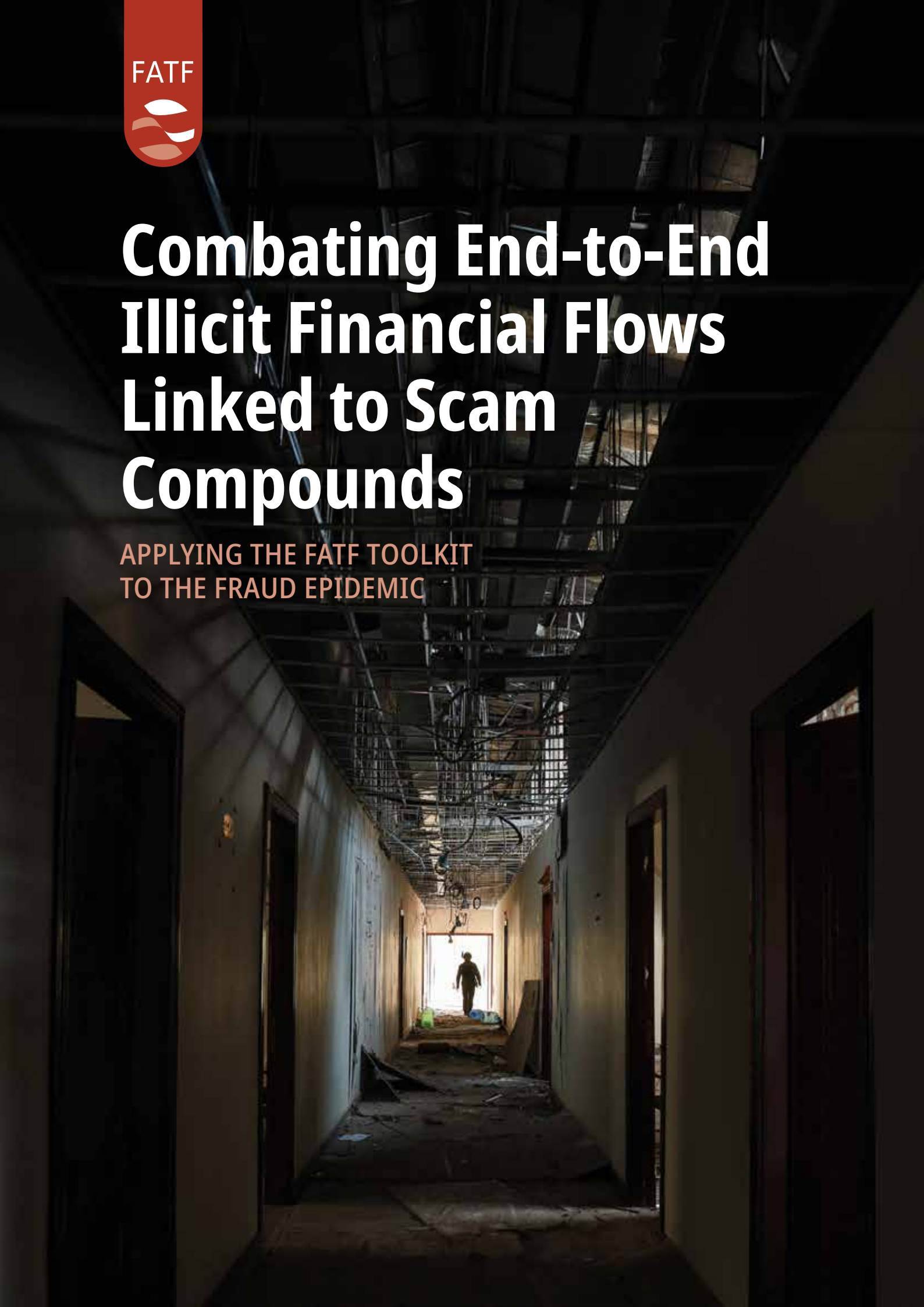
FATF

Combating End-to-End Illicit Financial Flows Linked to Scam Compounds

APPLYING THE FATF TOOLKIT TO THE FRAUD EPIDEMIC



The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. It sets international standards that aim to prevent these illegal activities and the harm they cause to society. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

FATF (2026), *Combating End-to-End Illicit Financial Flows Linked to Scam Compounds: Applying the FATF Toolkit to the Fraud Epidemic,* FATF, Paris, https://www.fatf-gafi.org/en/publications/Methodsandtrends/combating-illicit-financial-flows-linked-to-scam-compounds.html

© FATF/OECD 2026

Attribution 4.0 International (CC BY 4.0)

This work is made available under the Creative Commons Attribution 4.0 International licence. By using this work, you accept to be bound by the terms of this licence. For information about reproduction, distribution and translation please see the Terms, Conditions and Disclaimers published on the FATF public website. You must not use the FATF logo, visual identity or cover image without express permission or suggest the FATF endorses your use of the work. Any dispute arising under this licence shall be settled by arbitration in accordance with the Permanent Court of Arbitration (PCA) Arbitration Rules 2012. The seat of arbitration shall be Paris (France). The number of arbitrators shall be one.

Cover image: A Thai soldier walks along a corridor inside a compound in the O'Smach area that the Thai military said was used for scam operations, at the Chong Chom-O'Smach border crossing Oddar Meanchey province, Cambodia, March 2026.
© Reuters/Chalinee Thirasupa

Table of contents

1. Executive summary 2
2. Acronyms 8
3. Introduction 9

SECTION 1. **Illicit financial flows linked to scam compounds: state of play** 16
4. Business models 17
5. Contextual drivers 24
6. Enabling financial and non-financial infrastructures 27
7. End-to-end financial flow model 34

SECTION 2. **Cross-cutting challenges for competent authorities and the private sector** 38
8. Detection and prevention 39
9. Information sharing and intelligence fusion 40
10. Financial intelligence, investigation and prosecution 41
11. International co-operation 42
12. Asset tracing, freezing, recovery and restitution 43
13. Victim reporting and victim-centred outcomes 44

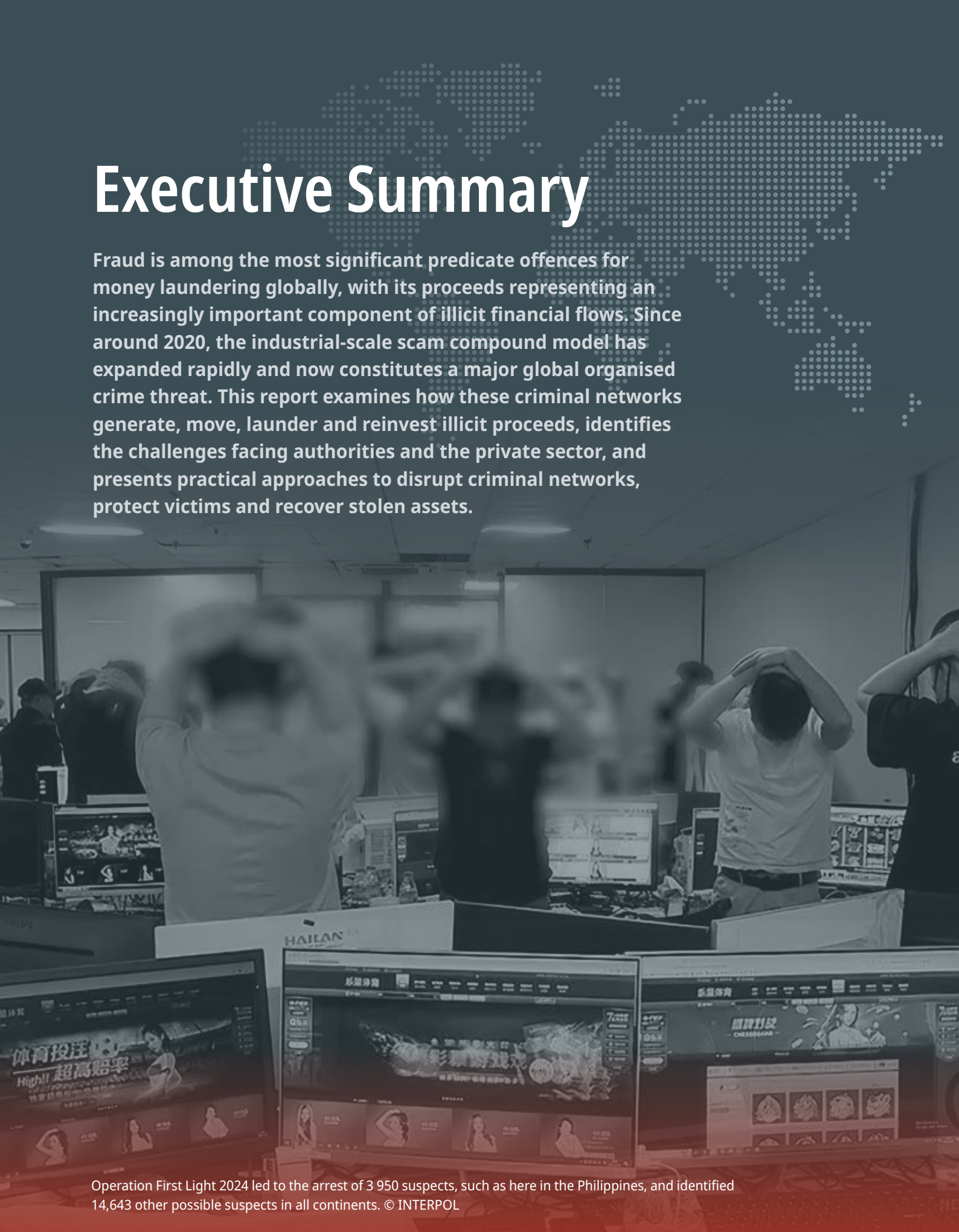
SECTION 3. **Mitigation strategies and operational tools** 46
14. Strategic principles 47
15. Co-ordination models 52
16. Operational toolkit 60

Annex 1. FATF Principles for Combating Illicit Financial Flows Linked to Scam Compounds 76

Annex 2. Additional Case Studies and Good Practice Examples 78

Executive Summary

Fraud is among the most significant predicate offences for money laundering globally, with its proceeds representing an increasingly important component of illicit financial flows. Since around 2020, the industrial-scale scam compound model has expanded rapidly and now constitutes a major global organised crime threat. This report examines how these criminal networks generate, move, launder and reinvest illicit proceeds, identifies the challenges facing authorities and the private sector, and presents practical approaches to disrupt criminal networks, protect victims and recover stolen assets.



Operation First Light 2024 led to the arrest of 3 950 suspects, such as here in the Philippines, and identified 14,643 other possible suspects in all continents. © INTERPOL

- **Fraud is estimated to cost approximately USD 500 billion globally each year[1]. Rates of fraud and related proceeds have increased sharply in recent years, driven by greater online exposure, technological innovation and faster payment systems, trends accelerated by the COVID-19 pandemic.** Fraud is among the most significant predicate offences for money laundering (ML) globally, and fraud proceeds represent an increasingly important component of illicit financial flows. At this scale, fraud can also undermine the integrity and resilience of the financial system and the digital economy by generating operational and financial risks, eroding trust in financial services and creating potential financial stability concerns.

- **Fraud differs from many other forms of financial crime because the laundering of proceeds is often closely intertwined with the commission of the predicate offence itself, making the FATF toolkit central to the response.** Cyber-enabled fraud further exploits the scale, reach and speed of digital financial services, creating particular challenges for traditional anti-money laundering responses. In many scam typologies, victims are manipulated into authorising payments themselves, meaning that transactions may appear legitimate to financial institutions (FIs) unless transaction data are combined with contextual fraud risk signals typically not held or received by FIs.

- **The industrial-scale scam compound model expanded rapidly from around 2020**, although precursor cases of trafficking for forced online fraud predate the COVID-19 pandemic. This expansion has contributed to the wider growth in cyber-enabled fraud. Scam compounds are among the most rapidly expanding forms of organised crime globally, with annual losses estimated to be in the tens of billions of USD. They have as a result became an urgent issue for the FATF in its work to combat ML/TF/PF. They may encompass both large physical compounds and linked or decentralised operational structures.

- **This report represents a first step in the FATF's broader anti-fraud roadmap and will inform further FATF work on fraud.** The report applies an end-to-end financial flow lens to the generation, movement, laundering and reinvestment of proceeds linked to scam compounds. Although illicit financial flows are only one component of this multidimensional threat, they underpin the profitability and resilience of scam compounds and provide critical opportunities for prevention, detection, investigation, disruption and recovery. Across this lifecycle, the report also identifies the functional dependencies on which scam compound operations rely—that is, the capabilities, services, infrastructure and relationships that enable particular functions to be performed—and the points at which direct action and broader anti-fraud capabilities can disrupt them.

- **The report demonstrates a multi-disciplinary approach**, combining contributions from FATF Global Network jurisdictions, Observers, other international organisations, private sector stakeholders, civil society and academic experts.

Nature of the threat

- **Scam compounds are operational nodes within industrialised, professionalised and transnational organised crime ecosystems in which cyber-enabled fraud converges with trafficking in human beings (including for the purpose of forced criminality), corruption, cybercrime and ML.** Harms extend beyond financial loss: persons trafficked into scam operations may face debt bondage, confinement, violence, sexual exploitation, torture and threats, while online scam victims and their families may suffer severe economic, psychological and social harm. In certain settings, the scale and reach of these operations may also have wider implications for peace and security.

- **Scam compounds combine increasingly integrated criminal business models with a professionalised crime-as-a-service economy.** Criminal networks may control, procure or outsource worker and victim recruitment, scam execution, technical enablement, payment collection, ML, cash-out and reinvestment, often across jurisdictions. Victim targeting is global, segmented and adaptive: cyber scam hubs have targeted persons in more than 100 jurisdictions.

1. Global Anti-Scam Alliance (GASA) (2026), *GASA Policy Agenda 2026,* available at: https://gasa.org/knowledge-base/blog/gasa-policy-agenda-2026.

- **Scam operations are diversifying from large physical compounds into smaller, dispersed and mobile structures.** Enforcement pressure may fragment, relocate or rebrand operations while common controllers, financial infrastructure and specialised service providers remain in place.

- **The financial model is circular and modular, rather than a single linear chain performed by the same actors**: scam networks spend to establish and sustain physical and digital infrastructure and acquire workers and victims; generate revenue; collect, move, layer, cash out and integrate proceeds; and reinvest profits in further activity and expansion. Related flows can move within minutes across accounts and wallets, while misuse of online platforms including social media networks and telecommunications service providers generates and enables activity throughout the lifecycle.

- **The objective of financial investigation and disruption should be to identify and disrupt the wider criminal network and the functions sustaining it, rather than focus on the physical scam site alone.** These functions may be performed within a compound, by affiliated cells operating elsewhere or by external service providers.

Challenges for competent authorities and the private sector

- **Effective action is constrained by a mismatch in speed and visibility.** Scam-related funds can move across accounts, virtual asset (VA) wallets, asset types and jurisdictions within minutes, outpacing victim reporting, institutional escalation, suspicious transaction report (STR) filing and analysis, law enforcement action and international co-operation. Detection is also fragmented: FIs, virtual asset service providers (VASPs), competent authorities, technology and telecommunications providers and civil society often hold different parts of the same value chain without the means to connect these views swiftly enough for effective action.

- **Investigation and disruption are complicated by multi-layered financial flows, opaque beneficial ownership (BO) and corporate structures, electronic evidence held across providers and jurisdictions, corruption or official protection, and the need to integrate financial investigation with cybercrime, trafficking, immigration and asset recovery.** Treating the trafficking and financial crime dimensions separately can leave recruitment networks and organisers intact and may result in trafficked persons being misclassified as offenders.

- **The transnational nature of the threat magnifies these challenges**: delayed co-operation can allow funds, evidence, infrastructure and criminal actors to move beyond reach, while delayed or incomplete reporting by online scam victims and trafficked persons reduces network visibility and the already narrow window for payment intervention—that is, measures to prevent, suspend, delay, reject, recall or otherwise interrupt victim payments and subsequent transfers before proceeds are dissipated—asset preservation, recovery and restitution.

Mitigating the threat

- Evidence of sustained effectiveness remains limited and uneven, but available experience points towards a holistic approach rather than reliance on a single institutional model or technological tool. Effective responses target the wider criminal ecosystem; combine upstream and downstream intervention; connect intelligence and capabilities across sectors and borders; match the transnational nature of the threat; maintain a victim-centred approach; and remain adaptive and outcome-focused. These responses operate on two complementary levels: direct action against scam compound networks, their enabling infrastructure and related financial flows; and measures that strengthen the broader anti-fraud system and its capacity to detect, prevent, investigate, disrupt and recover proceeds from fraud. These dimensions cut across the upstream/downstream distinction: upstream and downstream describe where intervention occurs across the lifecycle, while direct action and broader system strengthening describe how the response is delivered. Evidence is strongest for the operational capability and case-level impact of downstream interventions, while upstream disruption and sustained degradation of shared criminal capabilities remain less developed or less well evaluated.

- **At the broader anti-fraud system level**, available experience supports combining institution-level monitoring with system and network-level analysis and insights from earlier intervention. Anti-scam centres, shared fraud data infrastructures, collaborative analytics and rapid response arrangements—many of which involve public-private partnerships—can connect financial, law enforcement, victim, technology and telecommunications indicators that no actor can see alone. Early fraud signals arise before a financial transaction occurs, including fraudulent advertising, recruitment activity, domains, phone numbers and suspicious telecommunications indicators associated with fraud. The objective of the information sharing systems anchoring these mechanisms is not to maximise the volume of information exchanged, but to route sufficiently reliable and actionable signals through escalation pathways, clear legal gateways and trusted contact points. Accordingly, the primary operational role in payment intervention lies with the relevant FI or VASP with direct operational control over the payment, account or wallet and the ability to act in real time or near real time. Anti-scam centres, financial intelligence units (FIUs) and other competent authorities should enable and support such action through intelligence, co-ordination, escalation and, where necessary, formal powers, rather than being expected to intervene transaction by transaction.

- **For investigation and disruption** of scam compound networks, multi-agency teams should integrate financial, anti-trafficking, cybercrime, corruption, electronic evidence and asset recovery capabilities. Parallel financial investigations, FIU and network analysis, BO and corporate-link analysis and financial and VA tracing can connect victim payments, operating expenditure, accounts, wallets, legal structures, assets and service providers to the wider enterprise.

- **Where preventive controls fail, speed and pre-established relationships are critical**: the first 24–72 hours after detection or reporting are particularly important for tracing, recovery and restitution. Rapid response arrangements should route actionable information quickly to the relevant FIs, VASPs and other payment providers so that they can execute payment holds, recalls and account or VA wallet restrictions, while connecting these immediate interventions with FIU, law enforcement and asset recovery powers and rapid cross-border channels. Formal co-operation remains necessary where evidence or coercive measures are required.

- **Victim-centred arrangements** should protect both online scam victims and persons trafficked or coerced into scam activity, including through appropriate screening, non-punishment safeguards and access to support. Victims should not be treated principally as sources of intelligence; however, information obtained through safe, lawful and victim-sensitive reporting and debriefing can reveal accounts, wallets, recruitment networks, communications infrastructure, compounds and shared criminal networks. Reporting and referral arrangements should ensure that this information is rapidly routed to the actors able to act, including relevant FIs and VASPs for payment intervention and competent authorities for investigation, asset recovery and victim protection, while retaining the information needed for restitution and improving future detection and preventive efforts.

What jurisdictions should do

- **Jurisdictions should combine direct action against scam compound networks with measures that strengthen the broader anti-fraud system.** Across both, they should prioritise the development of upstream capabilities while preserving and strengthening downstream measures for which the report identifies the strongest evidence of operational capability and case-level impact. This requires action both against the upstream infrastructure and services that enable scams to be established and scaled and against the downstream financial flows through which criminal proceeds are received, moved, laundered, integrated and reinvested.

- **Domestically**, jurisdictions should understand their exposure to scam compound-related illicit financial flows and, on that basis, establish clear leadership and co-ordination among authorities responsible for financial intelligence, law enforcement, anti-trafficking, cybercrime, anti-corruption, asset recovery and supervision. They should connect public- and private-sector intelligence, including through public-private partnerships and, where legally permissible, private-private arrangements.

Where scam compound-related fraud constitutes a significant national threat, jurisdictions may consider whether treating fraud as a national security priority could strengthen whole-of-government co-ordination, data use, resource allocation and sustained disruption of organised scam networks.

- **Internationally**, jurisdictions should connect these domestic capabilities through trusted FIU, law enforcement and asset recovery networks, joint investigative or operational arrangements and timely formal co-operation where evidence or coercive measures are required. Co-operation should enable rapid exchange of financial, trafficking, technical and digital intelligence; preservation and transfer of electronic evidence; tracing and provisional preservation of assets; victim identification and safe repatriation; and co-ordinated action against leadership, shared infrastructure and specialised service providers across relevant jurisdictions. Where needed, targeted technical assistance and capacity building should support the development of these capabilities, particularly in jurisdictions hosting or exposed to scam compound activity.

Combating end-to-end illicit financial flows linked to scam compounds: dependencies, actions and intended impact

END-TO-END ILLICIT FINANCIAL FLOW MODEL FOR SCAM COMPOUNDS		SCAM COMPOUND FUNCTIONAL DEPENDENCIES What operations rely on	DIRECT ACTIONS AGAINST SCAM COMPOUND NETWORKS	STRENGTHENING THE BROADER ANTIFRAUD SYSTEM	INTENDED OPERATIONAL IMPACT
UPSTREAM Stages 1-3	Establish operations	• Secure premises, power/connectivity, roads/crossing • Social media/messaging accounts, domains/hosting, SIMs/cloud • Front companies, corporate accounts, nominees • Trusted access, brokers, cross-border facilitators	• Map physical infrastructure and access routes • Disrupt digital & telecom infrastructure • Investigate corporate and legal structures and opaque BO • Identify shared criminal relationships and facilitators	• Corporate registry and BO access • Telecom and platform participation • Multi-agency operational co-ordination	• Earlier identification of enabling structures • Reduced capacity to establish and regenerate operations
	Recruit workers	• Social media/messaging accounts • Trusted access, brokers, cross-border facilitators • Roads/crossings, premises • Protection corruption	• Identify recruitment channels, brokers and access routes • Trace payments linked to recruitment and control • Identification and protection of trafficked workers	• Trusted reporting channels • Law enforcement co-ordination • Cross-border contact points	• Workers identified and supported earlier • Recruitment networks and controllers disrupted
	Acquire victims	• Victim data • Fraudulent advertising campaigns • Social media/messaging accounts, fake platforms • Domains/hosting, SIMs/cloud, automation/ deepfakes	• Disrupt digital & telecom infrastructure and fake platforms • Continuously monitor fraud campaigns • Controlled scam-hunting and preventive payment control	• Shared fraud data and cross-sector signal exchange • Anti-scam centres and PPPs • Platform and telecom participation	• Reduced victim acquisition opportunities • Scam indicators identified before first payment
PAYMENT WINDOW Stage 4	Execute scams	• Fraudulent advertising campaigns, fake platforms • Automation/deepfakes • Social media/messaging accounts • Premises, power/connectivity • Protection/corruption	• Detect and interrupt active campaigns and fake platforms • Share victim and scam indicators rapidly • Preventive payment controls before transfer	• Real-time information sharing • Co-ordinated platform, telecom and FI responses • Victim-centred reporting channels	• Reduced campaign reach and persistence • Earlier detection before funds are transferred
DOWNSTREAM Stages 5-7	Collect payments	• Mule accounts/networks • Bank accounts, payment services • MVTS • Corporate accounts • VA wallets, VASPs, P2P and OTC brokers	• Disrupt mule accounts and apply preventive payment controls • Identify connected receiving accounts and wallets • Rapid intervention and preservation	• FI, VASP and MVTS participation • Rapid response networks • Real-time account and transaction intelligence	• Faster intervention after payment • More proceeds stopped before onward transfer
	Move / launder funds	• Mule networks • Underground banking • Corporate accounts and bank accounts • VA wallets, VASPs, P2P, OTC brokers • Professional intermediaries/DNFBPs • MVTS	• Fund tracing and VA tracing • Parallel financial investigations of corporate links and intermediaries • Cross-border FIU and law enforcement co-ordination	• Financial intelligence integration • Blockchain analytics capability • Trusted cross-border operational channels	• Greater visibility across linked accounts and wallets • Reduced ability to layer and dissipate proceeds
	Cash out / integrate	• VA wallets, VASPs, P2P, OTC brokers • Front companies, corporate accounts, professional intermediaries/DNFBP, nominees • MVTS	• Preserve and recover assets across FI and VA channels • Analyse BO, corporate links and gatekeepers • Victim-linked recovery and restitution protocols	• Asset recovery and restitution procedures • Claimant and loss data • Rapid international co-operation	• More assets preserved and recovered • More funds returned to victims • Reduced criminal incentives

Note: This visual summary synthesises the findings across the end-to-end lifecycle, linking the principal functional dependencies of scam compound operations with direct actions, broader anti-fraud capabilities and their intended operational impact.

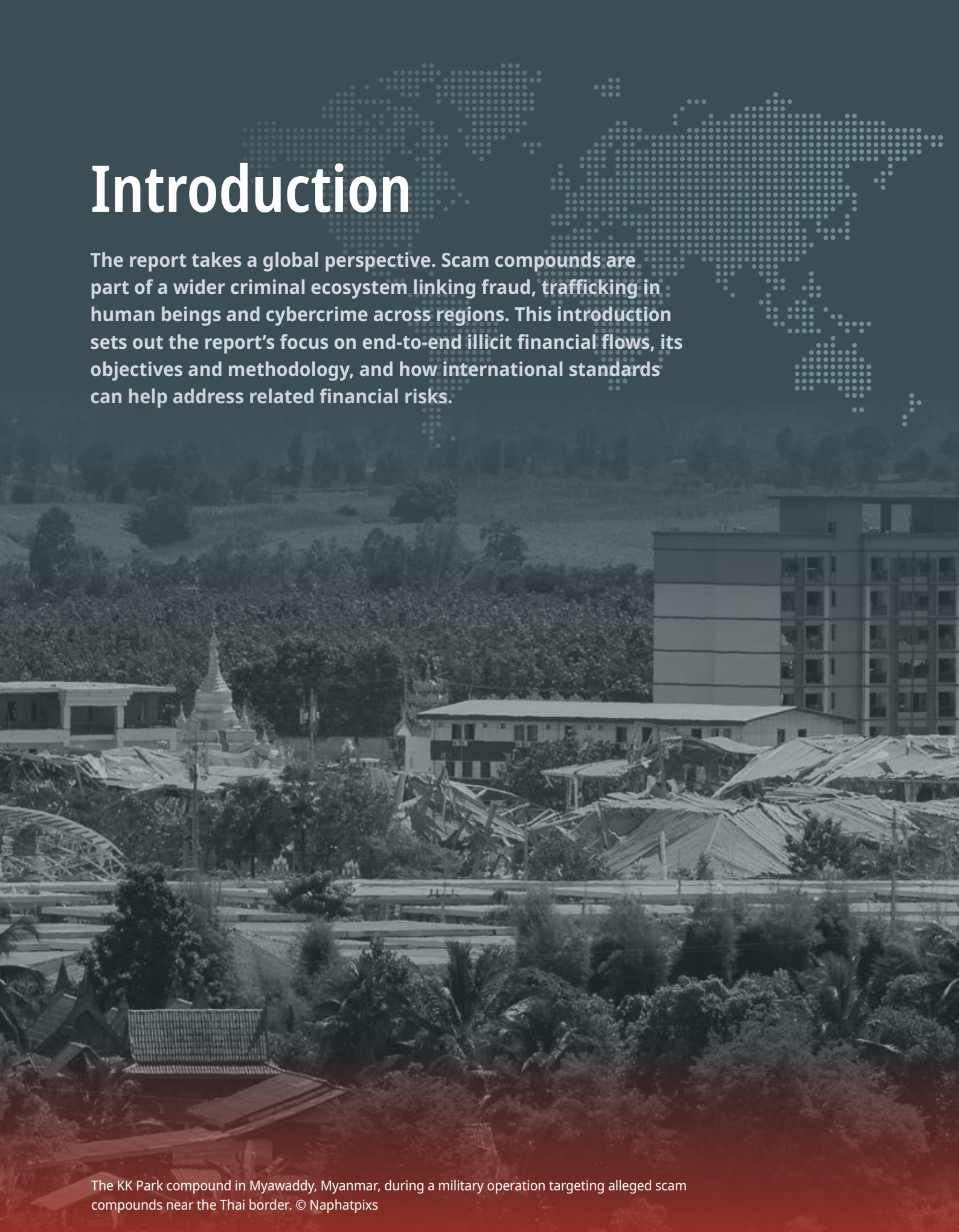
- **Success should ultimately be judged not by the number of alerts, investigations, arrests, account closures, takedowns or asset freezes generated, but by whether interventions protect victims and sustainably degrade the criminal business model.** Measurement should distinguish intermediate outputs such as payments intercepted, accounts or wallets restricted and assets frozen from final outcomes including victim losses prevented, confiscation, recovery and restitution, victim protection and safe return or reintegration, and durable degradation of shared or difficult-to-replace criminal capabilities. It should also assess displacement and substitution so that relocation, rebranding or replacement of disrupted infrastructure is not mistaken for sustained impact.

- **At the FATF, this report will inform the next phase of its work on fraud** as members consider how to further mobilise the FATF's capabilities to combat fraud.

Acronym	Meaning
AI	Artificial intelligence
BO	Beneficial ownership
BPO	Business process outsourcing
CDD	Customer due diligence
DeFi	Decentralised finance
FI	Financial institution
FIU	Financial intelligence unit
KYC	Know-your-customer
LEA	Law enforcement authority
MER	Mutual evaluation report
ML	Money laundering
MLA	Mutual legal assistance
MVTS	Money or value transfer service
NGO	Non-governmental organisation
OTC	Over-the-counter
P2P	Peer-to-peer
PEP	Politically exposed person
PET	Privacy-enhancing technology
PF	Proliferation financing
PML	Professional money laundering
PPP	Public-private partnership
PSP	Payment service provider
STR	Suspicious transaction report
TF	Terrorist financing
VA	Virtual asset
VASP	Virtual asset service provider
VPN	Virtual private network

Introduction

The report takes a global perspective. Scam compounds are part of a wider criminal ecosystem linking fraud, trafficking in human beings and cybercrime across regions. This introduction sets out the report's focus on end-to-end illicit financial flows, its objectives and methodology, and how international standards can help address related financial risks.



The KK Park compound in Myawaddy, Myanmar, during a military operation targeting alleged scam compounds near the Thai border. © Naphatpixs

Scope and key terminology

Scam compounds are a multidimensional criminal phenomenon in which fraud intersects with trafficking in human beings (including for the purpose of forced criminality), cybercrime, corruption and the misuse of financial, technological and telecommunications infrastructure, which may be procured with or without the knowledge of providers. Scam compound activity may also have broader implications, including for regional and international peace and security.

This report does not seek to address all dimensions of that phenomenon. Consistent with the FATF mandate and comparative advantage, it applies an **end-to-end financial flow lens** to the generation, movement, laundering, reinvestment, disruption and recovery of illicit financial flows linked to scam compounds. This work forms part of the broader FATF anti-fraud roadmap.

Fraud is already recognised as a major money laundering (ML) risk across the FATF Global Network. According to the FATF 2026 report on cyber-enabled fraud[1], 90% of assessed jurisdictions explicitly identify fraud as a major ML risk. Its prominence is increasing in FATF Mutual Evaluations: discussion of fraud and scams in the first seven fifth-round mutual evaluation reports (MERs) is approximately 2.5 times as extensive as in fourth-round MERs, adjusting for report length. Malaysia's fifth-round MER is also the first to identify scam compounds in neighbouring jurisdictions as a named risk driver, reflecting growing recognition of the cross-border risks associated with this phenomenon.

The report focuses specifically on fraud and illicit financial flows linked to scam compounds rather than the full range of fraud typologies. Although scam compounds may conduct several forms of fraud, available evidence indicates a particular concentration on investment fraud, often preceded by romance or confidence-based grooming. Other fraud typologies that occur predominantly outside scam compound settings fall outside the scope of this report and may be considered separately under the broader FATF anti-fraud roadmap. This distinction also constrains quantification: definitions and reporting practices differ across jurisdictions, fraud is significantly under-reported, and estimates often cover cyber-enabled fraud more broadly rather than scam compound activity specifically.

The report takes a **global perspective**. Although scam compounds were initially concentrated in Southeast Asia, available information indicates a broader threat, with scam operations or trafficked victims connected to multiple regions. The report therefore considers whether similar financial flow patterns are emerging outside the Asia-Pacific region[2].

For the purposes of this report, **"scam compounds"** is used as an umbrella working term for organised scam operations displaying the industrialised and networked characteristics examined in the report, encompassing large physical compounds and linked or decentralised structures within comparable organised scam ecosystems. **The term is preferred to "scam centres"** to avoid confusion with "anti-scam centres", which are institutional mechanisms established to prevent and respond to scams. Terminology is not standardised: "scam centre" is generally the broadest operational term; "scam compound" refers to the more physically concentrated end of the spectrum, often involving dedicated premises and, particularly in Southeast Asia, trafficking in human beings and forced criminality; "scam hub" may refer to a physical or hybrid operation or a location concentrating scam activity; and "scam cell" to a smaller, dispersed or mobile unit that may remain connected to common controllers, infrastructure or specialised service providers[3].

1. FATF (2026), *Cyber-Enabled Fraud – Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks*, FATF, Paris, France, available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/cyber-enabled-fraud-paper.pdf.coredownload.inline.pdf
2. INTERPOL (2026), *Global Financial Fraud Threat Assessment*, Second Edition, INTERPOL, March 2026, available at: https://www.interpol.int/content/download/24291/file/INTERPOL%20Global%20Financial%20Fraud%20Threat%20Assessment%202026.pdf
3. Related terms such as "cyber scam hub", "online scam centre" and "call centre" generally describe particular settings, operating models or source terminology rather than distinct legal or financial crime categories. Where the report describes criminal scam activity rather than reproducing source terminology, it uses formulations such as "call centre-style scam operation" or "fraudulent call centre operation" to distinguish such activity from legitimate call centre and business process outsourcing services, which are outside the scope of this report.

This broader, network-based understanding has a direct operational implication: **financial investigation and disruption should focus on the wider criminal network and the functions supporting it**, rather than on the physical scam site alone. This does not mean that every organised online fraud operation constitutes a scam compound. Rather, it recognises that scam compound-related financial, technological and laundering functions may be distributed across jurisdictions and outsourced to actors serving the wider fraud ecosystem.

Objectives

The report seeks to identify: (i) how scam compound-related illicit financial flows are generated and moved end-to-end; (ii) the principal challenges faced by competent authorities and the private sector in preventing, detecting, investigating and disrupting them; and (iii) practical measures to prosecute related offences, disrupt the wider criminal networks involved and recover related assets. In doing so, it treats scam compound-related fraud as a networked, industrialised and transnational financial crime ecosystem rather than as a collection of isolated victim complaints.

Many jurisdictions and private sector actors have already developed tools to detect, disrupt and recover proceeds linked to scam compounds. The added value of this report is therefore to identify emerging evidence of what works, draw from national and regional experience and support the scaling of effective approaches across the FATF Global Network, including through typologies work, public-private engagement and targeted capacity building. This includes strengthening risk understanding and national prioritisation, improving typologies and indicators, promoting faster and more dynamic information sharing and, ultimately, encouraging operational approaches that move beyond predominantly post-event reporting towards prevention and disruption.

Feedback gathered from the FATF Global Network during this project supports this operational focus. The most frequently identified priority was stronger international co-operation, alongside training and guidance on tracing and recovering scam compound-linked assets, use of advanced analytics, practical rapid-response mechanisms and further scam compound typology work. Taken together, these findings provide an evidentiary basis for Part 2 of the FATF's work on fraud and for considering whether existing FATF Standards, guidance and operational mechanisms are being applied effectively to scam compound-related risks and where further appropriate and proportionate collective action may be useful.

Structure of the report

The report is organised in three sections. **Section 1 describes the state of play**, examining scam compound business models, contextual drivers, enabling financial and non-financial infrastructure and the end-to-end financial flow model. **Section 2 identifies the main cross-cutting challenges** for competent authorities and the private sector, including detection and prevention, information sharing, financial intelligence and investigation, international co-operation, asset recovery and victim reporting and outcomes. **Section 3 sets out mitigation strategies and operational tools**, structured around strategic principles, co-ordination models and practical measures for preventing, detecting, investigating and disrupting scam compound-related illicit financial flows. For ease of reference, the Annex 1 consolidates these findings into the FATF Principles for Combating Illicit Financial Flows Linked to Scam Compounds. Selected case studies and good practice examples are integrated throughout the report, with additional examples provided in Annex 2.

Methodology

The project is co-led by the United Kingdom and the United States and supported by a project team comprising 23 jurisdictions representing all FATF regions and 9 Observers[4]. It draws on the FATF's multi-disciplinary approach and global convening power.

The project team applied the following methodology:

(i) a literature review covering FATF publications and work produced by other international organisations, including the International Criminal Police Organisation (INTERPOL), the United Nations Office on Drugs and Crime (UNODC) and other United Nations entities, the Organisation for Economic Co-operation and Development (OECD) and the Organization for Security and Co-operation in Europe (OSCE), as well as FATF-Style Regional Bodies (FSRBs) and jurisdictions, think tanks and academic experts.

(ii) analysis of responses to a questionnaire to the FATF Global Network launched in August 2026 and of the comments of the Global Network on a first draft, which gathered inputs from 60 jurisdictions[5]; and

(iii) expert consultations and discussions throughout the project, including at the Global Anti-Scam Summit America 2026, held in San Francisco on 2–3 September 2026. On that occasion, the project co-leads convened two side meetings with representatives from the private sector, civil society and other stakeholders. These consultations also generated written contributions from 17 private sector and civil society stakeholders[6].

Selected case studies and good practice examples included in the report are illustrative rather than exhaustive. They were selected based on their specific relevance to scam compounds or, where relating to fraud more broadly, their sufficiently substantiated and transferable insights for addressing illicit financial flows linked to scam compounds, while also taking geographical balance into account.

Relationship with the FATF Standards

The FATF Standards provide the core AML/CFT framework for addressing the financial vulnerabilities exploited by scam compound networks and the laundering of proceeds. Scam compound activity also intersects with trafficking in human beings, cybercrime, corruption and the misuse of technological and telecommunications infrastructure, requiring AML/CFT measures to be co-ordinated with relevant complementary legal, regulatory and operational frameworks. Contextual conditions, including weak, fragmented or contested government control in some locations, may further facilitate or protect scam compound activity and are addressed separately in subsection 5. Where scam compound-related fraud and ML risks are material, effective implementation of the relevant FATF Recommendations can mitigate these vulnerabilities and strengthen prevention, detection, investigation, disruption and recovery.

4. Project team led by United Kingdom and United States. The project team comprised experts from 32 jurisdictions, including 18 FATF or Joint Members (Argentina, Australia, China, European Commission, France, India, Indonesia, Japan, Luxembourg, Malaysia, Mexico, Netherlands, Portugal, Singapore, Switzerland, United Arab Emirates, United Kingdom and United States), 1 FSRB Secretariat (APG Secretariat), 4 FSRB Members (Isle of Man, Jamaica, Nigeria and Thailand), and 9 Observers (CARIN, Egmont, Europol, IMF, INTERPOL, OECD, OSCE, UNODC and WB).
5. Argentina, Australia, Austria, Belarus, Belgium, Botswana, Brazil, Cambodia, Canada, China, Eswatini, European Commission, Europol, France, Germany, Greece, Hong Kong China, Hungary, Iceland, IMF, Indonesia, Ireland, Jamaica, Japan, India, International Organisation of Securities Commissions, INTERPOL, Italy, Korea, Luxembourg, Malaysia, Mauritius, Mexico, Mozambique, Namibia, Netherlands, New Zealand, Nigeria, OECD, OSCE, Portugal, Philippines, Romania, Russian Federation, Saudi Arabia, Seychelles, Singapore, Sweden, Switzerland, Chinese Taipei, Thailand, Tunisia, Türkiye, Turkmenistan, United Kingdom, United States, UNODC, Uzbekistan, Vietnam and Zambia.
6. AARP, Association of Certified Anti-Money Laundering Specialists, Amnesty International, Aspen Institute, Chainanalysis, Consumers International, Future of Financial Intelligence Sharing, Gates Foundation, Global Anti-Scam Alliance, GSM Association, Humanity Consultancy, Institute of International Finance, Paypal, RUSI, TRM Labs, Victim Support Europe and Wolfsberg Group.

Table 1 summarises the principal linkages between the FATF Standards and the scam compound-related risks examined in this report. Consistent with the risk-based approach, measures should be targeted and proportionate, strengthening safeguards against criminal misuse while avoiding unnecessary impediments to legitimate financial activity, innovation and efficient cross-border payments.

TABLE 1. **Main FATF Standards relevant to scam compound-related illicit financial flows**

Scam compound-related area / vulnerability	Relevant FATF Standards / guidance / effectiveness framework	Operational implication for scam compound-related risk
Holistic, national risk-based responses and co-ordination	**R.1** (Assessing Risks and Applying a Risk-Based Approach); **R.2** (National Co-operation and Co-ordination); **IO.1** (Risk, Policy and Co-ordination); FATF risk-based approach guidance relevant to R.1	Jurisdictions should identify and assess material scam compound-related fraud and ML risks according to their exposure—including as host, victim, recruitment/source, transit, laundering, asset-holding or infrastructure-hosting jurisdictions—and reflect those risks in national or sectoral assessments, policies, resource allocation and mitigation. Relevant authorities should be able to co-ordinate effectively across the AML/CFT, fraud, cybercrime, trafficking, corruption and asset recovery dimensions.
Sound legal, regulatory and supervisory framework	Preventive measures under **R.9–23**, including **R.10** (CDD), **R.11** (Record-keeping), **R.15** (New Technologies and VASPs), **R.16** (Payment Transparency), **R.20** (Reporting of Suspicious Transactions); **R.26–28** (Regulation and Supervision); **R.34** (Guidance and Feedback); **R.35** (Sanctions); **IO.3** and **IO.4**	Building on this risk understanding, jurisdictions should ensure that FIs, VASPs and relevant DNFBPs are subject to effective risk-based preventive measures and supervision capable of identifying scam compound-related accounts, entities, transactions and service-provider activity. Supervisors should understand relevant exposure, provide appropriate guidance and feedback, and apply effective, proportionate and dissuasive sanctions where obligations are breached.
Resilience of financial services and payment systems to cyber-enabled fraud	**R.10** and **R.11; R.15; R.16; IO.3/IO.4**; FATF Digital ID Guidance (2022)	Effective customer identification and verification, ongoing due diligence, record-keeping, payment transparency and appropriate controls for digital financial services can reduce the misuse of personal, corporate and mule-controlled accounts and wallets. For VAs, effective VASP controls, including applicable Travel Rule requirements and reliable on-/off-ramp information, can support attribution and tracing. Digital identity solutions can strengthen customer identification where appropriately designed and risk-based.
MVTS, VAs/VASPs and other high-risk financial channels	**R.14** (MVTS); **R.15**; relevant **R.16** requirements; **R.26** where applicable; **IO.3/IO.4**	Licensing or registration, risk-based supervision and effective preventive controls can reduce exploitation of unlicensed or unregistered MVTS, inadequately supervised VASPs, VA conversion services and other channels used for collection, layering, cross-border transfer and cash-out of scam compound proceeds. This is particularly relevant because unlicensed or unregistered MVTS, offshore VASPs, P2P and OTC arrangements are identified as important channels in scam compound-related financial flows.

Table 1 continued ...

Scam compound-related area / vulnerability	Relevant FATF Standards / guidance / effectiveness framework	Operational implication for scam compound-related risk
Collaborative and adaptive fraud prevention and information sharing	**R.2; IO.1** and **IO.6**; Consolidated FATF Standards on Information Sharing (2017); Guidance on Private Sector Information Sharing (2017); Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing (2022); Information Sharing to Combat Illicit Finance (2026)	Timely public-public, public-private and, where legally permissible, private-private information sharing can connect fraud, financial, VA, telecommunications, technology and victim-derived indicators that no single actor can see alone. Jurisdictions should provide sufficiently clear legal gateways, safeguards and operational arrangements so that high-confidence scam signals can reach actors able to prevent payments, identify linked accounts or wallets, preserve assets or disrupt enabling infrastructure.
System-wide fraud detection and network-level analysis	**R.15, R.16, R.20, R.29; IO.6;** FATF information sharing work cited above; FATF fraud work and reports (2023 and 2026)	Institution-level monitoring should be complemented by system- and network-level analysis capable of connecting victim payments, mule accounts and wallets, corporate structures, VASP activity and other scam indicators across institutions and cases. FIU analysis, shared fraud data infrastructures and collaborative analytics can help identify the wider criminal network rather than treating activity as isolated fraud or suspicious transactions.
Opaque ownership, shell/front companies, nominees and legal arrangements	**R.24** and **R.25; IO.5** (Beneficial Ownership Transparency); where professional intermediaries are involved, relevant requirements under **R.22, R.23** and **R.28**	Adequate, accurate and up-to-date BO information that competent authorities can access efficiently can help identify persons controlling shell/front companies, nominee structures, legal arrangements, businesses and assets used to operate scam compound networks, move proceeds or conceal criminal beneficiaries. Relevant preventive and supervisory measures for DNFBPs can also address professional facilitation of such structures.
Financial intelligence, investigation and effective criminal sanctions	**R.3** (ML offence); **R.20; R.29–31; R.35; IO.6** and **IO.7**	FIUs and LEAs should have the powers, information, expertise and resources necessary to obtain, analyse and act on financial intelligence and reconstruct high-velocity, multilayered flows. Proactive parallel financial investigations can connect scam proceeds, operating expenditure, mule networks, VAs, corporate structures and assets to the wider organised criminal enterprise, while effective criminal sanctions should apply where relevant offences are established.
Physical cross-border transportation of cash and bearer negotiable instruments	**R.32**	Jurisdictions should have declaration or disclosure systems and powers enabling competent authorities to detect and restrain suspicious or falsely declared physical cross-border transportation of currency and bearer negotiable instruments and take appropriate follow-up action. This can address one element of scam compound-related value movement, but R.32 should not be presented as imposing a general requirement to control territory or prevent criminal occupation of border areas.

Table 1 continued ...

Scam compound-related area / vulnerability	Relevant FATF Standards / guidance / effectiveness framework	Operational implication for scam compound-related risk
Co-ordinated response, rapid asset preservation and recovery	**R.4** (Confiscation and Provisional Measures); **R.30–31; R.38** (Mutual Legal Assistance: Freezing and Confiscation); relevant **R.15/R.16** provisions; **IO.8** (Asset Recovery)	Jurisdictions should be able to identify and trace criminal property and take sufficiently rapid provisional action before high-velocity scam proceeds are transferred, converted or dissipated. Effective implementation should connect FI/VASP detection and tracing with competent-authority freezing, restraint, confiscation and recovery powers, including where assets are located abroad.
Domestic cross-sector co-operation	**R.2; IO.1;** FATF information sharing work cited above; FATF fraud reports/ work (2023 and 2026)	Effective responses require AML/CFT authorities to connect, where relevant, with fraud, financial consumer protection, cybercrime, anti-trafficking, immigration, corruption, asset recovery and supervisory authorities, as well as relevant private-sector actors. This is particularly important because scam compound indicators are distributed across financial, technological, telecommunications and victim-reporting environments.
Cross-border co-operation, co-ordination and information sharing	**R.37–40; IO.2; F**ATF information sharing work cited above; FATF fraud reports/work (2023 and 2026)	Scam compound cases routinely span source, transit, host/ hub, victim, laundering and asset-holding jurisdictions. MLA and other forms of international co-operation should therefore be sufficiently rapid, constructive and effective to preserve evidence, financial intelligence, criminal property and investigative opportunities, support extradition where relevant and enable co-ordinated action before assets, evidence or criminal actors move beyond reach.

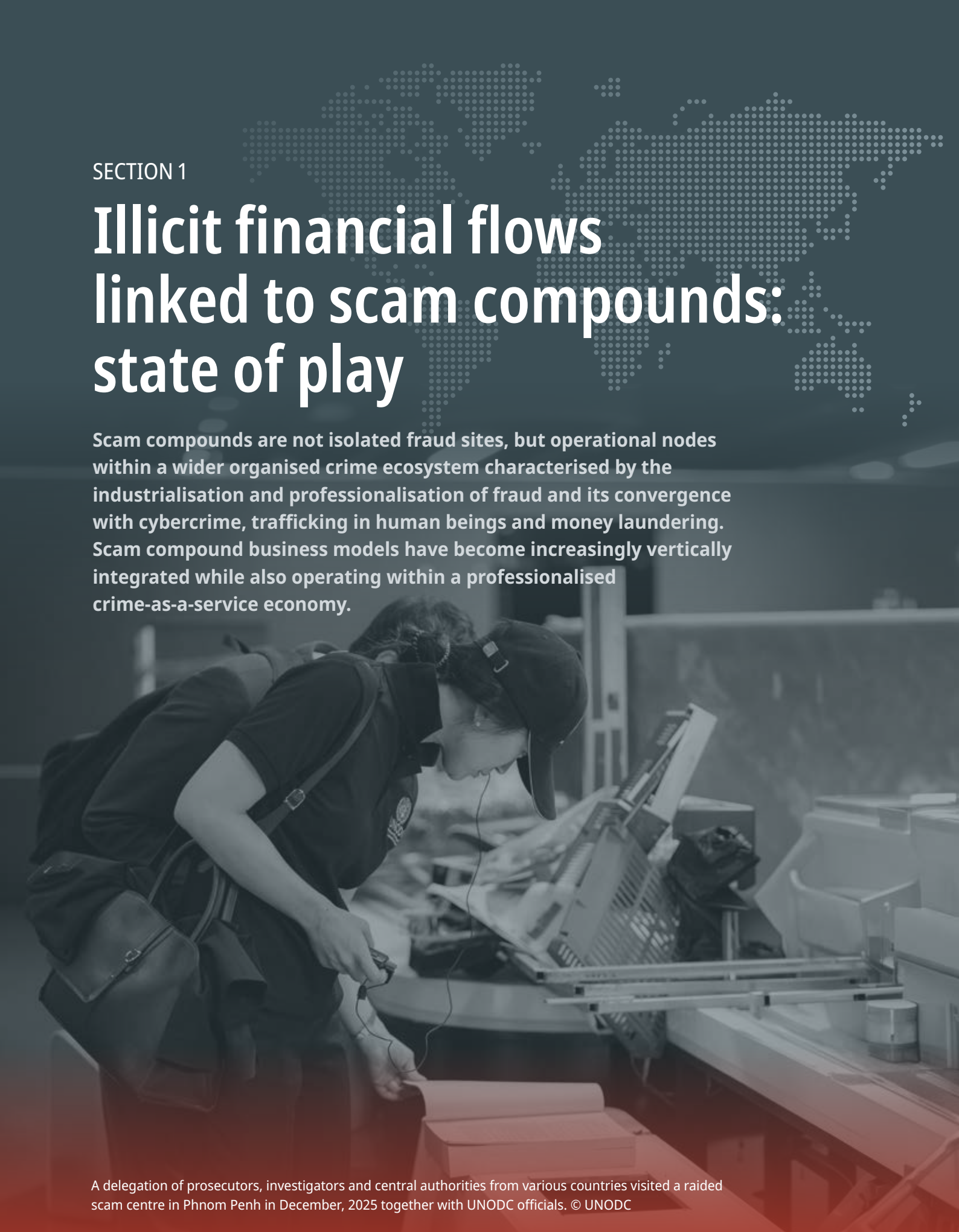


Working in appalling conditions: 3 222 potential victims have been rescued in an operation targeting scam centres. © Harald Nooij/Interpol

SECTION 1

Illicit financial flows linked to scam compounds: state of play

Scam compounds are not isolated fraud sites, but operational nodes within a wider organised crime ecosystem characterised by the industrialisation and professionalisation of fraud and its convergence with cybercrime, trafficking in human beings and money laundering. Scam compound business models have become increasingly vertically integrated while also operating within a professionalised crime-as-a-service economy.



A delegation of prosecutors, investigators and central authorities from various countries visited a raided scam centre in Phnom Penh in December, 2025 together with UNODC officials. © UNODC

4. Business models

Industrialised and professionalised fraud ecosystems

The industrial-scale scam compound model expanded rapidly from around 2020, although precursor cases of trafficking for forced online fraud predate the COVID-19 pandemic. Pandemic-related travel restrictions and casino closures disrupted gambling-based criminal business models, while increased online activity and economic disruption expanded opportunities for online fraud and deceptive recruitment. In Southeast Asia, organised crime groups were able to repurpose pre-existing casino and online-gambling infrastructure into large-scale scam operations (see subsection 5.2).

Scam compounds are not isolated fraud sites, but operational nodes within a wider organised crime ecosystem characterised by the industrialisation and professionalisation of fraud and its convergence with cybercrime, trafficking in human beings and ML. For some transnational organised criminal groups, fraud is a major proceeds-generating predicate offence, and scam compounds can function as revenue-generating nodes within broader criminal enterprises, with proceeds supporting criminal enrichment, control and influence. The criminal leadership and controllers directing or benefiting from these operations may themselves be located in jurisdictions different from those hosting the physical compound, exercising control remotely through intermediaries, shared infrastructure and cross-border financial arrangements. Recent US enforcement actions have also identified "Chinese organised crime syndicates" among those operating scam compounds and related criminal service infrastructure in Southeast Asia and, more recently, Africa[1]. The scam compound ecosystem combines physical premises, persons subjected to trafficking in human beings including for the purpose of forced criminality, digital infrastructure, specialised ML channels, and protection networks.

Scam compound business models have become increasingly vertically integrated while also operating within a professionalised crime-as-a-service economy. The same or connected criminal networks may control, procure or outsource specialised capabilities across victim acquisition, scam execution, technical infrastructure, payment collection, ML and reinvestment. Fragmentation may also occur within larger compound-based networks. The Uganda survivor-led research described in Box 24 has identified subdivisions and franchising arrangements within scam compound networks, with affiliated companies conducting different scam operations within a wider group structure. This modular service model allows operators to rely on professional brokers and providers for functions they do not perform in-house, increasing scale and resilience by enabling disrupted capabilities to be replaced rapidly. It also complicates attribution and end-to-end financial tracing.

Victim acquisition is global but segmented by market and adaptive, rather than determined by the location of the scam compound. Available evidence indicates that cyber scam hubs have targeted persons in more than 100 jurisdictions, while individual operations may specialise by country, language, platform or victim demographic[2]. Target selection may reflect language and cultural familiarity, including the skills and nationalities of the workforce, while multilingual recruitment, translation tools, victim data and online platforms enable expansion into additional markets[3]. Available reporting indicates that target markets have broadened over time, with operators adapting

1. U.S. Department of Justice (2026), *Scam Center Strike Force Takes Major Actions Against Southeast Asian Scam Centers Targeting Americans*, 23 April 2026, available at: https://www.justice.gov/opa/pr/scam-center-strike-force-takes-major-actions-against-southeast-asian-scam-centers-targeting; U.S. Department of Justice (2026), *Scam Center Strike Force Conducts Seizures of Chinese-Run Illicit Scammer Marketplace, and Restrains $52 Million in Laundered Crypto Scammer Funds In One Day*, 9 September 2026, available at: https://www.justice.gov/usao-dc/pr/scam-center-strike-force-conducts-seizures-chinese-run-illicit-scammer-marketplace-and
2. APG (2026), *Cyber Scam Hubs and Human Trafficking Report*, Asia/Pacific Group on Money Laundering, Sydney, Australia.
3. Amerhauser, K. and Goodwin, A. (2026), *A World of Deceit: Mapping the Landscape of the Global Scam Centre Phenomenon*, Global Initiative Against Transnational Organized Crime (GI-TOC), Geneva, Switzerland, March 2026, available at: https://globalinitiative.net/wp-content/uploads/2026/03/Kristina-Amerhauser-Alex-Goodwin-A-world-of-deceit-Mapping-the-landscape-of-the-global-scam-centre-phenomenom-GI-TOC-March-2026-1.pdf; OSCE (2026), *Trafficking into Cyber Scam Operations: Implications for the OSCE Region – Exploratory Assessment*, Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, Vienna, Austria, April 2026, available at: https://cthb.osce.org/sites/default/files/documents/publications/2026/04/Cyber%20Scam_Screen_260429.pdf

language, scam narratives and victim acquisition methods to different jurisdictions and victim profiles. Jurisdictions with higher levels of disposable income and financial access may be particularly attractive, although target profiles vary by scam typology[4]. However, the available evidence establishes neither a single global victim profile nor that English-speaking populations are systematically the most targeted across scam compounds. Contributions from jurisdictions instead show that scam narratives are adapted to specific target markets.

Artificial intelligence (AI) and related digital tools, including large language models, chatbots, voice-cloning tools and automated scripts, can industrialise scam operations through personalised automated messaging, predictive targeting, deepfake-enabled deception and the rapid generation of multilingual content. The principal significance of AI in this context may be as a scale and adaptation multiplier: it can reduce the marginal cost of generating, localising and varying scam content and enable criminal networks to test and replace scripts, identities and approaches more rapidly. AI may also support operational functions beyond content generation, including target research, back-office account management, evaluation of scam tactics, credential theft or authentication-bypass techniques, and the generation of new identities or transfer networks for moving illicit funds. Digital tools, including AI-assisted analysis, may also be used to detect law enforcement activity online and around criminal premises. They can support fake job advertisements, sextortion, romance and investment fraud and impersonation schemes, expanding victim outreach while reducing or changing labour requirements. Private-sector reporting also indicates rapid growth in AI-enabled scam activity, although the available evidence is not specific to scam compounds. As automation changes workforce requirements, for example through the adoption of AI agents, some models may become less dependent on large trafficked workforces and the corruption associated with maintaining large physical sites, while becoming more dependent on reliable electricity, connectivity and digital infrastructure.

Emerging agentic AI systems—which can autonomously plan, execute and adapt multi-step tasks with limited human intervention—may extend these risks beyond automated fraudulent content generation. Such systems could enable more sophisticated scam activity, for example by dynamically adapting scam workflows, generating new scam variants, or interacting with victims across multiple channels. At the same time, agentic AI may introduce new vulnerabilities. These could include the manipulation of AI agents through malicious external content or fraudulent websites, or interference with communications and tool integrations on which such agents rely. These developments should be monitored, particularly as agentic systems become more closely connected to communications, identity and payment functions.

Revenue generation

Scam compounds should be analysed as organised, revenue-generating criminal enterprises. Their profitability is generated by several revenue streams, including:

(i) **Scam proceeds.** The principal revenue source is fraud conducted from, or linked to, scam compounds. Available evidence indicates particular reliance on investment fraud, including relationship-based schemes in which offenders build trust before inducing progressively larger investments, and fake online trading schemes using fabricated dashboards, apparent initial returns and obstructed withdrawals. Romance or confidence-based techniques may facilitate these schemes rather than constitute the ultimate fraud objective. Other typologies include impersonation, phishing, business email compromise, online-gambling-related schemes and other frauds, many of which also occur outside scam compound ecosystems. Victim funds may be transferred by wire or instant payment into personal or corporate accounts or digital or VA wallets, including mule-controlled accounts or

4. UNODC (2024), *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*, Technical Policy Brief, United Nations Office on Drugs and Crime, October 2024, available at: https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf; U.S.-China Economic and Security Review Commission (USCC) (2025), *China's Exploitation of Scam Centers in Southeast Asia*, Commission Spotlight, 18 July 2025, available at: https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf

wallets, and then rapidly dispersed through further accounts or wallets, decentralised finance (DeFi) bridges, OTC brokers and other less regulated or unregulated financial channels.

(i) **Proceeds related to trafficking in human beings and exploitation, including forced criminality.** Revenue may derive from payments for trafficking services, recruitment fees, commissions paid to facilitators, transportation charges, and the sale or resale of trafficked workers between compounds. These amounts may be paid or received by the victim, recruiter, trafficker, third-party sponsor or fake employer. Forced-labour extraction also takes the form of unpaid or underpaid labour, withheld wages, inflated deductions for food, medicine and accommodation, financial penalties for failing to meet quotas and debt bondage. Some workers receive commissions, prepaid cards or virtual assets (VAs), while costs incurred within the compound are deducted from their pay.

(ii) **Ransom and release payments.** Victims or their families may be required to pay significant sums to secure release from scam compounds. Some criminal groups accept "headcount" arrangements under which victims must recruit other persons to the compound as an alternative to paying a ransom. Ransoms paid by family members and friends to criminal groups or brokers may be made in cash, through bank or other electronic transfers, or in VAs.

(iv **Recovery, refund and clearance-fee scams.** Scam compounds may re-victimise previous scam victims through recovery, refund, unlock, quota or clearance-fee schemes. Fraudulent recovery agents may claim that stolen funds have been located and request an advance fee for their return, while operators may demand additional payments before allowing the withdrawal or supposed refund of earlier investments.

(v) **Online gambling and parallel illicit services.** Online gambling and related services may provide both revenue and ML functionality, including as channels for transferring, commingling or layering scam-related proceeds. Scam compounds associated with offshore online gambling operators may combine trafficking in human beings, illegal online gambling, romance scams, VA scams and online sports betting. Illicit online gambling sites may steal player funds, harvest personal data, co-mingle revenue with other criminal proceeds and move value through tiered mule networks and high-volume, low-value micro-laundering, sometimes referred to as "scambling"[5]. Illicit online marketplaces may also monetise stolen data and sell malware, fraud tools, underground banking, ML, and cybercrime services.

(vi) **Reinvestment in criminal infrastructure and diversification.** Illicit revenue may be retained as criminal profit or converted into assets for controllers and other criminal beneficiaries, while other proceeds are reinvested to sustain, expand and diversify the criminal enterprise. Proceeds may be used to acquire geographical influence and land, construct compounds, operate front businesses, pay recruiters and transporters, bribe officials, cover lodging, documentation and transportation costs, acquire luxury goods and real estate, procure additional mule accounts and finance new scam campaigns. In addition, proceeds may also support expansion into other criminal activities, including trade-based money laundering, tax crimes, environmental crimes and other predicate offences. This reinvestment creates a self-sustaining ecosystem in which illicit capital supports further physical and digital expansion, operational diversification and the growth of the criminal group.

Organisational fragmentation, decentralisation and geographical expansion

Scam compound activity spans a spectrum of organisational models rather than a single physical form, ranging from large, fixed compounds to smaller, dispersed and mobile structures that may remain connected through common controllers, financial infrastructure and specialised service providers.

5. AUSTRAC (2025), *Scambling: the nexus between scams, money mules and micro-laundering*, November 2025, available at: https://www.austrac.gov.au/sites/default/files/2025-12/Scambling%20-%20the%20nexus%20between%20scams%2C%20money%20mules%20and%20micro-laundering.pdf

The most extensively documented model remains the large physical scam compound, often involving trafficking in human beings and forced criminality. Organised criminal groups may establish or repurpose compounds, casinos, hotels, offshore-gaming-operator-style facilities or similar premises to accommodate workers and conduct online fraud at scale. Workers may be recruited through fraudulent job offers, transported across borders and subjected to debt bondage, confinement, violence, document confiscation or performance quotas before being forced to conduct scams. Their recruitment and workforce footprint is highly transnational: UNODC reports that people from at least 80 countries and territories have been identified in scam compounds in Southeast Asia, with recruitment networks operating through transit hubs in Asia, the Middle East and Africa[6]. Forced criminality can also reach substantial scale within individual host jurisdictions: in 2023, OHCHR reported that credible sources indicated that at least 120 000 people across Myanmar may have been held in situations where they were forced to carry out online scams[7]. A single compound or criminal network may simultaneously conduct several scam typologies and other criminal activities, and generate and launder proceeds through multiple revenue streams (see subsection 4.2). These overlaps can complicate classification and illustrate the close operational convergence between organised crime, cyber-enabled fraud and trafficking in human beings in generating criminal proceeds that can support the expansion of criminal operations, assets and influence.

This organisational model is evolving, particularly in parts of Southeast Asia. Sustained enforcement pressure appears to be pushing some operators away from large fortified compounds towards smaller, dispersed and more mobile structures, including scam cells and call centre-style operations in apartments, houses, hotels, commercial premises and business-process-outsourcing-style facilities. These structures may remain connected through common controllers, financial infrastructure or service providers.

Organisational trajectories, however, are not uniform. In the Philippines, for instance, reported adaptations include rebranding as business process outsourcing (BPO) businesses or digital marketing firms and dispersal across residential areas, casinos, resorts and special economic zones (see subsection 5.2). The Philippines reports an evolution from large integrated offshore gaming operator-style compounds towards more dispersed operating models. These include call centre or boiler-room operations of around 20–300 personnel on leased floors in office towers and condominiums and smaller mobile cells of around 5–50 persons operating from rented houses that can be abandoned on short notice.

Geographic expansion is occurring alongside this organisational diversification. Scam compounds have evolved from a regional phenomenon into a global threat, with new centres reported beyond Southeast Asia, including in the Middle East and North Africa, Central America and West Africa[8] (see Box 1). This expansion may involve both the transplantation of established scam compound models by transnational criminal networks and the emergence or adoption of similar models by domestic or regional criminal groups. Individual operations may likewise vary in reach, from globally targeted models to operations focused on particular countries or regions.

Evidence cautions against equating every geographical expansion of organised scam syndicates with replication of the large physical compound model. Some operations may instead consist of smaller geographically dispersed call-centre or scam-cell operations orchestrated by a common leadership structure. Mexico, for example, reports suspected scam compound-type activity involving small and medium-sized clandestine call centre operations

6. UNODC (2026), *An Interconnected Criminal Ecosystem: Transnational Organized Crime Threat Assessment for South-East Asia*, July 2026, available at: https://www.unodc.org/roseap/uploads/documents/Publications/2026/TOCTA_South-East_Asia_2026.pdf
7. Office of the United Nations High Commissioner for Human Rights (OHCHR) (2023), *Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response*, 28 August 2023, available at: https://bangkok.ohchr.org/sites/default/files/wp_files/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf
8. INTERPOL (2026), *Global Financial Fraud Threat Assessment*, Second Edition, INTERPOL, March 2026, available at: INTERPOL (2026), *Global Financial Fraud Threat Assessment*, Second Edition, INTERPOL, March 2026, available at: https://www.interpol.int/content/download/24291/file/INTERPOL%20Global%20Financial%20Fraud%20Threat%20Assessment%202026.pdf

in urban commercial or residential premises, including timeshare fraud primarily targeting U.S. and Canadian citizens. The United Arab Emirates similarly reports confirmed domestic scam compound activity, principally call centre-style operations and smaller mobile cells in rented urban premises (see Box 2).

Several OSCE participating States have reported forced cyber-scam operations, including trafficking-linked call centre operations in Austria, Belarus, Croatia, Lebanon, Montenegro, North Macedonia, Poland and Türkiye[9]. Belarus also reports confirmed scam compound activity using call centre models in business centres in regional cities. Türkiye reports a 2024 scam compound-linked case involving an office-based call centre in Istanbul staffed by 20 persons; the network used impersonation schemes to defraud victims, transferred proceeds through mule accounts and subsequently converted them into VAs or gold. Austria reports suspected scam compound-linked activity involving Austrian bank accounts, locally based money mules and Austrian telephone numbers, while assessing its exposure primarily as a destination, transit and laundering jurisdiction rather than as a host jurisdiction. Identified activity included both larger call centre operations in commercial premises and smaller groups operating from hotels or private rooms. Taken together, these cases illustrate that organised scam operations outside Southeast Asia may operate from ordinary urban or commercial premises rather than large fortified compounds, and may take the form of call centres, boiler-room investment-fraud operations, trafficking-linked schemes, hotel-based operations or smaller scam cells.

The trafficking footprint extends considerably beyond the locations in which scam operations have been identified. Persons trafficked into cyber-scam operations in OSCE participating States have included nationals of countries across Western, Eastern and South-Eastern Europe, the South Caucasus and Central Asia, as well as persons from Mongolia, South America and Eastern Africa.

BOX 1. **Examples of scam compound activity and operating models in Africa**

Nigeria: In November 2024, authorities identified a gated boiler-room scam compound in Abuja housing 113 foreign nationals, followed by scam compound activity in Lagos and Delta State. Nigeria reports a shift from predominantly foreign-operated activity towards mixed and indigenous operators and is also identified as a recruitment and source jurisdiction for persons trafficked to scam compounds in Southeast Asia. Nigeria further reports a 2025 trafficking-linked cybercrime operation in Oyarifa, Ghana, involving 231 Nigerian nationals, many recruited through deception and coerced into cybercrime, and assesses the case as indicative of networks relocating into neighbouring West African jurisdictions in response to enforcement pressure in Nigeria.

South Africa: GI-TOC reports that Nigerian confraternity-based criminal networks operate small, highly networked scam cells in South Africa, generally comprising up to six persons and operating from houses, hotel rooms and apartments. Rather than centralising activity in a single compound, these micro-cells form part of larger collaborative networks overseen by the confraternities and draw on shared technology, expertise and resources. This dispersed model can support industrial-scale scamming despite a limited physical footprint.

Recent reporting also indicates increasing scam compound activity and exposure in Africa. GI-TOC identifies 14 African countries as particularly at risk from the expansion of industrial-scale scam operations and reports underground banking and informal value transfer systems used to launder scam proceeds in at least 10 of them. Reported operating models include hotels and resorts, call centre or BPO-style facilities and casino-linked sites, suggesting that expansion into Africa may reproduce operational and laundering infrastructure observed in Southeast Asia

9. OSCE (2026), *Trafficking into Cyber Scam Operations: Implications for the OSCE Region – Exploratory Assessment*, Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, Vienna, Austria, April 2026, available at: https://cthb.osce.org/sites/default/files/documents/publications/2026/04/Cyber%20Scam_Screen_260429.pdf

while adapting to local conditions[10]. Contributions from ESAAMLG members provide further evidence from Southern Africa. These cases illustrate that emerging African operating models may range from ordinary urban commercial premises to larger workforce-intensive sites and may depend on cross-border financial infrastructure.

Taken together, these developments indicate that enforcement pressure may displace or reconfigure rather than eliminate the underlying activity. Operations may close, relocate, rebrand or re-emerge in smaller forms, while associated platforms and service providers may migrate or be replaced. As such, Cambodia reports that enforcement against larger scam compounds has been followed by fragmentation into smaller and more mobile operations, including rented rooms or apartments, coffee shops and moving vehicles, as well as more remotely organised distributed workforces. Germany similarly reports cases in which call centre operations relocated from Türkiye to Lebanon following successful law enforcement action, illustrating the capacity of such operations to shift jurisdiction in response to enforcement pressure. **A decline in visible large-scale compounds should therefore not, without further analysis, be interpreted as a decline in the underlying networks or related illicit financial flows.**

Operating costs and associated financial flows

Operating expenditure provides a complementary financial lens to the revenue streams described in subsection 4.2 and the enabling infrastructure described in subsection 6. The same transaction may constitute revenue for a recruiter, facilitator or service provider and expenditure for a scam compound network. This subsection therefore focuses on expenditure-side financial and operational footprints associated with establishing and sustaining scam activity.

The main operating costs and associated financial or operational footprints include:

(i) **Premises and physical infrastructure.** Expenditure may include the acquisition of land, construction of purpose-built compounds, and the conversion, rental or use of casinos, hotels, apartments, business parks and other commercial premises, as well as server-room rentals and expenditure on Internet infrastructure. Once established, large compounds require continuous Internet connectivity, electricity, fuel, food supplies, technical and networking equipment, transport and security, and therefore remain dependent on physical supply and access routes despite the digital nature of their scam activity. Relevant indicators may include unusually high or continuous electricity and Internet usage, high-bandwidth activity at unusual hours, regular food deliveries, purchases and deliveries of large quantities of electronic equipment, shuttle vehicles transporting workers, secured perimeters, armed guards and facilities operating continuously.

(ii) **Workforce recruitment and transportation.** Scam compound networks may pay recruiters, trafficking facilitators, document handlers and transporters and cover air tickets, passports, visas, ferry or road transport, accommodation, lodging and other travel-related expenses. Funds may also be used to pay recruitment-processing fees and bribes to corrupt officials involved in the trafficking chain. Transportation costs may be paid by traffickers or recruitment agents, third-party sponsors, purported employers or the victims themselves. Such payments may be made through bank accounts, cash withdrawals or VA wallets, potentially linking recruiters, facilitators, source-country agents and compound operators.

(iii) **Labour costs.** Labour costs vary according to whether workers are complicit, nominally employed or subjected to forced criminality. Some cases refer to monthly salaries or compensation, differentiated in certain instances by language skills or nationality and accompanied by food, accommodation or travel. Other workers receive no salary, have their wages withheld, or are subjected to financial penalties, debt bondage and demands to repay recruitment and travel expenses. Forced labour allows compounds to maintain a low-cost, productive and replace-

10. Tower, J. G. (2026), "China-linked scam operations pivot to Africa, presenting new challenges for at-risk countries", Global Initiative Against Transnational Organized Crime (GI-TOC), 19 May 2026, available at: https://globalinitiative.net/analysis/china-linked-scam-operations-pivot-to-africa-presenting-new-challenges-for-at-risk-countries/

able workforce while transferring part of the operating costs to trafficked persons and their families. Where an operation presents itself as a legitimate employer or business, relevant financial footprints may include payroll or purported salary payments, unusually low expenditure on wages, food, medical care and other necessities relative to the reported workforce, payments for dormitory-style accommodation, and transactions associated with the sale or transfer of workers between compounds.

(iv) **Digital and communications infrastructure.** Scam networks incur expenditure on the technology and telecommunications infrastructure described in subsection 6.6, including accounts and telephone numbers, connectivity, domains and hosting, server or cloud services, paid advertising and fraud-enabling tools. VAs are a primary means used by organised crime groups to pay for crime-as-a-service subscriptions, virtual private networks (VPNs) and malicious domain hosting; where such services support scam compound activity, these payments form part of the upstream financial footprint and may complicate attribution to higher-level organisers. At scale, automated and AI-enabled scam activity may also create material demand for computing capacity, data storage and bandwidth, whether procured directly or through cloud and other service providers. Related payments and usage patterns may therefore provide indicators of scam activity, including payments to providers, purchases of communications and networking equipment, including unusual bulk purchases of pre-paid SIM cards, domain registration and hosting records, and account, device and network metadata.

(v) **Financial and laundering infrastructure.** Maintaining access to the financial and laundering infrastructure described in subsections 6.1–6.5 also generates costs, including compensation for mule accounts or VA wallets and payments to account providers, facilitators, payment intermediaries, VASPs, OTC brokers, unlicensed or unregistered money or value transfer services (MVTS) and professional money laundering (PML) service providers. Jurisdictional experience also indicates that scam proceeds may be collected through offshore accounts or VA wallets while recurring domestic operating expenditure—including payroll, rent, utilities, procurement, security and permits—is settled through the offshore regulated financial system on comparatively predictable cycles. Payroll and unusually large electricity and Internet expenditure may provide useful indicators, while locally held land, buildings, vehicles and corporate structures may provide more persistent targets for financial investigation, freezing and forfeiture.

Decentralisation may therefore shift operating footprints from concentrated expenditure associated with large compounds towards smaller and more dispersed financial and operational indicators across multiple locations and service providers.

Relationship between scam compounds and the broader fraud ecosystem

Scam compound activity sits at the intersection of cyber-enabled fraud and transnational organised crime and forms part of the broader cyber-enabled fraud ecosystem rather than a separate category of fraud. Elements of the financial and technological infrastructure supporting scam compounds may also be shared with or exploited by other illicit actors. Jurisdictional experience shows that many associated fraud typologies and elements of the underlying financial architecture—including mule-controlled accounts and wallets, FIs, MVTS, VASPs, P2P and OTC channels, cash, shell or front companies and underground banking networks—are shared with other fraud networks, as are professional providers of fraud-enabling, payment and laundering services. Other forms of securities market misconduct may arise in the same online investment and promotional environment without constituting scam compound activity. IOSCO has, for example, identified risks of market manipulation and insider trading by finfluencers. Such conduct should not in itself be treated as evidence of scam compound activity and falls within the scope of this report only where it is linked to scam compound-related actors, illicit financial flows or enabling infrastructure[11]. Scam compounds nevertheless remain distinctive in the industrialised organisation of fraud through physical or linked decentralised structures, frequently combined with trafficking in human beings and forced criminality, creating a

11. International Organization of Securities Commissions (IOSCO) (2025), *Finfluencers*, Final Report, FR/08/2025, May 2025, available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD795.pdf

dual-victim model and additional financial flows linked to worker recruitment and exploitation, ransom or release payments, premises and protection, and reinvestment. Financial indicators common to the broader fraud ecosystem should therefore not, in isolation, be treated as evidence of scam compound activity. The relevant feature is their connection to this wider operational and financial infrastructure.

5. Contextual drivers

Contextual drivers enabling the development, operation and expansion of scam compound-related activity arise from a combination of structural conditions, victim-side vulnerabilities and weaknesses in prevention and detection. OECD analysis of financial scams and frauds more broadly identifies four mutually reinforcing drivers—rapid digitalisation, low digital financial literacy or capabilities, increasing scam sophistication and inadequate detection systems. Although not specific to scam compounds, these factors are relevant where they increase victim exposure, facilitate scam execution or weaken early intervention[12]. Labour-market conditions may also increase vulnerability to recruitment into financial scams and frauds: in some jurisdictions, unemployment, underemployment and limited access to legitimate employment opportunities may increase exposure to deceptive job offers used for recruitment.

Questionnaire responses provide additional empirical support for several contextual drivers more directly associated with scam compounds. Border environments—particularly border areas and corridors used to move trafficked persons, cash, supplies and other criminal logistics, where law-enforcement access or oversight may be uneven—were the most frequently identified factor, followed by weaknesses in government control and oversight and corruption; special economic or free-trade zones are identified less frequently. The relevance of these factors is context specific and they should not be treated as universal drivers of scam compound activity[13].

Weak, fragmented or contested government control, border environments and special zones

Large, labour-intensive scam compounds have historically been concentrated, particularly in the Mekong subregion, in locations where effective government control or law enforcement access is weak, fragmented or contested, including border areas and, in some cases, areas influenced or controlled by armed or paramilitary groups. Compounds are reported both in very remote locations, including jungle areas without road access, and in more conventional border region and urban settings. Thailand illustrates the cross-border dimension, reporting exposure to neighbouring scam compounds as a target jurisdiction, transit corridor for trafficked workers and criminal logistics, and financial-routing hub. Checkpoints and corridors along its borders with Cambodia and Myanmar have also been used to move trafficked persons and criminal logistics and to smuggle cash[14].

Such environments are not necessarily governance vacuums: state, armed, militia-linked or other local actors may exercise overlapping or brokered control over territory and key passage routes, facilitating or restricting flows of workers, supplies and other resources and creating opportunities for protection and rent extraction.

Border-area compounds often coincide with special economic and other designated free zones. In July 2026, for example, Malaysian authorities dismantled two sc am compound networks operating across 27 apartments and five bungalows in Forest City, an special economic zone/free zone-linked development area in Johor. Such zones are not inherently less regulated: vulnerabilities may arise where preferential customs or business arrangements, high volumes of international activity or complex corporate and ownership structures coincide with unclear jurisdictional

12. OECD (2026), *Protecting Consumers from Financial Scams and Frauds*, OECD Publishing, Paris, Chapter 2, available at: https://doi.org/10.1787/d41817bb-en

13. UNDP (2026), *Countering Digital Scams: Stemming the Tide on an Urgent Development Challenge*, UNDP Issue Brief, United Nations Development Programme, 26 February 2026, available at: https://www.undp.org/sites/g/files/zskgke326/files/2026-02/undp-countering-digital-scams.pdf

14. APG (2026), *Cyber Scam Hubs and Human Trafficking Report*, Asia/Pacific Group on Money Laundering, Sydney, Australia.

authority, limited enforcement access or other oversight gaps. These conditions may facilitate scam operations and the movement of proceeds through companies, accounts and other financial or commercial channels, while enabling operators to relocate or rebrand rapidly under pressure and foreign workforces to attract less scrutiny.

However, **as scam operations decentralise into smaller and more mobile structures, fixed locational characteristics become less determinative.** Operations can increasingly function across a wider range of urban, residential, commercial and other settings, even where the governance, border or special-zone conditions historically associated with large compounds are absent.

BOX 2. **Examples of decentralisation of scam compound operations**

Japan: Japan reports scam compound-related operations using rental condominiums, offices and apartments, ordinary and public housing, vehicles, hotels and private lodging facilities, with identified activity in 2025 concentrated mainly in densely populated urban areas. Criminal groups are considered to seek to evade law enforcement detection and disruption by dispersing the functions of their operational bases, reducing the scale of individual sites, and diversifying the types of premises used. These practices reduce their physical visibility and disperse their financial and operational footprints.

Lao PDR: In Lao PDR, GI-TOC reports that scam activity historically concentrated around the Golden Triangle Special Economic Zone has also been observed in smaller compounds in Vientiane Capital and Khammouane Province, illustrating this geographical dispersal.

United Arab Emirates: In a 2025 case currently under trial, UAE authorities identified a suspected short-term mobile fraud centre operated by five foreign nationals from three adjoining hotel rooms in Ajman. The group allegedly used fraudulent social-media advertisements and foreign SIM cards to obtain victims' bank-card data and one-time verification codes, which were used to purchase smartphones for subsequent cash resale.

Casinos, online gambling and former gambling infrastructure

Scam compounds and related operations may also be located in or around casinos and online-gambling facilities. The development of many large scam compounds in Southeast Asia was closely linked to online-gambling ecosystems, with operators, premises and supporting infrastructure subsequently repurposed or expanded into scam activity, particularly during and after the COVID-19 period. Casinos, hotels and Philippines offshore gaming operator-style facilities could provide both physical infrastructure and cover for scam operations, while casinos, junkets, illegal online casinos, e-junkets and VA exchange services—including VASPs and unlicensed or unregistered providers—also form important components of underground banking and ML infrastructure in East and Southeast Asia.

Heightened risks arise where casino junkets, online gambling platforms, OTC VA services and FIs operate within the same ecosystem. Reported arrangements include junket operators accepting USDT in exchange for casino chips, VA exchange services operating in or near casinos, and financial services providing access to several currencies within high-risk casino environments. Such arrangements may combine gambling, VA exchange, cross-border value transfer and ML activity, obscuring the full criminal-finance chain, particularly where customer due diligence (CDD), BO transparency and supervision are weak.

Corruption and protection networks

Corruption and protection networks can be critical enablers of the establishment, operation and protection of scam compounds, particularly large, labour-intensive operations requiring sustained access to land, infrastructure, cross-border movement and protection from enforcement. Corrupt or complicit officials—including police, border and immigration personnel and officials in licensing bodies—may facilitate access to or acquisition of land, premises, infrastructure and real estate; trafficking and cross-border movement, including through the circumvention of visa or entry controls; security and armed escorts; and the shielding of criminal operations from enforcement. Protection arrangements may also facilitate continued access to transport and supply routes, the movement or relocation of workers and operations and, in some reported cases, advance warning of enforcement action. High-level political and business protection can further sustain these operations. Evidence has identified links between scam compound networks and politically exposed persons (PEPs), including in cases involving shell companies, real estate transactions, foreign exchange activity, VA transactions, land acquisition and the construction of compounds. Operations against online-scam activity identified senior officials suspected of bribery, abuse of authority or collusion with criminal actors; relevant officials were arrested and are subject to prosecution, while associated assets were frozen. Bribes and other corruption payments may therefore form part of the operating costs of scam operations.

Opaque beneficial ownership and misuse of legal and regulated structures

Opaque BO and misuse of legal persons can enable those controlling scam compound networks to conceal their ownership or control of businesses, assets and operational infrastructure and to operate through apparently legitimate structures. Cross-border ownership chains, nominees, shell or front companies and multilayered corporate structures can obscure links to the persons directing or benefiting from scam compound activity.

Criminal networks can further exploit complicit employment and travel agencies and businesses in hospitality, real estate and logistics to provide a façade of legitimacy, facilitate recruitment, trafficking, cross-border movement and access to premises, and support wider operational activities. Controllers and beneficiaries may rely on professional intermediaries in jurisdictions where they establish residence, companies or assets—including, where relevant, trust and company service providers, legal and accounting professionals, real estate intermediaries and migration or residence service providers—to establish legal structures, acquire or manage assets or facilitate cross-border mobility. Scam compound-linked criminal actors may also exploit citizenship-by-investment or residence-by-investment arrangements, investment-linked acquisition of citizenship and multiple nationalities to facilitate cross-border mobility and complicate law enforcement identification, attribution and asset tracing[15].

These risks may arise from complicit facilitation or failures to identify red flags. In investment fraud schemes, misuse of licensed or apparently regulated entities, cross-border financial services arrangements and complex corporate structures can facilitate regulatory arbitrage and create an appearance of regulatory legitimacy that increases victim trust and reduces suspicion[16]. More broadly, complex corporate structures, including shell or front companies, are identified as a primary means of laundering scam compound proceeds.

Digitalisation, scam sophistication and victim exposure

Digitalisation increases both the reach of scam networks and the exposure of potential victims. Widespread use of mobile devices, social media, messaging, online platforms and digital financial services enables scam networks to target victims remotely and operate across jurisdictions at scale. Low digital financial literacy or capabilities may increase vulnerability to fraudulent investment platforms, impersonation, social engineering and other deceptive

15. U.S. Department of the Treasury (2026), *Treasury Sanctions Cambodian Senator Kok An and Scam Center Network Defrauding Americans*, 23 April 2026, available at: https://home.treasury.gov/news/press-releases/sb0469

16. FinCEN (2026), *FinCEN Alert on Money Laundering Activity Associated with Digital Asset Investment Scam Centers*, FIN-2026-Alert005, 3 September 2026, Financial Crimes Enforcement Network, U.S. Department of the Treasury, available at: https://www.fincen.gov/system/files/2026-08/FinCEN-Alert-Scam-Centers.pdf

online activity, while increasingly sophisticated techniques—including AI-enabled content, deepfakes and automation—can make scams harder to identify even for more experienced users. These factors can reinforce one another as digital services expand and scam techniques evolve (see subsection 4.1).

Weak or fragmented oversight and prevention and detection systems

Weak, fragmented or inconsistent oversight, prevention and detection systems can create gaps that scam compound networks exploit to establish and sustain operations, access financial and commercial services and generate, move or conceal proceeds. Vulnerabilities may arise where regulatory responsibilities or perimeters are unclear; oversight does not keep pace with evolving business models, payment channels or digital services; or FIs, VASPs and other relevant actors lack sufficiently effective or timely systems to identify higher-risk or fraud-induced transactions. In fast payment environments, these vulnerabilities may be exacerbated where limited information sharing between FIs and VASPs participating in the same payment flow prevents the timely identification and disruption of suspicious transactions. In jurisdictions hosting scam compounds or associated ML infrastructure, weaknesses in risk-based supervision of FIs and VASPs may further reduce detection of activities associated with those networks (see also subsection 8). For VAs, such vulnerabilities may be amplified where implementation and enforcement of applicable R.15/INR.15 requirements are uneven across jurisdictions, allowing criminal activity to shift towards offshore or weakly supervised VASPs and unlicensed or unregistered providers, as well as P2P and OTC arrangements[17]. These vulnerabilities are exacerbated where jurisdictions require VASPs to be licensed or registered only if physically established in their territory. Offshore VASPs may therefore provide services into a jurisdiction, including to scam compounds, without being subject to its licensing or registration regime, potentially limiting the jurisdiction's legal basis to monitor or take action against them. Supervisory, licensing or other regulatory action against individual institutions or service providers may nevertheless have limited systemic effect where criminal networks retain access to substitute channels or continue to benefit from weak enforcement, corruption or official protection. Such measures should therefore be connected to network-level investigation and disruption targeting controllers, assets, shared infrastructure and specialised facilitators.

6. Enabling financial and non-financial infrastructures

Illicit financial flows linked to scam compounds are increasingly enabled by interconnected financial and non-financial infrastructure that increases the speed, scale and concealment of criminal proceeds. Questionnaire responses also underline the continued importance of off-chain channels: cash is the most widely observed financial flow channel linked to scam compounds, followed by informal MVTS and underground banking. The principal enablers are examined below.

Bank and non-bank financial institutions

Scam compound-related financial flows can move at high velocity: instant or fast payment systems, digital wallets and other payment or value transfer methods may carry funds from the initial victim payment to onward transfer or cash-out within hours or even seconds. These funds involve obliged entities at multiple points of the flow: through victim customers sending funds to mule accounts; through customers acting as perpetrators, money mules, front companies or end beneficiaries; and indirectly through correspondent banking or other similar relationships—such as nested VASP relationships—used to transmit or facilitate related proceeds. In addition to this speed, the use of virtual account numbers, such as virtual IBANs, may add opacity by obscuring the relationship between the account identifier presented to the customer and the underlying account or FI. Overall, the resulting speed of payment execution and subsequent ML can significantly reduce the practical window for payment suspension, freezing, recall and recovery. Scam networks may also adapt to controls by shifting funds towards cash-based and other less regulated non-bank

17. FATF (2026), *Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers (oVASP)*, FATF, Paris, France, available at: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/understanding-mitigating-risks-offshore-vasps-2026.html

channels. Jurisdictional experience further indicates that mobile money platforms can be significant collection and transfer channels in some African contexts: Mozambique, for instance, reports mobile VA wallets as the principal payment method in cases it associates with scam compounds.

Money mule networks

Money mule networks provide a critical interface between victims, payment channels and subsequent ML activity. Criminal groups may recruit or exploit vulnerable persons—including older persons, young people and those in economic distress—to provide personal or corporate accounts and digital or VA wallets, sometimes without understanding the underlying criminal activity. Mule acquisition increasingly also involves buying, selling or stealing identities to open multiple accounts or wallets across providers, enabling repeated use of the same identity and circumvention of name-matching controls. Victim funds may then move through further accounts, VA wallets and FIs, with transfer speed determined principally by the underlying payment method; instant payments, wallet-to-wallet transfers and VA transfers can move funds onward within minutes, in some reported cases within two minutes. Specialised facilitators, shared devices, repeated account-opening arrangements and corporate structures can further obscure the wider mule network.

VASPs and VA

VAs remain a central ML channel for scam compound proceeds. The use of offshore VASPs, P2P VA transfers, OTC brokers and crypto ATMs has been repeatedly identified in scam compound-related typologies. Jurisdictional submissions identify patterns in which proceeds collected from domestic victims through local mule accounts or e-wallets are rapidly converted through P2P VA transactions and transferred offshore to scam compounds. They also identify cases in which dedicated OTC counters operate inside scam compounds for VA exchange and domestic fund transfer, illustrating that payment and VA-conversion functions may in some cases be physically embedded within compound operations rather than wholly outsourced. In Southeast Asia, recent UNODC reporting identifies USDT issued on the TRON network as particularly prominent in scam-related laundering, reflecting its widespread availability, high

BOX 3. **Use of proprietary VA infrastructure to circumvent freezing measures**

United States: In one significant documented case, a Cambodia-based conglomerate linked to the laundering of proceeds from Southeast Asian scam operations developed proprietary VA infrastructure intended to reduce its reliance on regulated VASPs and circumvent freezing measures. The conglomerate, which was also linked to a major illicit online marketplace, launched a proprietary USD-backed stablecoin that it promoted as resistant to freezing and not subject to restrictions imposed by traditional regulatory authorities. Issued on several blockchains, the stablecoin formed part of broader proprietary infrastructure that included a blockchain, wallet, exchange and payment services.

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) subsequently assessed that the group transitioned operations from one payment-service entity to a successor entity in an effort to evade public scrutiny and circumvent the special measure imposed against it. In June 2026, FinCEN expressly extended the restriction to H-Pay Service PLC and future successor entities, illustrating the importance of accounting for rebranding and successor structures when designing and monitoring financial restrictions.

Although this remains a unique documented case rather than evidence of a broader trend, it illustrates how an entity supporting a scam compound ecosystem may integrate stablecoin issuance, payment and exchange services to retain greater control over illicit financial flows and reduce the ability of stablecoin issuers, VASPs and LEAs to freeze or recover criminal proceeds.

liquidity, relative price stability and usability across VA platforms, wallets and jurisdictions. The same reporting identifies Telegram-advertised "U-merchants" that exchange USDT, other VAs and fiat currency for money launderers through arrangements that may bypass standard know-your-customer (KYC) controls[18]. Criminals may also adapt to VA controls by shifting exit routes towards cash-based and other less regulated non-bank channels, including through OTC brokers operating as unlicensed or unregistered MVTS.

Corporate structures

Legal persons and corporate accounts can function as transactional infrastructure for scam compound networks, receiving, transferring, commingling or integrating proceeds and connecting mule networks with FIs, MVTS and VASPs, as well as OTC brokers and underground-banking providers.

Professional fraud and PML service providers

Scam compound networks rely on specialised providers supplying payment facilitation and financial rails, gateway services, mule accounts and wallets, unlicensed or unregistered MVTS, VA conversion and OTC services, underground banking and specialised ML services. Other providers may supply hosting, synthetic identities, compromised data and accounts, malware, fake investment platforms, scam scripts, deepfake tools, AI-enabled content-generation, localisation, impersonation or automation services, and other fraud-enabling capabilities. Reflecting the importance of professional facilitators, APG members reported widespread involvement of professional intermediaries and other facilitators in laundering proceeds from scam compounds and trafficking in human beings. Gateway companies and other intermediaries connect scam operations with ML providers through encrypted communications and digital payment platforms. This crime-as-a-service model allows operators to outsource specialised functions and replace disrupted infrastructure rapidly, increasing operational resilience while complicating attribution and end-to-end tracing.

BOX 4. **Guarantee marketplaces as shared criminal infrastructure**

United States: In September 2026, US authorities took co-ordinated action against Xinbi Guarantee, a Chinese-language illicit online marketplace operating through Telegram and used by scam compound operators to procure criminal services. The US Treasury described Xinbi as a central node connecting transnational criminal syndicates, including scam compound operators, with merchants providing financial services, technology and other goods and services supporting criminal operations, and as providing escrow services to scam operators, ML networks and cybercrime syndicates. Treasury further described the platform as being used extensively by Chinese cybercriminals. The US Department of Justice alleged that vendors advertised services including custom scam investment websites, ML services and the recruitment of trafficking victims for work in Southeast Asian scam compounds. US authorities seized relevant Telegram channels and VA wallets and restrained more than USD 52 million associated with Xinbi and its vendor network. Treasury reports that Xinbi processed more than USD 24 billion equivalent in digital assets and fiat currency since around 2022 and that criminal activity shifted towards Xinbi following US action against Huione Pay.

Illicit online marketplaces, including Telegram-based guarantee or escrow marketplaces, can function simultaneously as marketing venues, payment infrastructure and trusted intermediaries between criminal participants. They may hold payments in escrow and provide dispute-resolution or transaction-insurance mechanisms, while connecting scam operators with PML and underground banking networks and facilitating access to VAs, OTC conversion, accounts, social media account services, targeting, phishing and other fraud-enabling tools. Disruption of individual marketplaces may lead to rapid reconstitution through successor groups, rebranding or alternative infrastructure, underscoring the importance of identifying the wider service-provider network.

18. UNODC (2026), *An Interconnected Criminal Ecosystem: Transnational Organized Crime Threat Assessment for South-East Asia*, July 2026, available at: https://www.unodc.org/roseap/uploads/documents/Publications/2026/TOCTA_South-East_Asia_2026.pdf

Technology and telecommunications infrastructure

Technology and telecommunications infrastructure can support functions across the scam compound lifecycle, including the recruitment of workers, identification and communication with victims, scam execution and co-ordination of related activity. Criminal networks may exploit legitimate services alongside illicit infrastructure; the relevant risk lies in their criminal exploitation rather than in the technologies or services themselves. Relevant infrastructure includes social media and messaging services, telecommunications networks and SIM infrastructure, including SIM boxes and SMS-blasting or rogue base-station equipment used to disseminate malicious messages, encrypted communications channels, Internet domain and hosting infrastructure including the domain name system (DNS) sector, online advertising, fraudulent websites and applications, server and cloud infrastructure, VPNs, satellite Internet equipment, data brokers, fake investment platforms, customer relationship management tools and illicit online marketplaces. Social media and online platforms can disseminate fraudulent advertisements and investment promotions; where connected to scam compound activity, including through misleading or fraudulent finfluencer content, such channels can form part of upstream victim acquisition (see subsection 4.1). AI-enabled tools, including deepfakes, voice cloning, chatbots, large language models, automated scripts and multilingual content, can further increase the scale and sophistication of victim targeting and engagement.

Taken together, the contextual conditions described in subsection 5 and the financial and non-financial infrastructures described in subsection 6 form the wider enabling ecosystem within which scam compound networks can establish, operate and expand. These enablers may support different functions across the scam compound lifecycle rather than correspond to a single stage. Infographic 1 summarises these interacting enablers. These enablers are not equally important or equally replaceable: their disruption value depends in particular on the functions they support, whether they are shared across multiple criminal networks, and how readily the network can substitute them.

Functional dependencies, bottlenecks and replaceability

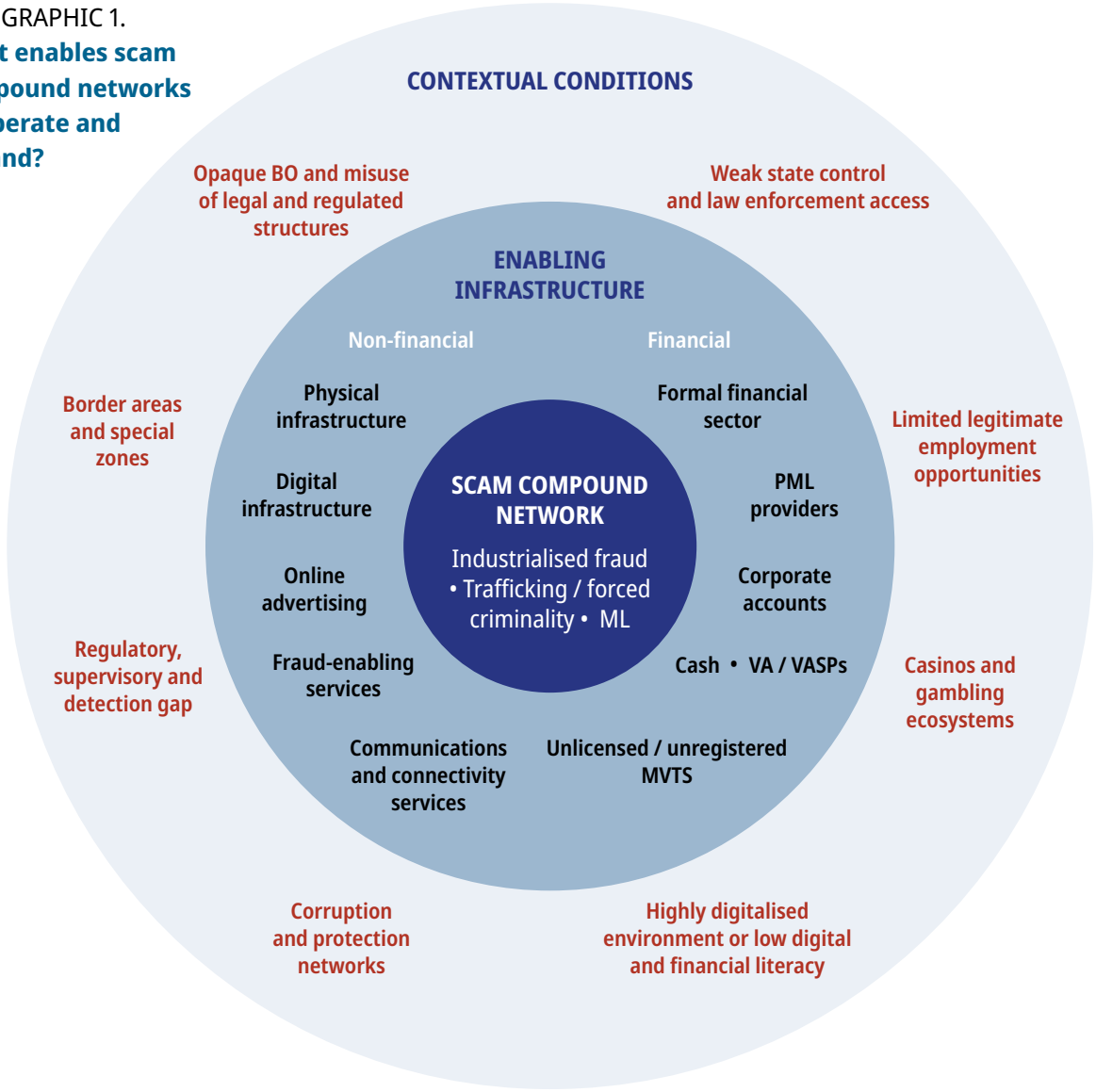
For the purposes of this report, functional dependencies are the capabilities, services, infrastructure and relationships on which scam compound networks rely to perform functions across their lifecycle. The concept focuses on what enables a function to be performed, irrespective of whether the capability is provided internally, by an affiliated entity or by an external provider. Scam compound ecosystems increasingly exhibit a functional and international division of labour. Different actors may specialise in worker or victim recruitment, scam execution, technical enablement, payment collection, mule recruitment, VA conversion, laundering or cash-out, while common service providers may support multiple scam operations or criminal networks.

Jurisdictional experience suggests that the allocation of functions across scam compound ecosystems can be understood along a spectrum of organisational integration and outsourcing. These models are not mutually exclusive: different functions within the same criminal network may follow different arrangements, and networks may move between models over time.

(i) **Vertically integrated models**, in which the same criminal organisation controls most of the principal functions required to operate the scam compound, potentially including workforce and victim recruitment, scam execution, technical infrastructure, payment collection, movement and laundering of proceeds and reinvestment. Individual functions may be performed by specialised teams, but remain under common organisational control rather than being outsourced to independent providers.

(ii) **Hybrid or core and outsourced models**, in which the criminal organisation retains control of core functions—typically scam execution and some operational, managerial or financial capabilities—while selectively outsourcing other functions to external facilitators. Outsourced functions may include worker recruitment, mule account acquisition, payment gateways, cash collection, VA conversion, telecommunications, victim data, domains, hosting or other technical services.

INFOGRAPHIC 1.
What enables scam compound networks to operate and expand?



(iii) **Distributed network models**, in which functions or scam operations are allocated across distinct cells, affiliated entities or geographically dispersed components linked by common controllers, shared infrastructure or financial arrangements. Individual units may specialise in victim-facing scams, recruitment, payment collection, money movement, technical support or other functions, or may conduct separate scam operations within a wider group structure. This model can allow the wider network to remain operational even when an individual site or component is disrupted.

(iv) **Externally serviced or crime-as-a-service models**, in which substantial capabilities are procured from specialised providers operating outside the core scam organisation and potentially serving multiple criminal networks. These may include PML providers, mule account and front company suppliers, underground banking or VA conversion services, victim-data brokers, telecommunications and hosting providers, fraudulent-website developers and illicit marketplaces or intermediaries that connect scam operators with such services.

BOX 5. **Functional specialisation and outsourcing across scam compound ecosystems**

Belarus reports distributed models in which direct fraud is separated from financial and technological support, with external intermediaries providing accounts and payment instruments, cash-out and cross-border fund movement, VA conversion, SIM cards, domains and hosting and fictitious profiles.

India reports cases in which HR functions, including salary payments, and IT and physical set-up were performed within the compound, while recruitment of trafficked persons, illegal payment gateways, SIM sourcing, cross-border calling through SIM-box operators, cash-to-VA conversion and data brokerage were outsourced.

The United Arab Emirates reports self-contained operations in which victim list management and social media communication, worker supervision and scam execution, fund and VA transfers, security and IT support are performed within the same operation.



The KK Park compound in Myawaddy, Myanmar, during a military operation targeting alleged scam compounds near the Thai border. © Naphatpixs

Spatial dispersion and compartmentalisation are cross-cutting characteristics rather than separate organisational models. Functions under common control may be performed across several premises or jurisdictions, while externally provided services may operate alongside or even within a scam site. Similarly, personnel may have visibility only over the function they perform, regardless of whether that function is controlled internally, by an affiliated entity or by an external provider. For financial investigation and disruption, the key questions are therefore which actor controls each function, whether the capability is internal, affiliated or externally supplied, whether it is shared across multiple operations or networks, and how readily it can be replaced.

Capabilities that are shared across multiple operations or depend on scarce expertise, trusted access, concentrated infrastructure or established criminal relationships may represent high-value disruption points because they are harder to replace.



SCAM COMPOUNDS

INFOGRAPHIC 2. **Functional dependencies and potential high-value disruption points**

●●● Critical dependency	●● Important dependency	● Supporting/substitutable

		END-TO-END ILLICIT FINANCIAL FLOW MODEL FOR SCAM COMPOUNDS						
		UPSTREAM			PAYMENT WINDOW	DOWNSTREAM		
FUNCTIONAL DEPENDENCIES		Establish operations	Recruit workers	Acquire victims	Execute scams	Collect payments	Move/launder funds	Cash out/integrate
Digital & telecom infrastructure	• social media messaging • domains/hosting • SIMs/cloud	●●●	●●	●●●	●●●	●	●	●
Specialised fraud-enabling services	• victim data • ads • fake platforms • automation/deepfakes	●	●	●●●	●●●	●	●	●
Corporate & legal structures	• front companies • corporate accounts • nominees • opaque BO	●●	●	●	●	●●	●●	●●●
VA / VASP / OTC channels	• wallets • VASPs • P2P • OTC brokers	●	●	●	●	●●	●●●	●●●
Shared criminal relationships	• trusted access • brokers • cross-border facilitators	●●●	●●	●	●	●	●●	●●
Physical infrastructure & access routes	• premises • power/connectivity • roads/crossings • security/corruption	●●●	●●	●	●●	●	●	●
Money mule & PML services	• mule controlled accounts • mule networks • professional intermediaries/ DNFBPs • underground banking	●	●	●	●	●●●	●●●	●●
FI & MVTS	• bank accounts and wallets • payment services • MVTS	●●	●	●	●	●●●	●●	●●●

Note: This infographic maps 54 functional dependencies across the scam compound lifecycle, grouped indicatively according to their operational importance and replaceability. **Critical dependencies** are necessary for the relevant criminal function to continue at scale and are difficult, costly or slow to replace; **important dependencies** materially support the scale, speed, efficiency or profitability of operations but can be replaced through substantial adjustment or less efficient alternatives; and **supporting dependencies** are generally more readily replaced or circumvented. The classification may vary according to the operation, jurisdiction and availability of alternatives and considers both the immediate effect of disruption and the time, cost and organisational effort required to restore the capability. Fourteen dependencies are highlighted as potentially critical.

7. End-to-end financial flow model

Building on the wider enabling ecosystem and functional dependencies described above, this section sets out the end-to-end financial flow model.

The end-to-end financial flow model depicts scam compounds as criminal enterprises that generate, move, launder and reinvest illicit proceeds through linked operational and financial stages.

The seven stages should not be read as a single sequential chain performed by the same actors. Each stage may involve different specialist providers and overlapping financial, technological and telecommunications enablers. The model is modular rather than mandatory: not every operation will exhibit every stage, and established or decentralised networks may enter or re-enter the cycle at different points without establishing a new physical operating site.

(i) **STAGE 1 — Set-up of operating sites and enabling infrastructure.** Scam compound operators establish or access physical or hybrid operating sites, often supported by bribery and corruption, opaque legal structures, local facilitators, digital infrastructure, ML service providers and professional intermediaries, including relevant DNFBPs where applicable. At this stage, operators may establish access to the accounts, wallets, payment services and laundering channels needed to receive and move funds, including through mule networks, MVTS, VASPs and other intermediaries. Relevant financial flows at this stage include payments for premises, construction or rental, telecommunications and IT equipment, recruitment, transport, documentation, security, bribes, front companies, mule accounts, and access to VA or underground banking channels.

(ii) **STAGE 2 — Workforce and victim acquisition.** Two principal forms of victimisation may overlap: trafficked persons recruited, transported and coerced into conducting scams, and scam victims targeted online from other jurisdictions. Trafficked workers may be recruited through false job advertisements, often moving from public-facing recruitment channels to private messaging services and combining relocation, housing, visa or travel support, before being transported across borders and forced to conduct online social-engineering scams. Scam victims may be approached through social media, messaging platforms, dating apps, fake investment platforms, online gambling platforms or other digital channels. Victim acquisition may also be inbound: deceptive advertising, sponsored search results or fraudulent websites may prompt victims to initiate contact with the scam operation for the advertised investment or service.

(iii) **STAGE 3 — Scam execution and revenue extraction.** The principal incoming flows often derive from investment fraud, frequently preceded by romance- or confidence-based grooming. Other incoming flows may derive from impersonation schemes, phishing, business-email compromise, online-gambling-related schemes, ransom and release payments, and recovery or refund scams. Scam compound operators may use fabricated dashboards, small initial payouts presented as investment returns, repeated "top-up", "tax", "unlock", "clearance" or "withdrawal" demands, and recovery agent impersonation to extract additional payments from the same victim. Some scam compound-linked operations also use approval phishing, whereby victims are induced to sign blockchain approvals granting the scammer permission to transfer tokens from the victim's wallet, enabling subsequent extraction without a further victim-initiated transfer.

(iv) **STAGE 4 — Collection and initial placement.** Victim funds are commonly received in bank accounts, including personal, corporate and mule-controlled accounts, as well as digital wallets—including wallets provided by MVTS—and VA wallets or other accounts controlled by the scam operation. Funds may be transferred through wire transfers, instant payment systems or wallet-to-wallet transfers. Victim payments may also be collected directly in cash; in other cases, funds transferred to bank accounts may be rapidly withdrawn and collected in cash. In some cases, they are moved within two minutes of the victim's payment. Less commonly, victims may also be instructed to transfer value through precious metals or gift cards, including through the purchase of gold for collection by scam-linked couriers. Reported cases also involved the use of misappropriated card credentials to purchase high-value consumer goods through an e-commerce platform, creating in-kind proceeds that were subsequently resold for cash. Reported call centre fraud models include collectors who retrieve cash or jewellery directly from victims and pass the proceeds to logisticians for onward transfer to higher-level perpetrators. Some collectors may themselves be recruited without full awareness of the underlying criminal activity.

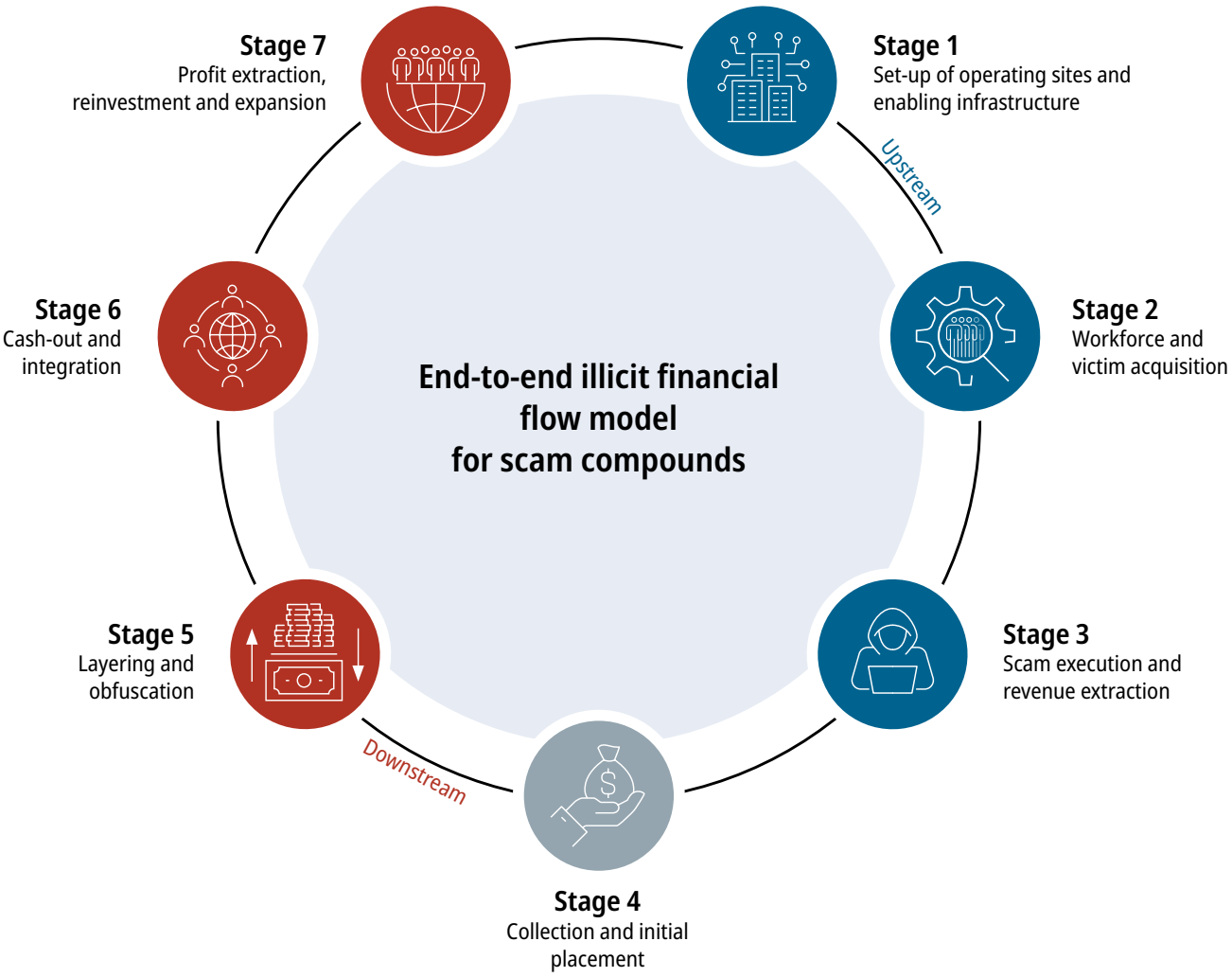
(v) **STAGE 5 — Layering and obfuscation.** Once collected, proceeds may be rapidly dispersed through mule networks, downstream corporate accounts, digital wallets and P2P VA flows. Funds may be moved domestically or across borders through interconnected payment systems, wallet-based remittance services, unlicensed or unregistered MVTS, P2P VA arrangements, OTC brokers, domestic or offshore VASPs[19], and underground banking providers. Proceeds may be converted into stablecoins to facilitate transfer or value storage, and may be further obscured through DeFi bridges, mixers, chain-hopping, crypto ATMs or online gambling platforms. Within this criminal marketplace, gateway companies, mule networks, PML service providers operating networks of mule accounts—sometimes referred to as 'motorcades'—and OTC-style U-merchants facilitate transfers between accounts and wallets, conversion between fiat currencies and VAs, and access to specialised ML services. Jurisdictional experience also identifies underground banking arrangements in which domestic currency proceeds are paid to an operator in one jurisdiction while an overseas correspondent disburses equivalent value in foreign currency to the scam compound network, reducing the need for a direct cross-border transfer of the same funds.

19. FATF (2026), ***Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers (oVASPs)***, FATF, Paris, France, available at: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/understanding-mitigating-risks-offshore-vasps-2026.html

(vi) **STAGE 6 — Cash-out and integration.** Laundered proceeds may be withdrawn as cash, converted back into fiat through domestic or offshore VASPs and OTC brokers, moved through hawala and other similar service providers, stored in vaults, routed through online gaming or gambling platforms, or integrated into real estate, luxury goods, vehicles, precious metals, front companies and other assets. Reported patterns include victim funds received through bank accounts being withdrawn in cash by intermediaries and passed to higher-level actors for cross-border transport, including by vehicle or parcel, or transfer through hawala networks. Other cases involve proceeds funnelled through mule-controlled personal and corporate accounts, converted into VAs and transferred through hosted wallets at VASPs, then converted back into fiat through network-controlled FI accounts for cash withdrawal and physical cross-border smuggling.

(iv) **STAGE 7 — Profit extraction, reinvestment and expansion.** Some proceeds are retained as criminal profit or converted into assets for controllers and other criminal beneficiaries; others are recycled to pay workers, guards, recruiters, transporters and other operating costs or reinvested in premises, digital infrastructure, recruitment, corruption and new scam activity. This circular recycling sustains the business model, enables relocation or decentralisation and increases the scale and resilience of the scam compound ecosystem.

INFOGRAPHIC 3. **End-to-end illicit financial flow model for scam compounds**



SECTION 2

Cross-cutting challenges for competent authorities and the private sector

Detection of scam compound-related financial flows remains largely reactive and fragmented. Illicit funds can move faster than victim reporting, suspicious transaction reporting, financial intelligence analysis, law enforcement action and international co-operation. Critical information is often scattered across sectors and borders. Some of the earliest indicators of scam activity may be held by actors outside the traditional anti-money laundering framework, even before any financial transaction occurs or victim report is made.



A police officer inspects a scam compound known as "My Casino", which police said was owned by former tycoon and casino owner Ly Kuong who was arrested on 15 Jan 2026, Kampot province, Cambodia. © Reuters

The main cross-cutting challenges for competent authorities and the private sector in tackling end-to-end illicit financial flows linked to scam compounds are set out below.

8. Detection and prevention

Detection of scam compound-related financial flows remains largely reactive and fragmented. Cases may surface only after victim reporting or other post-event information emerges, while relevant indicators are dispersed across institutions, sectors and stages of the scam lifecycle. Individual authorities and private sector actors often see only part of the underlying network, and signals arising outside the financial sector or before victim payments may not be connected to related financial activity. Where activity is treated as generic consumer fraud, isolated mule activity or individual suspicious transactions, links to a wider organised criminal network, shared infrastructure or scam compound may therefore remain unidentified.

FIs and VASPs may struggle to distinguish mule-controlled, corporate transit and rapid pass-through activity from legitimate customer behaviour. This challenge arises on both sides of the payment: while the victim's FI or VASP may observe an apparently legitimate authorised payment, receiving institutions may hold different indicators of the same network, including repeated incoming victim payments and links across beneficiary, mule or corporate accounts and wallets. Relevant patterns may include small test transfers, rapid onward movement, structured activity and unusual cash-out behaviour, but may be difficult to identify where accounts appear legitimate or payments are initiated and authorised by the victim. Where scam compounds or associated laundering infrastructure are located within a jurisdiction, limited supervisory understanding of these risks may further weaken their identification by supervised FIs and VASPs.

The speed of scam compound-related financial flows can significantly exceed the speed of victim reporting, institutional escalation, suspicious transaction reports (STRs), FIU analysis, law enforcement action and international co-operation. This mismatch narrows the window in which payments can be interrupted or proceeds preserved before they are transferred, converted, withdrawn or moved across jurisdictions. Jurisdictional experience illustrates the narrow intervention window: Thailand reports that illicit funds can move from a victim's account to an exit point from the financial system within 3–5 minutes, while victims take around 20 hours on average to realise that they have been scammed. Banking-sector experience similarly indicates that effective recovery can become substantially more difficult very quickly once funds have been transferred onward. STR reporting nevertheless remains an important source of financial intelligence and can generate or support investigations, including into organised criminal networks behind fraud. However, because STRs are not designed primarily as a real-time fraud-disruption mechanism, they should be complemented by faster preventive and operational channels where immediate payment intervention (i.e. measures to prevent, suspend, delay, reject, recall or otherwise interrupt victim payments and subsequent transfers before proceeds are dissipated) or asset preservation is required.

The velocity challenge is not uniform across the criminal network. Wolfsberg Group members report that some scam compound-linked front companies and professional laundering nodes maintain apparently legitimate profiles and remain active for months or years while processing substantial volumes, creating a longer investigative window than rapidly rotating mule accounts. Such more persistent nodes can provide valuable targets for network analysis, financial investigation, disruption and asset recovery.

Case classification creates a further detection gap. Among jurisdictions that had not identified confirmed or suspected scam compound-linked activity since 2021, recurrent explanations included difficulties identifying links to scam compounds and the absence of a separate scam compound case classification. Non-identification should therefore not automatically be interpreted as evidence that no relevant activity exists. Related fraud, ML, trafficking

and criminal association offences may also fall under different bodies of rules and institutions or departments, increasing the risk that elements of the same flow or network are investigated separately.

A particularly difficult detection gap may arise during the trust-building phase between initial contact and the first significant payment. At this stage, the victim may not perceive any reason to report, while the financial system may observe little or no anomalous transactional activity. Scam activity may therefore progress without generating conventional financial or victim-reporting signals.

A related detection challenge is that some of the earliest indicators of scam activity may sit with technology and telecommunications providers, before any financial transaction occurs or victim report is made. Social media platforms, messaging services, advertising providers and other online services may observe fraudulent advertisements, impersonation, suspicious recruitment activity, scam accounts, malicious links, repeated communications patterns or other indicators associated with scam infrastructure. Where detection relies predominantly on user reporting or post-event referrals, these signals may not be identified or acted upon in time to disrupt the activity before victims are engaged or payments are made.

To mitigate this challenge → ***System-wide and network-level detection and mapping***; ***Shared fraud data infrastructures***; ***Digital, telecommunications and platform detection***; ***Infrastructure disruption***; *and* ***Preventive payment controls***. *See subsections 15.3, 16.1, 16.2 and 16.4, and Infographic 4.*

9. Information sharing and intelligence fusion

Information relevant to scam compound-related financial flows is fragmented across public and private actors and may remain confined to individual institutions, sectors or cases. This can prevent authorities and private sector actors from connecting related fraud, trafficking, cybercrime, gambling and ML activity to the same wider criminal network.

A central information sharing challenge is converting fragmented and heterogeneous signals into sufficiently reliable, specific and contextualised intelligence to support action. Individual indicators or data points may be ambiguous, short-lived or readily replaceable, and their significance may become apparent only when assessed holistically alongside other financial, technological, telecommunications, behavioural or victim-derived information. Even where relevant data exist, participating actors may lack the analytical capacity, common data structures or operational arrangements needed to combine and assess them within operational timeframes. Legal and institutional frameworks for public-private, private-private and cross-sector information sharing also remain uneven, and uncertainty over privacy and data protection requirements may inhibit sharing even where it is legally permissible. In some jurisdictions, legal gateways may enable information sharing for ML, terrorist financing (TF) or proliferation financing (PF) purposes without expressly covering fraud prevention or disruption.

A further challenge is ensuring that relevant information reaches the actor positioned to use it in time. Limited feedback and information sharing can result in related activity being reported independently by different institutions without the wider network being recognised or relevant findings being fed back as actionable intelligence. Wolfsberg Group members report cases in which different FIs reported activity associated with apparently related scam networks months or years apart, with the connections becoming apparent only through subsequent information sharing. These routing and feedback gaps may be compounded where the information holder has no direct customer, transactional or jurisdictional nexus to the account, wallet or payment concerned, creating uncertainty as to the legal basis, permissible scope and conditions for sharing.

Information sharing arrangements also remain predominantly domestic in many cases, while scam compound-related flows and infrastructure span multiple jurisdictions. Limited cross-border fraud-risk sharing, inconsistent case classification and the absence of common approaches to fraud data exchange can make it difficult to connect cases and co-ordinate action against financial flows and associated scam infrastructure across jurisdictions. Recent questionnaire responses illustrate this visibility problem directly: Hungary, for instance, reports both difficulties in identifying scam-compound links and the absence of a separate case classification, while Mexico similarly has no autonomous legal or institutional category and distinguishes suspected scam-compound-type activity from fraud or cybercrime more generally.

To mitigate this challenge ⟶ ***Anti-scam centres***; ***Shared fraud data infrastructures and cross-sector signal exchange***; ***Rapid response networks***, *and* ***Cross-border FIU and law enforcement co-ordination networks***. *See subsections 15.1 and 15.3, 15.4 and 15.5, and Infographic 4.*

10. Financial intelligence, investigation and prosecution

FIU visibility can be constrained where reporting is neither sufficiently timely nor of sufficient quality, or where relevant financial, digital, telecommunications and victim-related information cannot be connected across reporting entities, jurisdictions, mule-controlled accounts and wallets, corporate accounts, VASPs and informal MVTS. Most scam compound investigations have been triggered by victim reports rather than STRs, while STRs more often relate to scams generally than to scam compounds specifically. Jurisdictional experience varies: in some cases, victim reporting and traditional police investigation identify relevant activity first, with financial intelligence contributing subsequently to the identification of perpetrators; in others, STR-based financial intelligence has identified suspected scam compound-related activity through receipts from multiple individuals, rapid movement of funds, transactions inconsistent with stated economic activity and analysis of relationships between accounts and parties. Classification can create a further visibility challenge: jurisdictions report that scam compound-related activity may lack a specific legal or administrative category and instead be recorded under broader fraud, organised-crime, money-mule, trafficking or ML classifications, including as generic fraud, online gambling, cybercrime, trafficking in human beings or ML. This can limit the ability of FIUs and other authorities to identify the wider organised crime network.

A further investigative challenge is reconstructing high-velocity, multi-layered flows across mule and corporate accounts, digital wallets, FIs, VASPs, P2P channels, OTC brokers, informal MVTS, cash withdrawals and front businesses, **while simultaneously building an admissible evidential chain** across financial, digital, corporate, trafficking and cross-border sources.

Investigations are further complicated by the need to integrate financial enquiries with cybercrime, trafficking in human beings, immigration, corruption and asset recovery work. Law enforcement authorities (LEAs) may face difficulties identifying and dismantling the organised criminal syndicates behind scam compounds and linking individual victim complaints, financial flows, trafficking routes, digital evidence and BO information to the wider network. This challenge must also be addressed with appropriate victim-centred safeguards to avoid treating trafficked persons forced to commit scams as offenders.

Competent authorities may face legal, technical and operational difficulties in preserving, obtaining, authenticating, analysing and presenting electronic evidence held on devices and computer systems operated from scam compounds or by FIs, VASPs, telecommunications providers, social media and messaging services, domain and hosting providers, cloud-service providers and other persons. Challenges include delayed preservation or production of data, information held or processed abroad, encryption, limited retention periods, large data volumes, inconsistent admissibility requirements and insufficient digital forensics capacity. The absence of secure and efficient technical

channels for cross-border transmission can itself cause delay: electronic evidence may still be transferred using encrypted physical storage media, creating additional processing time and information security risks (see Box 21).

Attribution may be impeded where BO information, company records or cross-border corporate information is incomplete, fragmented or slow to obtain. This can make it difficult for authorities and private sector actors to connect accounts, assets and apparently legitimate businesses to the persons controlling or benefiting from scam compound networks (see Box 22).

Corruption, complicit local authorities, and structures linked to PEPs may facilitate as well as protect scam compound operations, including through access to premises and land, licensing, telecommunications infrastructure, cross-border movement, security and the laundering or integration of proceeds. This creates additional challenges where relevant indicators overlap with politically connected businesses, real estate, casinos, luxury assets or apparently legitimate commercial activity.

A central prosecution challenge is capturing the wider organised criminal enterprise rather than isolated fraud transactions, mule accounts or trafficking events. This may require charges addressing fraud, ML, trafficking in human beings—including, where relevant, trafficking for the purpose of forced criminality—illegal detention, cybercrime, corruption, illegal gambling and organised crime, while proving the links between predicate conduct, laundering activity, assets and the persons controlling the network. Effectiveness may be further constrained by legal framework gaps, difficulties determining where offences occurred, lengthy judicial processes and limited specialist expertise. Jurisdictional experience indicates that prosecutions with the greatest strategic value focus on criminal leadership, financial facilitators, PML service providers, infrastructure operators and recruitment networks rather than low-level workers alone, supported by investigations integrating financial intelligence, cyber intelligence and victim testimony.

Case information is not always converted quickly into updated indicators, sector guidance, private sector controls or cross-border alerts. Weak case tagging and statistics make it difficult to measure the scale of proceeds, identify compound-specific typologies, assess recovery outcomes or determine which interventions are effective. Feedback loops between FIUs, LEAs, supervisors, FIs, VASPs, technology and telecommunications providers, blockchain analytics providers, and victim-support organisations are therefore essential.

To mitigate this challenge → ***Multi-agency taskforces and joint operational teams***; ***Parallel financial investigations***; ***BO, corporate-link and professional intermediaries analysis***; *and* ***VA tracing***. *See subsections 15.2 and 16.5, 16.6 and 16.7, and Infographic 4.*

11. International co-operation

Scam compound activity can operate across borders at the speed and scale enabled by digital technologies, while law enforcement powers and legal frameworks remain primarily national. Scam compound cases frequently involve source, transit, hub, victim, laundering, asset-holding and infrastructure-hosting jurisdictions, and the physical compound, criminal leadership and controllers, trafficked workforce, scam victims, mule accounts and wallets, VASPs, shell companies, payment intermediaries, ML providers, assets and beneficial owners may all be located in different jurisdictions. Authorities may therefore need to navigate multiple legal, procedural and jurisdictional frameworks to investigate and disrupt activity that can move rapidly across borders. This creates operational gaps between authorities responsible for trafficking, cybercrime, fraud, ML, asset recovery, immigration, corruption, corporate registration and financial supervision, as well as between FIs, VASPs, telecommunications providers, technology platforms and domain, hosting and cloud-service providers. A jurisdiction may also become relevant to an

investigation because it hosts data centres, domains, hosting, cloud or other technical infrastructure used by actors elsewhere, even where it has not itself identified a scam compound or associated financial flows.

Differences in legal frameworks—including dual-criminality requirements and gaps in applicable treaty coverage—**together with delays, limited responsiveness, language and translation constraints, limited reciprocity and restrictions on information sharing may prevent authorities from linking individual victim reports to the wider network, preserving and transferring electronic evidence or acting before funds dissipate.** These challenges may be compounded by uneven specialist capabilities across jurisdictions. A particular challenge is delayed or limited co-operation from jurisdictions where scam compounds, ML nodes or supporting technology and communications infrastructure are located. Because funds, victims and digital infrastructure may move, change or be disabled rapidly, such delays may prevent authorities from securing evidence, freezing assets or identifying and repatriating trafficked persons in time.

A distinct international co-operation challenge arises immediately after scam compound disruption, when financial, evidential and victim-protection needs converge across jurisdictions within a narrow time window. Relevant devices, witness information, financial intelligence, assets and persons of interest may be dispersed across multiple authorities and jurisdictions, while persons found at the site may be relocated or repatriated quickly. Where post-disruption information sharing breaks down, evidence can be lost, assets dissipated, controllers escape and opportunities to connect the disrupted site to the wider criminal and financial network can be missed.

Cross-border victim identification and protection create a parallel challenge. Differences in nationality or status determination, trafficking screening, safety and re-trafficking risk assessment, referral, repatriation and continuity-of-support arrangements can delay safe return or result in relevant information being lost between jurisdictions. A further tension can arise between rapid protection and repatriation and the preservation of victim-derived information for follow-on investigations, without making protection or safe return conditional on co-operation.

To mitigate this challenge → ***Joint operational teams***; ***Rapid cross-border fund-interception and Asset preservation and recovery networks***; ***Cross-border FIU and law enforcement co-ordination networks***; *and* ***Cross-border PPPs***. *See subsections 15.2, 15.4, 15.5 and 16.8, and Infographic 4.*

12. Asset tracing, freezing, recovery and restitution

Many jurisdictions report limited ability to estimate the value of assets linked to scam compounds and trafficking in human beings and limited success in tracing and seizing them. The short intervention window (see subsection 8) is a major constraint: by the time preservation or freezing action becomes available, proceeds may already have moved through multiple accounts, VA wallets, VASPs, cash-out points and jurisdictions.

Beyond this timing constraint, effective asset tracing and preservation depend on timely detection, actionable intelligence, co-operation from FIs and VASPs, access to blockchain analytics and sufficiently rapid legal and operational powers (see Box 23). **Authorities** may need to reconstruct complex flows across VAs and other financial channels, identify assets held through foreign nominees, front persons or opaque corporate structures, and act before funds are converted, withdrawn, transferred abroad or otherwise dissipated. These efforts may be hindered by incomplete BO information, poor inter-agency co-ordination, limited financial investigation expertise and resources, legal barriers to information exchange and delays in domestic or international co-operation.

Confiscation, recovery and restitution raise distinct subsequent challenges once assets have been identified or preserved. Proceedings may be prolonged by lengthy judicial processes, legal or evidential constraints and difficul-

ties obtaining confiscation orders where perpetrators are abroad, unavailable or unidentified, particularly where the applicable framework depends on a criminal conviction. Even where assets are successfully confiscated or recovered, restitution or compensation may be constrained by difficulties linking those assets to specific online scam victims or persons trafficked into scam operations across jurisdictions. Effective recovery arrangements therefore need to preserve claimant and loss information throughout the investigative and asset recovery process so that recovered property can, where appropriate, be returned or otherwise applied to victim restitution.

To mitigate this challenge → ***Rapid response asset preservation networks; VA tracing; Automated and network-wide fund tracing***; *and* ***Victim-linked recovery and restitution protocols***. *See subsections 15.4 and 16.7, 16.8 and 16.9, and Infographic 4.*

13. Victim reporting and victim-centred outcomes

Both victim groups—persons trafficked into compounds and forced to conduct scams, and online scam victims defrauded by those operations—face significant reporting barriers. Under-reporting and reporting delays substantially narrow the short window available for payment intervention, freezing and asset recovery, weaken the financial-intelligence picture and limit the ability of authorities to connect individual reports to wider scam compound networks. GI-TOC estimates that around 70% of scam victims do not report the crime[1]. Online scam victims may delay or avoid reporting because of shame, stigma, uncertainty, continued manipulation, poor awareness, fear of consequences, the belief that their losses are unrecoverable or the illicit or gamified nature of the platforms involved. Even where they do report, victims will often be unable to identify the persons, criminal network, scam compound or jurisdiction behind the fraud, having interacted only with false identities, online accounts, websites, platforms, telephone numbers or payment instructions. Trafficked persons may fear retaliation, criminal liability, immigration consequences or being treated as offenders.

Reporting arrangements may be fragmented or insufficiently accessible. Victim reports may be submitted through consumer protection bodies, police, non-governmental organisations (NGOs), embassies or other channels without being routinely transmitted to FIUs or private sector actors able to intervene. This may be particularly significant where NGOs have close access to trafficking victims, local communities or informants in areas affected by scam compound activity (see Box 24). Individual reports may also contain only fragments of the wider picture—such as a beneficiary account, wallet address, telephone number, username, URL or platform identifier—which may acquire investigative value when aggregated and cross-referenced with other reports and intelligence. Reporting channels may further lack visibility, public confidence, clear escalation pathways or the capacity to process reports consistently. This fragmentation can weaken risk understanding, prioritisation, case-tagging, statistics, resource allocation, typology development and asset recovery, and hinder the identification of links between apparently separate cases and compound-specific outcomes.

Persons trafficked or coerced into scam compounds may be compelled to engage in conduct that, viewed in isolation, appears criminal, including communicating with scam victims or moving fraud proceeds. This creates a significant risk that they are misclassified as offenders, irregular migrants or willing participants rather than identified as potential victims of trafficking or forced criminality. Such misclassification can suppress reporting and co-operation, result in removal or deportation rather than referral to appropriate protection, and cause authorities to lose valuable intelligence or evidence on recruiters, compound operators, financial flows and the wider criminal network.

1. GI-TOC (2026), *A world of deceit: Mapping the landscape of the global scam centre phenomenon*, Global Initiative Against Transnational Organized Crime, Geneva, available at: https://globalinitiative.net/wp-content/uploads/2026/03/Kristina-Amerhauser-Alex-Goodwin-A-world-of-deceit-Mapping-the-landscape-of-the-global-scam-centre-phenomenom-GI-TOC-March-2026-1.pdf

Appropriate screening and victim-identification procedures are therefore important both to safeguard trafficked persons and to preserve investigative opportunities.

Online scam victims may suffer unrecoverable losses once funds are cashed out, moved offshore or converted into VAs and may subsequently be targeted through recovery or refund scams. Although not specific to scam compound-related fraud, industry studies suggest that scam losses may represent a higher share of GDP in developing economies, while advanced economies tend to experience higher individual losses. Victims may also face deliberate and repeated exploitation through the reuse or resale of victim data, recovery or refund scams and coercive grooming into criminal roles. AI-enabled fraud can further scale such re-victimisation with reduced human intervention. These practices deepen victim harm and may complicate victim identification and law enforcement responses where the boundary between victimisation and criminal involvement becomes obscured.

A further challenge is that case outcomes may be assessed primarily through arrests, prosecutions, seizures or the dismantling of compounds, without adequately capturing victim-centred outcomes. Gaps in victim identification, referral and follow-up may leave trafficked persons without repatriation, immigration safeguards, psychological and other support, reintegration assistance or protection from retaliation, re-trafficking and renewed exploitation. Online scam victims may similarly lack financial recovery, psychological support and protection from further exploitation. Restitution and compensation may be impeded by delayed reporting, incomplete claimant and loss information, difficulties linking recovered property to specific victims, the movement of funds and assets across multiple jurisdictions and the absence of mature cross-border mechanisms covering both victim groups. Outcomes may be further weakened where asset preservation is delayed, case-tagging is unreliable or co-ordination between financial investigation, criminal-justice, civil society and victim-support mechanisms is fragmented. Limited follow-up support may also reduce victim co-operation, weaken evidence collection and leave victims exposed to renewed exploitation.

To mitigate this challenge → ***Single-entry or "no-wrong-door" reporting and referral***; ***Trafficking screening and non-punishment safeguards***; ***Trauma-informed debriefing***; ***Rapid routing of victim-derived indicators to payment and asset preservation channels***; *and* ***Claimant- and loss-data recovery protocols***. *See subsections 15.1, 15.4 and 16.9, and Infographic 4.*



Aftermath of enforcement activity at suspected scam compound in Sasaabi, Accra region of Ghana, 2026.
© United States Department of Justice

SECTION 3

Mitigation strategies and operational tools

An effective end-to-end response combines upstream action against the infrastructure and services sustaining scam compounds with downstream measures to interrupt illicit financial flows, trace and recover criminal proceeds, and return stolen assets to victims. It targets the wider criminal networks rather than individual sites, through co-ordinated action, rapid intelligence sharing and effective co-operation across sectors and borders.



A delegation made by the Ministry of Foreign Affairs of Japan and UNODC visited Thailand's Anti Cyber Scam Center (ACSC), launched in late 2025 under the Central Investigation Bureau (CIB) and Royal Thai Police. Bangkok, Thailand – March 2026. © UNODC / Laura Gil

An effective end-to-end response should combine upstream and downstream intervention:

(i) **Upstream action** seeks to identify and disrupt the capabilities, infrastructure and expenditure required to establish, sustain and scale scam compound activity—including worker and victim recruitment, victim leads and data, advertising, telecommunications, domains and hosting, fraudulent platforms, premises and specialised service providers—before or alongside the generation of scam proceeds.

(ii) **Downstream action** focuses on victim payments and generated proceeds, including payment intervention, mule account and wallet disruption, financial and VA tracing, freezing, confiscation, recovery and restitution. Downstream financial intelligence and asset action can also support broader disruption measures, including targeted sanctions or other asset-denial measures, arrests and compound closure.

The distinction is analytical rather than rigid: financial intelligence and investigation can operate across both, including by identifying expenditure supporting scam compound operations and tracing the subsequent movement and reinvestment of proceeds.

For the purposes of this report, disruption means co-ordinated action that prevents, interrupts or degrades the ability of scam compound networks to establish, operate, scale or profit from their activities. It can target criminal leadership and facilitators; recruitment and trafficking networks; financial, technological and communications infrastructure; accounts, wallets and payment channels; compounds; and criminal proceeds and assets, through measures including preventive controls, infrastructure takedowns, asset denial, targeted financial measures, arrests, prosecutions, compound closures, freezing, confiscation and recovery. **Sustained disruption requires durable degradation of these underlying capabilities, rather than their temporary displacement, rebranding or replacement.**

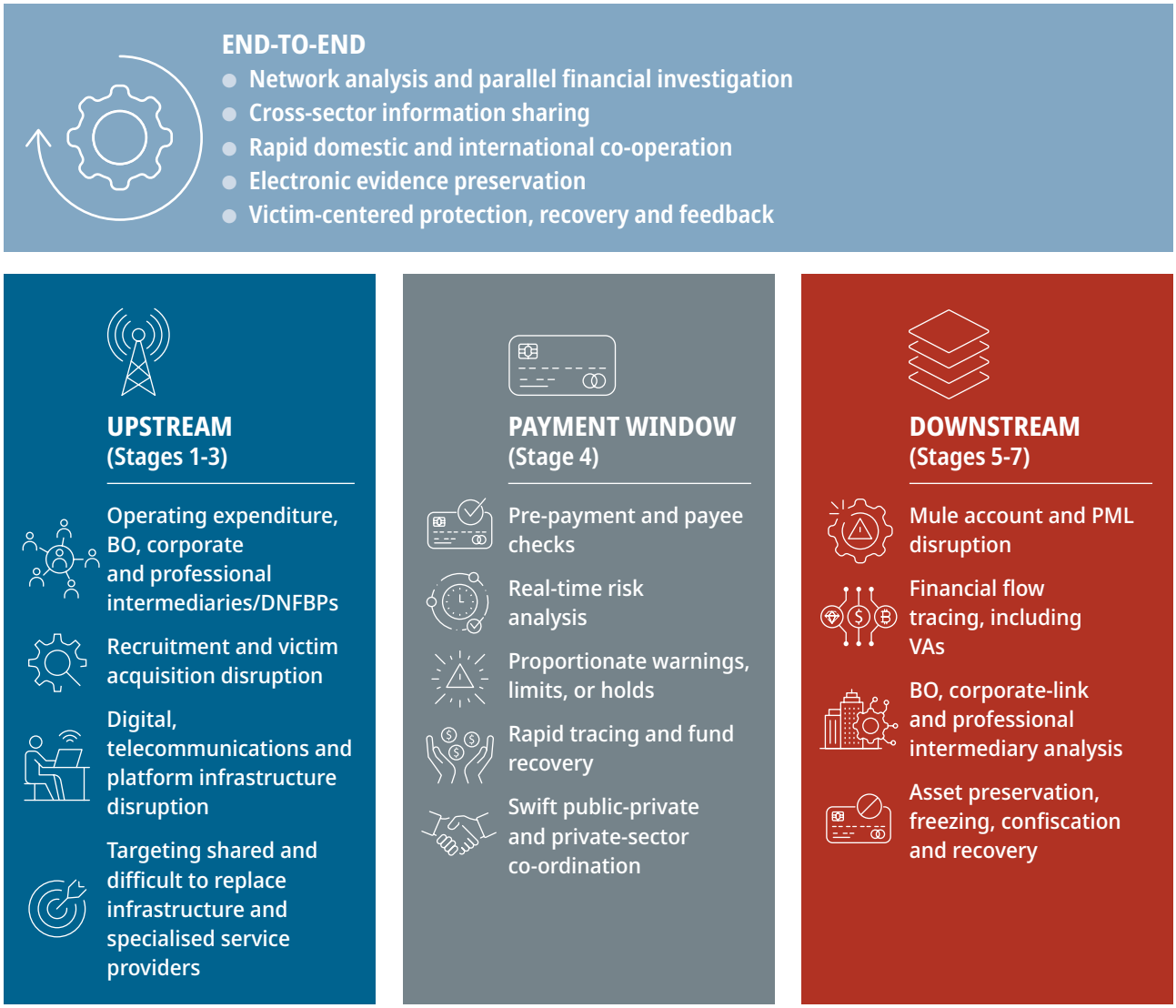
Where a jurisdiction hosts scam compounds or linked decentralised scam operations, the end-to-end approach should place particular emphasis on the domestic infrastructure sustaining those operations. Consistent with assessed risk and the FATF Standards summarised in **Table 1**, this includes identifying controllers and beneficial owners; investigating front companies, premises, assets and operating expenditure; conducting parallel financial investigations and rapid asset preservation action alongside investigations into fraud, trafficking in human beings, corruption and other connected offences; and applying risk-based supervision to exposed FIs, VASPs and relevant DNFBPs. Financial, corporate and electronic evidence should, where possible, be preserved at the time of raids or other disruption. Host jurisdictions should also connect domestic action promptly with victim source, transit, laundering, asset-holding and infrastructure-hosting jurisdictions so that action against an operating site contributes to disruption of the wider network and its proceeds. Where trafficking, coercion or forced criminality is indicated, enforcement action should be co-ordinated with appropriate victim identification and protection arrangements (see Box 9).

Building on the seven-stage end-to-end model in Infographic 3, Infographic 4 maps the principal operational interventions across upstream stages 1–3, the payment window at Stage 4, downstream stages 5–7, and the capabilities that operate end-to-end. The remainder of this section explains the strategic principles, co-ordination models and operational tools through which these interventions can be implemented.

14. Strategic principles

This subsection sets out the overarching strategic principles that should guide efforts to prevent, detect and disrupt illicit financial flows linked to scam compounds. **Effective national responses also require sustained political commitment, clear leadership and accountability**, with sufficient convening authority to align priorities, mobilise resources and resolve operational or legal barriers across participating authorities and sectors, particularly where corruption, official protection or fragmented government control may otherwise impede action.

INFOGRAPHIC 4. **Operational interventions across the end-to-end financial flow**



Targeting the wider criminal ecosystem

Financial prevention and disruption measures are central to disrupting scam compound business models and should be integrated with action against other critical dimensions, including trafficking in human beings, cybercrime, corruption, digital infrastructure and other enabling activity. They should therefore be sufficiently specialised to address scam compound-related illicit financial flows while being embedded, where appropriate, in wider national responses to fraud, organised crime, trafficking in human beings, cybercrime, corruption and asset recovery. Scam compounds should be treated as networked, industrialised and transnational criminal infrastructures rather than as isolated victim complaints, mule account networks or VASP-related ML cases.

Disruption should target syndicate leadership, shared financial and operational infrastructure and specialised service providers sustaining multiple compounds or decentralised cells, rather than individual sites alone, including where leadership or controllers operate from other jurisdictions. Priority should be informed by the operational importance and replaceability of the relevant capability, as illustrated in Infographic 2. This is particularly important where enforcement pressure fragments operations while common controllers, financial infrastructure, ML services and digital enablers remain in place. Where criminal leadership, shared infrastructure or specialised service providers are distributed across jurisdictions, co-ordinated international action may be necessary to disrupt the wider

network rather than individual domestic nodes alone. Where available under domestic law, financial investigations and prosecutions, asset tracing and freezing, denial of access to financial and VA services, targeted sanctions or other asset-denial measures can impose costs across the wider network.

To operationalise this principle → ***Network mapping of controllers, shared dependencies and specialised providers***; ***Multi-agency taskforces and joint operational teams***; ***Parallel financial investigations***; *and* ***BO, corporate-link and professional intermediary analysis***. *See Subsections 15.2, 16.1, 16.5 and 16.6, and Infographic 4.*

BOX 6. **Co-ordinated action against the Prince Transnational Organised Crime Group**

Cambodia / China / Hong Kong China / Singapore / Korea / Chinese Taipei / Thailand / United Kingdom / United States: From October 2025, co-ordinated US–UK action against the Prince Transnational Organised Crime Group included sanctions, the seizure of over USD 15 billion in assets and the US indictment of its leader, Chen Zhi. Korea and other jurisdictions subsequently imposed sanctions, seizures or freezing measures. In November 2025, KoFIU designated 15 individuals and 132 entities connected to scam compound crimes for financial transaction restrictions under the Act on Prohibition against the Financing of Terrorism and Proliferation of Weapons of Mass Destruction, freezing their funds. The designations included persons and entities linked to the Prince Group and Huione Group. Other jurisdictions also imposed sanctions, seizures or freezing measures. Cambodia reports that its domestic investigation led the National Bank of Cambodia to revoke Prince Bank's licence and initiate its liquidation; court orders froze 42 individual and 32 legal-entity accounts associated with shareholders and related persons or entities; and investigations encompass 35 Cambodia-based companies and linked offshore entities. Cambodia further reports the freezing of bank funds amounting to hundreds of millions of US dollars, more than 1 000 immovable properties and other movable assets, alongside international co-operation with China, the United States and INTERPOL. Chen Zhi was later arrested in Cambodia and transferred to China following the revocation of his Cambodian citizenship. China, Hong Kong China and Singapore report that investigations into related cases are continuing.

Disrupting illicit financial flows end-to-end

Disrupting scam compound-related illicit financial flows end-to-end **requires intervention across both upstream operating inputs and downstream victim payments and proceeds.**

Upstream, financial analysis should seek to identify expenditure on the operating inputs described in subsection 4.4 and, where lawful and proportionate, support action that denies or disrupts access to difficult-to-replace infrastructure or specialised service providers, informed by the dependency analysis in Infographic 2. Such action can increase the cost and operational risk of sustaining scam compound activity before further victim losses and criminal proceeds are generated.

At the downstream end, flows may move through mule accounts, cash-out points, cross-border channels or VAs within minutes or hours; a predominantly post-event response based on STRs or victim complaints is therefore unlikely to match the threat. Intervention should occur as early as possible and make high-risk financial channels less attractive through targeted, risk-based measures (see Box 11).

To operationalise this principle → ***Upstream expenditure and dependency mapping***; ***Digital, telecommunications and platform infrastructure disruption***; ***Preventive payment controls***; *and* ***Rapid fund and VA tracing and asset preservation***. *See subsections 16.1, 16.2, 16.4 and 16.7 and 16.8, and Infographic 4.*

Connecting intelligence and capabilities across sectors

Because scam compound networks operate across financial, technological and telecommunications systems, **siloed investigations and reactive information sharing are insufficient.** No single actor sees the full attack and financial flow chain. Effective disruption therefore requires these partial views to be connected across FIs, VASPs, technology and telecommunications providers, financial consumer protection and other relevant regulatory authorities, law enforcement, financial-intelligence and civil society actors—including NGOs and victim-support organisations—and converted into actionable intelligence (see Box 10). Where legally permissible, relevant indicators should be shared as early as possible, including at the pre-contact stage where fraudulent advertisements, recruitment activity, domains, accounts, phone numbers or other infrastructure can be identified before a victim is engaged. Jurisdictions should therefore develop or strengthen PPPs and information sharing arrangements, supported by clear legal gateways, governance arrangements and proportionate data protection and privacy safeguards, so that relevant intelligence reaches the actor best positioned to act on it sufficiently rapidly to support prevention, tracing, investigation or disruption before proceeds are generated, layered, converted or cashed out.

To operationalise this principle → ***Anti-scam centres***; ***Shared fraud data infrastructures and cross-sector signal exchanges***; ***Rapid response networks***; *and* ***Interoperable networks of networks***. *See subsections 15.1, 15.3, 15.4 and 15.6, and Infographic 4.*

Matching the transnational nature of the threat with international co-operation

Cross-border co-operation should, where possible, move beyond case-by-case requests by combining, as appropriate, timely informal and operational channels with formal co-operation where required and supporting the exchange of targeted financial, technical and operational information. Co-operation should enable timely sharing of information on victims, mule accounts, VA wallets, shell companies, payment corridors, recruitment patterns, domains, phone numbers and social media, messaging and other online platform identifiers, particularly in multi-jurisdictional cases and with lower-capacity jurisdictions that may host, transit or enable parts of the network. Depending on the case, such co-operation may include joint investigative or operational teams, time-bound operational data-sprint or case-linkage exercises and co-ordinated multi-jurisdictional disruption actions, alongside formal co-operation where evidence or coercive measures are required (see Box 13).

Effective cross-border co-operation should be supported, where necessary, by targeted technical assistance and capacity building, particularly for jurisdictions hosting or exposed to scam compound activity. Priority capabilities include understanding scam compound typologies and network structures, parallel financial investigations, digital forensics and electronic evidence handling, financial and VA tracing, cross-border case-building, asset preservation and international co-operation. Regional initiatives can combine these capabilities. Where scam compound activity involves trafficking in human beings or forced criminality, relevant capacity building may also need to strengthen specialised victim identification and referral, safe and trauma-informed interviewing and debriefing, applicable non-punishment safeguards, and cross-border victim-support and repatriation co-ordination. Where technology-enabled detection forms part of the response, capacity building may also need to address access to relevant data and computing resources, specialist analytical skills and cross-sector co-ordination. Particularly where capacity is limited, implementation and technical assistance may need to be sequenced according to existing legal, institutional and operational prerequisites, beginning with measures that can be deployed through existing capabilities while progressively building the conditions for more resource- or reform-intensive interventions.

BOX 7. **Regional capacity building to counter scam compound-related illicit financial flows**

Japan: Through regional initiatives with UNODC, INTERPOL and ASEANAPOL, Japan supports authorities across Southeast Asia with specialised investigative equipment and training for scam-related investigations; guidance on detecting, tracing and disrupting cyber-enabled-fraud financial flows; VA tracing tools and investigative support; and exchanges on anti-scam-centre practices linked to trafficking in persons and forced criminality.

To operationalise this principle → ***Multi-jurisdictional joint operational teams***; ***Rapid cross-border interception and asset preservation networks***; ***Cross-border FIU and law enforcement co-ordination networks***; *and* ***Asset recovery networks***. *See subsections 15.2, 15.4, 15.5 and 16.8, and Infographic 4.*

Ensuring a victim-centred response

Mitigation strategies should remain victim-centred and protect both online scam victims and persons trafficked or coerced into scam compounds for forced criminality. Where credible indicators of trafficking, coercion or forced criminality exist, persons should be screened and referred to appropriate specialised identification and protection procedures before being treated primarily as offenders or immigration violators. For persons identified as trafficking victims, the non-punishment principle should be applied, consistent with applicable legal frameworks, to unlawful conduct they were compelled to commit as a direct consequence of their exploitation. Access to appropriate protection and victim-support services should not be made contingent on a victim's ability or willingness to provide operational intelligence or co-operate with an investigation. Reporting, debriefing, repatriation and reintegration should be safe and victim-sensitive, including appropriate assessment of retaliation and re-trafficking risks and, in cross-border cases, referral and continuity of support. Online scam victims should likewise have access to practical recovery guidance, appropriate support and protection from recovery scams and repeat targeting. Civil society, survivor-led and victim-support organisations should, where appropriate, be integrated into the broader mitigation architecture while preserving their distinct and trusted support role.

To operationalise this principle → ***Single-entry or "no-wrong-door" reporting and referral***; ***Trafficking screening and non-punishment safeguards***; ***Trauma-informed debriefing and victim-generated intelligence***; *and* ***Claimant- and loss-data recovery and restitution protocols***. *See subsections 15.1 and 16.9, and Infographic 4.*

Maintaining an adaptive, technology-enabled and outcome-focused response

The response should be adaptive and make effective use of relevant digital and analytical tools. Scam compound models continue to evolve through decentralisation, AI-enabled social engineering, including deepfakes and multilingual content generation, automation, digital marketplaces, synthetic identities, fast-changing domains and the ability to shift between multiple payment channels. As technical controls strengthen, scam compound networks may also adapt by placing greater reliance on social engineering and other forms of victim manipulation, including techniques designed to induce victims to authorise payments or disclose credentials. Mitigation strategies should therefore support continuous typology development and feedback loops between competent authorities and relevant private sector actors, enabling controls, tools and operational approaches to evolve with the threat. Where feasible, this should include horizon-scanning and anticipatory analysis to identify emerging scam tactics, technologies, infrastructure, payment channels and indicators of geographic displacement, and enable controls, resources and operational responses to adapt before new methods or operating locations become entrenched.

Mitigation measures should be assessed against operational outcomes and impact rather than activity or institutional outputs alone. When considering practices for possible replication, jurisdictions should distinguish novelty or activity from demonstrated operational impact and assess the conditions for scalability across institutions, sectors and jurisdictions. Relevant considerations include whether an intervention increases the cost of conducting scams, reduces scam success or losses, improves enforcement or recovery outcomes, and degrades a capability that is difficult for the criminal network to replace[1]. Jurisdictions should, where feasible, establish baselines and a limited, sufficiently standardised set of indicators mapped across the end-to-end lifecycle. Relevant indicators may include, where measurable, scam activity or victim payments prevented or interrupted; the time between the earliest actionable signal or report and intervention; fraud losses; the value and proportion of proceeds preserved, confiscated, recovered and returned; the incidence and timely resolution of material false positives generated by preventive controls; links between individual cases and wider criminal networks; sustained disruption; and, where relevant, victim-centred outcomes such as identification and referral, access to appropriate support, safe return and reintegration, restitution or compensation and protection from re-trafficking or repeat victimisation. Monitoring should also capture displacement and substitution, including shifts towards smaller cells, less regulated financial channels or successor platforms and service providers (see Box 3), to distinguish genuine degradation of criminal capabilities from relocation or reconfiguration. As improved detection and reporting may initially increase recorded fraud volumes, trends should be interpreted alongside these broader outcome indicators and used to adjust controls, resources, tools and co-ordination arrangements.

To operationalise this principle → ***Campaign-level tagging and interoperable fraud classifications***; ***Continuous platform and telecommunications monitoring***; ***Controlled scam-hunting***; ***Periodic simulation testing of rapid response arrangements***; *and* ***Outcome and displacement metrics****, including time-to-intervention and assets preserved, recovered and returned. See subsections 15.4, 16.1, 16.2 and 16.8, and Infographic 4.*

15. Co-ordination models

Co-ordination models provide the institutional and operational arrangements through which relevant actors combine information, capabilities and powers to prevent, detect and disrupt illicit financial flows linked to scam compounds. Partners should be identified by the information they hold and their ability to act at specific lifecycle stages rather than by institutional category alone. Where relevant, arrangements should connect AML/CFT and financial crime authorities with financial consumer protection authorities and other actors across the anti-fraud ecosystem, including telecommunications and technology providers, so that complaints, supervisory information, fraud indicators and operational intelligence contribute to a common picture and co-ordinated response. Arrangements may be public, public-private or private, operate within or across sectors, and use centralised, federated or other privacy-preserving models. The models below perform different but complementary functions: anti-scam centres provide standing co-ordination; taskforces and joint operational teams pursue specific networks or disruption objectives; shared-data infrastructures create network-level visibility; rapid response networks preserve the intervention window; cross-border FIU and law enforcement networks connect national action; and networks-of-networks seek interoperability across these mechanisms. Effective arrangements require common operational objectives, clear roles and responsibilities, trusted legal and technical information sharing mechanisms, escalation pathways, expected response times and feedback mechanisms. Co-ordination arrangements should also identify material disincentives to timely information sharing, preventive action or intervention, including where the benefits from providing a legitimate service accrue to one actor while the costs of its criminal misuse fall primarily on others. Where relevant, competent authorities and participating sectors should consider how such disincentives can be reduced. Their effectiveness

1. Peng, X. (2026), *Checkpoints, conflict and scam logistics: Mobile control and the politics of circulation in the China–Myanmar–Thailand borderlands*, DIIS Working Paper Series, Roadblocks and Revenues No. 13, Danish Institute for International Studies (DIIS), Copenhagen, available at: https://pure.diis.dk/ws/files/31998653/DIIS-WP-series-Roadblocks-13-Checkpoints-conflict.pdf

should be assessed by whether they generate new intelligence, reduce response times, enable payment intervention or asset freezing, connect apparently separate cases or produce sustained disruption.

Anti-scam centres

Anti-scam centres can provide a national focal point for co-ordinating detection, investigation and disruption of scam compound-related financial flows. Models vary from predominantly public arrangements to public-private structures and may connect FIUs, LEAs, supervisors, financial consumer protection authorities, FIs, VASPs and, where relevant, telecommunications, technology and victim-support actors to support scam reporting, intelligence sharing, rapid tracing, payment intervention, action against accounts or wallets and victim protection. Many jurisdictions have established anti-scam centres or comparable arrangements, while others are considering similar models.

BOX 8. **Examples of a national anti-scam centre and a comparable arrangement**

India: The Indian Cyber Crime Co-ordination Centre (I4C) operates an integrated platform architecture spanning victim reporting, financial intervention, infrastructure disruption and inter-State law enforcement co-ordination. CFCFRMS, integrated with the National Cybercrime Reporting Portal, connects cyber-fraud complaints with FIs, payment aggregators, e-commerce platforms and VASPs through API-based interfaces to support real-time money-trail identification and asset tracing/freezing. Sahyog supports VASP data requests and online-content takedown requests, while Samanvaya supports inter-State case linkage and investigative and techno-legal assistance, including a dedicated module covering persons rescued from scam compounds and illegal recruiters.

United Kingdom: The UK follows a decentralised model, with anti-scam functions distributed across relevant LEAs, public bodies and private sector actors rather than concentrated in a single national anti-scam centre. Report Fraud, launched by the City of London Police in December 2025 to replace Action Fraud, provides a central reporting channel for cybercrime and fraud in England, Wales and Northern Ireland, supported by a national crime analysis function that analyses reports and disseminates viable cases to police forces.

Multi-agency taskforces and joint operational teams

Multi-agency taskforces and joint operational teams can support scam compound investigations requiring the rapid integration of financial flows, trafficking indicators, cyber infrastructure, platform activity and organised crime links. They bring together financial and cyber intelligence, law enforcement powers, anti-trafficking expertise, asset-tracing capabilities and, where necessary, international liaison to support co-ordinated action against proceeds, premises, digital devices, shell companies, traffickers, money mules and laundering facilitators. Unlike anti-scam centres, which generally provide a standing co-ordination hub for scam reporting, detection and rapid intervention, taskforces and joint operational teams are typically more investigation- or operation-focused and may be established to pursue specific cases, networks or disruption objectives. In federal or otherwise decentralised systems, such arrangements can also connect local or subnational cases to national analytical, financial and cross-border capabilities, allowing individually lower-value complaints to be aggregated and tested for links to wider scam networks.

Participating actors should combine fragmented indicators into clear, prioritised leads that identify relevant persons, accounts, wallets, infrastructure and links, explain what has been verified and flag any legal or technical limitations. This allows investigative and disruption powers to focus on the most actionable targets.

BOX 9. **Multi-agency and joint operational responses to scam compounds**

Australia: Operation FIRESTORM, conducted through the Joint Policing Cybercrime Co-ordination Centre and supported by the AFP International Network, co-ordinates domestic and international action against offshore scam compounds. Australia reports that FIRESTORM has identified at least 11 scam compounds in Cambodia, Myanmar and Laos actively targeting Australian victims and, through investigations and assistance to foreign law enforcement, has been associated with 13 raids on scam centres and 560 arrests. Its intelligence picture draws on victim reporting, financial intelligence and STRs, international law enforcement intelligence, reporting from technology companies, FIs, telecommunications providers and VA exchanges, and debriefings of victims and persons repatriated from scam compounds. In one case, real-time intelligence supported Thai enforcement action and approximately AUD 1.3 million (approximately USD 0.85 million) was seized or frozen by Australian banks for return to victims.

Nigeria: In April 2025, the Attorney-General established the Joint Case Team on Cybercrimes (JCTC), bringing together the Federal Ministry of Justice, NAPTIP, NPF-NCCC, NFIU and ONSA to share expertise, intelligence and operational capabilities in complex cybercrime cases. In a January 2026 Delta State scam compound case, intelligence from a foreign jurisdiction, supported by a social-media platform, enabled NPF-NCCC to geolocate and raid the site, arresting seven suspects. Digital-forensic analysis of seized devices identified more than 50 000 social-media and messaging identifiers and numerous stolen identities.

Philippines: In a 2024 operation against a suspected scam compound, PNP-CIDG and PAOCC co-ordinated the law enforcement action, rescue of workers and seizure of electronic, documentary and physical evidence, while AMLC conducted a parallel financial investigation into related persons, companies, accounts, properties and cross-border financial links. Financial intelligence exchanged with foreign FIUs expanded the investigation beyond the Philippines, while domestic co-ordination supported Freeze and Bank Inquiry Orders and subsequent civil forfeiture proceedings. The case illustrates how criminal, financial, asset recovery, immigration and regulatory action can be developed in parallel against the wider enterprise rather than only the persons conducting scams.

United States: Established in 2025, the interagency Scam Center Strike Force brings together US federal and foreign LEAs and private sector partners to target scam compound leadership, enabling infrastructure and illicit financial flows. Its operational priorities include disrupting US-based infrastructure used by scam compounds, identifying and prosecuting their leaders, tracing and restraining stolen VAs for potential return to victims, and preventing further victimisation. Actions to date include charges against leaders linked to scam compounds in Myanmar and Cambodia; seizure of a Telegram channel used to recruit persons for trafficking to a Cambodian scam compound and more than 500 fraudulent VA-investment websites; restraint of more than USD 938 million in VAs; co-ordination with the US Department of the Treasury on sanctions against perpetrators and enablers; and proactive work with private companies to disrupt access to US-based infrastructure. In June 2026, a targeted public-private "Disruption Week", involving US and foreign law enforcement and technology, VA and analytics firms, disrupted approximately 1.4 million social media and email accounts and malicious network infrastructure, supported arrests in Thailand and led to the voluntary freezing of more than USD 3.8 million in VAs. Reflecting the geographic expansion of scam operations beyond Southeast Asia, the Strike Force also deployed a team to Madagascar to support local authorities in an operation against 13 suspected scam centres and the examination of more than 3 200 electronic devices

Shared fraud data platforms, registries and analytical infrastructures

National fraud platforms, central fraud registries and other shared fraud data infrastructures can support scam compound-related detection and disruption by connecting information across FIs, competent authorities and other relevant actors, providing network-level visibility, shared analysis, fund tracing and timely intervention. Governance may be public, public-private or private-private, and models may combine these arrangements or extend across sectors. Public arrangements can provide authoritative information and common procedures; public-private models can combine public-sector intelligence, legal gateways and authorities' powers with private-sector transactional visibility and intervention capabilities; and private-private arrangements can reveal connected activity not visible to individual institutions. Cross-sector participants may include FIs, VASPs, stablecoin issuers, blockchain analytics providers, telecommunications companies, social media and technology platforms, DNS, domain and hosting providers and, where relevant, gambling-sector actors. Connecting financial information with upstream indicators such as fraudulent advertisements, accounts, phone numbers, domains and platform identifiers—including indicators detected before victim contact—can support earlier prevention, payment intervention, investigation and infrastructure disruption. Box 10 illustrates how these functions can be delivered through distinct public and private sector governance models. Shared-data infrastructures may also provide the signals and tracing capabilities used in preventive payment controls and rapid asset preservation workflows; this subsection should therefore be read together with subsections 16.4 and 16.8.

The objective is not merely to increase the quantity of information exchanged, but to create trusted environments in which relevant signals can be shared under common legal, governance, semantic and technical conditions, integrated into relevant investigative, detection, case-management and preventive workflows, and converted rapidly into proportionate action.

BOX 10. **Examples of shared fraud data and information sharing infrastructures across different governance models**

Publicly managed arrangements

France: The FNC-RF, managed by the Banque de France, enables PSPs to share IBANs associated with suspected or confirmed fraud and requires participating institutions to investigate and update flagged accounts. The register can support pre-validation and payment-intervention measures providing a transferable model where suspicious IBANs are linked to scam compound victim payments or mule networks.

Korea: The Financial Services Commission operates the AI-based ASAP platform, through which FIs and investigative authorities share information on fraud-linked accounts. The relevant voice-phishing legislation was amended to provide a legal basis for sharing account-holder personal information for this purpose. KoFIU separately operates a system through which FIs, investigative authorities and KoFIU share fraud-account information and the status of transaction suspensions for emerging forms of voice phishing outside the special-law framework.

Private sector initiatives

National Fraud Portal model: A general National Fraud Portal model can enable fraud reports to enter a shared case management workflow for validation, prioritisation and investigation. Its money tracing functionality can trace funds across successive accounts in real time, identify previously unknown mule accounts and feed resulting intelligence back into fraud detection controls.

Continued on next page ...

... Box 10 continued

Global and cross-border sharing of scam indicators: Global information sharing mechanisms involving public authorities and private sector entities across jurisdictions and sectors, including technology, financial and telecommunications actors, enable the timely exchange of actionable scam signals, such as malicious URLs, scam-related websites and fraudulent phone numbers. Such co-operation supports the identification and disruption of transnational scam-related infrastructure, including the rapid removal of fraudulent online content, social media accounts and pages, and facilitates co-ordinated action across borders to prevent the further use of infrastructure associated with scams.

Scam Signals: Developed by UK mobile operators, UK Finance, participating banks and GSMA, Scam Signal enables banks to receive privacy-preserving mobile-network risk indicators in real time at the point a customer is authorising a payment, including whether the customer is on a call and the call's direction and duration. GSMA reports that the service is live across major UK mobile networks, covering approximately 85% of UK mobile users, and that UK-bank use of this type of signal has been associated with a 41% reduction in people scammed, a 44% decrease in fraud losses and a 55% reduction in false positives. Although not specific to scam compounds, the model is relevant where scam compound social engineering keeps a victim on a call while a payment is authorised and illustrates how telecommunications signals can complement financial data to enable earlier payment intervention.

Effective shared-data infrastructures require clear legal, governance and operational foundations. These include clear legal bases and sharing conditions; defined participants and purposes; common data fields, formats and escalation thresholds; secure workflows; standards for data quality, provenance, permitted use and proportionate retention; appropriate evidential or confidence thresholds where information may lead to adverse action against a person or account; feedback mechanisms—including, where legally permissible, mechanisms through which FIUs and LEAs can return sufficiently actionable network-level indicators and typologies to relevant private-sector actors—and safeguards for sensitive information. Relevant indicators should, where available, be accompanied by sufficient contextual information—such as validation status, relevant timestamps, fraud typology and relevant transactional or behavioural context—to enable recipients to assess their relevance, urgency and appropriate operational use. Jurisdictions should provide sufficient clarity on what information may be shared, with whom and for what purpose, including fraud prevention and disruption, and on the conditions under which recipients may use and act upon shared information. Where appropriate, they may consider safe-harbour or similar protections for good-faith information sharing within defined legal and operational parameters, including to facilitate domestic or cross-border private-private and cross-sector sharing among relevant financial, technology and telecommunications actors. Supervisory guidance and other proportionate legal or regulatory measures may also reduce uncertainty or disincentives to timely and reciprocal sharing without displacing applicable reporting obligations, privacy requirements or other safeguards. Competent authorities can further reduce operational uncertainty by providing and, where necessary, promptly updating practical guidance on permissible information sharing scenarios.

Private-private arrangements should, where useful, move beyond ad hoc bilateral exchanges towards repeatable networked models capable of routing relevant signals to actors positioned to act. Where legally permissible and appropriately safeguarded, such models may enable one-to-many sharing of high-confidence warnings before every receiving institution has independently identified a direct customer or transactional nexus. Where shared information may result in preventive or adverse action, arrangements should include clear purpose limitations, confidence thresholds, permitted-use rules and mechanisms for correction or review. Where appropriate, competent-authority support or endorsement may help clarify legal parameters, escalation and feedback without requiring direct participation in every exchange. Interoperability need not depend on a single proprietary platform: shared and reusable scam typologies or detection-rule libraries and open technical standards may reduce implementation

friction and allow validated patterns to be adapted across differently resourced participants. Such tools should be locally validated, regularly updated and governed under the same legal, data-quality and safeguarding requirements as other shared-data arrangements.

Time-bound pilots can test and refine these capabilities and help determine whether they can be scaled into standing information sharing arrangements. Pilot evaluation should distinguish operational readiness and barriers to participation; the usefulness and actionability of different signal types; the actions actually enabled by shared information; measurable impact on detection, prevention or disruption; and the conditions required for scaling across sectors and jurisdictions. Where legally permissible and appropriately safeguarded, pilots using live scam victim or mule account leads may also identify previously unknown accounts or VA wallets and support timely restriction, asset preservation or recovery action. Their primary purpose should nevertheless be to validate scalable capabilities that can subsequently be embedded in standing arrangements. Standardised reporting formats, structured or API-enabled interfaces, common fraud-pattern languages, tokenised or pseudonymised identifiers, federated learning and other privacy-enhancing technologies (PETs) may further reduce operational friction, support network-level and cross-border analysis and limit unnecessary exchange of raw or directly identifiable data.

Rapid response and asset preservation networks

Rapid response networks provide pre-established co-ordination arrangements through which relevant actors can respond quickly when suspected scam compound-related proceeds are identified. Their purpose is to enable timely payment intervention and asset preservation action by establishing trusted contact points, escalation pathways and arrangements for rapid domestic or cross-border co-ordination. A critical operational objective is to minimise the time between the earliest actionable indicator—including, where available, at the stage of victim contact or payment instruction—and intervention as funds move through payment execution, onward transfer, VA conversion and other subsequent stages towards asset preservation. Given the speed and volume of relevant transactions, these arrangements should enable actionable information to reach FIs, VASPs and other actors with direct operational control over the payment, account or wallet quickly enough for them to intervene before funds dissipate.

Such arrangements should clearly allocate the roles and responsibilities of participating actors, including which institutions receive and validate alerts, which actors are positioned to intervene, and how cases are escalated between sending and receiving institutions, competent authorities and relevant private sector participants. Where immediate payment or asset preservation action is required, arrangements should recognise the distinct roles of private sector actors able to execute holds, recalls, restrictions or other available interventions in real time, and of competent authorities responsible for intelligence, investigation and formal coercive measures.

Rapid response networks may operate domestically or across borders, through public-public, public-private or private-private partnerships. Where payment systems or other financial infrastructures are interconnected across borders, compatible contact, notification and escalation arrangements can help avoid operational gaps and preserve the window for intervention before formal international co-operation processes are completed.

Rapid response arrangements should, where appropriate, be periodically tested through operational or simulation exercises. Testing can identify weaknesses in contact chains, escalation thresholds, response times, information sharing procedures and co-ordination capabilities and inform adjustments to procedures, resources and capacity. Where feasible, testing should assess elapsed time across key hand-offs in the response chain and identify points at which delays allow funds to move beyond effective intervention or preservation.

Domestic allocation of freezing powers can limit the speed of cross-border asset preservation. Therefore, **rapid response networks depend not only on fast information exchange, but also on clear domestic legal pathways** for provisional asset preservation and timely escalation to authorities able to act.

BOX 11. **Rapid response mechanisms for fund interception and asset preservation**

Egmont Group: The Cyber-Enabled Fraud Rapid Response Program provides a structured FIU-to-FIU mechanism to accelerate cross-border tracing and recovery in cyber-enabled fraud cases and is co-ordinated with INTERPOL's I-GRIP. For scam compound-related flows, it can support rapid exchange of standardised financial information and escalation to competent domestic authorities while the window for interception or asset preservation remains open.

Europol: In July 2026, Europol launched the Rapid Response Protocol (RRP) Pilot Initiative to accelerate alerts, notifications and requests for provisional interception in serious cases involving cross-border money flows. The RRP aims to support the timely interception, blocking and freezing of funds pending further police or judicial action, or to facilitate their direct return to victims' bank accounts.

INTERPOL: I-GRIP provides a rapid cross-border mechanism for intercepting illicit funds in high-velocity fraud cases. Since its inception with increasing usage over the years, I-GRIP has processed approximately 2,700 requests, resulting in the interception of criminal proceeds valued at USD 130 million.

Cross-border competent authority co-ordination networks

Scam compound cases require co-operation between source, transit, hub, victim, laundering and asset-holding jurisdictions. Cross-border FIU and law enforcement networks can support rapid information exchange, joint investigative action, victim identification and repatriation, asset tracing and provisional freezing, and co-ordinated



In April 2024, police forces from five jurisdictions raided 12 call centres identified as the source of thousands of daily scam calls. 21 persons were taken into custody during this Europol-supported action day, which took down a criminal network responsible for defrauding thousands of victims.
© Europol

disruption of transnational criminal networks. Relevant mechanisms include Egmont FIU channels, regional Asset Recovery Inter-Agency Networks, INTERPOL I-FIU Connectivity, INTERPOL Silver Notices and Diffusions (see Box 12), MLA, pre-established law enforcement escalation pathways and cross-border VASP outreach. INTERPOL's I-FIU Connectivity Initiative can support this function by enabling participating FIUs to enrich financial-intelligence analysis with relevant INTERPOL police information and support more timely investigative follow-up. Where a VASP operates across several jurisdictions, these arrangements should also enable authorities to identify rapidly the FIU or other competent authority able, under the applicable framework, to obtain and share the relevant customer and transaction information. Where scam compound-linked investment fraud engages securities regulators, sectoral regulator-to-regulator frameworks can complement FIU and law enforcement channels. IOSCO's Multilateral MoU Concerning Consultation and Cooperation and the Exchange of Information and Enhanced Multilateral MoU Concerning Consultation and Cooperation and the Exchange of Information (EMMoU) provide one example, supporting cross-border exchange of enforcement information, including unsolicited assistance; the EMMoU additionally covers powers including asset freezing and access to internet-service-provider and telephone records.

BOX 12. INTERPOL Silver Notices for cross-border identification of criminal assets

The Silver Notice, launched as a pilot in January 2025, enables law enforcement authorities to identify, trace and monitor criminal assets that have been moved, concealed or otherwise placed beyond the reach of investigators across jurisdictions. In scam compound-related cases, where criminal proceeds and assets may be held outside the jurisdiction conducting the investigation, the mechanism can support cross-border asset tracing and identify assets for subsequent preservation and recovery. A Silver Notice does not itself provide a legal basis to freeze, seize or confiscate assets; appropriate action against identified assets must instead be taken in accordance with domestic law or through established international co-operation mechanisms, such as mutual legal assistance. INTERPOL reports that cases under the initiative seek approximately USD 2 billion in assets and that Silver Notices have already contributed to the identification and location of approximately USD 36 million in criminal assets. Illustrating the speed with which the mechanism can operate, following a Silver Notice concerning USD 18 million in criminal proceeds, an Oceanian member country identified approximately USD 6 million in assets within five days.

Information obtained from foreign counterparts through these channels can support parallel financial investigations, intelligence development and rapid asset preservation action. Informal co-operation can complement formal mechanisms by enabling earlier intelligence exchange, helping identify relevant persons, transactions and assets and, where formal assistance is subsequently required, supporting more targeted and timely requests. Formal international co-operation remains necessary for obtaining evidence or taking coercive or judicial action where required, but should be complemented, where possible, by faster operational channels that enable authorities to intervene before evidence, assets or investigative opportunities are lost. Where permitted by applicable legal and operational frameworks, diagonal co-operation between different types of competent authorities across jurisdictions may also help connect complementary financial, law enforcement and other relevant information and expertise[2]. Early use of asset recovery and liaison networks can also improve the subsequent formal co-operation process. ARO and CARIN channels can help identify relevant asset locations, competent counterparts and appropriate investigative measures, while early clustering of related victims, payment flows, accounts, suspects and criminal networks can enable authorities to present the wider criminal activity through a more coherent MLA request rather than fragmented case-by-case requests.

2. FATF – Egmont Group – INTERPOL – UNODC (2025), *International Co-operation on Money Laundering Detection, Investigation, and Prosecution Handbook*, FATF, Paris, France, available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/International-Co-operation-ML-Detection-Investigation-Prosecution.pdf.coredownload.pdf

BOX 13. **Cross-border co-ordination to disrupt scam-related illicit financial flows**

INTERPOL: In 2026, Operation FIRST LIGHT brought together 97 countries and territories to target social-engineering scams and associated ML, including cyber scam centres, resulting in 5 811 arrests, USD 293 million in illicit assets intercepted and more than 31 000 bank accounts blocked. Both operations used INTERPOL mechanisms to support co-ordinated cross-border investigation, fund interception and asset preservation.

Singapore: Established in 2024, FRONTIER+ is a cross-border anti-scam collaboration platform connecting anti-scam and law enforcement agencies through real-time intelligence sharing and analysis, joint operations and co-ordinated enforcement against transnational scams. Operation FRONTIER+ III brought together law enforcement agencies across ten jurisdictions in a co-ordinated two-month operation, during which close to 102 000 scam-tainted bank accounts were frozen and more than USD 161 million in illicit funds seized. In one Singapore-linked case, rapid co-ordination between Singapore's Anti-Scam Centre and Hong Kong China's Anti-Deception Co-ordination Centre resulted in the seizure of more than USD 11.1 million from bank accounts in Hong Kong China and associated VA wallets. In another case, USD 6.6 million transferred to Oman was fully recovered after a FRONTIER+ partner in the United Arab Emirates facilitated liaison between Singapore and Omani authorities.

Networks of networks

National anti-scam centres and other co-ordination mechanisms can be strengthened through trusted cross-border contact points, shared escalation protocols and rapid information exchange. A network-of-networks approach could connect existing capabilities—including anti-scam centres, fraud registries, FIU channels, PPPs, private-private platforms, VASP-facing alert systems and cross-sector scam-signal exchanges—through common classifications, interoperable indicators, legal gateways, safeguards and trusted contact points. Interoperability should also address identifier fragmentation. Where customer, entity, account, wallet or case identifiers differ across jurisdictions or systems, reliable mapping between existing identifiers and compatible data conventions can reduce reconciliation frictions and improve cross-border matching, subject to applicable legal, privacy and data protection safeguards. Interoperable national fraud platforms and analytical infrastructures could provide building blocks by enabling domestically identified fraud and mule account indicators to be exchanged or queried across borders. This would not require a single global operational platform, but could enable actionable indicators to be transmitted rapidly and lawfully to the actors best placed to prevent payments, freeze accounts or wallets, disrupt infrastructure, identify trafficked persons, trace assets or connect cases to wider networks. Countries may prioritise such interconnection according to their risk context, payment ecosystem and existing or planned links between payment systems.

Comparable regional approaches have also been proposed: GIABA, for example, has recommended a regional forum linking national cybercrime platforms in West Africa to facilitate networking and the exchange of information and intelligence.

16. Operational toolkit

This subsection sets out practical operational tools that competent authorities and private sector actors can use to detect, trace and disrupt illicit financial flows linked to scam compounds and the criminal networks that sustain them. These tools are complementary and are most effective when deployed in combination at the appropriate stages of the end-to-end financial flow model. They should be read together with the relevant FATF Standards, guidance and policy foundations mapped in Table 1 and the strategic principles and co-ordination models above; they operationalise those foundations rather than replace them.

BOX 14. **Example of a cross-cutting operational toolkit**

UNODC: The Public-Private Partnership Toolkit Against Organized Fraud provides a general framework for establishing, governing and evaluating anti-fraud PPPs, including problem and risk definition, participant selection, governance and accountability, lawful and secure information sharing, data protection, implementation and iterative review.

Risk assessment, system-wide detection and network mapping

Jurisdictions should first understand their exposure to scam compound-related fraud and ML, including through national and sectoral risk assessments, consistent with the risk-based approach under Recommendation 1.

Where feasible and operationally safe, jurisdictions should also consider publishing sufficiently aggregated, non-sensitive data on relevant fraud and scam compound indicators to support trend analysis, typology development and targeted prevention by public and private stakeholders. Relevant sources may include victim and consumer reports, law enforcement data, FI and VASP reporting, telecommunications and technology-sector information, civil society sources and, where relevant to physical operating sites, information from local authorities, utility and connectivity providers, commercial lessors, private-security providers and economic-zone administrators. The end-to-end lifecycle and dependency analysis in this report can help jurisdictions identify whether they are principally exposed as host, victim, recruitment/source, transit, laundering or asset-holding jurisdictions, and which sectors, products, services, channels and financial and non-financial dependencies present material risks or require priority mitigation. This assessment may also consider whether locally hosted operations are externally controlled, domestically rooted or mixed, and whether their victim targeting is global or regionally concentrated, to help identify relevant cross-border dependencies and co-operation needs.

Where formal data are limited, targeted research and multi-stakeholder assessments can help identify exposure, intervention points and capability gaps. Low reporting volumes should not, in isolation, be interpreted as low exposure where awareness, reporting mechanisms or institutional capacity are limited. This broader risk understanding should in turn inform risk-based supervision. Supervisors should understand the exposure of supervised FIs and VASPs to the receipt, transit and cash-out of related proceeds and ensure that these risks are appropriately reflected in supervisory priorities and intensity. Mitigation priorities should be calibrated to the jurisdiction's principal role or roles in the scam-compound ecosystem: victim jurisdictions may place greater emphasis on victim reporting, preventive payment intervention and rapid outbound co-operation; host jurisdictions on controllers, operating infrastructure, trafficking, corruption and domestic asset preservation; and laundering or asset-holding jurisdictions on network-level detection, tracing, freezing and recovery. Jurisdictions may perform several of these roles simultaneously.

Network mapping by FIUs and, where appropriate, other competent authorities can complement national, sectoral and institutional risk assessments by combining reporting from multiple entities with transaction analysis, victim reports, FI and VASP data, fund flow reconstruction, device and location indicators—including, where safely and lawfully available, survivor or civil society-derived geospatial information on suspected operating sites—IP/MAC addresses, open source and social media information, and tax or corporate information. Where non-governmental actors hold credible information on scam compound locations, ownership structures or related financial flows, jurisdictions may also consider secure channels for voluntary transmission of relevant information to competent authorities, subject to appropriate confidentiality, source-protection and safety safeguards. Where appropriate under domestic frameworks, network mapping may also incorporate relevant information from anti-trafficking, immigration and customs authorities, security or intelligence services, and DNFBPs or other professional service providers involved in premises, legal structures or asset transactions. Such analysis can identify connections not apparent from individual reports, reveal wider syndicate structures involving trafficking, mule accounts, unlicensed or unregistered MVTS, VAs

and VASPs, shell companies and gatekeepers, and support the development of scam compound-related indicators. Where relevant information is available, it should also examine expenditure associated with recruitment, victim leads and data, advertising, telecommunications, domains and hosting, fraudulent platforms, premises and specialised providers, together with relevant transport, supply and access routes and other physical-logistics dependencies, to identify shared dependencies, preparations for new or expanding operations and prioritise upstream disruption opportunities, informed by the dependency analysis in Infographic 2. Where corruption or protection networks are material, mapping should also examine bribery and protection payments, links between criminal controllers and public officials or politically connected businesses, patterns of selective enforcement or advance warning, and other financial or institutional dependencies that help sustain scam compound operations.

BOX 15. **Network mapping through combined financial, corporate and open source analysis**

Türkiye: In one reported scam compound-linked cross-border investment-fraud case, suspected scam compound-linked cross-border investment-fraud activity was identified by combining open source research and foreign-regulator information with bank transfers, VA transactions and company records. Analysis of common owners, managers, addresses, employees and financial transactions helped identify a wider network of connected companies and trace flows between foreign online platforms and Türkiye-based entities.

Detection of scam compound activity should combine institution-level monitoring with system- or network-level analysis. Shared or collaborative analytics can identify cross-institutional patterns, connected beneficiary accounts and wallets, mule networks and co-ordinated scam activity not visible to any single FI, VASP or other actor. Where such arrangements are in place, governance frameworks should clearly define how analytical outputs are validated, who can access and act on them, and how relevant findings are escalated and shared to support operational action.

Technology and telecommunications providers can provide important upstream signals of scam compound activity. Subject to applicable law and safeguards, proportionate monitoring and analysis may identify fraudulent advertising or recruitment, impersonation, malicious domains or URLs, suspicious accounts or telephone numbers, and co-ordinated activity or telecommunications anomalies. High-confidence indicators should feed the cross-sector detection and disruption arrangements described in subsection 16.2.

Detection should also combine indicators rather than rely on individual red flags, particularly for recruitment-related activity. An OSCE exploratory assessment highlights recurring features including messaging-app routing, rapid onboarding, relocation, housing or visa support, vague role descriptions and fraud-adjacent occupational framing. Where relevant indicators arise before victim contact, timely cross-sector sharing with other technology and telecommunications providers, FIs, VASPs and competent authorities can support intervention at the earliest stage of the scam. High-confidence indicators should support timely protective action—including warnings, restriction or removal of fraudulent content or accounts and preservation of relevant information—and, where legally permissible, be shared through established channels with actors able to prevent victim engagement or payments, identify related infrastructure or support investigation and disruption.

Where lawful and proportionate, relevant actors could also test controlled scam-hunting techniques—including honeypots, automated or agentic scam-interaction tools or adaptation of brand-monitoring capabilities—to identify live campaigns, generate reusable account, domain, communications and payment-destination indicators capable of supporting both upstream infrastructure disruption and downstream financial intervention and, where feasible, impose operational costs by diverting scammer time or capacity before successful variants scale. Such approaches should be subject to appropriate legal, privacy, safety and evidential safeguards and evaluation of operational effectiveness.

Consistent case classification can strengthen aggregation, clustering, network analysis and cross-sector and cross-border information sharing. Existing fraud taxonomy and classification initiatives illustrate complementary approaches to structuring incident data and adversary behaviours for these purposes (see Box 16). Where feasible, actors should also seek to identify and tag scam campaigns, understood operationally as clusters of communications, accounts, domains, advertisements, beneficiary accounts or VA wallets, behaviours or other indicators linked by common infrastructure or modus operandi. Campaign-level analysis can help connect rapidly changing variants even where scammers alter scripts, platforms, domains or identities, reducing reliance on static typologies that may quickly become obsolete. Relevant fields may include victim or target category; contact medium; scam typology or modus operandi; financial product or service and payment method; detection method; payment initiation and authorisation, including whether the payment was initiated by a customer following manipulation or by the fraudster; licensing status of the entity involved in the transaction; recovery status; and links to wider or cross-border criminal networks[3]. For scam compound-related cases, classification may also capture relevant recruitment or forced-criminality indicators, associated digital or telecommunications infrastructure and the stage or stages of the end-to-end financial flow concerned. Consistent classification can also connect apparently separate cases and help assess whether preventive controls were triggered, effective or bypassed. Within FIs, fraud-prevention and AML/financial crime functions should work together through intra-institutional data flows, compatible classifications and

3. OECD (2026), *Protecting Consumers from Financial Scams and Frauds*, OECD Publishing, Paris, available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/06/protecting-consumers-from-financial-scams-and-frauds_3887b249/d41817bb-en.pdf



Singapore Police Force (SPF), Cyber Command. © Singapore Police Force

escalation pathways so that both fraudster-initiated unauthorised transactions and authorised payments induced by manipulation can be connected to beneficiary, mule and laundering activity.

Where reporting systems permit, scam compound-specific tags can facilitate aggregation, analysis and feedback. Agreed network- or case-level tags can also serve an operational routing function by helping FIUs, LEAs and participating private-sector actors recognise interconnected reporting and direct high-priority information to the appropriate specialist teams. Wolfsberg-led private-private information sharing exercises report reduced response times where common tags were used for this purpose. Structured technical indicators—such as phone numbers, online identifiers, wallet addresses and transaction hashes, apps, URLs, domains and IP addresses—and information on connected service providers can also help link financial reporting to wider scam infrastructure. Where reporting entities identify apparently connected fraud-related activity, reports should, where practicable, include relevant network-level context—such as linked beneficiary accounts, VA wallets, corporate entities, devices or recurring payment patterns—rather than presenting each victim transaction in isolation, without displacing applicable STR reporting requirements or thresholds. PETs may, where appropriate, facilitate the sharing of network-level indicators while helping to minimise the disclosure of unnecessary personal information.

For scam compound-related activity, **the practical objective is not to adopt a single taxonomy, but to use sufficiently consistent and interoperable classifications** to connect victim reports, fraud methods, digital infrastructure and financial flows to common campaigns and criminal networks, while allowing classifications to evolve as scam tactics change.

BOX 16. **Examples of complementary fraud taxonomy and classification frameworks**

The Euro Banking Association Fraud Taxonomy provides a common payment-fraud classification structured around the method of first contact or compromise, the fraud modus, who initiated the affected payment transaction, optional labels or tags and the payment instrument. It is designed to reduce overlap in fraud-type classification and improve the consistency of fraud statistics, and is subject to regular updating as fraud patterns evolve. For scam compound-related analysis, this structure can help distinguish the victim-contact channel and scam technique from the manner in which the payment was initiated, including customer-initiated payments resulting from manipulation and fraudster-initiated unauthorised transactions. The taxonomy focuses on payments rather than on scam compounds specifically and therefore provides a complementary classification layer rather than a standalone taxonomy for scam compounds.

The OECD's 2026 typology for financial scams and frauds classifies incidents across ten dimensions: target; contact medium; modus operandi; financial product or service; payment method; licensing status of the entity involved in the transaction; detection method; payment authorisation; recovery status; and links to perpetrators. A corresponding classification template supports consistent recording, aggregation and analysis of fraud data.

The MITRE Fight Fraud Framework (F3) provides a behaviour-based taxonomy of fraud actor tactics and techniques. Drawing on the ATT&CK model, it provides a common language for connecting cyber and fraud observations and mapping how fraud activity develops through to monetisation.

The Federal Reserve classification models, Stripe's FT3 framework and FS-ISAC's Cyber Fraud Prevention Framework illustrate additional and complementary approaches focused respectively on consistent fraud and scam classification, fraud tactics and techniques, and cross-functional co-ordination.

Digital, telecommunications and platform infrastructure disruption

Digital, telecommunications and platform infrastructure disruption should target the assets and services used to acquire victims and sustain scam campaigns, including fraudulent advertisements and accounts, malicious domains and websites, phone numbers, SIM infrastructure for large-scale malicious messaging, fake applications and investment platforms, hosting and other technical services. Investigations into scam compound-related fraud have found that offenders may use numerous telephone numbers while relying on a substantially smaller number of physical devices, making device-level analysis potentially useful for identifying shared infrastructure despite changes in telephone numbers. Where large-scale scam calling or messaging relies on SIM farms or comparable telecommunications infrastructure, jurisdictions may also consider proportionate controls on the bulk acquisition, activation or use of SIMs and associated equipment, alongside telecommunications-sector mechanisms to trace fraudulent calls or messages to their origin and identify infrastructure for upstream disruption. Such measures may also include caller-number authentication or comparable anti-spoofing controls, while recognising that scam networks may circumvent domestic controls by shifting communications to messaging services, satellite connectivity, offshore providers or other infrastructure outside the effective reach of national authorities[4]. Post-disruption monitoring may also draw on anomalous SIM-box traffic, bulk-SIM registration, number-recycling or porting anomalies and roaming patterns consistent with cross-border SIM-farm activity to identify successor telecommunications infrastructure. Restriction or takedown should, where possible, be combined with the preservation and sharing of relevant identifiers, as removal from one service may simply displace activity to another provider or jurisdiction. Where scam compound networks rely on shared crime-as-a-service or backend hosting infrastructure, co-ordinated disruption should, where legally available, seek not only to disable the relevant service but also to preserve and exploit associated server, subscriber, account and other operational data so that takedowns generate leads on connected criminal users, infrastructure, victims and financial flows across jurisdictions. High-confidence indicators should therefore be shared through trusted channels with other actors able to identify the same campaign, prevent victim contact or payments, preserve evidence or disrupt associated infrastructure.

Technology and advertising platforms can also reduce victim acquisition through risk-based controls applied to advertisers and advertising activity. Relevant measures may include proportionate advertiser verification; enhanced verification of higher-risk advertisers; checks, where relevant, against authoritative registers of licensed or regulated financial-service providers and regulatory warnings concerning unauthorised or suspicious firms, websites or activities; continuous reassessment using behavioural, relational and trusted external signals; and monitoring of landing pages and destination URLs to identify changes or cloaking after initial review. Where platforms rely on official licensing or authorisation registers, jurisdictions should seek to ensure that relevant registers are accurate, current and, where feasible, machine-readable and interoperable, with sufficiently granular identifiers—including authorised domains—to support scalable verification[5]. Confirmed or high-confidence intelligence on fraudulent advertisers, domains, payment identifiers and related infrastructure should feed updated detection and restriction controls to reduce repeated use of the same infrastructure. Jurisdictions and platforms may also establish trusted-notifier or priority-referral arrangements through which competent financial or securities authorities can flag unauthorised or suspicious financial service providers, advertisements, websites or domains for expedited review and, where warranted, restriction or removal, while preserving relevant identifiers for further analysis and information sharing.

4. Peng, X. (2026), *Checkpoints, conflict and scam logistics: Mobile control and the politics of circulation in the China–Myanmar–Thailand borderlands*, DIIS Working Paper Series, Roadblocks and Revenues No. 13, Danish Institute for International Studies (DIIS), Copenhagen, available at: https://pure.diis.dk/ws/files/31998653/DIIS-WP-series-Roadblocks-13-Checkpoints-conflict.pdf
5. International Chamber of Commerce (ICC) and Global Anti-Scam Alliance (GASA) (2026), *Best practices for combating scams in advertising*, June 2026, available at: https://iccwbo.org/news-publications/principles/best-practices-for-combating-scams-in-advertising/

BOX 17. **Cross-border regulatory warnings for upstream scam detection**

IOSCO: The International Securities & Commodities Alerts Network (I-SCAN) consolidates warnings submitted by securities regulators on suspicious firms, websites and activities into a global repository accessible to third parties. Since its launch in March 2025, more than 16 500 alerts have been submitted. A standardised API enables online platforms, banks and other FIs to integrate these regulatory alerts into compliance, risk-management and security workflows. Although not scam compound-specific, I-SCAN provides a transferable model for converting cross-border supervisory warnings into timely and scalable upstream screening and detection where unauthorised or suspicious investment activity is linked to scam compound-related fraud.

Given its role in victim acquisition, online advertising should be separately captured in scam typologies and operational analysis. Where available, relevant information may include the advertiser or advertising account and associated identity or verification information; payments for advertising; landing pages and domains; target audiences; linked or successor advertisements; and connections to subsequent communications and payment infrastructure. Where malicious advertising is paid for, associated billing and payment data may provide financial intelligence linking upstream victim-acquisition infrastructure to accounts, wallets, intermediaries and wider criminal networks and should, where legally permissible, be preserved and routed through established information sharing channels. For financial-services advertising, analysis may also consider whether the purported provider is authorised by the relevant regulator and whether associated domains and other identifying information are consistent with authoritative registers. Referrals and disruption workflows should, where feasible, capture linked domains, advertiser identifiers, payment-related indicators and off-platform destinations rather than the advertisement alone, helping identify recurring campaigns and migration across services.

BOX 18. **Mapping and disrupting scam-enabling infrastructure**

Hong Kong China: In August 2024, the Hong Kong Police Force disrupted four locally based telecommunications network centres providing telecommunications services to overseas scam compounds. Eleven persons were arrested and around 80 000 pre-paid SIM cards, modem pools and computers equipped with remote-access software were seized. Examination of the computers indicated that the centres were interlinked and could be controlled remotely from overseas, enabling fraudulent calls to be routed through Hong Kong China's mobile network. The case illustrates how scam-compound networks can outsource victim-contact telecommunications infrastructure to criminal operators in other geographical locations.

United Kingdom / New Zealand / Meta: The United Kingdom and New Zealand report on cross-border public-private disruption sprints involving LEAs and Meta. In a Bangkok sprint in March 2026, Thai authorities arrested 21 persons and Meta disabled more than 150 000 accounts linked to scam compounds networks. The United Kingdom reports that a subsequent sprint in Washington DC in May 2026 resulted in 1.5 million Meta account takedowns and USD 3 million in illicit funds frozen, alongside domain takeovers linked to scam compounds in Cambodia and the identification of companies in Vietnam linked to the compromise and generation of Meta accounts sold to scam compounds. Under Project WINTERPROOF, similar time-bound operational intensifications bring together UK and foreign LEAs and private-sector partners. The United Kingdom also reports that actionable intelligence provided by Meta to the NCA and subsequently shared with Nigerian partners contributed to NPF-NCCC's disruption of a scam compound in Delta State targeting victims in the United Kingdom and United States.



A delegation of prosecutors, investigators and central authorities from various countries visited a raided scam compound in Phnom Penh in December, 2025 together with UNODC officials. © UNODC

Mule account disruption tools

Mule accounts are a core mechanism for the collection and layering of scam compound-related proceeds. Because mule networks may include both knowing participants and persons recruited, deceived or exploited without full awareness of the underlying criminal activity, operational responses should be appropriately risk-based and proportionate while seeking to identify the wider criminal network controlling or facilitating the accounts. Measures should distinguish, where possible, between deliberate facilitation and conduct resulting from deception, coercion or exploitation, and should avoid unnecessary or disproportionate financial exclusion. Assessment should remain evidence-based in both directions: persons should not be treated as complicit merely because they moved funds, while self-identification as a scam victim should not, by itself, preclude examination of evidence indicating knowing facilitation of the wider laundering network. Operational measures should combine shared mule account intelligence with institution- and network-level analysis to identify individual accounts and wider mule networks. Relevant techniques include clustering accounts by common identity, device, IP address, location, transaction timing or cash-out patterns, and graph analytics to identify relationships between accounts and transactions, including previously unknown accounts and multi-generation mule chains. As criminal networks increasingly acquire or misuse identities to establish multiple accounts or VA wallets across providers, analysis should extend beyond individual account clustering to identify repeated or anomalous use of the same identity across accounts and providers, as well as indicators of identity misuse and synthetic fraud.

Confirmed or high-confidence mule account intelligence should support rapid, risk-based intervention, including the restriction or closure of identified accounts and, where appropriate, sharing of relevant leads between FIs and VASPs. Information sharing and resulting account-level measures should be subject to appropriate data protection, privacy, accuracy, retention and review safeguards, particularly where information may affect a person's future access to financial services. Mechanisms should, where appropriate, allow erroneous or outdated information to be corrected and avoid indefinite adverse treatment of persons who were deceived or exploited. Where identity misuse is identified, relevant intelligence should also support the identification of other accounts or VA wallets established or controlled using the same identity, subject to applicable legal and data protection requirements. Information generated through post-settlement investigation should in turn be used to enhance ex-ante detection and risk scoring models, shared mule account intelligence and other preventive controls. FIs and, where relevant, VASPs should also apply risk-based controls to suspected mule accounts or VA wallets displaying pass-through or cash-out behaviour, including rapid or high-value incoming credits followed by immediate onward transfers to one or multiple beneficiaries or large cash withdrawals, with proportionate restriction, enhanced due diligence or escalation where warranted.

BOX 19. **Public-private tools to detect and disrupt mule networks**

Europol: The recurring European Money Mule Action (Operation EMMA) brings together law enforcement, judicial authorities and thousands of FIs to identify and disrupt cross-border mule networks. Since 2016, successive actions have identified tens of thousands of money mules and hundreds of recruiters ("herders"), supported thousands of investigations and arrests, and, in EMMA 9 in 2023, prevented EUR 32 million (approximately USD 34.8 million) in losses.

INTERPOL: I-Checkit enables authorised private-sector users to screen specified information against INTERPOL databases through a secure connection. INTERPOL is extending this model to the financial sector so that institutions can screen new and existing clients against relevant INTERPOL data, strengthening due diligence and the detection of mule accounts established or operated using stolen or fraudulent identities.

Singapore: Since October 2025, Singapore's Facility Restriction Framework has provided for restrictions on access to financial, telecommunications and national digital identity services for persons meeting defined scam-mule criteria, including persons subject to prior enforcement action and certain persons under investigation assessed as at risk of further facilitating scams. As at 30 June 2026, Singapore reports that 1 423 money mules, 1 439 telecommunications mules and 53 corporate mules had been placed under restrictions.

Preventive payment controls

Preventive payment controls should, where appropriate, be embedded in payment products, services and infrastructures to enable intervention before transactions are executed. This is particularly important in fast or instant payment environments and where victims are manipulated into authorising payments themselves. Controls should therefore address not only unauthorised transactions but also unusual or higher-risk authorised payments. Relevant measures include pre-payment warnings, beneficiary alignment checks, including confirmation or verification of the beneficiary, combined with customer risk profiles, transaction, account and behavioural data, recent scam typologies and relevant external intelligence to identify higher-risk payments. Where legally and technically feasible, real-time behavioural or cross-sector signals may further strengthen pre-payment risk assessment, including anomalies observable within an FI's own digital channels and trusted telecommunications indicators—such as recent SIM or eSIM changes—when combined with unusual transaction activity. Preventive friction should be targeted, proportionate and adaptive. Controls should minimise unnecessary friction for legitimate payments, including cross-border payments, while maintaining effective safeguards against fraud. Generic warnings may suffer from alert fatigue and may be ineffective where prolonged grooming has caused the customer to place greater trust in the scammer than in the institution intervening. Higher-risk situations may therefore require progressively stronger or variable interventions—such as enhanced verification, tailored warnings, temporary cooling-off periods or other risk-based controls—rather than repeated generic alerts. For higher-risk customer-authorised payments, enhanced verification may also seek to establish whether the customer understands the nature of the transaction and relevant scam indicators, rather than merely reconfirming that the customer technically authorised the payment.

Consumer-side digital tools may provide an additional opportunity for earlier intervention. Jurisdictions and firms could test AI-enabled analytical or decision-support tools capable of identifying scam-risk indicators during communications, checking claims or counterparties against trusted information and prompting additional customer confirmation or escalation before payment authorisation. More experimental models could include user-controlled communication-verification agents—sometimes described as 'digital twins'—that independently assess communications or instructions on the user's behalf. Such approaches remain prospective and should be evaluated for privacy and security risks, false positives, susceptibility to manipulation and demonstrated effectiveness before being treated as established good practice.

Where pre-payment risk assessment indicates elevated scam risk, controls should escalate proportionately, including to temporary payment holds, transaction limits, delay or rejection where warranted, supported by clear escalation procedures. Risk-based friction may also be applied to higher-risk onboarding or changes in account capability, including requests to increase transaction limits, where available information indicates elevated scam or mule risk, subject to appropriate review and safeguards. For higher-risk outbound transfers, relevant factors may include payment speed, value and volume, changes in transaction behaviour or limits, and transfers to new or higher-risk beneficiaries. Where payment systems are interconnected, such controls should operate consistently across participating systems so that weaker points are not readily exploited by scam networks. Intervention procedures should also provide for timely review and correction where legitimate payments or customers are incorrectly flagged, including prompt release of a payment hold or other restriction where the basis for intervention is not sustained.

BOX 20. **Examples of preventive payment controls and payee verification**

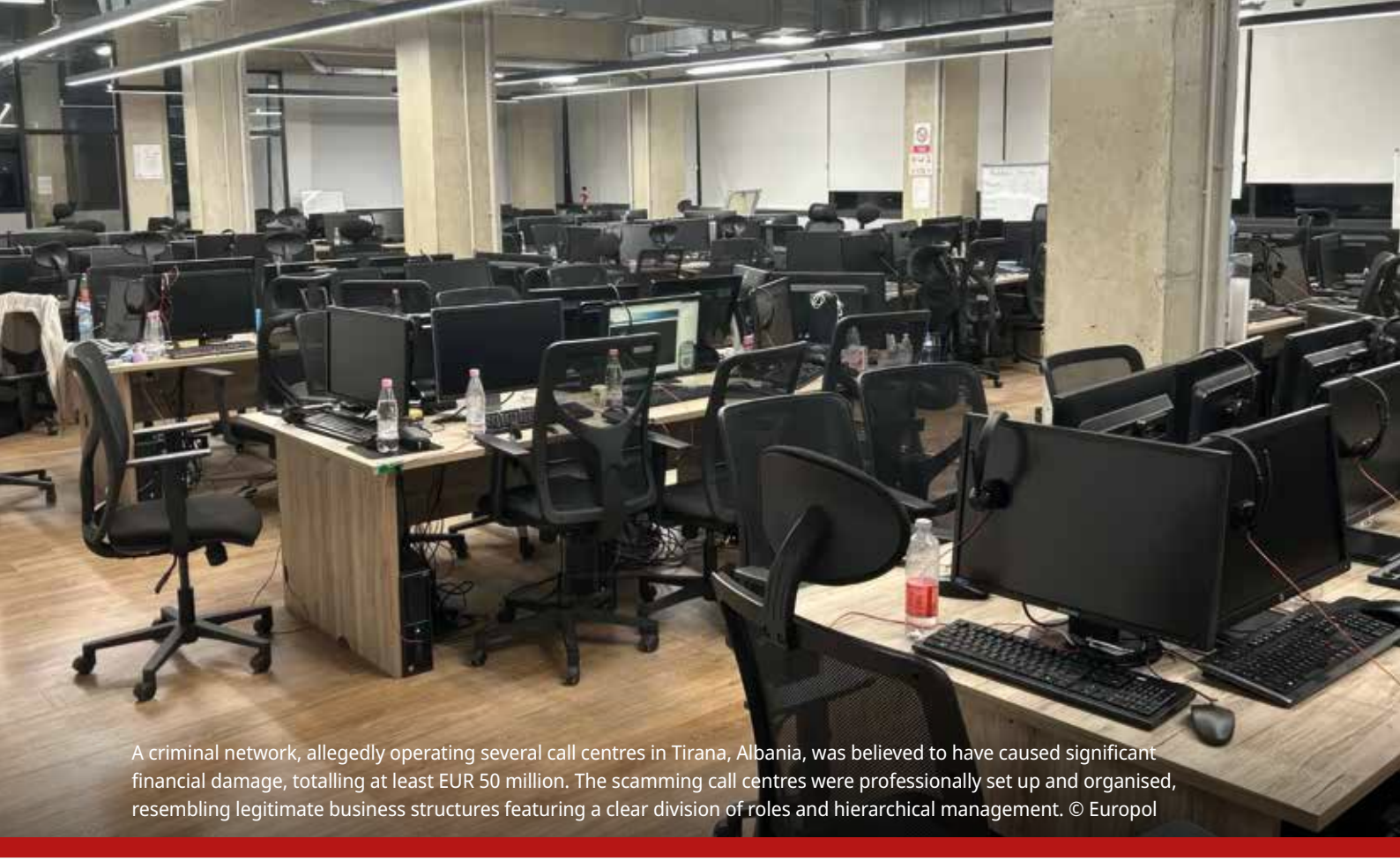
CPMI: The Committee on Payments and Market Infrastructures (CPMI) work on payment pre-validation covers alignment checks under revised Recommendation 16, including confirmation of payee, with particular attention to cross-border usability. Although not specific to scam compounds, these measures can support the identification of payment discrepancies and intervention before higher-risk payments are executed.

European Union: Under Regulation (EU) 2024/886, PSPs must verify the payee's name against the account information associated with the IBAN before executing standard or instant SEPA credit transfers and inform the payer whether there is a match, close match or no match. The requirement applies in the euro area from 9 October 2025 and is intended to reduce fraud, including impersonation and authorised push-payment fraud, and misdirected payments. The European Payment Council's (EPC) Directory Service acts as the routing table providing reachability, while a direct real-time flow occurs between requesting PSP and responding PSP.

Parallel financial investigation

Parallel financial investigations should be conducted alongside investigations into scam compound-related fraud, trafficking and other connected offences to identify proceeds, reconstruct financial flows, preserve assets and support prosecution. They should systematically integrate victim statements, STRs, FI and VASP records, wallet and transaction data, blockchain analytics, platform and immigration records, digital-device evidence, corporate and BO information and, where relevant, information from foreign counterparts. Operational teams should have timely access to digital forensic capabilities to preserve, extract and analyse evidence from seized devices and online accounts, and to integrate financial, digital and trafficking evidence into a coherent evidential picture. Appropriate chains of custody should be maintained, including procedures demonstrating the integrity and provenance of digital evidence transferred between authorities or across borders and, where feasible, compatible or standardised forensic-extraction and transmission protocols to facilitate authentication, admissibility and timely use by receiving authorities.

Where relevant electronic evidence is held by third-party service providers or abroad, early preservation requests, trusted law enforcement contact points and timely engagement with relevant technology and platform providers can help secure potentially volatile data pending formal production or transfer. Where locally accessible collection or laundering nodes are identified, including scam-linked couriers collecting cash or precious metals, investigators can use these actors and transactions as entry points to identify facilitators, downstream laundering networks and higher-level organisers, while assessing rather than assuming the intermediary's knowledge or complicity. This is particularly relevant to Recommendation 30, which requires proactive parallel financial investigations in cases involving major proceeds-generating offences, including where the associated predicate offence occurs abroad.



A criminal network, allegedly operating several call centres in Tirana, Albania, was believed to have caused significant financial damage, totalling at least EUR 50 million. The scamming call centres were professionally set up and organised, resembling legitimate business structures featuring a clear division of roles and hierarchical management. © Europol

BOX 21. **Preserving and authenticating digital evidence**

Chinese Taipei: Chinese Taipei uses the Judicial Alliance Blockchain (b-JADE), a multi-agency blockchain-based mechanism to support the integrity and authentication of digital evidence. Rather than storing evidential content on the blockchain, b-JADE records cryptographic hash values generated from digital evidence across participating judicial and law enforcement nodes. The hash can subsequently be recalculated and compared with the original record to verify whether evidence has remained unchanged, including following inter-agency or cross-border transfer. Chinese Taipei reports that this can support rapid authentication while strengthening the chain of custody and reliability of digital evidence in subsequent proceedings.

Beneficial ownership, corporate-link and professional intermediary analysis

BO and corporate-link analysis can help identify the persons and legal structures used to conceal control, move or reinvest scam compound-related proceeds, as well as assets held through those structures and professional intermediaries or other facilitators enabling those arrangements. Where relevant, the analysis should extend to professional intermediaries—including relevant DNFBPs where applicable—involved in incorporation, property acquisition, asset management or residence arrangements. Relevant techniques include tracing ownership and control across shell and front companies, nominees and cross-border corporate chains; where relevant to identified subjects, linking corporate and asset records with citizenship, residence or immigration information, including investment-linked citizenship or residence arrangements; analysing corporate life-cycle patterns, including changes in ownership, directorships, registration status, names or successor entities following enforcement or regulatory action; and identifying common directors, addresses, contact details or other links across apparently separate entities. Findings should support further investigation and, where appropriate, referral or feedback to relevant competent authorities and supervisors. Where front companies are suspected of processing scam compound proceeds, analysis may also draw on cross-border payment and correspondent banking information, including payment recall information and relevant payment message data, to identify recurring counterparties, linked entities and higher-volume laundering nodes. Wolfsberg Group members report that such analysis has helped identify potential front companies associated with complex fraud networks.

BOX 22. **Beneficial ownership and corporate-link analysis**

Philippines: In the Bamban and Porac cases, authorities combined financial, corporate and BO analysis to identify dummy and shell companies, nominee incorporators, PEP-linked structures, common contact information, CDD inconsistencies and significant property-related transactions. Corporate and financial analysis also linked the Porac operation to the Bamban network, demonstrating that apparently separate physical sites could form part of the same wider enterprise. The cases illustrate how registered or licensed businesses and nominee structures can provide an appearance of legitimacy while obscuring effective control, and how corporate-link analysis can support asset preservation and freezing action.

Türkiye: In a scam compound-linked forex investment-fraud case, financial analysis traced approximately TRY 600 million (approximately USD 13.1 million) in proceeds from 269 victims through money mule cash-out activity and 76 shell companies to VA exchanges and cold VA wallets, with further flows into companies operating in the petroleum, energy, gas distribution and foreign exchange sectors. The investigation culminated in a June 2026 operation across 26 provinces in which 95 suspects were apprehended and 79 remanded in custody; court-appointed trustees were assigned to four companies, 15 filling stations and one fuel-and-gas filling company with a combined value of approximately TRY 4.6 billion (approximately USD 100 million).

Virtual asset tracing tools

On-chain activity should not be analysed in isolation. Where blockchain analytics are used to attribute VA wallets or clusters to a scam compound or related actor, analytical conclusions should be supported by sufficiently transparent and testable methodologies, with the basis for entity attribution, address clustering and risk classification documented and, where appropriate, corroborated through off-chain information. Effective attribution, disruption and recovery generally require blockchain analysis to be connected to off-chain information, including VASP due diligence and Travel Rule data, fiat on- and off-ramp information, devices, communications, corporate information and other financial intelligence. VA tracing should reconstruct scam compound-related flows across VA wallets, blockchains and VASPs using blockchain analytics, forensic wallet tracing, transaction hashes, address clustering and analysis of consolidation VA wallets, fiat-to-VA conversion, P2P and OTC activity, DeFi protocols and cross-chain swaps, mixers, chain-hopping and other obfuscation techniques. Analysis should also test for pooling across multiple victims or scam campaigns and for links between consolidation VA wallets, gambling services, OTC brokers and other shared laundering infrastructure, while avoiding attribution based on on-chain activity alone. Where funds reach an identifiable VASP, centralised stablecoin issuer or other intermediary with relevant customer information or technical control over the asset, timely outreach and use of applicable AML/CFT, investigative and asset preservation powers can support attribution, investigation and, where legally available, preservation of the assets.

Rapid asset preservation, freezing and recovery guidelines

Building on the rapid response arrangements described in subsection 15.4, operational guidelines should enable rapid tracing and asset preservation once scam compound-related proceeds are identified and before funds are withdrawn, converted or further layered[6]. The first 24–72 hours after detection or reporting are particularly critical, as opportunities to identify and preserve linked assets can decline sharply thereafter and may be significantly reduced after a week. Given the speed and volume of scam-related payments, FIs—including relevant non-bank FIs providing payment services—and VASPs executing, receiving or holding the relevant funds are often best positioned to detect risk indicators and intervene before proceeds dissipate.

6. FATF (2025), *Asset Recovery Guidance and Best Practices*, FATF, Paris, France., available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Asset recovery-Guidance-Best-Practices.pdf.coredownload.pdf

BOX 23. **VA tracing in scam compound investigations**

Chainalysis / International Justice Mission: Chainalysis reports that identifying information provided through its partnership with International Justice Mission was used to seed blockchain-cluster analysis of VA wallets attributed to the KK Park scam compound. Chainalysis subsequently mapped more than USD 100 million in victim inflows to the associated wallet cluster and traced flows through laundering layers and towards cash-out points. The example illustrates how off-chain information concerning a specific scam compound can anchor on-chain attribution and expand a known indicator into a wider financial footprint.

China: China reports a case involving two professional ML gangs that provided laundering services to scam compounds in the Kokang region of Myanmar. The networks converted fraud proceeds between fiat currency and USDT and physically transported cash to relatives of fraud offenders in China; investigations established that more than RMB 400 million (approximately USD 59.6 million) in fraud proceeds was laundered and transferred. Police seized more than RMB 14 million (approximately USD 2.09 million) in cash and physical assets and ultimately recovered RMB 370 million (approximately USD 55.1 million).

INTERPOL: In an Oceania member jurisdiction hosting a scam compound, an INTERPOL Operational Support Team analysed VA wallets and related financial flows and co-ordinated communication between the host authorities and a stablecoin issuer, contributing to the preservation of approximately USD 1.6 million in stablecoins suspected to be linked to scam call-centre investigations.

Because competent authorities cannot provide transaction-by-transaction intervention at the speed and scale required, rapid preservation should connect their powers with the immediate intervention capabilities of relevant payment and VA service providers. Subject to applicable law, safeguards and sufficiently reliable information, available measures may include payment recalls or holds, account or wallet restrictions, temporary suspension or preservation pending formal freezing or restraint, VASP or, where relevant, centralised stablecoin-issuer outreach. Where permitted by domestic law, such action may be initiated without awaiting final attribution, full evidential development, completion of STR filing or a full investigation, without displacing applicable reporting obligations. Competent authorities remain critical for intelligence development, investigation, formal freezing or restraint and subsequent recovery.

For cross-border payments, jurisdictions should ensure, consistent with applicable law and safeguards, that FIs—including non-bank FIs providing payment services—have clear legal and operational pathways to transmit sufficiently reliable fraud and financial crime-risk information to counterparties positioned to recall, hold, restrict or otherwise preserve funds before they dissipate[7]. Operational protocols should establish relevant contact points and clarify applicable legal authority, authorised requesting bodies, evidential or confidence thresholds, any provider-specific eligibility or minimum-value thresholds, and request-format and information requirements for rapid engagement with VASPs and centralised stablecoin issuers, including in cross-border cases.

Account closure or termination of a customer relationship should not, by itself, be treated as disruption of the wider laundering network. Where a suspected scam compound-linked front company or laundering node is identified, relevant actors should, consistent with applicable law and safeguards, preserve associated intelligence and consider available tracing, payment-hold, restriction or other asset preservation measures before or alongside closure, so that action against one account does not merely displace activity to successor accounts or entities.

7. Financial Stability Board (FSB) (2024), *Recommendations to Promote Alignment and Interoperability Across Data Frameworks Related to Cross-border Payments: Final report*, Recommendation 9, 12 December 2024, available at: https://www.fsb.org/uploads/P121224-1.pdf

Network-wide fund tracing can support near real-time reconstruction of money trails across successive beneficiary and mule-controlled accounts. This can identify previously unknown downstream accounts, prioritise blocking or freezing action, identify additional victims or connected cases, and estimate potentially recoverable funds before proceeds leave the participating financial network. Such capabilities are particularly valuable where participating FIs or VASPs can act on tracing results within the transaction lifecycle rather than awaiting case-by-case intervention by a competent authority.

Asset preservation should be distinguished from subsequent confiscation, recovery, restitution or compensation. Where consistent with fundamental principles of domestic law, jurisdictions should ensure that non-conviction-based confiscation mechanisms can be used in appropriate scam compound-related cases, including where a criminal conviction cannot be obtained because the perpetrator is unavailable or unidentified. Given the transnational nature of scam compound networks and asset holdings, operational guidelines should also account for the use of such mechanisms through international co-operation where relevant assets are located abroad. Operational planning should extend beyond obtaining a freezing or confiscation order to its practical execution, including custody and transfer arrangements where assets are held abroad or through a VASP; a legal order does not itself amount to completed recovery. Once assets have been frozen or seized, effective asset management should also seek to preserve their economic value pending final disposition. Where permitted by domestic law, this may include interlocutory sale or other value-preservation measures for assets that are rapidly depreciating, deteriorating or disproportionately costly to maintain, so that value remains available for confiscation, recovery and, where appropriate, restitution or compensation. Recovery workflows should therefore preserve the information needed to link assets to the relevant scams, trafficking activity, ransom payments or recruitment fees and, where appropriate, to identifiable victims. Detailed claimant, restitution and victim-protection arrangements are addressed in subsection 16.9.

Jurisdictions should, where feasible, assess the effectiveness of these guidelines by monitoring the value and proportion of identified proceeds preserved, confiscated, recovered and, where appropriate, returned or restituted to victims, together with the time elapsed between detection or reporting, intervention, freezing, recovery and return.

Victim-centred reporting, victim-generated intelligence and recovery protocols

Victim-centred engagement should recognise both victims' protection and support needs and the value of the information they provide for prevention, financial investigation, disruption and recovery. Information from persons trafficked or coerced into scam compounds and from online scam victims may reveal recruitment networks, compound locations and hierarchies, scam typologies and narratives, impersonated organisations, communications infrastructure, account and wallet identifiers, payment channels, compound financing, laundering methods and perpetrators. Aggregated or appropriately anonymised victim and civil society information can also inform risk assessments, typology development, reporting system design and prevention, rather than being used only in individual investigations.

Reporting arrangements should minimise practical barriers and the stigma associated with being deceived. Public-facing terminology and engagement should be clear, accessible, empathetic and non-judgemental and avoid implying victim blame or culpability. Victims should, where appropriate, be informed of available support and relevant rights; why information is collected and how it may be used or shared; and immediate steps to limit further loss and preserve recovery opportunities, including prompt notification of the relevant FI or VASP where intervention remains possible. Jurisdictions should seek simple, well-publicised and accessible reporting and referral arrangements operating on a single-entry or "no-wrong-door" basis where feasible. This need not require a single public channel: law enforcement, anti-scam mechanisms, FIs, consumer protection bodies and trusted civil society or victim-support organisations can feed into an integrated system that consolidates reports and rapidly routes them to actors able to intervene and, where necessary, to victim-support or protection services.

Victim- and civil society-derived information should, where appropriate, be analysed and cross-referenced with relevant financial, law enforcement and private sector data. Consistent classification can reveal recurring scam narratives, recruiters, beneficiary accounts and wallets, domains, telephone numbers, platform identifiers and recruitment routes, connect apparently separate reports to common networks and generate operational leads. Where shared analytical infrastructure exists, confirmed indicators should feed case-management, fund tracing and preventive payment controls.

Where legally permissible, confirmed indicators should also be shared with relevant technology and telecommunications providers to support detection, user warnings and disruption of related or successor accounts, content and infrastructure.

Such sharing should apply appropriate purpose limitation, confidentiality and data minimisation safeguards, use anonymised or pseudonymised information where individual identification is unnecessary, and preserve the distinction between confidential victim support and voluntary or operational information sharing.

Victims should be able to report even where they cannot identify the perpetrator, criminal network or location of the scam. Reporting systems should therefore capture the information needed to connect cases, trace funds and preserve recovery opportunities, including claimant and loss information; account, transaction, beneficiary and wallet identifiers; communications and platform identifiers; scam timelines and payment instructions; and, where relevant, recruitment information and indicators of trafficking, coercion or forced criminality. Relevant sources may include law enforcement and anti-scam channels, embassies and migrant-worker channels, NGOs and victim-support organisations, and structured debriefings. In heavily affected regions, civil society organisations may hold otherwise unavailable information and facilitate links with competent authorities and relevant technology-sector actors. Where trafficking, coercion or forced criminality may be involved, safety and protection needs should be addressed before or alongside information gathering. Debriefing should use victim-sensitive and trauma-informed procedures, trained personnel and interpretation where needed; where participation or information sharing is voluntary, ensure informed consent and clarity as to how information may be used or shared; minimise unnecessary repetition of interviews; assess retaliation or re-trafficking risks before identifying information is recorded or shared; and, where relevant, distinguish operational intelligence gathering from formal evidential interviewing. Where a victim or potential victim remains in contact with a suspected offender, including where the person may also be moving funds, investigative contact should be risk-assessed to protect the victim and preserve support while avoiding unnecessary alerting of the criminal network or compromise of an investigation or disruption opportunity. Victim protocols should also provide a clear pathway after reporting, including appropriate updates, referrals and measures to reduce re-victimisation, including recovery scams.

High-confidence information should be rapidly converted into actionable packages for payment intervention, infrastructure disruption, financial or VA tracing and asset preservation. Where immediate recovery is not possible, relevant information should be retained for use when funds or assets subsequently reach a regulated or law enforcement-responsive touchpoint. Recovery protocols should capture the claimant and loss information needed to link preserved or recovered assets to individual victims and support restitution or compensation, while protecting against re-victimisation, including fraudulent recovery schemes. Where legally possible, victims should receive appropriate information on recovery or restitution processes, and claimant information already collected should be reusable across competent channels so that cross-border claims do not require unnecessary repetition of reporting.

Information from fraud investigations and reporting should also inform co-ordinated public warnings and consumer education by relevant authorities and private-sector actors, including financial consumer protection and financial-education bodies. Consumer education is a supporting preventive measure, not a sufficient line of defence on its own. It should translate current fraud indicators into timely, practical warnings on tell-tale signs of fraud, fake VA investment schemes, employment and recruitment scams and money-mule recruitment; encourage reporting;

and strengthen financial and cyber literacy. Public- and private-sector collaboration can amplify these efforts, while consumer awareness should be reinforced by safeguards within financial and digital systems, timely information sharing and fraud-prevention controls. Victim-support and civil society organisations can further identify emerging recruitment and scam patterns, barriers to reporting and communities that may be particularly exposed or less likely to engage with authorities, helping to target warnings, outreach and prevention.

BOX 24. **Victim reporting, intelligence, classification and recovery workflows**

Cambodia / India / United Kingdom: In late 2025, a public SOS from Indian nationals held in a Bavet scam compound was detected by the Indian Embassy, which established contact with the persons concerned and tasked I4C to geolocate the site using open source information. Escalation to Cambodian authorities led to the rescue of 81 Indian nationals over two days. Separately, in December 2025, intelligence obtained by the UK NCA from the debrief of a British national who had escaped a suspected scam compound in Cambodia was used to support a Cambodian National Police operation. Cambodian authorities raided the site, confirmed that it was being operated as a scam operation and safeguarded persons from Cambodia, China, Pakistan and Bangladesh.

India / Lao PDR / Myanmar: Debriefings of 15 Indian nationals repatriated from scam compounds in Cambodia, Lao PDR and Myanmar in 2023–2024 identified common recruitment, trafficking and operating patterns. The persons had been recruited for purported high-paying customer-service or IT jobs, generally transported through Thailand and subsequently coerced into scam activity. The cases were evenly distributed across the three host jurisdictions. Cases involving Lao PDR identified sub-agents facilitating onward transfers to inland sites, while the Myanmar cases involved compounds in conflict-affected locations. Recruitment fees of INR 50 000–70 000 (approximately USD 560–780), paid in cash or online, contributed to debt bondage. The debriefings also generated information on compound locations, trafficking routes, coercion methods and the scam typologies victims were required to conduct.

Indonesia: Reports concerning Indonesian migrant workers allegedly trafficked to scam compounds may enter through victims or families, NGOs, diplomatic and migrant-worker protection channels. PPATK traces associated financial flows through recruiters and facilitators to mule accounts and VA wallets, using indicators including irregular recruitment fees, bulk third-party flight bookings and recurring transfers to unlicensed individual accounts. Resulting financial intelligence is disseminated to law enforcement to support investigation and asset freezing, while anti-trafficking, foreign affairs, migrant worker and immigration authorities use the intelligence to target recruitment networks and support victim repatriation.

Uganda: A survivor-led study by the Phoenix Survivor Network based on interviews with 250 Ugandan survivors trafficked to scam compounds in Cambodia generated information on trafficking routes and the organisational structure of the criminal network. Among those interviewed, 93 had transited through Vietnam before reaching Cambodia. The research also identified subdivisions and franchising arrangements within the wider group and differentiated scam operations conducted by affiliated companies.

ANNEX 1

Principles

FATF Principles for Combating Illicit Financial Flows Linked to Scam Compounds

Scam compounds are **networked, industrialised and transnational criminal infrastructures**. They may operate through large physical compounds, smaller or decentralised cells and specialised service providers connected through common controllers, financial infrastructure and operational dependencies. Effective responses should therefore target the wider criminal ecosystem and the financial flows that sustain it, rather than individual sites, transactions or actors in isolation. Implementation should be **risk-based**, reflecting each jurisdiction's exposure and role in the scam compound ecosystem, and supported by **sustained political commitment, clear leadership and accountability**.

1. Target the wider criminal ecosystem

Target the network, not only the physical compound. Identify and act against criminal leadership and controllers, recruitment and trafficking networks, beneficial owners and corporate structures, shared financial and operational infrastructure, and specialised service providers sustaining scam compounds or linked decentralised operations. Financial prevention, investigation and disruption should be co-ordinated with action against connected trafficking in human beings, cybercrime, corruption, misuse of digital and telecommunications infrastructure and other enabling activity.

Target critical dependencies. Map the financial and non-financial functions on which scam compound networks depend and prioritise the disruption of capabilities that are shared across multiple operations or difficult for the network to replace.

2. Disrupt illicit financial flows end-to-end

Act both upstream and downstream. Upstream action should identify and disrupt the infrastructure, services and expenditure required to establish, sustain and scale scam compound activity—including worker and victim recruitment, victim leads and data, advertising, telecommunications, domains and hosting, fraudulent platforms, premises and specialised providers. Downstream action should target victim payments and generated proceeds through preventing, delaying or recalling victim payments before funds are dissipated, disruption of mule-controlled accounts and wallets, financial and virtual asset tracing, freezing, confiscation, recovery and restitution.

Prevent and disrupt the movement of proceeds. Intervene as early as possible against victim payments, mule-controlled accounts and wallets and money laundering channels; trace financial and virtual asset flows; preserve and freeze assets before proceeds are transferred, converted, withdrawn or moved beyond reach; and pursue confiscation, recovery and restitution.

3. Connect the networks

Connect intelligence and capabilities across sectors and borders. Scam compound networks span financial, technological and telecommunications systems and multiple jurisdictions. Financial institutions, virtual asset service providers, competent authorities, technology and telecommunications providers, financial consumer protection authorities and civil society actors may each hold only part of the picture. No single actor sees the full financial flow chain.

Turn information into action. Use clear legal gateways, trusted contact points, common and interoperable classifications, appropriate safeguards and, where legally permissible, public-public, public-private and private-private arrangements to route reliable and actionable signals rapidly to the actors best placed to prevent victim engagement or payments, preserve assets or disrupt enabling infrastructure.

4. Act at speed across borders

Preserve the intervention window. Establish rapid-response arrangements and escalation pathways in advance so that payments can be prevented, suspended, recalled or otherwise interrupted and account, wallets and assets preserved before proceeds are transferred, converted, withdrawn or moved beyond reach.

Match the transnational nature of the threat. Connect domestic capabilities through trusted financial intelligence, law enforcement and asset recovery networks, joint investigative or operational arrangements and timely formal co-operation. Faster operational channels should complement formal co-operation where evidence or coercive measures are required.

5. Put victims at the centre

Protect all forms of victimisation: Responses should protect online scam victims and persons trafficked or coerced into scam compounds for forced criminality, including through accessible reporting, appropriate trafficking screening, specialised identification and protection procedures, non-punishment safeguards and protection from repeat victimisation, recovery scams, retaliation and re-trafficking.

Integrate victim protection with prevention and recovery. Victims should not be treated principally as sources of intelligence. However, victim-derived information obtained safely and lawfully should be used, where appropriate, to prevent or interrupt payments before funds are dissipated, support investigations and asset recovery efforts, and facilitate restitutions.

6. Adapt and focus on lasting impact

Adapt as the threat evolves. Scam operations can decentralise, relocate, rebrand and replace disrupted infrastructure, while exploiting AI-enabled social engineering, deepfakes, automation, synthetic identities, changing domains and new payment channels. Jurisdictions and relevant private sector actors should continuously update typologies, indicators, analytical tools and operational approaches and monitor displacement and emerging operating models.

Measure outcomes, not activity alone. Success should be judged by whether interventions protect victims and sustainably degrade the scam compound business model—including through losses prevented, faster intervention, assets preserved, confiscated, recovered and returned, and disruption of shared or difficult-to-replace capabilities. Monitoring should distinguish genuine degradation from displacement, rebranding or rapid replacement.

ANNEX 2

Additional Case Studies and Good Practice Examples

1. Shared illicit-finance infrastructure across criminal threats

FATF: A Cambodia based financial services conglomerate linked to Southeast Asian scam compound operations combined payment, VA exchange and illicit online marketplace services. FATF reports that the same infrastructure was also exploited by DPRK affiliated actors to launder proceeds from state sponsored VA thefts. The case illustrates how shared financial and ML infrastructure supporting scam compound ecosystems can also facilitate PF linked illicit finance[1].

1. FATF (2026), *Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs*, FATF, Paris, France, paras. 29–30, available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtualassets-vasps-2026.html

2. Scam compound activity and operating models in Africa

Mozambique: Mozambique reports activity it associates with scam compounds in which a group of Chinese nationals operated an investment-fraud scheme through a formally structured company from a rented house in central Maputo. Prospective clients were induced to deposit substantial sums into the company bank account on the promise of investment returns, after which the operators disappeared with the funds. The example illustrates that reported scam compound-type activity in Africa may use ordinary urban premises and apparently legitimate corporate structures rather than large fortified sites.

Namibia: Seychelles reports a strongly suspected physical scam compound-type operation in Namibia involving more than 150 workers, with part of the proceeds traced to VASP accounts in Seychelles.

3. Co-ordinated action against scam compounds and their wider criminal infrastructure

Europol: Operation JuicyFields illustrates co-ordinated cross-border action against a decentralised investment fraud network and its financial infrastructure. In April 2024, authorities across 11 countries, supported by Europol and Eurojust, acted against a Berlin-based Ponzi scheme through which around 186 000 persons had transferred funds and estimated losses reached approximately USD 735 million. Proceeds were dispersed through mule networks, VA exchanges and real estate. Authorities conducted nine arrests and 38 searches and seized or restrained approximately USD 5.4 million in bank accounts, USD 1.7 million in VAs, EUR 106 000 (approximately USD 121 000) in cash and USD 3 million in real estate.

Netherlands: Although not identified as a scam compound case, Operation Sunflower illustrates co-ordinated action against an industrialised, decentralised investment fraud network operating through around 20 call centres across multiple jurisdictions, with more than 700 personnel under central co-ordination and estimated proceeds exceeding approximately USD 113.7 million per month. Dutch investigators combined financial and digital traces, including IP address data, to identify operational locations, suspects and key infrastructure. A suspected key organiser was arrested in Poland, with further arrests in Cyprus, Belgium and Greece. Dutch authorities also worked with commercial service providers to take key digital infrastructure offline and shared intelligence through Europol to support further enforcement action.

4. Mapping and disrupting scam-enabling infrastructure

Chinese Taipei: In an investigation into a transnational telecom-fraud network operating call centres across Cambodia and the United States, authorities identified SIM-bank and GOIP gateway infrastructure used to route fraudulent calls. A joint operation with the U.S. FBI reportedly dismantled four call centres, neutralised 2 432 fraudulent mobile phones and blocked more than 1.26 million scam calls per day. The case illustrates how identifying and disrupting shared telecommunications infrastructure can interrupt victim acquisition at scale.

Zambia: In the 2024 Golden Top Support Services case, authorities searching a call centre-style scam operation in Lusaka seized 135 computers, 23 mobile phones, 11 SIM boxes and 37 000 SIM cards. Telecommunications analysis identified an unlicensed mobile network and SIM cards registered under stolen identities. Twenty Chinese nationals and one Cameroonian were subsequently convicted, with custodial sentences of up to 11 years reported, and property recovered during the operation was forfeited.

5. National anti-scam centres, comparable arrangements and supporting guidance

Australia: The National Anti-Scam Centre is led by the Australian Competition and Consumer Commission and works in partnership with other organisations including the Australian Federal Police, State and Territory Police, other government agencies and private sector expertise. It supports scam detection, investigation and disruption, intelligence sharing and proactive measures.

Cambodia: The Commission for Combating Online Scams (CCOS), established in February 2025 under the chairmanship of the Prime Minister, provides a high-level whole-of-government co-ordination mechanism bringing together ministries, LEAs, financial intelligence authorities, prosecutors and other competent authorities to co-ordinate prevention, investigation, disruption, prosecution and asset-recovery action against online scam networks.

Canada: The Canadian Anti-Fraud Centre (CAFC), jointly managed by the Royal Canadian Mounted Police, the Ontario Provincial Police and the Competition Bureau, serves as Canada's national fraud-reporting centre. It supports public reporting and fraud awareness, gathers and shares fraud intelligence, assists law-enforcement prevention and enforcement efforts, and provides information to domestic and international partners.

Europol: Europol is establishing the EU Anti-Scam Platform as a central operational hub to address the industrialisation of online fraud, drawing on expertise from EC3 and EFECC. It will support intelligence sharing, rapid interception and recovery of illicit proceeds, operational co-ordination and deconfliction, threat monitoring and early warning, and public-private co-operation and prevention. By consolidating analytical and operational capabilities, the Platform aims to support a shift from reactive case handling towards proactive disruption and prevention.

Hong Kong China: The Anti-Deception Co-ordination Centre operates 24/7 as a central point for stop-payment requests and works with 28 retail banks through a round-the-clock mechanism under which participating banks maintain a two-hour response pledge. Through the Anti-Deception Alliance, staff from ten retail banks work alongside police officers in a shared workplace, enabling direct processing of stop-payment requests and rapid intelligence exchange.

Indonesia: The Indonesia Anti-Scam Centre (IASC), established under the 2023 Financial Sector Development and Reinforcement Law and operated by the Financial Services Authority (OJK) with the Task Force for Eradicating Illegal Financial Activities (Satgas PASTI), provides an integrated operational hub connecting 22 government ministries/agencies and nine financial and technology industry associations. Scam reports may be submitted directly by victims, routed through FIs or generated proactively by FIs. The IASC co-ordinates rapid blocking of identified accounts and multilayer tracing across downstream FIs to preserve remaining funds and support their return to verified victims. Identified perpetrators, fraudulent accounts and related profiles are recorded in the Financial Sector Criminal Database (SiPelaku) to support investigation and prosecution. Across scam cases more broadly, Indonesia reports that the IASC blocked over 702 833 accounts and returned approximately USD 11.55 million to victims between November 2024 and September 2026.

INTERPOL: Its Anti-Scam Centre Guideline recommends that anti-scam centres provide accessible channels through which foreign scam victims can file police reports. Where permitted by domestic law, reporting in a jurisdiction through which the proceeds have moved may enable an earlier domestic ML investigation and asset preservation action without awaiting a formal MLA request from the victim jurisdiction.

Malaysia: The National Scam Response Centre (NSRC), established in 2022, operates as a 24/7 rapid-response mechanism accessible through the 997 hotline and brings together the Royal Malaysia Police, Bank Negara Malaysia, the Malaysian Communications and Multimedia Commission, FIs and telecommunications providers. It co-ordinates scam reporting and rapid intervention, including tracing and recovery of scam-related funds, and is complemented by the National Fraud Portal.

Singapore: The Anti-Scam Centre, an operational unit of the Singapore Police Force, with real-time co-ordination between banks, VA platforms, telecommunication companies and e-commerce platforms, including through co-located bank staff, supports rapid fund tracing, intervention and recovery for both fiat and VAs.

Chinese Taipei: Suspicious Account Early-Warning and Investigation Centers across prosecutors' offices are supervised as part of a broader public-private early-warning mechanism involving the FIU, other public authorities and FIs. Chinese Taipei also reports a rapid freezing and verification mechanism under which banks and VASPs may apply reasonable control measures when suspicious transactions are detected and rapidly refer the matter to police for verification; following verification, the restriction may be maintained or lifted as appropriate. Associated financial activity can then be traced to the wider fraud syndicate.

Thailand: Inter-agency taskforces are supported by public-private "war room" arrangements that facilitate timely information exchange, sharing of criminal typologies, tracing of financial flows and freezing of accounts linked to criminal activity.

6. Multi-agency and joint operational responses to scam compounds

Belarus / Russia / Kyrgyzstan / Kazakhstan: Belarus reports a completed investigation into an international criminal organisation operating fraudulent call centres in Minsk, Moscow and Bishkek. The investigation concerned 15 alleged leaders and 40 participants who, between 2018 and 2024, used purported investments in non-existent financial companies to obtain more than USD 1 million from victims. Three international investigative and operational teams involving authorities from Belarus, Russia, Kyrgyzstan and Kazakhstan were

established during the investigation. Belarus reports that more than USD 200 000 in victim losses was compensated and property of the accused worth more than USD 1 million was seized.

Cambodia: In April 2026, Cambodian authorities raided a suspected scam operation in Phnom Penh, arresting 20 foreign suspects and seizing 846 mobile phones, 31 computers, several thousand international SIM cards, conversation scripts and training materials. A parallel financial investigation involving law-enforcement and prosecutorial authorities, the National Bank of Cambodia and CAFIU traced the alleged ringleader and a person suspected of providing the premises; ML charges were added against both, identified domestic bank accounts were frozen and further asset tracing remains ongoing.

Cambodia / Korea: The Cambodia–Korea Joint Task Force brings Cambodian and Korean law enforcement together in Cambodia to investigate and disrupt online scam-related crime affecting Korean nationals. Established through a bilateral agreement, it supports joint intelligence sharing, investigation and operational action; subsequent joint operations have resulted in arrests, victim rescue and seizure of digital evidence linked to suspected scam operations. Korea also reports an on-the-ground Korean Desk, established with Cambodian support, through which Korean law-enforcement authorities conduct or support investigations in Cambodia.

China / Myanmar / Thailand: China reports that sustained police co-operation with Myanmar and a ministerial-level China–Myanmar–Thailand co-ordination mechanism supported concentrated action against scam compounds in northern Myanmar and Myawaddy, including repeated repatriation operations and physical disruption of compound infrastructure. China reports that more than 59,000 suspects were apprehended and transferred in northern Myanmar-related operations and that more than 600 buildings at the KK Compound in Myawaddy were demolished. Bilateral police-liaison channels are also used for real-time exchange of fund-flow and personnel information and joint case analysis.

Indonesia: Authorities cross-reference intelligence concerning persons returning from overseas scam compounds with PPATK financial intelligence and IASC data on known scam networks and modus operandi. Indonesia reports that this process contributed to five joint investigations involving persons recently returned from scam compounds in Cambodia who were also linked to suspicious financial transactions or suspected scam networks.

INTERPOL / United Kingdom: Launched in March 2026, Operation SHADOW STORM is an INTERPOL-led Global Fraud Taskforce jointly developed with the United Kingdom, initially targeting scam compounds in Southeast Asia. Through INTERPOL co-ordination and tools, the taskforce targets financial fraud linked to scam centres together with its connections to cybercrime and trafficking in human beings, including trafficking for the purpose of forced criminality.

Montenegro: In 2020, Montenegrin police identified a call centre operation in which trafficking victims from Chinese Taipei were being forced to partake in fraudulent scams. The modus operandi was identified in co-operation with INTERPOL and Europol. Montenegro conducted a financial investigation and seized assets, and the prosecution was subsequently handed to the competent prosecutor's office in Chinese Taipei.

Myanmar / Thailand: An operation against the Shunda compound identified around 5 000 persons and enabled the repatriation, through Thailand, of approximately 55% of those found. Seized evidence was transferred to Thai authorities, while forensic analysis of 31 devices generated intelligence supporting further investigation.

Nigeria: In April 2025, the Attorney-General established the Joint Case Team on Cybercrimes (JCTC), bringing together the Federal Ministry of Justice, NAPTIP, NPF-NCCC, NFIU and ONSA to share expertise, intelligence and operational capabilities in complex cybercrime cases. In a January 2026 Delta State scam compound case, intelligence from a foreign jurisdiction, supported by a social-media platform, enabled NPF-NCCC to geolocate and raid the site, arresting seven suspects. Digital forensic analysis of seized devices identified more than 50 000 social-media and messaging identifiers and numerous stolen identities.

Türkiye / Czechia / Ukraine: Following transmission of a Czech case through INTERPOL, Turkish authorities identified a Türkiye-based call-centre operation targeting Czech victims through impersonation of public officials and bank personnel. A joint investigation team involving Türkiye, Czechia and Ukraine conducted joint analytical work in Prague and identified 100 suspects. A subsequent Istanbul operation in July 2026 apprehended 56 suspects, 45 of whom were remanded in custody.

7. Shared fraud data and information sharing infrastructures across different governance models

China: The People's Bank of China and Ministry of Public Security jointly built the Management Platform for Risk Events of New Types of Telecom and Online Fraud Transactions, linking police with banks and payment institutions nationwide. The platform supports expedited account inquiries, emergency payment suspension, rapid freezing and cross-institution sharing of risk-account information. China also reports a police–bank liaison mechanism under which banks and payment institutions deploy personnel to the National Anti-Fraud Center.

Hong Kong China: Launched in 2023, FINEST facilitates bank-to-bank information sharing to support the detection and disruption of fraud and financial crime.

Hungary: Since July 2026, the HFIU may share information derived from operational analysis with selected obliged entities, sectors or all obliged entities for defined risk-mitigation purposes, including bank-account numbers, IP addresses, device IDs and information on natural or legal persons, trends and methods. Where the information relates to financial transactions, the authorised period of use may not exceed 90 days. Although the mechanism is not scam-compound-specific, it provides a transferable model for time-limited FIU-to-private-sector dissemination of mule-account and related network indicators.

Japan: A police–financial sector public-private framework enables police to make online inquiries to participating FIs through the National Police Agency and receive prompt responses. The arrangement supports rapid identification and tracing of illicit fund flows, bank-account freezing and recovery, as well as the apprehension of suspects.

Luxembourg: Following a legislative amendment adopted in July 2026, Luxembourg's FIU (Cellule de Renseignement Financier – CRF) is empowered to share fraud-related tactical and operational information directly with specified credit institutions, payment-sector entities and VASPs. This may include bank-account and SWIFT identifiers together with the associated fraud type, enabling relevant private-sector actors to identify related activity and support earlier intervention in scam-related payment flows. The mechanism is intended to support a shift from ex-post fraud detection towards earlier preventive intervention.

Malaysia: Launched in August 2024 and jointly led by Bank Negara Malaysia, Payments Network Malaysia (PayNet) and participating FIs, the National Fraud Portal (NFP) provides a shared financial data infrastructure complementing

the National Scam Response Centre. It integrates transaction and mule-account data across participating institutions and automates the workflow from incident reporting through fund tracing and case escalation, replacing sequential tracing processes and supporting faster validation and intervention. Aggregating transaction data, money trails and mule-account information also enables analysis of multi-layer transfers and withdrawal points and can help develop syndicate-level intelligence beyond the treatment of individual victim reports.

Singapore: The National Scams List, under development by the Singapore Police Force and Home Team Science and Technology Agency, is designed to enable real-time public-private exchange of known scam accounts, including bank accounts, phone lines and online accounts, allowing further potential scam-linked accounts to be proactively detected and disabled before being used to perpetrate further scams. In trials with selected banks, Singapore reports that each scam-linked bank account shared by police enabled participating banks to identify and disrupt at least one additional previously unreported scam-linked account.

Thailand: Although developed for digital fraud more broadly, Thailand's Central Fraud Registry (CFR) provides a transferable model for identifying and disrupting scam-related mule and payment flows. It consolidates fraud reports and transaction-level money trails across commercial banks, e-payment service providers and digital-asset operators, and BOT requires FIs to integrate CFR information into transaction monitoring. Identified mule account information can support restrictions on outgoing transfers and the identification of linked transactions. The CFR also supports the AOC 1441 "one-call" model, connecting the victim, a bank representative and police within a single reporting workflow, and is being upgraded towards API-based information exchange.

Wolfsberg-Beacon: The TradFi–Crypto Fraud Sprint tested private-private information sharing between banks and VASPs using high-confidence victim and mule account leads. The pilot identified previously unknown accounts and wallets and supported wallet closures and asset recovery.

8. Rapid response mechanisms for fund interception and asset preservation

Brazil: In a fraud case whose suspected scam compound nexus rested on on-chain tracing and remained unconfirmed, Brazilian authorities used an open electronic form to aggregate victim-supplied transaction identifiers. This enabled the case to meet the applicable T3FCU rapid response threshold and supported direct outreach through provider-designated channels, without a pre-existing agreement. A centralised stablecoin issuer subsequently froze approximately 1.43 million USDT across about 60 addresses associated with self-custody wallets. Brazil verified in September 2026 that the addresses remained blacklisted, although no subsequent confiscation or restitution was reported. The case illustrates both the potential reach of issuer-level preservation beyond VASP-hosted wallets and the continuing gap between rapid preservation and final recovery.

Beacon Network/T3FCU: The Beacon Network/T3FCU brings together relevant VASPs, blockchain-analytics capabilities and public sector partners through trusted, time-sensitive escalation arrangements to identify illicit VA flows and route high-confidence alerts to actors able to restrict or preserve assets before onward transfer.

United States: FinCEN's Rapid Response Program links FinCEN, US law enforcement and foreign FIUs to accelerate financial-intelligence exchange and support counterpart authorities in interdicting fraudulent transfers and freezing or recalling funds under their respective domestic frameworks. Although the mechanism applies to fraud more broadly, it provides a directly transferable model for high-velocity cross-border scam compound-related flows.

Cambodia: Cambodia reports that, following a request from law enforcement, CAFIU can place a 48-hour hold on bank accounts, with first intervention typically occurring within 24–48 hours. This provides a short initial preservation window while competent authorities pursue further tracing, freezing or seizure action.

Hungary: A fraud-related objective-reporting mechanism creates a rapid notification chain following a victim or police report. Where the victim's bank is notified within 24 hours of the transaction, it must notify the beneficiary bank within 12 hours; the beneficiary bank then reports to the HFIU without delay. The HFIU conducts automated structured risk analysis, including cross-checks against SAR and police data, and disseminates risk-relevant cases to Police. Although not scam-compound-specific, the mechanism illustrates a transferable workflow linking victim reporting, inter-bank notification, FIU analysis and law-enforcement escalation within the narrow asset-preservation window.

Korea: Under the Act on the Prevention of Loss and Refund of Voice Phishing Damage, financial institutions may suspend payments from accounts linked to voice phishing following a report by a victim or investigative authority. KoFIU has also introduced a transaction-suspension mechanism for emerging forms of voice phishing outside the scope of that law, applying enhanced customer due diligence and halting transactions until the suspicion is resolved. Korea reports that, during its first two months of operation, the latter mechanism froze funds in fraud-linked accounts associated with roughly 6,000 reported cases of damage. Although these outcome data are not scam compound-specific, the mechanism illustrates a transferable rapid-preservation capability where relevant accounts can be linked to scam compound-related flows.

Malaysia: The National Scam Response Centre combines international rapid response channels with domestic asset preservation powers. Malaysia reports using I-GRIP and Egmont Secure Web to support urgent cross-border tracing and intervention. Domestically, section 116D of the Criminal Procedure Code empowers LEAs to direct FIs to temporarily withhold transactions or freeze suspected proceeds of crime pending further investigation, while section 413 supports restitution of recovered property or money where ownership can be established.

Türkiye: Türkiye has complementary mechanisms for rapid transaction and account suspension. Under Article 19/A of Law No. 5549, transactions suspected of being linked to ML or TF may be postponed for up to seven working days to enable MASAK to verify and analyse the suspicion; implementing arrangements allow postponement to be initiated at the request of an obliged party, ex officio by MASAK or following a request from a foreign competent authority, subject to applicable conditions. Separately, Article 128/A of the Criminal Procedure Law, adopted in December 2025, permits relevant bank or non-bank FI providing payment services, or VASPs, where reasonable suspicion exists regarding specified aggravated fraud, theft or card-related offences, to suspend relevant accounts for up to 48 hours, with immediate notification to the Public Prosecutor and provision for rapid review.

9. Cross-border co-ordination to disrupt scam-related illicit financial flows

Greece: In a multi-jurisdictional call-centre fraud investigation led by Germany with Europol support, requests transmitted through Europol/SIENA enabled the Hellenic Asset Recovery Office to provide information on persons concerned, including bank accounts and account holders. Greece assessed the rapid information exchange and direct operational co-ordination between participating authorities as useful, illustrating how established law-enforcement channels can mobilise asset-recovery information across borders during an ongoing investigation.

Hong Kong China / Singapore: Operation Targus Hawk illustrates bilateral law enforcement co-ordination through extensive information sharing and joint investigations between the Singapore Police Force (SPF) and the Hong Kong Police Force (HKPF) relating to Technical Support Scams of losses at least SGD 17.9 million (approximately USD 13.61 million). In August 2024, following extensive information sharing and joint investigations by the SPF and HKPF, officers from the HKPF raided three premises in Hong Kong China and arrested one mastermind of the syndicate, three syndicate members and three money mules, aged between 33 and 43. Cash amounting to HKD 300,000 (approximately USD 38,480) and over 60 bank cards were recovered and seized as case exhibits. Through further follow-up investigations and intelligence sharing, another HKD 1.3 million (approximately USD 166,748) in crime proceeds was successfully recovered in Hong Kong China and the SPF arrested another Singaporean for his involvement in ML activities.

INTERPOL: In 2025, Operation HAECHI VI co-ordinated action across 40 countries and territories against cyber-enabled financial crime and associated ML—including investment and romance scams—recovering USD 439 million, blocking more than 68 000 bank accounts and freezing close to 400 VA wallets.

10. Network mapping through combined financial, corporate and open source analysis

Italy: Aggregate analysis of 200 STRs, combined with previous investigations, connected more than 12 000 subjects and approximately EUR 30 million in suspicious flows within a large transnational fraud and ML network displaying recurring investment- and job/task-scam indicators associated with scam-compound typologies. Network analysis identified a foreign crypto platform as a central collection and redistribution node and extensive use of UK-based vIBANs through which funds moved from Italian accounts towards crypto-asset ecosystems. The case illustrates how STR aggregation, network analysis, international co-operation, OSINT and blockchain analysis can expose shared collection and laundering infrastructure, including where the link to a specific physical scam compound remains unconfirmed.

11. Digital, telecommunications and platform infrastructure disruption

Europol: Operation SIMCARTEL illustrates co-ordinated disruption of shared telecommunications infrastructure enabling industrial-scale fraud. An Austria–Estonia–Latvia investigation supported by Europol and Eurojust targeted a cybercrime-as-a-service network supplying anonymised phone numbers through SIM boxes for fraud, phishing/smishing and investment scams. In October 2025, authorities arrested seven suspects, seized 1 200 SIM-box devices containing 40 000 active SIM cards and hundreds of thousands of additional SIMs, and took over and shut down five servers and two websites. The infrastructure offered numbers from more than 80 countries and had facilitated an estimated 49 million fake online accounts. The network was linked to more than 3 200 fraud cases and approximately USD 5.7 million in losses; authorities also froze approximately USD 0.50 million in bank accounts and USD 333 000 in VAs.

GASA: The GASA Enforcement Working Group is carrying on a project on “Disrupting Scams Infrastructure” examining the infrastructure exploited by scam networks and identifying practical disruption opportunities. The ongoing initiative aims to bring together cross-sector expertise to identify solutions and next steps for disrupting scam-enabling infrastructure.

Malaysia: The Malaysian Communications and Multimedia Commission works with telecommunications providers, social media platforms and LEAs to disrupt scam-related communications infrastructure, including by blocking suspicious calls and SMS, identifying and blocking spoofed calls originating from international gateways, restricting or terminating telephone numbers and facilitating removal of fraudulent online content and accounts. Across scam activity more broadly, Malaysia reports that telecommunications providers blocked 2.60 billion suspicious calls and 3.10 billion SMS between 2022 and July 2026, and identified and blocked 101.66 million spoofed calls from international gateways between February and July 2026. These figures measure operational outputs rather than scam-compound-specific impact, but illustrate the scale at which upstream telecommunications controls can be deployed.

New Zealand: In a six-month cross-sector pilot from October 2025 to March 2026, Static Technologies' Avengyr ThreatShield operated across New Zealand's three major telecommunications networks, alongside participating banks, an online marketplace and public sector intelligence partners, to detect and block malicious domains and phishing links. The pilot blocked more than 23 000 malicious domains and intercepted 3.1 million access attempts, while preventing approximately USD 13.7 million from reaching scammers.

South Africa: An anonymised member of the Institute of International Finance reports that co-ordinated action by domestic and international law enforcement, banks and mobile-network operators disrupted seven SIM-farm operations and three rogue call-centre syndicates; interventions against three call centres resulted in 65 arrests. Recurring infrastructure included bulk-messaging platforms, GSM routers, large volumes of SIM cards and outbound-calling systems.

12. Public-private tools to detect and disrupt mule networks

India: I4C maintains a suspect registry containing tax, email, mobile and IP identifiers associated with mule accounts and makes relevant information available to FIs, telecommunications providers and State police. The registry can support risk-based action including declining transactions, refusing onboarding where appropriate, deactivating associated SIMs and identifying linked bank accounts.

Saudi Arabia: The Saudi Central Bank's fusion centre disseminates fraud and mule-related indicators, including device fingerprints, through a structured Fraud Threat Advisory mechanism, accompanied by standardised scanning tasks and structured reporting of results. This is complemented by recurring inter-bank mule-account information sharing using a common methodology and periodic proactive monitoring across banks and selected non-bank FIs, illustrating a centrally co-ordinated model for converting indicators into sector-wide detection and feedback.

Singapore / Malaysia: Information sharing between a Singapore FI and the Singapore Police Force's Anti-Scam Centre identified a Malaysia-based syndicate as the source of a series of scam-linked bank accounts. Intelligence shared with Malaysian authorities led to a raid on the syndicate's premises and the seizure of 83 mobile phones, 45 bank tokens and operating software. A subsequent bilateral case conference generated further account intelligence, which supported co-ordinated enforcement in Singapore against 18 persons who had knowingly opened or surrendered bank accounts or digital-access credentials for financial gain.

Sweden: Participating banks share confirmed first-line money mule information, enabling them to identify previously unknown mule accounts, strengthen monitoring, investigate and offboard confirmed cases; relevant information is also shared with police. Although not reported as scam compound-specific, the example

illustrates how high-confidence private-private mule intelligence can expose related financial networks and support earlier intervention.

13. Beneficial ownership and corporate-link analysis

Australia: Although not scam compound-specific, the AUSTRAC/Fintel Alliance Scambling project identified corporate-abuse patterns involving mule accounts, shell companies and fake businesses, including companies registered in the names of recruited mules. The analysis supported identification of links between apparently legitimate legal entities and wider illicit gambling and micro-laundering networks.

14. VA tracing in scam compound investigations

Namibia / Seychelles: In a strongly suspected Namibia-based scam compound-type operation, blockchain tracing linked part of the proceeds to two VASP accounts associated with Seychelles. Co-operation between Namibian investigators and financial-intelligence authorities, Seychelles authorities and the VASP enabled KYC disclosure, account restriction and preservation, followed by a Namibian forfeiture order covering 112 334.50 USDT. Execution required subsequent testing and transfer arrangements in Seychelles.

OSCE: Investigations involving Tether, OKX, Chainalysis and U.S. authorities led to the voluntary freezing of approximately USD 225 million in USDT held in self-custodied wallets linked to a money laundering network associated with a Southeast Asian scam compound. The frozen USDT was subsequently burned and reissued to wallets controlled by the U.S. Department of Justice.

Philippines: STRs filed by FIs triggered an investigation into VA exchanges and shell companies linked to scam compound proceeds. AMLC, the PNP Anti-Cybercrime Group and international partners traced funds through VASPs, mixers, chain-hopping and P2P channels, supporting wallet identification and asset-freezing action.

15. Victim reporting, intelligence, classification and recovery workflows

Cambodia: During scam compound interventions, multidisciplinary teams comprising specialised anti-trafficking police, immigration officers, prosecutors and social workers screen persons found at the site; identification does not depend on a person's initial self-identification as a victim or on immigration status. Presumed victims can be referred to protective accommodation with interpretation and consular support, while identified trafficking victims may benefit from immigration non-punishment safeguards and facilitated, protection-sensitive repatriation. Cambodia also seeks continuity of support through consent-based information transfer to relevant authorities and IOM in countries of origin. Cambodia notes, however, that repatriation before criminal proceedings conclude can complicate cross-border restitution and is examining representation and co-operation mechanisms to enable departed victims to pursue compensation.

Malaysia: Under Bank Negara Malaysia's Fraud Response Policy Document, FIs are required to maintain dedicated 24/7 reporting channels and designated personnel able to validate fraud alerts, trace funds and initiate fund-withholding action following victim reports. Victim reports must be recorded, while the framework provides

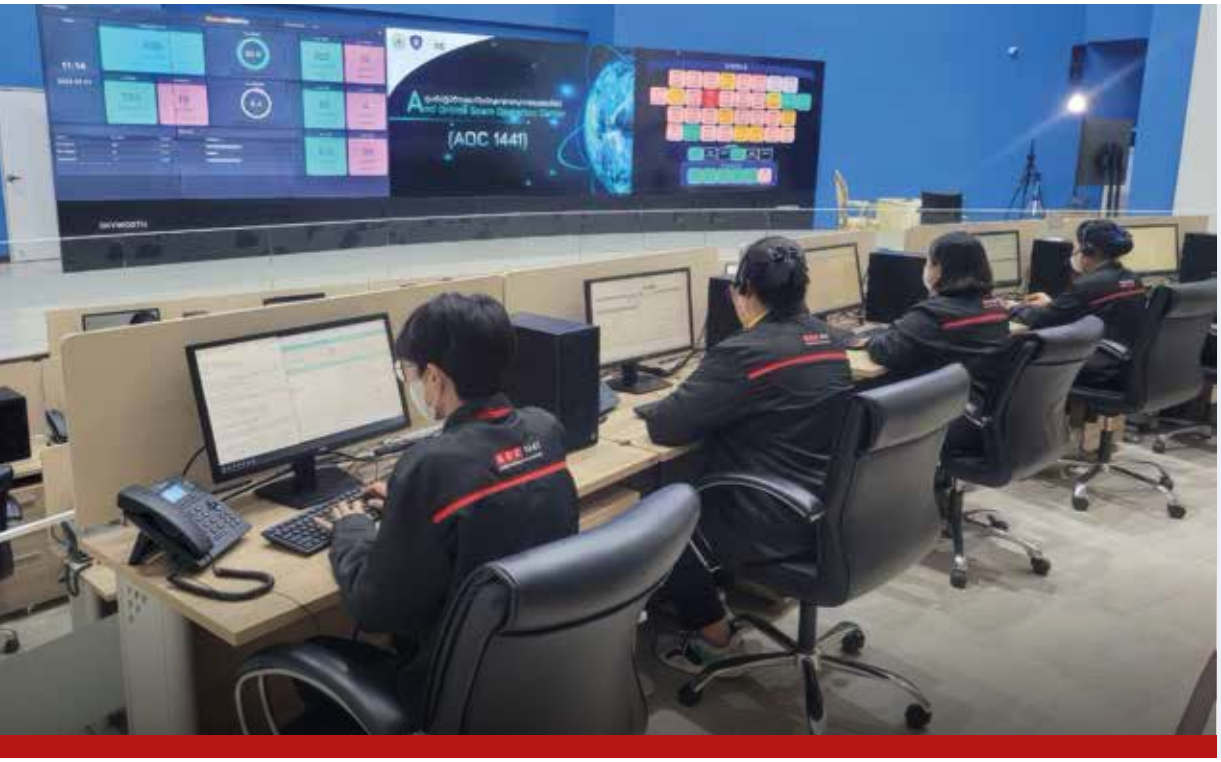
for delaying the outflow of suspected fraudulent funds in appropriate circumstances and for the return of fraudulent funds following the required assessment, including where applicable pursuant to a release or court order.

Netherlands: The Fraud Helpdesk provides a national entry point for fraud reports, using reporting data to identify trends and inform public warnings. A pilot with the Dutch Police introduced direct "warm referrals", with victims' consent, to support reporting to police and improve information flows; following positive results, the model was rolled out nationally in 2026.

Philippines: In the Las Piñas compound case, complaints from survivors and concerned citizens were channelled through a Department of Justice hotline and combined with migrant worker, embassy, financial and digital information. The resulting investigation supported fund tracing, freezing of connected accounts and subsequent forfeiture and prosecution action.

Chinese Taipei: Under the Human Trafficking Prevention Act, proceeds derived from trafficking offences are returned to victims in priority, with only the remaining property subject to confiscation, while property may be seized during investigation or trial to preserve it for subsequent return. Confiscated trafficking proceeds and recovered value also contribute to a dedicated account providing subsidies to trafficking victims.

Thailand: The National Referral Mechanism uses specialised multidisciplinary and trauma-informed screening for persons returning from scam compounds, including a reflection period of up to 45 days. Thailand applies a non-punishment principle to immigration offences directly linked to trafficking and provides for co-ordinated safe and voluntary repatriation. Victims may also seek compensation through available mechanisms, including, where applicable, from assets confiscated following financial investigations into scam and trafficking syndicates. The model illustrates how victim identification and protection can be connected to financial investigation, asset recovery and restitution.



In 2023, Thai authorities launched the Anti-Online Scam Operation Center (AOC) to combat the growing problem of cybercrime in Thailand. This initiative aims to streamline the reporting and remediation process for victims of online crimes and enhance the government's ability to pursue cybercriminals. © Ministry of Digital Economy and Society (MDES)



Financial Action Task Force
www.fatf-gafi.org