabilities, consumer awareness campaigns, and specialized expertise needed to deliver on the action plan. It explicitly accounts for fast-evolving technologies, such as artificial intelligence, ensuring that skills, resources, knowledge, and IT capabilities can be upgraded in line with technological developments.

BOX 3. Digital Finance and Cyber-Enabled fraud: Examples of Trade-Offs

Policymakers need to find the right balance in the trade-offs between promoting innovation, managing the different levels of risk, and issuing regulation. Innovation in digital financial services such as digitalization, fast payments, and the use of new technologies brings efficiency by lowering costs, increasing speed and accessibility, and increasing user convenience (for example, real-time transactions, personalized services). It may support financial inclusion and deepening and should be encouraged and supported by policymakers. At the same time, the same features that drive efficiency—speed, scale, automation, and cross-border reach—also expand the attack surface for cyber-enabled fraud. Insufficient safeguards to accompany emerging innovations can erode trust, generate consumer harm, and create operational and financial stability risks. Overly restrictive rules can reduce efficiencies, slow adoption, fragment markets, and undermine inclusion. Therefore, the right balance lies in designing rules adapted to the risk and proportionate to the business model, complexity, and size of the regulated entity, which, at the same time, do not stifle useful innovation. Such trade-offs are carefully balanced in the context of each key consideration in the Bangkok Blueprint, as illustrated by the service offerings in the following examples.

Example 1: Digital Payments

Digital payments demonstrate this balance clearly. Their growing ubiquity has made them central to commerce, public services, remittances, person-to-person transfers, merchant payments, and access to broader financial services for households and firms. Across many markets, digital payments are also converging toward 24/7 availability, faster processing, and near-instant or instant crediting of funds to beneficiaries. These features improve convenience, liquidity, competition, and inclusion, but they also compress the time available to detect, stop, or recover fraudulent transactions, particularly where payments are final or difficult to reverse once executed or settled. This can make social engineering scams, authorized fraud, account takeover, and other unauthorized fraud more damaging.

Policymakers, supervisors, financial infrastructure operators, and financial services providers therefore face choices over how much friction to introduce, such as transaction limits, confirmation or verification of payee, risk-based warnings, delayed transaction authorization or crediting for high-risk payments, stronger authentication, or real-time transaction screening, without undermining the efficiency and accessibility that make digital payments valuable. Regulatory responses increasingly emphasize shared responsibility among payment service providers, financial infrastructure operators, merchants, other ecosystem actors, and users, alongside real-time monitoring, information sharing,

clear liability rules, and recovery mechanisms that respect payment and settlement finality. The goal is not to slow digital payments but to embed fraud resilience into their design, governance, operation, and oversight (World Bank n.d.).

Example 2: Crypto Assets

Crypto assets push the trade-off further by combining innovation potential with elevated and novel risks. Digital ledger technology can lower barriers to entry, enable programmability, and facilitate cross-border value transfer, but pseudonymity, price volatility, weak governance, and lack of regulation in some jurisdictions have made crypto assets attractive vectors for fraud, scams, and illicit activity. Policymakers must weigh the innovation benefits against consumer protection, market integrity, and financial stability risks. Regulatory approaches increasingly focus on perimeter clarity—determining which activities and intermediaries fall under regulation—while applying technology-neutral standards for disclosure, custody, operational resilience, and anti-fraud controls. Here, as in digital payments, the objective is not to suppress innovation but to ensure that related gains do not come at the expense of trust and systemic safety. The international anti-money laundering/combating the financing of terrorism standards were amended in 2018 to cover crypto assets (virtual assets) and virtual assets service providers, to address the growing threat of their use for money laundering purposes, including to launder the proceeds of fraud. A number of countries are, however, still lagging in the implementation of the FATF Standards, and other international recommendations and guidance in this area, such as the International Organization of Securities Commissions (IOSCO) Crypto and Digital Assets Recommendations, Financial Stability Board (FSB) framework for crypto assets and stablecoins, Committee on Payments and Market Infrastructures and IOSCO Application of the Principles for Financial Market Infrastructures to stablecoin arrangements (CPMI-IOSCO 2022), and FATF’s guidance on stablecoins and unhosted wallets (FATF 2026c) and offshore virtual assets service providers (FATF 2026d). Numerous cases highlight how criminals exploit these regulatory gaps to launder proceeds of fraud involving crypto assets. Countries should implement international standards and requirements without delay.

Source: Authors

Assess whether existing legal mandates and operational capabilities are sufficient to deliver the strategy’s objectives and resulting actions and identify any necessary reforms. Such powers and capabilities cover regulation, supervision and oversight; sanctioning measures; collection and sharing of statistical data, incidents, and vulnerabilities; collaboration and information sharing (for example, Memorandums of Understanding for information sharing and incident management); the governance and cost-sharing of shared fraud utilities,⁵ and customer liability arrangements. Given the complex and fast-evolving nature of the risks, it is important that the national strategy call for a flexible and adaptive approach.

⁵ Fraud utilities refer to centralized or shared capabilities that support fraud prevention, detection, response, and recovery across multiple institutions or sectors. These may include shared fraud intelligence databases, transaction risk monitoring tools, centralized or federated scoring capabilities, mule account or scam account registries, and shared anti-scam centers that enable coordinated analysis, alerts, escalation, and action against fraud threats.

Include a plan for effective public communication on cyber-enabled fraud in the strategy. Public communication should be treated as a strategic and operational pillar of fraud mitigation, supporting prevention, rapid response, consumer empowerment, and trust preservation across the financial ecosystem. This can be achieved through formal public communication channels, with a strategic approach to consumer protection, awareness, and behavioral interventions, including coordination across sectors.

KC2—Establish a Sound Legal, Regulatory, and Supervisory Framework for Cyber-Enabled Fraud

Establish a robust legal, regulatory, and supervisory framework for cyber-enabled fraud that gives authorities the necessary powers, including a legal basis for liability allocation, adequate financial consumer protections, and expedited powers for information sharing and for freezing and recovering fraud proceeds while observing a risk-based, proportionate, and adaptable approach.

Establish robust legal mandates as a critical foundation to combat cyber-enabled fraud. The law should provide relevant authorities with the necessary regulatory, supervisory, and enforcement powers needed to act swiftly, with mandates that are clear and adequate to ensure that evolving fraud practices do not create gaps, including where risks arise outside their traditional remit. Legal reform may be required to enable existing authorities, or newly designated authorities, to take effective action against entities beyond the financial sector whose activities may contribute to fraud risk, such as technology service providers supporting critical financial services (for example, telecommunications, infrastructure, cloud, data processing, and web hosting).

Integrate fraud measures into supervisory frameworks through targeted reforms, particularly in jurisdictions where cyber-enabled fraud is treated solely as a criminal issue, and supervisors lack explicit authority to address it. Where cyber risk is recognized in prudential requirements but not as a trigger for supervisory intervention, additional tools may be warranted, particularly for fraud-enabled incidents that could impair the continuity of critical financial services and jeopardize financial stability. Further, authorities may wish to assess whether financial consumer protection frameworks provide adequate tools to address cyber-enabled fraud and protect and support victims.

Provide a clear statutory basis for allocating liability for fraudulent transactions. In addition to providing effective consumer redress mechanisms, the law should set a clear basis for allocating liability among financial institutions, customers, and technical service providers. The latter will provide courts with clear parameters for the exercise of their judgment, thereby avoiding inconsistent outcomes, unpredictable timelines, and heightened uncertainty—particularly in cases where customers were manipulated but technically authorized the contested payments. At scale, this legal uncertainty could result in significant financial losses, instability, and erosion of trust in the financial system.

Set out information-sharing gateways for cyber-enabled fraud in the legal framework. Privacy is a fundamental human right, and the protection of personal data is enshrined in the laws of most countries. Data protection agencies play a key role in ensuring the balance between protecting personal data and maintaining public interests, such as crime prevention and national security. Many countries have specific gateways or safe harbors for sharing data and information, including between private sector institutions. However, these are often underused because of a lack of clarity and limited incentives to share information for fraud prevention, detection, response, and related anti-money laundering efforts. Authorities should explore whether additional or clearer information-sharing gateways between private sector institutions are needed. These gateways need to clearly set out what information can be shared, the level of granularity of information (such as individual, sectoral, or aggregate), and under what circumstances, while protecting

private data as much as possible. Where such gateways already exist, authorities should explore what more can be done to ensure they are fully used.

Strengthen legal powers to expedite the freezing, seizure, and recovery of fraud proceeds. The inability to swiftly freeze, recover, or confiscate such proceeds can result in irrecoverable financial losses for victims as well as magnify contagion effects by weakening confidence in the system. This risk is magnified in legal regimes where the judicial processes are slow, or the legal definitions of recoverable assets in a digital setting are narrowly drafted. Legal reforms can be designed to grant authorities expedited powers, such as allowing the timely freeze or seizure of crypto-asset and other digital asset proceeds after a ransomware-linked cyber-enabled fraud to prevent systemic disruption, as has proven effective in some jurisdictions. Another reform involves the mutual recognition of freezing orders across borders, allowing authorities to rapidly immobilize fraud proceeds in cross-border digital accounts. Finally, laws, regulations, and program rules governing the functioning of payment systems should support fraud prevention and detection, and recovery of fraud proceeds, with adequate safeguards to avoid disrupting the efficient operation of the payment system.

Apply a risk-based, proportionate, and adaptable approach to supervising fraud risks. Financial supervisory authorities need a robust legal framework that enables them to develop new approaches to engage and monitor entities that do not fall under their remit and to enhance coordination with nonfinancial supervisory agencies. Setting up voluntary agreements with these entities that are risk-based and proportionate can pave the way for better prevention outside the regulatory perimeter. These agreements can, for example, require documented policies, procedures, metrics, and targets for combating cyber-enabled fraud. The supervisory approach should be flexible enough to respond to a continuously evolving cyber-enabled fraud landscape, supported by sufficient resources and capabilities.

Incorporate procedures in supervisory processes for assessing how financial institutions identify, measure, monitor, and mitigate cyber-enabled fraud risks and resulting consumer harm. Annual review, certification, reporting, and recordkeeping may serve as evidence of compliance. Publishing the results of dedicated assessments of regulated entities' anti-fraud systems can help disseminate best practices. Supervisors are encouraged to train their staff in areas such as digital finance, data analytics, cyber-enabled fraud, and cybersecurity. It is important that the supervisory process include specific procedures aimed at, for example, assessing fraud loss metrics and data; customer complaint volumes and narratives; fraud-detection model performance, validation, and documentation; and how financial entities mitigate the risk of mule accounts.

B. Strengthen the Fraud-Mitigation Life Cycle

KC3—Build Cyber-Enabled Fraud Resilience in Financial Products and Services Design

Mitigate cyber-enabled fraud through accessible, proportionate, and continuously adaptive safeguards embedded in the design of digital financial services.

Establish minimum risk-based fraud-mitigation standards for safe and trusted financial services. To guide the design of financial services, authorities may consider defining and enforcing minimum risk-based fraud-mitigation standards for financial services, financial infrastructures, and access points, and establish clear criteria for assessing compliance. These standards could:

- Support secure onboarding and trust frameworks (Garcia Rabadan and others 2026) to reduce impersonation, mule account risks, and unauthorized access.
- Set out the types of preventive measures expected, such as in-app transaction authentication, alerts, verification of payee, and real-time fraud transaction screening.
- Support adequate intervention and recovery measures while respecting payment finality, privacy, legal certainty, and other applicable legal constraints, particularly in systemically important financial infrastructure.
- Differentiate requirements for the service, infrastructure, or access point based on its nature, role, risk profile, and potential systemic impact.
- Require providers to use relevant and up-to-date fraud-risk signals that increase security without incorporating end-user friction, such as behavioral anomalies, and apply appropriate safeguards or interventions.
- Ensure that business models do not weaken fraud controls or externalize risk by, for example, excessively prioritizing customer experience over fraud prevention.
- Ensure that fraud-mitigation measures are designed and implemented in a way that is proportionate and accessible, so that stronger controls do not unnecessarily impair the customer experience and exclude or disadvantage low-income, low-literacy, older, or otherwise vulnerable users.

Account for system-wide fraud risks in the design of financial services. Authorities play a key role in ensuring that fraud risks arising from ecosystem integration are mitigated, including those linked to delegation third-party service models, and interconnection to financial infrastructure. Innovation across the financial system should incorporate fraud-risk considerations from the outset and can be permitted only when they embed adequate fraud-mitigation capabilities. The use of agentic AI in financial services is one example, as it could pose novel or heightened fraud risks, including unclear user boundaries, compromised or opaque agent behavior, and insufficient authorization for high-risk actions.

Safeguard user access points and key enablers to reduce fraud exposure. This includes identifying and safeguarding user access points that materially affect fraud risk, including those directly managed by financial service providers, such as mobile and internet banking, wallets, ATMs, agents, branches, and customer service channels, as well as key enablers outside their direct control, such as multi-issuer wallets, telecommunications services, devices, operating systems, and application marketplaces. Authorities and providers should ensure that access points and enabling channels used for financial services, such as calls, SMS, and messaging links, are used only by authorized financial service providers or by parties acting under their mandate. Where digital ID, authentication, onboarding, or other trust services support financial services, authorities should ensure they reinforce fraud mitigation and have adequate security safeguards.

Treat basic fraud mitigation as part of safe digital financial service provision, not as optional protections charged separately to end users or merchants. Authorities determine the minimum fraud-mitigation capabilities that need to be embedded in digital financial services to enhance security, support usage, and promote adoption. The cost of these basic capabilities (including fraud utilities) should not be borne by the end user but could be shared among relevant providers, ecosystem participants, and authorities in a transparent, proportionate, and risk-based manner that does not undermine policy objectives such as financial inclusion and competition.

KC4—Implement Collaborative and Adaptive Fraud Prevention

Implement prevention as a preemptive, coordinated, and financial system-wide function that identifies vulnerabilities early, adapts to emerging threats, and actively disrupts fraud actors and networks.

Operate fraud prevention as a coordinated, financial system-wide function. Extend this approach beyond defensive controls to actively target fraud actors, networks, and enabling structures. Preventive measures should limit the ability of fraudulent actors to establish legitimacy, including through mule accounts or fake providers, and to initiate transactions, or scale abuse through proportionate preventive safeguards. This includes ensuring that public-facing platforms and access channels make clear whether a provider, service, or access channel is authorized and meets applicable fraud-mitigation standards. Authorities should also support implementing timely and scalable procedures to take down fraudulent sites, ads, apps, and offers. These measures should be reinforced by risk-based coordinated escalation and automated preventive responses that operate in real-time across institutions, financial infrastructures, and relevant third parties.

Prioritize strong prevention frameworks for scams, including authorized push payment fraud, and other fraud involving transactions authorized by users. Authorities should address fraud risks where customers are correctly authenticated and transactions formally authorized, but induced through deception, manipulation, and coercion. Preventive safeguards should identify elevated fraud risk before execution and apply proportionate interventions, such as warnings, confirmation steps, cooling-off periods, assisted review, or temporary transaction delays. These safeguards should be designed to prevent or interrupt illegitimate transactions, not merely transfer liability to end users through disclosures or formal acknowledgments.

Tailor preventive safeguards to the risk profile and capability of users for effective and inclusive fraud prevention. Authorities and providers should ensure that preventive measures against fraud are adapted to different user segments and levels of vulnerability to manipulation or misuse, such as elderly users, first-time users, users with low digital literacy, and users operating under stress, urgency, or coercion, as the same product design may not provide equivalent protection for all users. These preventive measures may require differentiated design features, warning messages, transaction limits, confirmation steps, and dedicated assisted channels while preserving product usability and financial inclusion.

Leverage shared preventive infrastructure where institution-level controls are insufficient. Authorities should determine where effective fraud prevention requires shared arrangements, in addition to institution-level controls, because some individual providers may not have the resources or access to system-wide data to provide the appropriate level of protection. Where needed, authorities should support shared fraud utilities or centralized services that strengthen prevention across the financial system, such as shared authentication services, identity infrastructure, fraud intelligence platforms, confirmation or verification utilities, central fraud registries, anti-scam centers, or infrastructure-level controls. Funding and pricing for shared infrastructure should be transparent, proportionate, and subject to appropriate oversight, so that it supports policy objectives such as trust, competition, and financial inclusion without becoming a bottleneck or shifting costs disproportionately to smaller providers, merchants, or end users.

Strengthen the fraud resilience of common provider access points to reduce system-wide exposure and prevent fraud from scaling across the ecosystem. Authorities should focus on reducing system-wide exposure to fraud rather than shifting risk within the ecosystem. This includes shared or public-facing channels, interfaces, and infrastructure that may be used by multiple providers, customers, or noncustomers

to execute financial activity, such as POS terminals, QR acceptance points, multi-issuer wallets, and cash-in and cash-out channels. Authorities and providers should jointly identify and eliminate access points with low fraud-mitigation capacity across financial and nonfinancial service providers.

KC5—Build a System-Wide Fraud-Detection Architecture

Build a system-wide detection architecture for cyber-enabled fraud, combining institution- and ecosystem-level monitoring through enabling protocols, structured data sharing, and collaborative analytics.

Coordinate real-time fraud detection to identify, escalate, and respond to threats across the financial system.

Authorities should consider requiring and overseeing system-wide detection architectures and protocols to support the real-time and automated detection of fraudulent activity to support interruption, timely escalation, and coordinated response against fraud. This would require financial institutions to monitor, risk-rate transactions, and report fraudulent activity to authorities and other counterparts as part of their fraud prevention functions. This entails financial institutions, financial infrastructures, and relevant third parties maintaining proportionate detection capabilities at both institution and system levels. To avoid fragmentation, detection responsibilities would need to reflect each entity's role, visibility, and responsibility over delivery of financial services.

Treat detection as a continuous function that supports the fraud-mitigation life cycle. Detection ideally should intercept and escalate suspicious activity before fraud occurs to support early intervention and prevention. It incorporates end-user inputs such as transaction confirmation, behavioral validation, or contextual verification, as well as cybersecurity-related fraud-risk indicators. Insights from incidents should inform preventive actions and controls. Detection supports rapid containment, remediation, and recovery by generating actionable intelligence, such as fraud typologies, common enablers and access points, transaction paths and beneficiary relationships, and time-critical recovery opportunities.

Apply proportionate and adaptive ecosystem-level analytics for fraud detection. Authorities should consider requiring detection architectures to support data aggregation and analysis across providers, infrastructures, and relevant sectors to identify cross-institutional patterns, coordinated fraud activity, and emerging typologies that individual institutions cannot detect on their own. Centralized or collaborative tools, such as shared analytics platforms and centralized fraud repositories, may be used where appropriate, subject to privacy, data protection, and proportionality safeguards, and where appropriate, shared capabilities should leverage privacy enhancing technologies (PETs).⁶ Detection frameworks should aim to minimize unnecessary disruption to legitimate activity and should be calibrated to account for different fraud typologies and types of financial services. Detection expectations should reflect entity size, role, and systemic relevance to avoid imposing excessive burdens on providers and users.

KC6—Operationalize Coordinated Response and Recovery Mechanisms

Ensure that cyber-enabled fraud incidents are contained rapidly and their impacts limited through effective response and recovery, supported by strong coordination, preparedness, escalation planning, investigation, and standardized incident reporting across relevant institutions, financial infrastructures, and authorities.

⁶ Privacy enhancing technologies are technical tools that enable data to be used, analyzed, or shared while minimizing disclosure of personal or sensitive information.

Ensure rapid and coordinated response, containment, and escalation to limit losses and preserve recovery windows. Establishing and coordinating ecosystem-wide real-time response arrangements is necessary to enable rapid escalation and timely containment of cyber-enabled fraud incidents. This requires predefined, authority-led coordination mechanisms that enable institutions and financial infrastructures to act on shared risk signals in real time. Containment actions need to be executed consistently across participating institutions and infrastructures to prevent delay, fragmentation, or regulatory uncertainty during incidents. Effective response frameworks prioritize speed, containment, and harm limitation, allowing operational measures to be activated based on risk indicators alone, without requiring prior attribution or liability determination.

Promote coordinated contingency planning, escalation, and response protocols for major fraud events affecting end users. Contingency and escalation planning needs coordination across authorities, institutions, financial infrastructures, and relevant third parties to ensure operational readiness during major or systemic fraud events that affect end users. To further limit losses and restore trust, these arrangements should define clear roles and decision-making responsibilities, escalation thresholds, and communication protocols, and enable timely activation of containment, tracing, and recovery measures.

Ensure fraud incident reporting is timely and standardized. Regardless of size or outcome, authorities should stimulate timely and consistent reporting by victims of cyber-enabled fraud to financial service providers. Mandatory reporting obligations for supervised entities need to be complemented by accessible channels for voluntary reporting by end users. Financial service providers need to report incidents to designated competent authorities, including, where applicable, to the financial intelligence unit, financial consumer protection or conduct authorities, financial supervisors, or centralized repositories. Effective reporting frameworks define clear thresholds, standardized data elements, and common classification structures aligned with established fraud taxonomies and typologies. Reported information supports aggregation, trend analysis, and system-wide learning, and helps refine prevention, detection, and response measures. Where appropriate, reporting arrangements align with AML/CFT, cybersecurity, financial consumer protection, and operational incident reporting frameworks while ensuring proportionality, data protection, and confidentiality.

Require proportionate and system-wide recovery mechanisms for fraud losses borne by end users. Recovery efforts are prioritized in a calibrated and risk-based manner, based on recovery feasibility, aggregate harm, recurrence, systemic relevance, the potential to prevent further losses, and the impact on affected users. Recovery arrangements avoid de minimis thresholds that weaken deterrence while applying recovery resources proportionately and effectively. Financial infrastructures, interoperable networks, and critical access points embed tracing and recovery capabilities that operate across institutions and infrastructures, rather than relying only on bilateral arrangements, to identify, immobilize, and recover misappropriated assets.

Establish equitable and swift liability and compensation arrangements to strengthen user confidence and incentivize providers to mitigate fraud risks. Authorities enforce clear liability-sharing arrangements that swiftly determine predictable compensation measures across providers and end users for both authorized and unauthorized fraud, proportionate to responsibility, risk exposure, and conduct. Such arrangements reflect where control, information asymmetries, and risks reside within the design and delivery of financial services. These arrangements are based on a clear and transparent methodology for allocating losses, considering each actor's role and responsibility. End users do not bear fraud losses arising from system vulnerabilities beyond their reasonable control, such as misleading interfaces or design choices. Where other actors materially weaken fraud mitigation, liability may also extend beyond financial service providers.

Where actions or omissions by providers or other relevant actors materially contribute to cyber-enabled fraud or weaken mitigation, liability and compensation arrangements may be complemented by supervisory action or administrative sanctions. These arrangements incorporate safeguards against abuse while preserving fair and timely redress for legitimate victims.

Pursue structured and proportionate fraud investigations after incidents to support accountability, corrective action, and system-wide learning. Structured and proportionate investigations aim to establish how fraud occurred, identify exploited vulnerabilities, assess control failures, and determine whether misconduct, negligence, or systemic weaknesses contributed to the incident. Investigation leadership may be assigned based on each entity's role and visibility across the fraud chain, rather than solely on institutional boundaries. Investigation arrangements should operate in coordination with containment and recovery actions, without delaying time-critical interventions, and support accountability, remediation, liability sharing, and enforcement as appropriate. Outcomes of investigations inform corrective actions across the whole mitigation life cycle.

C. Leverage Existing Risk Mitigation and Enforcement Frameworks

KC7–Strengthen Financial Sector Cyber Resilience

Strengthen cyber resilience across the digital financial ecosystem to protect service providers, infrastructures, and users of financial services from cyber-enabled fraud by ensuring effective cybersecurity regulatory, supervisory, and risk-management frameworks.

Develop and strengthen cybersecurity regulations and supervisory frameworks. Authorities should ensure a legal and regulatory framework underpinning the implementation of regulation and supervision of cybersecurity risks is established and strengthened in line with international standards and sound practices (Wilson and others 2019; Gaidosch and others 2026). Although cyber-enabled fraud is relevant to cybersecurity regulations where it constitutes an information and communication technology-related incident or cyber threat, it should also be considered in the context of operational risk standards (BCBS 2021, 2023).

Safeguard the confidentiality, integrity, and availability of information and information and communication technology systems within relevant entities through cybersecurity regulations. This entails preventing, containing, and responding to cyber incidents, including those related to cyber-enabled fraud, caused by threats such as cyberattacks, data breaches, technology and process failures, human error, or natural or man-made disasters. Cyber-risk supervision should contribute to identifying vulnerabilities to and risks of cyberattacks and aim to strengthen financial institutions' cybersecurity capabilities and resilience, including against cyber-enabled fraud.

Establish and strengthen cybersecurity risk-management frameworks. Supervisory authorities should require and ensure that financial service providers develop and implement a structured approach to identify, detect, and respond to cyber threats, including by identifying and disrupting the tactics, techniques, and procedures used by threat actors. The framework should define, for example, security objectives, roles and responsibilities, and regulatory requirements or supervisory expectations for basic cyber hygiene. The cybersecurity risk-management framework needs to be documented, approved, and periodically reviewed. To be comprehensive, the framework needs to include an appropriate assessment of the cyber resilience

of third-party providers when service providers outsource activities or the provision of digital services to them. Given the interconnection with cyber-enabled fraud, the framework should also incorporate relevant fraud-risk-management measures.

Ensure and strengthen cyber hygiene standards. Financial service providers and their users should preserve the security and integrity of digital devices, networks, and data. Authorities could help establish standards for cyber hygiene, such as mobile banking security requirements and other methods for secure customer authentication to protect infrastructure, including systems, data, networks, and fraud-risk controls to protect transactions and user identities.

Include cyber-enabled fraud in cyber threat assessments and strategic planning. Authorities and providers are encouraged to incorporate developments related to cyber-enabled fraud into their analysis of the broader cybersecurity risk environment. Monitoring may be through direct coverage in regulatory and financial-sector-focused reports or indirect coverage in general threat landscape reports. Authorities may also consider reflecting cyber-enabled fraud in national and sectoral cybersecurity strategies.

Support information sharing for cyber-enabled fraud mitigation. Relevant public and private sector bodies should consider sharing information related to cyber-enabled fraud from Computer Emergency Response Teams (CERTs) or Information Sharing and Analysis Centers (ISACs), where appropriate. Whereas CERTs and ISACs mainly focus on cyber incidents, some focus on the financial sector and support work such as intelligence sharing and development of cyber-enabled fraud-mitigation frameworks for their communities (FS-ISAC 2025). Relevant stakeholders should continue to improve the capacity of these mechanisms to support timely information sharing on cyber-enabled fraud, including by adopting new technologies.

KC8—Leverage the Existing Anti-Money Laundering/Combating the Financing of Terrorism Framework to Address Cyber-Enabled Fraud

Leverage anti-money laundering measures to complement fraud-mitigation measures, bolstering the prevention and detection of cyber-enabled fraud, depriving fraudsters of illegal gains and disrupting those actors, including transnational organized crime groups.

Maintain a robust understanding of the risks of money laundering related to cyber-enabled fraud and take appropriate mitigating action. Pursuant to FATF Standards, countries should assess their money laundering and terrorist financing risks.⁷ This includes understanding which crimes generate the greatest amounts of illegal proceeds and how these proceeds are laundered. Based on their assessment, countries should ensure that appropriate mitigating measures are taken. The risk assessments should also inform private sector entities of the specific fraud threats that they face (including the types of fraud and how they are committed and the proceeds laundered). In particular, financial institutions and other FATF reporting entities⁸ should use the information produced as part of national risk assessment exercises to better detect and prevent fraud and related money laundering, including, for example, by informing red-flag indicators and transaction-monitoring rules.

⁷ FATF Recommendation 1.

⁸ Financial institutions, virtual asset service providers, and designated nonfinancial bodies and professions are collectively referred to as reporting entities, in line with their obligations under the FATF Standards (Recommendation 20) to report suspicious transactions.

Ensure that AML/CFT reporting entities are effectively applying the necessary measures to prevent, detect, and respond to incidents of fraud. Under the FATF Standards, reporting entities are required to implement a range of preventive measures to prevent the laundering of proceeds of crime, such as fraud. These include customer due diligence checks, recordkeeping requirements, payment transparency obligations, and reporting any suspicious activity. Whereas certain specific fraud prevention measures, such as confirmation of payee and in-application transaction verification, are put in place by certain reporting entities to protect themselves against financial loss and reputational damage, AML/CFT preventive measures are more generally focused on preventing financial crime and illicit proceeds from entering and flowing through the financial system. Nonetheless, many of these measures overlap; for example, real-time transaction monitoring can be designed to identify indicators of both money laundering and fraud.

Maintain up-to-date, dynamic AML/CFT systems and controls that evolve with the technologies and techniques used to commit fraud and launder the proceeds. Because of the criminals' ability to adapt quickly and misuse technological advances, reporting entities need to review their systems and controls on an ongoing basis to ensure they remain effective against cyber-enabled fraud. This could, for example, include ensuring that customer identification and verification measures are dynamic and equipped to identify AI-generated photos, videos, deepfakes, and other indicators of fraudulent activity. Although AI has enhanced criminals' ability to commit sophisticated and complex fraud and to launder the proceeds of this activity, it can also strengthen reporting institutions' abilities to respond, for example by assisting their internal investigations into and reporting of suspicious activity.

Ensure that AML/CFT supervisors focus appropriately on reporting entities' effective implementation of cyber-enabled fraud-related AML/CFT systems and controls. Effective risk-based supervision is key to ensure that reporting entities are appropriately mitigating the cyber-enabled fraud and related money laundering risks. For reporting entities exposed to significant risks of money laundering related to fraud, supervisors may consider targeted inspections to assess the quality of the AML/CFT measures most relevant to cyber-enabled fraud prevention depending on the supervised entity's business model. Supervisors may also use horizontal thematic reviews to evaluate financial institutions' controls relating to fraud and money laundering and identify broader lessons for the sector. Given the convergence of fraud and money laundering risks, countries may consider coordination arrangements between AML/CFT supervisors and other bodies involved in cyber-enabled fraud mitigation. In addition, some countries have mandated their AML/CFT supervisors with the responsibility of supervising the implementation of anti-fraud measures, whereas other supervisors have used their existing AML/CFT mandates to assess reporting entities' fraud controls, despite not specifically having fraud prevention as part of their remit.

Fully leverage the AML/CFT framework and other existing tools and platforms to address cyber-enabled fraud. In light of the significant increase in fraud, the FATF is examining how its AML/CFT Toolkit can be applied to mitigate the risks associated with fraud, and intends to convene policymakers, law enforcement authorities, Financial Intelligence Units (FIUs), financial institutions, financial services supervisors, technology companies, telecommunications firms, and social media platforms as part of this exercise. This aligns with the growing recognition of the usefulness and need to increase collaboration with social media platforms, telecommunications providers, and internet service providers to address the threat, through public-private partnerships or other mechanisms. Countries should support efforts to evaluate how existing international frameworks, tools, and mechanisms can be leveraged to better tackle cyber-enabled fraud.

Support cross-institutional information sharing to better detect and report fraud-related suspicious activity. Under the FATF Standards, financial institutions, virtual assets service providers and designated nonfinancial businesses and professions should report details of transactions and funds that they consider may be linked to criminal activity, including fraud, to their national FIU. There is no need for proof of a crime: if the facts, behavior, or pattern gives rise to suspicion, they should be reported. These reports are a key part of the intelligence used by law enforcement agencies to investigate financial crime, including fraud and the laundering of its proceeds. Because anti-fraud and AML measures share similar objectives, some reporting entities, particularly financial institutions, are integrating fraud prevention, cybersecurity, and AML functions to improve detection capabilities and enhance effective suspicious activity reporting. This can also help reduce institutional information silos and assist with methods such as pattern recognition.

Promote information sharing across the private sector to strengthen defenses against fraud and associated money laundering. Information sharing between financial institutions (and private sector entities more broadly) continues to be a challenge, which reduces the effectiveness of prevention and early detection of fraud and associated money laundering. Countries should support private sector efforts to share information, such as anti-fraud consortia and data-sharing platforms, and by clarifying safe harbors for information sharing and providing clear data governance frameworks and protections against civil liability, regulatory sanctions, or confidentiality claims where information sharing occurs to prevent, detect, or respond to cyber-enabled fraud events.

Facilitate cooperation between public and private partners to address fraud and associated money laundering. There are numerous examples of private sector entities (for example, financial institutions and technology companies) supporting AML/CFT authorities and law enforcement to address organized crime and money laundering. Countries should also consider establishing public-private partnerships (for example, anti-scam centers) to address cyber-enabled fraud. These types of arrangements are regularly highlighted as examples of good practice in assessments of countries' AML/CFT frameworks, as they have proven to be particularly useful in closing critical intelligence gaps, enhancing the speed and quality of financial investigations and fostering a culture of shared responsibility between governments and the private sector (FATF 2026b).

KC9—Deter Cyber-Enabled Fraud Through Effective Law Enforcement and Criminal Sanctions

Deter criminals from committing cyber-enabled fraud and related money laundering through effective law enforcement responses, proportionate and dissuasive sanctions, and the recovery of criminal proceeds. Publicizing successful law enforcement actions can strengthen deterrence and demonstrate to the broader public that criminals involved in fraud are being held to account.

Prioritize the investigation of fraud cases that have the greatest impact. The sheer volume of cyber-enabled fraud means that it is impossible for law enforcement agencies to investigate every case of fraud. Most law enforcement agencies need to prioritize resources and balance numerous conflicting priorities. Individual small-scale fraud cases are often unlikely to meet the threshold for investigations but may point to a larger-scale organized criminal activity. Investigations into fraud and associated money laundering should prioritize cases most likely to disrupt transnational organized crime groups and criminal facilitators, including professional money launderers. Law enforcement agencies should ensure they maintain sufficient knowledge and capacity to investigate complex fraud and money laundering plans, including those involving

advanced technology. Asset recovery should be a priority for fraud investigations in order to recover funds, deprive criminals of income, and prevent the financing of other crimes.

Participate in cross-border law enforcement efforts. Because fraudsters often operate across multiple countries, international law enforcement responses are needed. Cross-border operations have delivered significant outcomes in disrupting fraudsters and recovering the proceeds of fraud thanks to rapid intelligence sharing and coordinated interventions.⁹ Mechanisms such as Interpol's Global Rapid Interventions of Payments (I-GRIP) help reduce response times by facilitating the rapid exchange of critical information to allow authorities to halt transactions linked to fraud and prevent the funds from reaching the criminals committing the fraud. This is vital given the need for speed to prevent the proceeds of fraud from flowing across multiple jurisdictions in a short space of time. Countries should support and participate in bilateral, regional, and international initiatives, such as Interpol's Global Taskforce on Scam Centers,¹⁰ as they can bolster information, knowledge, and capacity sharing as well as ensure a stronger and more cohesive response. Initiatives to link anti-scam centers between countries (that is, anti-scam center regional networks) should also be supported, including by international organizations and standards setters.

Apply proportionate and dissuasive sanctions. Criminals convicted of committing or facilitating fraud or the related money laundering should receive sanctions proportionate to the seriousness of the offense. These sanctions should extend to legal persons (for example, shell companies used to promote fraudulent investment plans).

Ensure that the legal framework enables all necessary law enforcement action. Countries are required to ensure that their legal framework aligns with the FATF Standards and relevant conventions. Legal frameworks should also reduce excessive discretion by setting clear investigative powers, procedural safeguards, case prioritization criteria and accountability mechanisms. This helps level the playing field and ensure that all countries' law enforcement agencies have the necessary means to fight fraud effectively. Such means include the power to investigate fraud as well as to conduct parallel financial investigations and prosecution of fraud-related money laundering, as well as to freeze, seize, and recover stolen funds and criminal assets—ultimately also enabling their restitution to the victims of fraud. Countries should also ensure that they effectively sanction all forms of money laundering, including self-laundering and in particular third-party laundering, given that money-laundering-as-a-service is an important enabler of large-scale financial fraud.

Publicize the outcomes of criminal sanctions and enforcement action. Greater publicity of successful interventions deters criminals because it reinforces that there can be significant consequences for individuals and groups involved in cyber-enabled fraud and increases public confidence and trust in competent authorities. Cases involving successful international cooperation can further demonstrate that those targeting victims across borders will be investigated, prosecuted, and convicted.

⁹ For example, Operation First Light, a global police operation spanning 61 countries, led to the seizure of assets totaling \$257 million and disrupted the transnational organized crime networks involved. <https://www.interpol.int/en/News-and-Events/News/2024/USD-257-million-seized-in-global-police-crackdown-against-online-scams>.

¹⁰ Codenamed Operation Shadow Storm, the new task force will combine the intelligence powers of INTERPOL's 196 member countries to take the fight directly to fraudsters. Jointly developed by the UK and INTERPOL, the new unit will target the scam compounds driving a growing share of global fraud, with an initial focus on dismantling criminal operations across Southeast Asia.

D. Expand Domestic and Cross-Border Coordination and Cooperation

KC10—Promote Domestic Collaboration for Cyber-Enabled Fraud Mitigation

Promote systematic, risk-based collaboration between public and private stakeholders that strengthens cyber-enabled fraud mitigation in the financial sector, addresses vulnerabilities originating outside it, and enables rapid coordinated action across the fraud-mitigation life cycle.

Strengthen domestic collaboration and information-sharing arrangements between public and private stakeholders to mitigate cyber-enabled fraud, including relevant stakeholders outside the financial sector.

Authorities should establish and oversee formal collaboration and information-sharing frameworks, within and across sectors, that enable effective fraud mitigation across financial and nonfinancial sectors, including telecommunications, digital platforms, cybersecurity, identity, and law enforcement. These arrangements should clarify the roles and responsibilities for joint actions such as supervision, investigations, disruption, takedown, and recovery. Cross-sector collaboration frameworks should be designed to share pertinent information under proper safeguards, coordinate responsibilities, sequence interventions, and optimize efforts across relevant functions. Governance arrangements should ensure comprehensive and enforceable participation of relevant stakeholders in fraud mitigation, prevent weakest-link vulnerabilities, reduce duplication and conflicting requirements, and remain adaptable as fraud, technologies, business models, and interdependencies evolve.

Extend life cycle-wide fraud mitigation beyond the financial sector through clear responsibility allocation.

Authorities should collaborate to ensure that the fraud-mitigation life cycle is applied across cross-sector interactions and integrations with the financial system, including where fraud leverages nonfinancial services and access points. Authorities should promote a clear allocation of responsibilities whereby nonfinancial entities that embed, enable, or rely on regulated financial services are expected to apply proportionate safeguards aligned with financial sector guidance. Although regulated financial institutions retain responsibility for the safety and integrity of licensed services, nonfinancial actors that enable customer interaction, transactions, or product distribution should implement complementary controls without transferring supervisory or regulatory mandates across sectors.

Use cross-sector tools and intelligence to strengthen fraud mitigation by reducing fragmentation and systemic blind spots.

To support effective mitigation across the fraud life cycle, authorities should promote structured cross-sector collaboration that enhances the effectiveness of financial sector fraud-mitigation tools. This includes enabling financial authorities and regulated entities to use relevant capabilities held outside the financial sector, such as data, indicators and signals, detection capabilities, and threat intelligence, identity misuse signals, consumer complaint data (including from general consumer protection bodies), and law enforcement intelligence on organized fraud activity. These capabilities should be privacy compliant and aim to reduce fragmentation and systemic blind spots while enabling coordinated action. Where appropriate, these exchanges should leverage Privacy-Enhancing Technologies (PET) to preserve confidentiality and data.

Establish the institutional, legal, regulatory, and operational foundations needed to support coordinated fraud mitigation across the fraud life cycle and across relevant sectors. These foundations should:

- Clarify the mandates, powers, responsibilities, and collaboration duties of the different sectors' authorities, including financial, telecommunications, digital platforms, cybersecurity, identity, consumer protection, law enforcement, and other relevant authorities.

- Enable joint action through clear arrangements for collaboration across sectors, as described earlier, as well as for the operational use of shared information, fraud reporting, blocking of abusive communication channels, and action against mule networks.
- Set clear rules for permitted uses of information, access rights, confidentiality obligations, retention periods, liability protections for good-faith reporting, and accountability for misuse.
- Establish common data standards, fraud taxonomies, reporting templates, secure technical protocols, and national or sectoral fraud intelligence platforms, subject to appropriate safeguards, including governance, proportionality, cybersecurity, and privacy-by-design principles.

KC11–Harness Cross-Border Cooperation, Coordination, and Information-Sharing Frameworks

Ensure that cross-border cooperation, coordination, and information-sharing arrangements prevent and mitigate cyber-enabled fraud across jurisdictions.

Leverage and adapt existing international cooperation and coordination frameworks. Existing cross-border frameworks, such as through the Egmont Group of FIUs, and existing law enforcement mechanisms, mutual legal assistance treaties, supervisory cooperation frameworks including multilateral memorandums of understanding among financial and market regulators, as well as prudential, financial consumer protection, and AML/CFT supervisory frameworks provide a foundation for the formal and informal cross-border cooperation needed to combat cyber-enabled fraud.¹¹ To be effective, authorities will need to design and adopt accelerated procedures to support response and recovery in fraud cases where time is of the essence, such as those involving digital payments, including accelerated evidence sharing and coordinated provisional freezing of funds in time-critical payment fraud cases.

Strengthen the operationalization of cross-border cooperation and coordination targeting cyber-enabled fraud. Authorities can build operational cross-border mechanisms on existing cooperation frameworks across the cyber-enabled fraud-mitigation life cycle. This entails:

- Establishing clear legal, technical, and operational arrangements for timely cross-border exchange of fraud intelligence, including typologies, threat indicators, compromised identifiers, beneficiary information, and—where legally permissible—sanitized data (for example, mule account identifiers; see also Financial Stability Board 2024). Legal avenues that clarify permissible information sharing and provide appropriate safeguards and liability protections, combined with PETs, can facilitate secure cooperation and analytics sharing while preserving data security. Automated intelligence exchange and real-time detection at scale benefit from shared taxonomies, reporting standards, and machine-readable formats.
- Embedding consistent fraud-mitigation measures in the design, governance, and operational rules where financial systems are interconnected and enable cross-border financial activity involving end users, such as fast payment linkages or interoperability frameworks. It is key that participating jurisdictions and providers have adequate prevention, detection, response, and recovery capabilities. Divergent rules can create arbitrage and “weakest-link” vulnerabilities across jurisdictions. Alignment

¹¹ Informal cooperation channels in particular, such as the Egmont Group of Financial Intelligence Units (FIUs) and other law enforcement mechanisms, routinely share information related to cyber-enabled fraud, provide real-time cross-institution tracing, and coordinate provisional freezing of funds.

of fraud-mitigation standards and joint governance arrangements is therefore essential to safeguard interconnected financial systems.

- Establishing prenegotiated standing real-time operational protocols for high-risk cross-border payment corridors that enable immediate notification, coordinated transaction tracing, preservation of evidence, and provisional freezing of funds pending formal legal processes. Given the speed of cross-border financial activity, such corridor-specific arrangements are essential to preserve recovery and enforcement windows and prevent irrecoverable loss before traditional mutual legal assistance procedures can be completed.

Enable effective cross-border cooperation and coordination to support consumer redress and criminal enforcement. Cross-border cooperation and coordination is necessary for domestic consumer redress and for enforcement measures to remain effective when fraud spans jurisdictions. This includes authorizing cross-border recognition of claims, implementing compatible reporting channels, and establishing clear allocations of liability, so that victims can access timely redress and recovery mechanisms even when funds have moved across jurisdictions. Effective enforcement actions rely on formal and informal cooperation channels to obtain information and evidence, including reducing barriers that may impede timely tracing and recovery of stolen funds across jurisdictions. Joint investigations into transnational fraud networks and other targeted cooperation should be pursued where appropriate, to strengthen prosecutions. Jurisdictions should cooperate on sentencing and sanctions to reduce the risk that offenders exploit jurisdictional disparities.

Ensure cross-border frameworks are regularly tested, reviewed, and strengthened so they remain fit for purpose. To maintain their effectiveness, authorities should perform simulation exercises to test cross-border frameworks, and address any deficiencies identified through capacity building and technical assistance. Similarly, periodic reviews of cooperation agreements, measuring speed, consumer redress outcomes, and enforcement successes, will help strengthen them as needed in response to evolving threats.

E. Promote Consumer Protection and Resilience

KC12—Strengthen Consumer Protection, Empowerment, and Awareness against Cyber-Enabled Fraud

Strengthen existing financial consumer protection frameworks to ensure they are fit for purpose. Ensure that consumers understand cyber-enabled fraud risks, their rights and protections, and how liability, redress, and remediation arrangements apply when fraud occurs.

Leverage existing financial consumer protections and consider reviewing and revising or clarifying them as needed to ensure they are fit for purpose for cyber-enabled fraud. Existing rules, supervisory tools, complaints mechanisms, redress arrangements, and conduct expectations provide a foundation that can be built upon and updated or clarified as needed to adequately protect consumers from fraud and support victims of fraud. Authorities may wish to assess whether these frameworks offer sufficient tools to address cyber-enabled fraud, including powers relating to fair treatment, disclosure, complaints handling, redress, liability allocation, compensation, and safeguards for vulnerable users. Where frameworks remain confined to traditional misconduct or disclosure-based risks, they may need to be strengthened so that fraud-related consumer risks and harms can be addressed through supervisory and enforcement action.

Anchor fraud-related consumer protection in ecosystem-wide consumer outcomes. Consumer protection arrangements should go beyond information, warnings, and reporting channels to ensure that digital financial services produce safe, fair, usable, and trust-preserving outcomes. Authorities should set expectations for fraud-resilient product design and delivery, supported by evidence from market monitoring, complaints, consumer research, supervisory reviews, and provider governance. This approach should recognize that the consumer journey is shaped by multiple actors across and beyond the financial sector. Fraud-related consumer protection should therefore assess whether the ecosystem as a whole preserves safe access, fair treatment, usable safeguards, effective voice and redress, and continued trust, particularly for vulnerable users.

Address consumer awareness and empowerment gaps in digital financial services. Authorities' consumer empowerment and awareness measures could be enhanced by explicitly addressing fraud risks associated with digital financial services, including features such as transaction irreversibility, high speed, or complexity. These measures also need to consider interface design, choice architecture, and other features that may impair consumers' ability to recognize or avoid fraud (Chang, Duflos, and Chalwe-Mulenga 2026). Consumer empowerment complements, and does not substitute for, provider-side safeguards, fair treatment obligations, and effective recourse arrangements.

Promote end users' understanding of fraud risks in digital financial services. Comprehensive consumer-facing information and education measures support awareness of fraud risks across onboarding, access, product selection, transaction initiation, claims, redress, and post-transaction stages across payments, investment, insurance, credit, digital assets, and other financial services. These measures help consumers understand in plain language how fraud occurs, how attackers exploit urgency, impersonation, or social engineering, and how risk may vary across channels, counterparties, and transaction types. This also includes the provider's responsibility in explaining that a transaction may be validly authorized by the consumer but still be fraudulent when it is carried out under deception, manipulation, or coercion.

Equip consumers to recognize and respond to suspicious activity. Receiving clear, timely, and actionable information is essential for consumers to be able to identify potential fraud and respond quickly before harm occurs. This includes clear and contextual transaction information, effective warnings, and accessible channels to report suspicious activity or seek assistance, as well as clearly communicated options for consumers to pause or interrupt transactions related to authorized and unauthorized fraud. Authorities should ensure that these warnings, reporting channels, and intervention options are also effective for vulnerable consumers, including those subject to coercion, diminished capacity, or heightened susceptibility to social engineering. Authorities and providers may consider a single, nationwide reporting channel that is easy to access, with continuous availability, widely publicized, and able to coordinate with relevant authorities and institutions on the victim's behalf.

Support informed consumer use of available safeguards. Authorities need to ensure that financial institutions, infrastructures, and relevant nonfinancial actors offer consumers understandable, accessible, and usable consumer-facing safeguards, such as transaction alerts, account controls, scam warnings, reporting channels, and liability and redress frameworks. Safeguards should be transparent, clearly communicated, and supported by guidance that explains when and how they apply, what they can and cannot do, and how consumers should engage with them when fraud is suspected.

Enable trust-preserving communication with consumers. It is important that authorities ensure that communication with consumers during and after fraud incidents is clear, timely, and consistent across relevant actors. Effective communication clearly explains the nature of the incident or risk, the actions being taken, and the steps consumers should consider—in a way that preserves trust, reduces confusion, and avoids undue alarm while remaining accessible and inclusive for all consumers. Where fraud has occurred, these communications may be complemented by proportionate post-victim support aimed at helping affected consumers regain confidence in digital financial services.

Enhance consumer empowerment and awareness measures through continuous evaluation and improvement. To determine their continued effectiveness, authorities need to ensure that consumer-facing empowerment and awareness measures are subject to evidence-based, periodic evaluation. This may include user testing, behavioral analysis, focus groups, surveys, complaints data, and other relevant evidence. Effectiveness assessments should focus on whether measures genuinely support informed decision making and timely intervention among diverse user groups, rather than on formal compliance alone. Assessments should consider not only awareness levels but also whether consumers can successfully exercise their rights, access safeguards, and obtain timely assistance and redress when fraud occurs. Findings from these assessments need to be used to refine and strengthen consumer empowerment and awareness measures over time.

Annex 1. Cyber-Enabled Fraud Definition and Lexicon

International bodies have developed related definitions and typologies to better capture the evolving nature of digital fraud, support impact assessment, and inform policy responses. In financial services, cyber-enabled fraud refers to the use of digital technologies and psychological manipulation to obtain illicit gains, whether through authorized or unauthorized transactions, and involving actors within or outside the financial sector. Although terms such as digital fraud and online scams are used interchangeably, the Bangkok Blueprint adopts the term cyber-enabled fraud in line with usage by international standard setters like the Financial Action Task Force and well-established classification plans for the United Nations Office on Drugs and Crime (UNODC).

This lexicon comprises a set of core terms related to fraud, digital fraud, and cyber-enabled crime. It is intended to reference and support the work of relevant international standard-setting bodies, authorities, and stakeholders. The lexicon includes the following terms and definitions:

Term	Definition
Cyber-Dependent Crime	Offenses that target a computer or a computer system. These crimes can only be committed through an ICT infrastructure and are often criminalized as unauthorized access to, interception of, interference with, or misuse of computer data or computer/information systems. <i>Source: UNODC (International Classification of Crime for Statistics Purposes, ICCS)</i>
Cyber-Enabled Crime	Offenses where computers are used to commit traditional crimes such as theft, harassment, or fraud. These are offenses that can be committed without a computer but can also be facilitated by ICTs. <i>Source: UNODC (ICCS)</i>
Cyber-Enabled Fraud	Fraud that is enabled through or conducted in the cyber environment and that involves transnational criminality such as transnational actors and fund flows and deceptive social engineering techniques (that is, manipulating victims to obtain access to confidential or personal information). <i>Sources: FATF, the EGMONT Group and INTERPOL</i>
Digital Fraud	Fraudulent activities conducted through digital means (for example, emails, websites, malicious software, and so on) to steal banking assets or customer credentials. <i>Source: Basel Committee on Banking Supervision</i>
Financial Fraud	Understood as an umbrella category, encompassing those activities that aim at the procurement of financial gain through deliberate, deceitful actions against individuals and to their detriment. <i>Source: INTERPOL</i> Fraud involving financial transactions for the purpose of personal gain. This includes using financial consumer products such as bank accounts. Includes bank fraud; investment fraud; check/credit card fraud; store card fraud; online banking fraud; writing bad checks. <i>Source: UNODC (ICCS)</i>

(Continued)

Term	Definition
Fraud	Fraud is a crime that encompasses highly diverse actions and behaviors that are undertaken across a wide range of settings and against diverse victims. In academic research, fraud has been broadly defined as obtaining something of value or avoiding an obligation by means of deception. <i>Source: UNODC (UNCTOC)</i>
	Obtaining money or other benefit, or evading liability, through deceit or dishonest conduct. Includes mortgage fraud, financial fraud, quackery, impersonation, identity theft, possession, creation, or use of false weights for measure. <i>Source: UNODC (ICCS)</i>
	Fraud means obtaining money or other benefit or evading liability through deceit or dishonest conduct. It includes cyber-related fraud. <i>Source: EU (EUROSTAT)</i>
	A fraud plan is perpetrated with the intention of defrauding victims of their assets using false and deceitful pretexts, or with the use of cyberattack techniques. This results in the voluntary or involuntary transfer of personal or business information, money, or goods to criminals. <i>Source: EUROPOL</i>
	Fraudulent and deceptive commercial practices refers to those fraudulent and deceptive commercial practices that cause actual harm to consumers, or that pose an imminent threat to consumers, including misrepresentations of material fact, failure to deliver promised goods/ services, and unauthorized charges. <i>Source: OECD</i>
Online Harm	Financial fraud perpetrated on the Internet, primarily targeting retail investors in the securities and derivatives markets, orchestrated using deceptive acts, and misleading or fraudulent content, including user-generated content, where the author is unauthorized, or makes false or misleading claims or impressions, to induce the purchase of financial products and services. This may take the form of advertisements, videos, impersonator websites, social media posts, as well as comments or reviews. <i>Source: IOSCO</i>
Online Scam	Fraud where criminals use digital channels to manipulate or deceive individuals into authorizing payments, in good faith, to recipients they believe to be legitimate. <i>Source: Consumers International</i>
Fraudulent Payment Transactions	Unauthorized payment transactions made, including as a result of the loss, theft or misappropriation of sensitive payment data or a payment instrument, whether detectable or not to the payer prior to a payment and whether or not caused by gross negligence of the payer or executed in the absence of consent by the payer ("unauthorized payment transactions"); and payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the payment service provider, in good faith, to a payment account it believes belongs to a legitimate payee ("manipulation of the payer"). <i>Source: European Banking Authority</i>

Annex 2. Measuring Cyber-Enabled Fraud

The systematic collection of cyber-enabled fraud data is essential to understanding the scale, dynamics, and systemic implications of a rapidly evolving threat landscape. International experience demonstrates that complaint-based reporting provides a critical foundation for identifying trends, prioritizing enforcement resources, and informing prevention strategies, but it is only as robust as the underlying reporting volume and quality. In practice, cyber-enabled fraud now accounts for a dominant and growing share of reported cybercrime losses and is closely linked to the digitalization of financial services, posing risks not only to consumers but also to financial institutions and financial stability more broadly. However, major data gaps persist. Reporting mechanisms differ across agencies and jurisdictions, classification systems are not harmonized, and underreporting remains significant. This leads to an incomplete and sometimes biased representation of actual fraud activity. These limitations underscore the importance of strengthening standardized data collection frameworks to improve situational awareness, cross-border comparability, and early identification of systemic risk channels.

A systematic methodology for collecting cyber-enabled fraud data can be built on multisource reporting and standardized taxonomies. At the core lies a nationwide and centralized reporting platform where individuals, businesses, and financial institutions submit incident reports. These are complemented by regulatory reporting (for example, suspicious activity reports from financial institutions), law enforcement case management data, and supervisory data sets, with common definitions to ensure interoperability. An informative minimum data set captures for example: (i) incident characteristics (type of fraud, vector such as phishing or business email compromise), (ii) financial impact (attempted versus realized losses, recovery amounts), (iii) payment channels (for example, credit transfers, cards, direct debits, electronic money, crypto assets), (iv) victim characteristics (sector, demographics, geography), and (v) transaction attributes and cross-border elements.

To detect emerging risks, continuous data collection, with high-frequency internal reporting calibrated to institutional size, systemic importance, and risk profile (for example, monthly for major institutions and quarterly for smaller firms), is key, alongside an annual public release to support transparency and policy analysis. When aggregated and analyzed, these data enable authorities to identify concentration risks (for example, specific payment rails or fraud typologies), assess transmission channels to the financial system, evaluate the effectiveness of safeguards, and estimate broader economic impacts, including loss of consumer trust, financial infrastructure disruption, and potential spillovers to credit intermediation and growth. Improvements in reporting and detection may initially increase recorded fraud and temporarily worsen performance indicators, reflecting enhanced measurement rather than underlying deterioration. This effect should be considered when interpreting trends and assessing policy effectiveness.

A robust data collection framework supports the development of a clearly defined set of key performance indicators (KPIs). These can be structured across three analytical levels: (i) system-level indicators measuring aggregate fraud exposure and macrofinancial implications; (ii) institutional-level indicators assessing the effectiveness of prevention, detection, and response controls at supervised entities; and (iii) enforcement and recovery indicators tracking disruption of criminal networks and asset recovery outcomes.

International practice demonstrates that informative KPIs extend beyond aggregate loss statistics and include fraud rates relative to transaction volumes, reimbursement ratios, funds recovered, detection timing (before versus post-execution), and time-to-freeze metrics. KPI frameworks could also incorporate prevention-stage indicators, such as attempted fraud volumes, authentication challenge rates, and transaction blocking effectiveness, as these provide forward-looking insight into fraud pressure, the effectiveness of preventive controls, and potential impacts on user trust and payment system resilience before losses fully materialize.

Well-designed KPIs allow authorities to assess systemic vulnerabilities, compare performance across institutions and payment channels, identify emerging typologies, and monitor whether changes in fraud metrics are consistent with the intended effects of policy interventions such as authentication requirements, confirmation of payee, or reimbursement regimes.

Effective KPI frameworks also incorporate indicators of cross-institutional coordination and information sharing, recognizing that fraud mitigation depends on collaboration across relevant authorities (for example, data-sharing arrangements, escalation timelines, joint supervisory or enforcement mechanisms). Such indicators can also help assess the degree of coordination maturity, ranging from fragmented supervisory silos to partial information-sharing arrangements and, ultimately, to fully integrated cross-regulatory oversight frameworks.

To ensure that metrics remain adaptive to evolving fraud typologies, technological developments, and cross-border risk dynamics, KPI frameworks need periodic evaluation.

References

- Asia/Pacific Group on Money Laundering (APG). 2026. "Cyber Scam Hubs and Human Trafficking Report." [https://apgml.org/sites/default/files/2026-07/APG Cyber Scam Hubs Human Trafficking Report 2026.pdf](https://apgml.org/sites/default/files/2026-07/APG%20Cyber%20Scam%20Hubs%20Human%20Trafficking%20Report%202026.pdf)
- Bank of Thailand and Puey Ungphakorn Institute for Economic Research (BOT and PIER). 2026. *The Bangkok Blueprint in Action: Regional Experiences and Policy Lessons for Fraud-Resilient Financial Services*. Bangkok, forthcoming.
- Basel Committee on Banking Supervision (BCBS). 2021. "Principles for Operational Resilience." <https://www.bis.org/bcbs/publ/d516.pdf>
- Basel Committee on Banking Supervision (BCBS). 2023. "Digital Fraud and Banking: Supervisory and Financial Stability Implications." Discussion Paper. <https://www.bis.org/bcbs/publ/d558.pdf>
- Boeddu, Gian Luciano, Jennifer Chien, Rosamund Clare Grady, and Ivor Istuk. 2021. "Consumer Risks in Fintech: New Manifestations of Consumer Risks and Emerging Regulatory Approaches: Policy Research Paper (English)." Finance, Competitiveness and Innovation Global Practice: World Bank. <http://documents.worldbank.org/curated/en/515771621921739154>
- Chang, Salvador, Eric Duflos, and Majorie Chalwe-Mulenga. 2026. "Solutions to Protect Consumers from Fraud in Digital Finance." Working paper, CGAP. <https://www.cgap.org/research/solutions-to-protect-consumers-fraud-in-digital-finance>
- Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (CPMI and IOSCO). 2022. "Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements." <https://www.bis.org/cpmi/publ/d206.pdf>
- Financial Action Task Force (FATF). 2026a. "Cyber-Enabled Fraud: Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks." <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/cyber-enabled-fraud-paper.pdf.coredownload.inline.pdf>
- Financial Action Task Force (FATF). 2026b. "Information Sharing to Combat Illicit Finance." <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/information-sharing-ppp-data-protection-arrangements-2026.pdf.coredownload.inline.pdf>
- Financial Action Task Force (FATF). 2026c. "Targeted Report on Stablecoins and Unhosted Wallets." March. <https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf>
- Financial Action Task Force (FATF). 2026d. "Understanding and Mitigating the Risks of Off-shore Virtual Asset Service Providers." March. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Understanding-Mitigating-Risks-Offshore-VASPs.pdf.coredownload.inline.pdf>
- Financial Action Task Force (FATF), INTERPOL, and Egmont Group. 2023. "Illicit Financial Flows from Cyber-Enabled Fraud." <https://www.fatf-gafi.org/en/publications/Methodsand Trends/illicit-financial-flows-cyber-enabled-fraud.html>

- Financial Services Information Sharing and Analysis Center (FS-ISAC). 2025. "Leveling Up: A Cyber Fraud Prevention Framework for Financial Services." <https://www.fsisac.com/knowledge/cyber-fraud-prevention-framework>
- Financial Stability Board. 2024. "Recommendations to Promote Alignment and Interoperability across Data Frameworks Related to Cross-border Payments: Final Report." <https://www.fsb.org/uploads/P121224-1.pdf>
- Gaidosch, Tamas, Emran Islam, Tanai Khiaonarong, Rangachary Ravikumar, and Chris Wilson. 2026. "Good Practices in Cyber Risk Regulation and Supervision." IMF Departmental Paper 2026/001, International Monetary Fund, Washington, DC. <https://www.IMF.org/-/media/files/publications/dp/2026/english/gpcrrsea.pdf>
- Galicia Rabadan, Guillermo Alfonso, Harish Natarajan, Holti Banka, Nilima Chhabilal Ramteke, David Black, Peter Christian Moeller Jensen, and Maria Elizabeth Jackson. 2026. *ID Meets Instant: Enabling Trusted, Inclusive Fast Payments through Digital ID—Technical Note (English)*. Washington, DC: World Bank. <http://documents.worldbank.org/curated/en/099020526062040816>
- Global Anti-Scam Alliance and Feedzai (GASA and Feedzai). 2025. "Global State of Scams Report 2025." <https://www.feedzai.com/resource/global-state-of-scams-report-2025/>
- International Monetary Fund and World Bank Group (IMF and WBG). 2018. "The Bali Fintech Agenda, 2018." <https://www.IMF.org/-/media/files/publications/pp/2018/pp101118-bali-fintech-agenda.pdf>
- INTERPOL. 2026. "Global Financial Fraud Threat Assessment 2026." <https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat>
- Khiaonarong, Tanai, and Shanyuan Zheng. 2026. "The Rise of Cyber Events and Digital Fraud in the Financial Sector." IMF Working Paper WP/26/62, International Monetary Fund, Washington, DC. <https://www.IMF.org/-/media/files/publications/wp/2026/english/wpia2026062-source.pdf.pdf>
- Organisation for Economic Co-operation and Development (OECD). 2026. *Consumer Finance Risk Monitor 2026*. Paris: OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/03/consumer-finance-risk-monitor-2026_04395fbd/61f7dbe0-en.pdf
- UK Government. 2023. "Fraud Strategy: Stopping Scams and Protecting the Public." <https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public>
- UNDP. 2026. "Issue Brief: Countering Digital Scams: Stemming the Tide on an Urgent Development Challenge." <https://www.undp.org/sites/g/files/zskgke326/files/2026-02/undp-countering-digital-scams.pdf>
- United Nations Office on Drugs and Crime (UNODC). 2025. "Emerging Threats: The Intersection of Criminal and Technological Innovation in the Use of Automation and Artificial Intelligence in the Cybercrime Landscape of Southeast Asia." https://www.unodc.org/documents/Reports/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf
- US Department of the Treasury. 2026. "National Money Laundering Risk Assessment 2026." <https://home.treasury.gov/system/files/246/2026-NMLRA.pdf>

- Wilson, Christopher, Tamas Gaidosch, Frank Adelman, and Anastasiia Morozova. 2019. "Cybersecurity Risk Supervision." IMF Departmental Paper 19/15, International Monetary Fund, Washington, DC. <https://www.IMF.org/-/media/files/publications/dp/2019/english/crsea.pdf>
- World Bank. 2017. *Good Practices for Financial Consumer Protection, 2017 Edition*. Washington, DC.
- World Bank. 2021. *Universal Financial Access 2020: Lessons for the Future*. Washington, DC. <https://openknowledge.worldbank.org/entities/publication/dd043e0f-ddb1-4012-9080-b6a02820d047>
- World Bank. n.d. "Project FASTT (Frictionless Affordable Safe Timely Transactions)." <https://fastpayments.worldbank.org/>

