ADG CONSULT NZ

INSIGHT PAPER / TRANSNATIONAL CRIME & LAW ENFORCEMENT

Beyond Borders:

The Challenge of Investigating Transnational Scam Networks in Southeast Asia

Assessing the Evolution of Cyber-Enabled Organised Crime and the Future of International Law Enforcement Cooperation

FOCUS

Cyber-enabled organised crime | Scam networks | Regional cooperation

Thailand, Southeast Asia and the future of international investigative cooperation

ADG CONSULT NZ

AUGUST 2026

EXECUTIVE ASSESSMENT

Executive Summary

Transnational scam networks operating across Southeast Asia represent a significant evolution in organised crime. Their importance does not arise solely from the financial losses caused by online fraud, but from the way they combine digital deception, human trafficking, money laundering, technological infrastructure, cross-border mobility and, in some cases, access to territories where conventional law-enforcement authority is constrained. These organisations cannot be adequately understood as groups of cybercriminals working independently. They function as integrated criminal enterprises in which recruitment, victim targeting, communications, financial processing, technical support and physical security may be managed by different actors operating across several jurisdictions.

CENTRAL HYPOTHESIS

The central hypothesis of this paper is that conventional policing remains necessary but is no longer sufficient, when applied alone, to dismantle modern transnational scam networks. Traditional law-enforcement structures are primarily organised around territorial jurisdiction, defined offences, identifiable suspects and prosecution after a crime has occurred. Scam networks are structured to exploit the boundaries between those systems. A victim may be located in one country, contacted through infrastructure controlled from another, directed to transfer funds through accounts in several jurisdictions and defrauded by an operator working inside a compound in a territory beyond the immediate reach of the investigating police force. Senior organisers, financial facilitators and technical managers may remain physically separated from both the victim and the person conducting the fraudulent communication.

This structure creates an institutional imbalance. Criminal organisations operate as adaptable networks, while police powers remain divided by geography, legal mandate and agency responsibility. Cybercrime units, trafficking investigators, immigration authorities, financial intelligence units and foreign police agencies may each possess part of the relevant information without initially recognising that they are examining the same organisation. The principal investigative challenge is therefore not simply the collection of additional evidence, but the fusion of fragmented information into a coherent picture of the criminal system.

Thailand provides an especially relevant case study. Its importance results from geography, regional connectivity, financial infrastructure and proximity to scam-centre environments in Myanmar, Cambodia and Laos. Thailand has experienced direct victimisation, use of domestic accounts and communications infrastructure, movement of trafficked or rescued persons through its territory and growing demands for cooperation with foreign governments. It has also become an important operational and coordination platform for international anti-scam activity.

The paper does not assess Thailand as the origin of the regional scam-centre problem. Rather, it examines Thailand as a state positioned at the intersection of several aspects of the threat. This position creates operational pressure but also provides an opportunity for Thai authorities to shape regional investigative practice. Cooperation involving the Royal Thai Police, Thailand's Anti Cyber Scam Center, financial regulators, foreign law-enforcement agencies and private technology companies demonstrates that Thailand is increasingly participating in network-focused disruption rather than limiting its response to isolated domestic complaints.

The scam-compound model illustrates why this shift is necessary. Facilities operating in border and conflict-affected areas have combined physical control of workers with global digital access. Some individuals inside these compounds participate voluntarily, while others are recruited through deceptive employment offers, trafficked across borders and compelled to conduct fraud under threats or confinement. The resulting overlap between victim and offender status complicates arrest, screening, prosecution and witness handling. Investigators must distinguish organisers, managers, voluntary operators, financial facilitators and coerced workers rather than treating every person present at a compound as occupying the same role.

The most effective recent operations have addressed this complexity through intelligence-led and financially focused investigations. Their objectives extend beyond arresting the person who communicated with a victim. They seek to identify command relationships, preserve compound devices, interview former workers, trace cryptocurrency and bank transfers, freeze assets, remove fraudulent digital infrastructure and expose the companies or armed actors supporting the operating environment.

This approach changes the meaning of successful law enforcement. Arrest totals alone provide an incomplete measure of impact. Large numbers of low-level operators may be detained while leadership, recruitment channels, money-laundering structures and technical infrastructure remain intact. A more meaningful assessment considers whether an operation removed senior organisers, restrained criminal assets, protected trafficked persons, prevented continuing victim losses and reduced the network's ability to reconstitute itself elsewhere.

Foreign agencies are increasingly important within this model because no single national authority holds all relevant evidence. The Federal Bureau of Investigation, the United States Department of Justice, INTERPOL, the Singapore Police Force and other regional partners have contributed victim information, technical expertise, international financial intervention and access to overseas legal processes. In several cases, foreign authorities have worked with Thai investigators to examine devices or witnesses connected to scam compounds located outside Thai territory.

Such involvement is operationally valuable but must remain compatible with Thai sovereignty and domestic law. Foreign officers do not acquire independent enforcement authority merely because an investigation concerns overseas victims. Searches, interviews, arrests and evidence handling inside Thailand require appropriate Thai control and legal process. The strongest model is therefore structured partnership: Thai agencies retain authority over activity conducted within Thailand, while foreign partners provide information, specialist capability and access to evidence held abroad.

The development of this model also reflects the growing importance of professional relationships. Formal mutual legal-assistance procedures remain necessary for prosecution, but they may be too slow to stop funds that can move through multiple accounts and cryptocurrency

wallets within minutes. Rapid intervention increasingly depends on established police-to-police, financial-intelligence and institutional liaison channels capable of identifying and freezing assets before the laundering chain is completed.

Private companies have consequently moved from the periphery of investigations to the centre of operational prevention. Banks, telecommunications providers, social-media platforms, application stores and cryptocurrency exchanges control systems that scam organisations require in order to reach victims, maintain false identities and receive criminal proceeds. These companies may detect suspicious activity before police receive a complaint. Their ability to suspend accounts, block transactions, remove applications or preserve technical data can interrupt ongoing harm more quickly than a conventional criminal case.

This development has created a form of distributed enforcement responsibility. Police retain coercive authority and responsibility for criminal investigation, but private companies increasingly perform gatekeeping and early-warning functions. Banks identify mule-account networks and suspicious transfers. Telecommunications companies can disrupt criminal subscriber identities and calling infrastructure. Online platforms can detect coordinated account behaviour. Cryptocurrency exchanges can connect wallet activity to identifiable customers.

The paper concludes that such cooperation is essential but cannot be treated as a substitute for state capability. Corporate risk assessments, account suspensions and proprietary analytical labels are operational leads rather than legal proof. Police must independently establish identity, intent, control and criminal participation before arrest or prosecution. Excessive dependence on private companies or foreign agencies could also leave national authorities unable to evaluate the methodology underlying the information they receive.

Accountability is therefore as important as speed. Expanded data sharing can improve investigations, but the integration of banking, telecommunications, platform and device information also creates significant privacy and surveillance risks. Cooperation should be governed by clear purposes, access controls, evidential procedures and review mechanisms. Information obtained for urgent disruption should not automatically be treated as sufficient for criminal conviction.

Artificial intelligence intensifies each of these challenges. It allows criminal organisations to translate communications, personalise approaches, create synthetic identities, clone voices and automate portions of victim engagement. Its principal effect is not the invention of new offences but the reduction of labour, language and technical constraints that previously limited criminal scale.

AI-supported fraud also weakens visual and auditory trust. Familiar faces, voices and video calls can no longer be treated as reliable evidence of identity without separate verification. For individuals, companies and police organisations, the appropriate response is a movement from recognition-based trust to process-based verification. Financial requests, executive instructions and claims of police or government authority must be confirmed through independent channels rather than accepted because the caller appears or sounds authentic.

Synthetic media also creates evidential difficulties. Investigators must determine whether content has been altered, who produced or controlled it and how it was used within the wider criminal operation. The growing ability to fabricate convincing material may also allow suspects

to challenge genuine evidence as artificial. This increases the importance of original files, metadata, platform records and rigorous chains of custody.

Artificial intelligence will also be used defensively. Police, financial institutions and platforms will increasingly rely on automated systems to link complaints, identify mule-account networks, detect fraudulent accounts and analyse seized data. Such systems can prioritise investigative attention but should not determine guilt. Their outputs require human review, corroboration and a process through which errors can be identified and corrected.

The overall finding is that transnational scam networks are best understood as criminal ecosystems rather than collections of individual offences. Effective enforcement consequently requires an institutional ecosystem capable of integrating criminal investigation, financial intelligence, trafficking expertise, cyber forensics, private-sector intervention and international cooperation.

The future advantage will belong neither automatically to criminals using advanced technology nor to the state possessing the greatest formal authority. It will belong to the side capable of organising information, technology and personnel into the more coherent and responsive network. Law enforcement can meet that challenge, but only by adapting its structures while maintaining the legality, accountability and evidential standards that distinguish legitimate policing from the organisations it seeks to dismantle.

BACKGROUND

Introduction: The Transformation of Cybercrime into Organised Crime

The expansion of digital technology has fundamentally altered the global criminal environment. The internet, social media platforms, encrypted communications and digital financial systems have created significant benefits for societies and economies, but they have also provided organised criminal groups with new opportunities to operate at a scale and speed previously unavailable.

Online fraud has existed since the earliest development of internet commerce. Initial forms of cyber-enabled fraud were generally limited in scale and often involved individual offenders or small criminal groups conducting activities such as email scams, identity theft or fraudulent online transactions. Investigations were typically conducted within national jurisdictions because the offender, victim and financial systems involved were often relatively identifiable.

The modern transnational scam network represents a significant departure from this earlier model.

The contemporary criminal environment is characterised by professionalisation, specialisation and internationalisation. Criminal organisations increasingly operate according to business-like structures, with separate teams responsible for recruitment, victim engagement, technical support, financial management and operational security.

The importance of this development is that the criminal enterprise itself has become more significant than the individual criminal actor.

In traditional criminal investigations, the primary objective has often been identifying the person who committed the offence. In contrast, modern transnational investigations increasingly require authorities to understand the entire criminal ecosystem: who controls it, how it recruits personnel, how it generates revenue, how funds are transferred, how technology is exploited and where the organisation remains vulnerable.

This represents a fundamental change in investigative thinking.

A person conducting fraudulent online communications may be only one small component of a much larger organisation. Removing that individual may have limited impact if the recruitment system, financial infrastructure and leadership structure remain intact.

This has led international law enforcement organisations to increasingly describe scam networks as organised crime rather than simply cybercrime.

The distinction is important because it changes the investigative approach. Cybercrime investigations traditionally focused heavily on technical evidence, digital systems and individual perpetrators. Organised crime investigations focus on networks, hierarchy, financing, influence and disruption. Modern scam operations require both approaches simultaneously.

The United Nations Office on Drugs and Crime (UNODC), INTERPOL and other international organisations have highlighted this convergence between cyber-enabled fraud and traditional organised crime. Their assessments have identified Southeast Asia as a significant operating environment for scam networks that combine digital fraud with trafficking, coercion and illicit financial activity.

The emergence of these networks demonstrates that criminal organisations have adapted to globalisation faster than many law enforcement structures were originally designed to accommodate.

Police organisations remain primarily national institutions operating under domestic legal frameworks. Criminal organisations increasingly operate through international systems that do not recognise national boundaries.

> **This creates what can be described as a jurisdictional imbalance.**

The criminal group can select the location most advantageous for its operations, exploit differences between legal systems and move activities rapidly when pressure increases. Law enforcement agencies, by contrast, must operate through legal authorities, evidence requirements and international cooperation mechanisms that may require significant time.

The central question is therefore not whether police organisations remain capable of investigating crime. They do. The more important question is whether existing investigative models are sufficiently adaptable to confront criminal organisations specifically designed to exploit the limitations of those models.

The Industrialisation of Online Fraud and the Scam Compound Model

The development of scam compounds represents one of the most significant changes in the organisation of cyber-enabled crime.

The term "scam compound" generally refers to large physical locations where organised groups conduct online fraud operations. These facilities may contain accommodation, communication equipment, management structures and security arrangements. Unlike traditional criminal operations that attempt to avoid attention, scam compounds often operate openly within controlled environments.

The emergence of these compounds demonstrates the combination of digital crime and physical organised crime.

The digital component allows criminals to reach victims anywhere in the world. The physical component provides the infrastructure required to conduct operations at scale.

A modern scam operation may involve hundreds or thousands of operators conducting fraud simultaneously. Workers may use prepared scripts, fake online identities and psychological manipulation techniques designed to exploit victims' trust. Criminal organisations often develop specialised approaches targeting particular groups, including investment fraud, romance scams, cryptocurrency schemes and impersonation fraud involving government officials or financial institutions.

The industrial nature of these operations changes the economics of crime.

A single criminal may successfully defraud a limited number of victims.

A large organisation operating continuously with hundreds of workers can generate revenue on a much larger scale. This explains why organised criminal groups have invested heavily in developing these systems.

The business model depends on several interconnected components:

- Criminal organisations require a workforce. In many cases, individuals are recruited through fraudulent employment opportunities promising legitimate jobs in customer service, technology or business support roles. International investigations have identified cases where individuals travelled voluntarily but later discovered they had been deceived and forced to conduct criminal activities.
- Criminal organisations require technical infrastructure. This includes computers, communication systems, internet connectivity, databases and methods of concealing identity.
- Criminal organisations require financial systems. Fraud proceeds must be collected, transferred and laundered. Increasingly, investigations have identified the use of cryptocurrency, digital payment systems and international money movement networks.
- Criminal organisations require protection. Some operations have developed in areas where state authority is limited or where criminal groups have established relationships with local power structures. These conditions allow criminal enterprises to operate with reduced risk of intervention.

The result is a criminal model that resembles a multinational business structure, although its purpose is entirely illegal.

This evolution creates a fundamental challenge for law enforcement because the traditional distinction between cybercrime and organised crime has become increasingly blurred.

A scam operation may begin with an online message but involve human trafficking, illegal migration, financial crime and international organised crime by the time investigators examine the complete network.

Southeast Asia as a Criminal Operating Environment

The emergence of large-scale scam networks in Southeast Asia is not the result of a single factor. Rather, it reflects the convergence of several regional characteristics that criminal organisations have exploited. These include extensive cross-border movement, rapidly expanding digital economies, uneven levels of governance capacity, established migration patterns and the existence of areas where state authority is contested or limited.

It is important to emphasise that these conditions do not indicate that Southeast Asia is uniquely vulnerable to organised crime. Similar criminal adaptations have occurred globally, including cyber fraud networks operating from Eastern Europe, West Africa and other regions. However, Southeast Asia presents particular characteristics that have allowed certain criminal enterprises to establish large physical operating bases while simultaneously targeting victims internationally.

The region's geography is a significant factor. Southeast Asia contains some of the world's most active economic and migration corridors. Millions of people move across national borders each year for employment, education, tourism and trade. These movements are overwhelmingly legitimate and contribute significantly to regional economic development. However, criminal organisations exploit the same systems that facilitate legitimate activity.

The movement of labour is one example. Millions of workers from countries including Myanmar, Cambodia, Laos, Vietnam, Indonesia and the Philippines seek employment opportunities throughout the region. Criminal groups have exploited this demand by creating fraudulent employment opportunities designed to attract individuals into exploitative situations.

Similarly, the growth of digital financial systems has created both economic opportunity and criminal opportunity. The rapid adoption of online banking, mobile payments and cryptocurrency has increased financial inclusion but has also created additional channels through which criminal proceeds can be moved and concealed.

The challenge for law enforcement is that these systems cannot simply be restricted or eliminated. They are fundamental components of modern economies. The objective is therefore not preventing connectivity but identifying and disrupting criminal exploitation of legitimate systems.

Another important factor has been the existence of areas where criminal groups can operate with reduced interference. In some locations, particularly areas affected by conflict or political instability, criminal organisations have exploited governance gaps to establish operations. These environments provide several advantages: physical security, limited law enforcement access, proximity to international borders and the ability to control movement within specific locations.

The Myanmar border region provides one of the clearest examples of this dynamic.

Thailand as a Regional Case Study

Thailand represents a particularly valuable case study because it demonstrates the complexity of modern transnational crime. The country is not simply a target or victim of these networks. It is

simultaneously affected by criminal activity, involved in regional enforcement efforts and positioned as an important partner for international cooperation.

Thailand's geographical position places it between several major regional economic and security environments. Its borders connect Myanmar, Laos, Cambodia and Malaysia, while Bangkok serves as one of Asia's major transport and commercial centres. These characteristics make Thailand strategically important for legitimate trade and investment but also attractive to criminal networks seeking mobility, financial access and regional connectivity.

The impact of transnational scam networks on Thailand has occurred across several dimensions.

Domestically, Thai citizens have increasingly become targets of online fraud schemes. These have included investment scams, romance scams, impersonation fraud and fraudulent online trading platforms. Thai authorities have reported significant increases in cybercrime complaints, reflecting a broader regional trend in which criminals exploit public familiarity with digital platforms.

The Royal Thai Police, Ministry of Digital Economy and Society, Anti-Money Laundering Office (AMLO) and other agencies have increasingly focused on cyber-enabled crime, recognising that traditional investigative methods alone are insufficient against rapidly evolving digital threats.

Thailand has also experienced the consequences of scam operations located outside its territory.

The proximity of major scam compounds in Myanmar has created direct operational challenges. Foreign nationals seeking assistance, victims of trafficking, suspected criminals and intelligence targets have all moved through regional routes connected to Thailand. This has required Thai authorities to manage situations where law enforcement, immigration, humanitarian and diplomatic considerations overlap.

This complexity was particularly evident during the international attention surrounding scam compounds in Myanmar in 2025.

The Myanmar Border Environment and the Evolution of Criminal Sovereignty

The most prominent example of the changing nature of transnational scam networks has been the development of large-scale scam operations in Myanmar's Kayin State, particularly around the border town of Myawaddy.

Myawaddy is located opposite Mae Sot in Thailand's Tak Province. The area has long been economically connected through cross-border trade and population movement. However, the wider Kayin State environment has also been affected by decades of armed conflict involving ethnic armed organisations, the Myanmar military and various political actors.

This environment created conditions that criminal organisations were able to exploit.

The development of scam compounds in areas such as Shwe Kokko and KK Park attracted significant international attention because of their reported scale and operational sophistication.

Shwe Kokko, located north of Myawaddy, was initially promoted as a development project involving investment from Chinese-linked business interests. Over time, international media and government reports raised concerns regarding criminal activity associated with the area. The

exact relationships between legitimate investment, criminal organisations and local armed actors remain complex and have been subject to varying assessments.

KK Park, located near Myawaddy, became one of the most widely reported scam compound locations. International investigations and media reporting have linked the site to online fraud operations, human trafficking and forced criminality. However, because the area exists within a contested security environment, independent verification of all reported claims remains difficult.

The significance of these locations is not only the criminal activity occurring within them. They represent a broader phenomenon in which organised criminal groups exploit areas where state authority is limited.

Traditional organised crime historically sought secrecy. Modern transnational criminal groups sometimes seek controlled operating environments where they can openly manage infrastructure while remaining beyond effective enforcement reach.

This represents a form of what some analysts describe as "criminal sovereignty" — situations where criminal organisations establish practical control over territory, movement or economic activity without formal political authority.

The concept does not mean that criminal groups replace governments. Rather, it describes circumstances where criminal actors develop sufficient influence to restrict access, control resources or create operational environments where law enforcement intervention becomes extremely difficult.

The 2025 Myawaddy Scam Compound Crisis and Regional Response

International attention intensified in early 2025 following reports that large numbers of foreign nationals were being held in scam compounds in the Myawaddy area.

On 12 February 2025, Myanmar authorities announced that they had detained hundreds of foreign nationals connected to online scam operations in the Myawaddy area. Reports indicated that individuals from multiple countries were among those identified, including Chinese, Indonesian, Filipino and other foreign nationals.

The situation attracted significant diplomatic attention because it demonstrated the international nature of the problem. Individuals from multiple countries had been recruited, transported and exploited within criminal facilities operating in Myanmar.

Thailand became directly involved because many individuals were transferred through Thailand for identification, assistance and repatriation processes.

This placed Thai authorities in a challenging operational position. Authorities were required to distinguish between:

- individuals who were victims of trafficking;
- individuals who had knowingly participated in criminal activity;
- individuals who possessed intelligence relevant to wider investigations.

This distinction is extremely important.

A simplistic enforcement approach could treat all individuals found within scam compounds as criminals. However, international trafficking investigations have demonstrated that many individuals may have been coerced into participating in fraud operations.

The response therefore required coordination between police, immigration authorities, social services, foreign embassies and international organisations.

The Myawaddy situation demonstrated one of the central arguments of this paper:

> **Modern transnational crime cannot be addressed through policing alone.**

It requires cooperation between multiple government agencies and international partners because the criminal activity crosses traditional institutional boundaries.

The Human Trafficking Dimension and the Victim-Offender Challenge

The connection between scam networks and human trafficking represents one of the most significant developments in modern organised crime.

Traditional perceptions of cybercrime often focus on technical capability and digital expertise. However, investigations into scam compounds have revealed a human exploitation component that closely resembles traditional trafficking models.

Recruitment frequently begins through online advertisements offering attractive employment opportunities. Victims may be promised positions in customer service, marketing, translation or technology-related roles. Some individuals travel internationally believing they have accepted legitimate employment.

Upon arrival, some discover that the employment opportunity was fraudulent.

Reports from international organisations have documented cases where individuals were subjected to coercion, threats, physical abuse and restrictions on movement. Some were forced to conduct online scams against victims in other countries.

This creates a significant challenge for investigators because criminal responsibility becomes difficult to determine.

A person operating a fraudulent account may have committed an offence. However, if that individual was forced to participate under threat, the legal and humanitarian circumstances are fundamentally different.

This requires investigators to move beyond simple offender identification and examine the entire criminal structure.

The critical questions become:

- Who recruited the individual?
- Who transported them?
- Who controlled the facility?
- Who received the financial proceeds?
- Who provided protection?

- Who benefited from the criminal activity?

This approach mirrors intelligence-led investigations into terrorism and organised crime, where understanding the network is more important than identifying a single participant.

Implications for Thai Law Enforcement

The experience of Thailand demonstrates that modern transnational crime requires police organisations to operate simultaneously as investigators, intelligence collectors and international partners.

The traditional police role of responding after a crime has occurred remains essential, particularly for supporting victims and gathering evidence. However, the scale and speed of digital crime increasingly require earlier intervention.

Future effectiveness will depend on the ability to identify criminal networks before they fully mature.

This requires:

- stronger intelligence sharing;
- improved cyber investigative capability;
- financial analysis expertise;
- international liaison capability;
- cooperation with private technology companies.

The challenge is not that traditional policing has become irrelevant. Rather, traditional policing must be integrated with additional capabilities designed for a borderless criminal environment.

INTERNATIONAL RESPONSE

International Law Enforcement Response: The Development of a Multinational Investigative Model

The emergence of transnational scam networks has demonstrated that no single national police organisation possesses the capability required to independently dismantle these criminal structures. The geographic separation between victims, offenders, financial systems and criminal infrastructure means that effective investigation increasingly depends upon multinational cooperation.

This represents a significant evolution in international policing. Historically, foreign law enforcement cooperation was often activated after domestic investigative processes had reached a point where evidence or suspects were located overseas. In many traditional criminal investigations, international assistance was a supporting function.

Transnational scam networks have reversed this relationship.

International cooperation is now often required from the beginning of an investigation. The criminal activity itself is international from the moment it occurs. Investigators must frequently identify foreign connections, preserve digital evidence located overseas, trace financial

transactions through multiple jurisdictions and coordinate action against networks operating across several countries simultaneously.

The response has therefore shifted from a model of bilateral assistance towards a model of integrated intelligence cooperation.

This change has involved several major actors, including INTERPOL, national law enforcement agencies such as the United States Federal Bureau of Investigation (FBI), financial intelligence authorities, ASEAN regional police cooperation mechanisms and increasingly private technology companies.

INTERPOL and the International Coordination of Anti-Fraud Operations

INTERPOL has become one of the most significant organisations supporting international responses to transnational fraud networks. Its role is particularly important because it provides a mechanism for police organisations from different legal systems and operational environments to exchange information and coordinate investigations.

Unlike a national police force, INTERPOL does not conduct criminal investigations independently. Instead, it facilitates cooperation between member countries by supporting information exchange, operational coordination, analytical assistance and international alerts.

This function is increasingly important in relation to scam networks because the criminal organisations involved frequently operate across jurisdictions where direct police cooperation may otherwise be difficult.

INTERPOL's assessments have repeatedly identified the global expansion of online fraud networks and their increasing links to organised crime and human trafficking.

One significant development has been the recognition that fraud should not be treated solely as a financial crime issue. The involvement of trafficking, coercion and organised criminal structures has required a broader law enforcement response.

INTERPOL has supported international operations targeting fraud networks, including operations involving multiple countries across Asia.

For example, INTERPOL announced in 2025 and 2026 several global operations targeting online fraud, cyber-enabled crime and related financial networks. These operations involved coordinated action by law enforcement agencies across multiple jurisdictions, resulting in arrests, disruption of criminal infrastructure and the identification of organised networks.

The importance of these operations is not simply the number of arrests achieved. Their significance is that they demonstrate a change in investigative philosophy.

The objective is increasingly to identify the criminal ecosystem rather than simply arrest individual operators.

United States Law Enforcement Involvement

The United States has become increasingly involved in international efforts against transnational scam networks because American citizens have become major targets of online fraud operations.

The United States has a particularly strong interest in disrupting these networks because many scam operations target victims in the United States through investment fraud, cryptocurrency schemes, romance scams and impersonation fraud.

The primary US agencies involved include the Federal Bureau of Investigation (FBI), the Department of Justice (DOJ), the Department of Homeland Security (DHS), the Secret Service and financial authorities including the Department of the Treasury.

Each organisation contributes different capabilities:

- The FBI has traditionally focused on criminal investigations involving fraud, cybercrime and organised crime. Its international presence through legal attaché offices provides an important mechanism for cooperation with foreign police forces.
- The Department of Justice provides prosecutorial capability, particularly where criminal organisations, financial networks or individuals connected to the United States are involved.
- The Department of the Treasury contributes financial intelligence capabilities, including sanctions and financial disruption measures against individuals and organisations involved in illicit financial activity.

This multi-agency approach reflects the changing nature of modern crime.

A scam network is no longer simply a group committing fraud. It is a financial and operational system requiring law enforcement agencies with different expertise to cooperate.

The Role of US Foreign Law Enforcement Partnerships in Southeast Asia

The United States has developed extensive law enforcement relationships throughout Southeast Asia, including cooperation with Thailand.

The FBI maintains a legal attaché presence in Bangkok, supporting cooperation between US and Thai authorities on matters including cybercrime, terrorism, organised crime and transnational investigations.

The importance of these relationships is that they provide established communication channels before major incidents occur.

When a criminal network affects multiple countries, effective cooperation depends heavily on existing professional relationships, trust and understanding between agencies.

In the case of transnational scam networks, cooperation may involve:

- sharing intelligence regarding criminal groups;
- identifying financial flows;
- supporting digital evidence collection;
- coordinating investigations;
- assisting with extradition or prosecution processes.

However, international cooperation also faces challenges.

Different countries have different legal standards regarding evidence collection, data access and privacy protections. Information that can be rapidly accessed by investigators in one country may require lengthy legal procedures in another.

This creates tension between the speed required to respond to digital crime and the legal safeguards required in democratic societies.

ASEAN Regional Police Cooperation

The Association of Southeast Asian Nations (ASEAN) has increasingly recognised transnational crime as a regional security challenge.

ASEANAPOL, the ASEAN Chiefs of National Police organisation, provides a mechanism for regional police cooperation. Its purpose is to strengthen cooperation against crimes that cross national borders, including cybercrime, human trafficking, narcotics trafficking and organised crime.

The importance of ASEAN cooperation is particularly evident because many criminal networks operate within the region.

A criminal organisation may recruit workers in one ASEAN country, operate infrastructure in another, target victims in a third and move proceeds through a fourth.

Regional cooperation is therefore essential.

However, ASEAN cooperation also faces structural challenges. Member states have different legal systems, law enforcement capabilities and political priorities. Information sharing between countries requires trust and established procedures.

Despite these challenges, regional cooperation has become increasingly important because criminal networks have demonstrated their ability to exploit gaps between national systems.

Singapore-Led Regional Operations and the Expansion of Joint Investigations

Singapore has become one of the most active regional partners in combating transnational scams because of its position as a major financial centre and the significant number of scam cases affecting Singapore residents.

The Singapore Police Force has developed extensive capabilities in cybercrime investigation, financial intelligence and international cooperation.

A notable example was Operation FRONTIER, a series of multinational operations targeting transnational scams.

Operation FRONTIER+ III involved cooperation between Singapore and multiple international partners. According to the Singapore Police Force, the operation involved law enforcement agencies from several jurisdictions targeting scam networks and resulted in arrests and disruption of criminal activities.

The significance of such operations is not only the immediate enforcement results but the development of a regional investigative model.

Rather than each country investigating isolated incidents, authorities increasingly seek to identify common criminal networks responsible for multiple offences across different jurisdictions.

This approach is particularly relevant for Southeast Asia because criminal organisations frequently target victims throughout the region rather than limiting operations to a single country.

Financial Intelligence and Following the Money

One of the most important developments in combating transnational scam networks has been the increasing emphasis on financial investigation.

Historically, police investigations often focused on identifying offenders through physical evidence, witness testimony and surveillance. These methods remain important, but modern scam networks often leave extensive financial footprints.

Criminal organisations require money movement systems.

Fraud proceeds must be collected, transferred and converted into usable assets. This creates opportunities for investigators.

Financial intelligence units, banks and law enforcement agencies can identify:

- suspicious transactions;
- unusual account activity;
- patterns involving multiple victims;
- cryptocurrency transfers;
- money laundering networks.

The principle of "following the money" has become increasingly important because financial structures often reveal the organisation behind individual criminal acts.

A person operating a fraudulent account may be difficult to identify. However, financial patterns may reveal the broader network controlling the operation.

This approach also creates opportunities for disruption.

If authorities can freeze criminal proceeds, identify laundering networks and restrict access to financial systems, they may significantly reduce the operational capability of criminal organisations.

Cryptocurrency and Digital Financial Systems

Cryptocurrency has become an important issue in investigations involving transnational scams.

It is important to avoid the misconception that cryptocurrency itself causes criminal activity. Digital assets are legitimate financial instruments used by individuals and businesses worldwide. However, some characteristics of cryptocurrency systems, including rapid international transfers and pseudonymous transactions, have been exploited by criminals.

Investigators have increasingly developed cryptocurrency tracing capabilities to identify financial relationships between criminal actors.

The challenge is that cryptocurrency investigations require specialised technical expertise and international cooperation.

A criminal group may use multiple wallets, exchanges and conversion methods to obscure the origin of funds. Investigators therefore require cooperation from cryptocurrency platforms, financial intelligence units and foreign authorities.

This represents another example of how modern criminal investigations require capabilities beyond traditional policing.

The Increasing Role of Private Technology Companies

One of the most significant developments in modern law enforcement is the increasing involvement of private technology companies.

> **Social media platforms, telecommunications companies, online payment providers and cryptocurrency exchanges now possess information that may be essential to criminal investigations.**

For example, technology companies may be able to identify:

- networks of fraudulent accounts;
- coordinated influence campaigns;
- suspicious communication patterns;
- malicious advertisements;
- digital infrastructure used by criminal groups.

This creates both opportunities and challenges.

The advantage is speed and technical capability. Technology companies often possess the expertise and data necessary to identify criminal activity before traditional investigations can do so.

However, the increasing reliance on private companies raises important questions regarding privacy, legal authority and accountability.

A fundamental policy question is emerging:

To what extent should private companies become operational partners in law enforcement activity?

The answer will likely shape the future of cybercrime investigation.

ANALYTICAL FRAMEWORK

Analysis: The Emergence of a New International Policing Model

The response to transnational scam networks demonstrates that policing is undergoing a structural change.

The traditional model was based on national police forces investigating crimes occurring within their territory. International cooperation was important but usually secondary.

The modern model requires continuous cooperation between multiple agencies, countries and private organisations.

> **The investigation is no longer linear.**

It is network-based.

The primary objective is not simply identifying the person who committed the fraud. The objective is understanding and disrupting the criminal organisation.

This requires:

- intelligence analysis;
- cyber capability;
- financial investigation;
- international liaison;
- technology partnerships.

The countries and agencies most effective in combating transnational crime will likely be those able to integrate these capabilities rather than relying solely on traditional enforcement methods.

OPERATIONAL CASE STUDIES

Operational Case Studies: Recent Scam Network Investigations, International Operations and Lessons for Law Enforcement

The development of transnational scam networks has created a requirement for law enforcement agencies to adapt from traditional criminal investigations towards coordinated intelligence-led disruption. The following case studies demonstrate how criminal organisations have exploited jurisdictional gaps and how governments and international organisations have attempted to respond.

The purpose of examining these cases is not simply to document enforcement activity. The more important objective is to identify the operational lessons emerging from each incident and assess what these developments indicate about the future direction of policing.

The Myawaddy Scam Compound Crisis: A Regional Test of Transnational Law Enforcement Cooperation

The situation surrounding scam compounds in Myanmar's Kayin State, particularly in the Myawaddy area bordering Thailand, represents one of the clearest examples of the complexity created by modern transnational organised crime.

The Myawaddy area has historically been a commercially important border location because of its proximity to Thailand's Mae Sot district in Tak Province. The border crossing supports

legitimate trade and movement of people; however, the wider Kayin State environment has also been affected by long-running armed conflict and competing authorities.

This environment created conditions that criminal organisations were able to exploit.

By the early 2020s, international reporting began identifying the development of large-scale online scam facilities in the area. Locations including Shwe Kokko and KK Park became increasingly associated with cyber-enabled fraud operations targeting victims internationally.

The criminal significance of these facilities was not simply their physical location. Their importance was the combination of physical infrastructure and global connectivity.

A scam compound located in a remote border area could simultaneously provide:

- a controlled physical environment for hundreds of workers;
- access to telecommunications infrastructure;
- distance from foreign law enforcement agencies;
- proximity to international borders;
- access to regional financial systems.

This model represented a significant evolution from traditional cybercrime.

A criminal group no longer needed to hide completely online. Instead, it could create a physical operating base in an area where enforcement access was difficult while conducting criminal activity through digital platforms worldwide.

February 2025 Myanmar Scam Compound Operations and Regional Consequences

International attention increased significantly in early 2025 following reports of foreign nationals being held in scam compounds in Myanmar.

In February 2025, Myanmar authorities announced operations against scam centres in the Myawaddy area and reported the detention of significant numbers of foreign nationals associated with these facilities. International media reported that more than 1,000 foreign nationals were identified during this period, including individuals from multiple Asian countries.

The exact circumstances of every individual detained were complex and varied. Some individuals were reportedly involved in criminal activity, while others claimed to have been trafficked and forced to participate.

This distinction became one of the most important operational issues.

The incident demonstrated that modern law enforcement agencies must manage two parallel objectives:

- First, disrupting criminal organisations responsible for fraud, trafficking and financial crime.
- Second, identifying and protecting victims who may have been coerced into participating in criminal activity.

This is a significant departure from conventional investigations, where the offender and victim are usually easier to distinguish.

In the scam compound environment, a person operating a fraudulent online account may technically have participated in criminal conduct but may also have been acting under threats, confinement or coercion.

This creates significant investigative requirements.

Authorities must establish:

- the person's role within the organisation;
- whether participation was voluntary;
- who controlled the operation;
- who benefited financially;
- whether evidence exists linking individuals to senior criminal leadership.

The response also demonstrated Thailand's importance as a regional coordination point.

Because many individuals leaving Myanmar travelled through Thailand, Thai authorities became involved in screening, identification, humanitarian support and coordination with foreign governments.

This placed Thailand in a challenging position.

Authorities had to balance immigration enforcement, criminal investigation, humanitarian obligations and diplomatic coordination.

The situation highlighted a broader regional issue: criminal activity may occur outside a country's territory while still creating immediate operational consequences inside that country.

Analysis: Why the Myawaddy Model Matters

The significance of Myawaddy is not limited to one location or one criminal network. It demonstrates a broader transformation in organised crime.

Historically, organised criminal groups often depended upon controlling physical territory, local relationships and traditional illicit markets such as narcotics, extortion or illegal gambling.

Modern scam networks demonstrate a different model.

They require physical space, but their primary market is digital.

The victim may be thousands of kilometres away. The criminal proceeds may move through multiple countries. The technical infrastructure may be distributed globally.

This creates a mismatch between criminal organisation and law enforcement structure.

Criminal groups operate through networks.

Police organisations continue to operate primarily through jurisdictions.

> **The key lesson from the Myawaddy case is that territorial control alone is insufficient. Even if one physical location is disrupted, criminal networks may relocate, rebuild infrastructure elsewhere or adapt their methods.**

The strategic target therefore becomes the network itself.

Cambodia and the Development of Regional Scam Infrastructure

Myanmar has received significant attention because of the scale of reported scam compounds; however, Cambodia has also been identified as a major location associated with online scam operations.

Beginning in approximately 2022, international organisations, governments and media outlets reported increasing evidence of scam compounds operating in Cambodia, particularly in areas associated with significant foreign investment and special economic zones.

Locations including Sihanoukville received international attention due to reports linking some businesses and compounds to online gambling, fraud operations and organised criminal activity.

Cambodian authorities have conducted enforcement operations against suspected scam facilities, although the scale, organisation and international connections of these networks have remained difficult to fully assess.

The Cambodian example demonstrates another important characteristic of transnational crime: criminal organisations frequently adapt to enforcement pressure.

When scrutiny increases in one jurisdiction, networks may shift operations elsewhere.

This creates a form of criminal displacement.

A successful police operation in one country may reduce activity locally while unintentionally encouraging criminal groups to relocate to areas where enforcement pressure is lower.

This is why international coordination is essential.

A purely domestic response may simply move the problem rather than eliminate it.

INTERPOL Operations and the Globalisation of Fraud Investigations

INTERPOL's involvement in combating fraud networks reflects the changing nature of international policing.

One significant challenge for investigators is that online fraud often produces enormous numbers of victims but relatively limited visibility of the criminal organisation behind the activity.

A single scam campaign may involve:

- thousands of fraudulent online accounts;
- victims in multiple countries;
- multiple payment systems;
- cryptocurrency transfers;
- false identities;
- infrastructure located across jurisdictions.

Without international coordination, investigations may remain fragmented.

One country may investigate individual victims, another may investigate financial transfers, and another may investigate the physical criminal organisation. Without information exchange, authorities may not recognise that they are examining different parts of the same network.

INTERPOL's role is therefore increasingly focused on connecting these separate investigations.

The organisation has supported international anti-fraud operations involving numerous countries, including coordinated action against online fraud, cyber-enabled crime and associated financial networks.

These operations demonstrate a broader shift in law enforcement philosophy.

The objective is increasingly not simply:

"How many offenders were arrested?"

but:

"How much of the criminal network was disrupted?"

This distinction is important.

A scam network can replace low-level operators relatively easily. However, disrupting leadership structures, financial systems and technical infrastructure has a much greater long-term effect.

Singapore-Led Regional Cooperation: Operation FRONTIER and the ASEAN Model

Singapore provides an important example of how regional law enforcement cooperation is developing.

Singapore has experienced significant growth in scam-related offences and has invested heavily in cybercrime investigation, financial intelligence and international cooperation.

The Singapore Police Force has developed specialised capabilities through units focused on commercial crime, cyber investigations and financial intelligence.

Regional operations coordinated by Singapore have demonstrated the increasing importance of multinational cooperation.

Operation FRONTIER+ III, announced by the Singapore Police Force in 2026, involved cooperation between multiple jurisdictions targeting transnational scam networks.

The operation demonstrated several important developments.

- First, criminal networks are increasingly being investigated collectively rather than through isolated national cases.
- Second, financial disruption has become a central component of enforcement.
- Third, international cooperation is moving from information sharing towards coordinated operational activity.

The significance of this model extends beyond Singapore.

It demonstrates the direction in which regional policing is likely to develop.

Future investigations involving Thailand, Malaysia, Indonesia, Singapore and other regional states will increasingly require joint investigative frameworks rather than traditional requests for assistance after crimes occur.

Lessons Emerging from Recent Operations

Several consistent lessons emerge from these cases.

- Transnational scam networks cannot be effectively addressed through arrests alone. Arrests remain necessary, particularly against senior criminal actors, but the criminal model allows low-level personnel to be replaced quickly.
- Financial investigation has become central. Criminal networks exist because they generate revenue. Disrupting financial flows may therefore have greater strategic impact than arresting individual operators.
- Intelligence sharing must occur earlier. Waiting until a criminal investigation is fully developed before requesting international assistance is increasingly ineffective because digital evidence can disappear quickly and criminal networks can relocate.
- Law enforcement agencies must understand criminal ecosystems rather than individual offences. A fraud complaint represents only one visible part of a larger structure.

The future investigative question is increasingly:

"Who committed this crime?" but: "How does this criminal system function, and where can it be disrupted?"

INVESTIGATIVE EVOLUTION

The Evolution of Police Investigations: Intelligence-Led Policing, Financial Disruption, Digital Evidence and the Role of Foreign Agencies

From Individual Complaints to Network-Based Investigation

Transnational scam investigations increasingly begin with information that appears fragmented, low-level and geographically disconnected. A victim may report a fraudulent investment platform to police in one country, while a financial institution in another jurisdiction identifies unusual transfers into newly opened corporate accounts. A cryptocurrency exchange may detect transactions involving wallets associated with earlier fraud complaints, while immigration or trafficking investigators encounter foreign nationals who describe being forced to operate online accounts inside a compound located elsewhere. Viewed separately, these incidents may appear to concern unrelated fraud, money laundering, immigration violations or human trafficking. Viewed collectively, they may reveal different components of the same criminal enterprise.

This investigative reality requires a departure from the conventional assumption that a police inquiry begins with a clearly defined offence, crime scene and identifiable suspect. In a transnational scam case, the initial complaint may provide evidence of victimisation but little immediate information about the person responsible. The online profile used to communicate with the victim may be false, the telephone number may have been obtained through a virtual service, the fraudulent website may have been registered through an intermediary, and the receiving account may belong to a money mule with no direct knowledge of the criminal leadership. The operator who communicated with the victim may also have been working under coercion inside a scam compound and may not be the principal offender in any meaningful organisational sense.

The primary investigative task therefore becomes one of attribution and network reconstruction. Investigators must determine how the victim was approached, which communications infrastructure was used, where the funds moved, how the fraudulent platform was administered, whether similar complaints exist in other jurisdictions, and which persons or entities benefited from the proceeds. This does not replace traditional evidence gathering. Rather, it places conventional investigative work within a wider intelligence framework capable of identifying relationships between events that may initially appear unconnected.

An intelligence-led approach is particularly important because scam organisations frequently divide functions across countries and personnel. Recruitment may be conducted through social media accounts administered in one jurisdiction. Victims may be contacted by operators based in another. Fraud proceeds may pass through bank accounts opened by mules in several countries before being converted into virtual assets. Technical services, including web hosting, domain registration and communications platforms, may be provided by companies with no knowledge that their systems are being abused. Senior organisers may remain physically distant from both the victims and the workers carrying out the fraud.

This structure creates deliberate investigative friction. Each component of the crime may fall within a different police district, agency mandate or national legal system. Unless information is rapidly consolidated and analysed, the criminal organisation benefits from fragmentation within law enforcement itself.

The most effective modern investigations therefore increasingly rely on centralised anti-scam centres, financial intelligence units, cybercrime commands and multinational coordination platforms. These bodies allow individual complaints to be compared against broader datasets, including suspicious transaction reports, telephone numbers, device identifiers, domain names, cryptocurrency wallet addresses, travel records and intelligence supplied by foreign partners. The resulting picture may reveal that hundreds or thousands of apparently separate offences are linked to one operational network.

The Importance of Rapid Financial Intervention

The financial investigation has become one of the most time-sensitive components of the modern scam inquiry. Fraud proceeds can be transferred through multiple bank accounts, payment providers and cryptocurrency services within minutes. Once funds have moved through several jurisdictions or been dispersed across numerous wallets, recovery becomes substantially more difficult. The investigative value of an early complaint is therefore not limited to identifying an offender. It may provide the only practical opportunity to intercept the victim’s money before it disappears into the wider laundering network.

Operation FRONTIER+ III illustrates how rapid international coordination can change the outcome of a case. The operation was conducted from 10 March to 7 May 2026 and involved more than 3,200 officers from anti-scam agencies in ten jurisdictions, including Thailand’s Anti Cyber Scam Center. Across the participating jurisdictions, authorities arrested 3,018 people, investigated 7,553 subjects linked to more than 138,000 scam cases, froze approximately 102,000 suspected scam-linked bank accounts and seized more than USD 161 million. The reported losses connected to the cases examined during the operation were approximately USD 752 million.

The most important feature of FRONTIER+ III was not the overall arrest figure but the ability of participating agencies to act while funds remained recoverable. On 9 April 2026, the chief executive officer of a Singapore-based company received a WhatsApp call from a person impersonating the chairman of the company's headquarters. The caller instructed the executive to assume responsibility for a supposed acquisition. Between 13 and 17 April, USD 36.3 million was transferred into two accounts in Singapore, with funds originating from both a Luxembourg subsidiary and the Singapore company. After the fraud was discovered on 17 April, Singapore's Anti-Scam Centre seized USD 9.7 million locally and requested immediate assistance from the Hong Kong Police Force's Anti-Deception Coordination Centre. Hong Kong authorities subsequently seized more than USD 11.1 million from bank accounts and associated cryptocurrency wallets.

A second FRONTIER+ III case showed how minor manipulation of digital identity can produce major financial consequences. On 28 April 2026, employees of a Singapore-based commodity trading company received an email that appeared to originate from a legitimate supplier. The fraudulent domain differed from the genuine address through the transposition of two letters. Believing the request to be authentic, the company transferred USD 6.6 million to an account in Oman on 29 April. The fraud was identified the following day. Singaporean authorities engaged the United Arab Emirates Ministry of Interior and the Dubai Police Anti-Fraud Centre, which facilitated contact with the Royal Oman Police. With assistance from HSBC Singapore, the full amount was traced and recovered.

These cases demonstrate why modern anti-scam cooperation must operate more rapidly than conventional mutual legal-assistance procedures were designed to support. Formal evidence requests, extradition applications and prosecutorial cooperation remain essential during the later stages of an investigation, but they are often too slow to prevent the initial dissipation of funds. Effective financial intervention requires designated points of contact, established relationships with banks and exchanges, and procedures permitting urgent action while the necessary legal documentation is prepared.

INTERPOL has developed a comparable mechanism through its Global Rapid Intervention of Payments system, known as I-GRIP. During Operation First Light 2026, conducted from 15 January to 30 April 2026, authorities in 97 countries and territories used coordinated intelligence collection, account blocking, wallet intervention and operational activity against social-engineering fraud. INTERPOL reported 5,811 arrests, the interception of USD 293 million in illicit assets, the identification of more than 142,000 victims and the blocking of 31,014 bank accounts. The operation also generated 99 INTERPOL Notices and Diffusions and identified 15,606 suspects.

The scale of these results should not obscure the underlying methodological change. Financial recovery is no longer treated solely as an outcome to be pursued after conviction. It has become an immediate operational objective. The earlier model of investigation generally sought to prove the offence, prosecute the offender and then recover criminal assets. In contemporary scam cases, asset restraint may need to occur before investigators fully understand the criminal organisation. The financial transaction itself becomes both evidence and an intervention point.

Cryptocurrency Tracing and the Decline of Assumed Anonymity

Cryptocurrency has complicated scam investigations but has also created new forms of evidence. The popular assumption that virtual assets are inherently anonymous is inaccurate. Transactions

on many public blockchains are permanently recorded, although the identity of the person controlling a wallet may not initially be known. Investigative difficulty arises from the use of multiple wallets, decentralised exchanges, cross-chain bridges, token swaps, mixing services and accounts registered through false or stolen identities.

The investigative objective is therefore to connect blockchain activity with identifiable persons, devices, exchange accounts, bank transfers and communications. A cryptocurrency address alone may not establish criminal responsibility. Its significance emerges when combined with evidence showing that it received proceeds from multiple victims, transferred assets to wallets controlled by known facilitators, or interacted with an exchange account opened using a particular identity document.

A Thai case identified during Operation First Light 2026 illustrates the scale that may be hidden behind a small number of suspects. INTERPOL reported that Thai police arrested two people in connection with a money-laundering scheme that converted proceeds from romance scams into several cryptocurrencies. The scheme allegedly used cross-chain token swaps to make the financial trail more difficult to follow. According to INTERPOL, the digital wallet of one suspect, who was 20 years old, had processed more than USD 122.5 million during a ten-month period. INTERPOL did not publish the suspects' names, the date of arrest, the court in which charges were filed or a complete explanation of how much of the wallet activity represented confirmed criminal proceeds. Those limitations are important, and the reported transaction volume should not be treated as equivalent to proven profit or loss. Nevertheless, the case demonstrates how blockchain analysis can identify financial activity greatly exceeding what might be suggested by the apparent seniority or age of an individual suspect.

The case also illustrates the importance of distinguishing between account control and organisational leadership. A young person controlling a high-volume wallet may be a trusted financial facilitator, an account nominee, a recruited technician or a low-level participant using credentials supplied by others. Investigators must establish who directed the transactions, who controlled access keys, who selected the destination wallets and who ultimately received the economic benefit. A focus on transaction volume alone may identify an important financial node without revealing the true leadership structure.

Operation HAECHI VI, coordinated by INTERPOL between April and August 2025, further demonstrated the growing emphasis on simultaneous intervention against conventional accounts and virtual assets. The operation involved 40 countries and territories and targeted voice phishing, romance scams, sextortion, investment fraud, business email compromise, e-commerce fraud and laundering associated with illegal online gambling. Participating agencies blocked more than 68,000 bank accounts and froze almost 400 cryptocurrency wallets, recovering USD 342 million in government-issued currencies and USD 97 million in physical and virtual assets.

The operational lesson is that cryptocurrency tracing should not be isolated within a specialist technical unit after the principal investigation has concluded. It must be integrated from the beginning. Investigators examining victim communications, financial analysts reviewing fund flows and foreign liaison officers requesting information from exchanges must work from a shared evidential picture. Where these functions are separated, delays may allow funds to be converted, dispersed or transferred to less cooperative jurisdictions.

Digital Evidence Exploitation and the Shunda Compound Investigation

The investigation of physical scam compounds produces an unusually large and complex volume of digital evidence. A raid may recover thousands of mobile telephones, computers, storage devices, routers, surveillance systems and account credentials. The challenge is not simply accessing these devices. It is determining which material is relevant, preserving evidential integrity, identifying relationships between users and accounts, and linking the digital records to victims located across multiple countries.

The United States Department of Justice's public account of the Shunda compound investigation provides a recent example of this process. On 23 April 2026, the Department of Justice announced criminal complaints against Chinese nationals Huang Xingshan, also known as "Ah Zhe" and "Huang Xing Saan," and Jiang Wen Jie, also known as "Jiang Nan." The complaints alleged that the two men managed cryptocurrency investment fraud activity at the Shunda compound in Min Let Pan, Myanmar. The charges remain allegations unless and until proven in court.

According to the Department of Justice, the Shunda compound operated from at least January 2025 until approximately November 2025, when it was seized by the Karen National Liberation Army. The department alleged that trafficked workers were confined inside the compound and forced to operate fraudulent investment schemes under threats of violence. Following the seizure, Federal Bureau of Investigation personnel deployed to Thailand and worked with Thai authorities, including the Royal Thai Police's Anti-Cyber Scam Center task force, to examine thousands of mobile devices and hard drives recovered from the site. Investigators also interviewed dozens of former workers. The resulting evidence was used to reconstruct what the department described as a hierarchical organisation of Chinese managers and operators.

The Shunda investigation is significant because it demonstrates the continuing importance of physical evidence in a digital crime inquiry. Scam networks may communicate through online platforms, but their operations still generate devices, management records, access credentials, employee lists, punishment records, financial instructions and physical locations. The seizure of a compound can therefore provide an intelligence opportunity comparable to the exploitation of a terrorist safe house or organised-crime headquarters. The evidential value depends on whether investigators can rapidly preserve, catalogue, translate and analyse the recovered material.

The multinational nature of the victim base creates a second challenge. A device seized in Myanmar and examined in Thailand may contain evidence relating to victims in the United States, Europe, East Asia and elsewhere. Thai investigators may have immediate custody of the material, while foreign agencies possess the victim reports necessary to interpret it. The effective investigation therefore depends on a lawful process for sharing selected intelligence and evidence without surrendering control of the entire inquiry or compromising domestic legal requirements.

The case also demonstrates the potential value of interviewing former compound workers as sources of organisational intelligence. Device extraction may identify communications and transactions, but witnesses can explain terminology, command relationships, work routines, quotas, punishment systems and the meaning of coded messages. At the same time, investigators must assess whether a former worker was trafficked, participated voluntarily,

occupied a management role or moved between victim and offender status over time. Testimony must be corroborated and should not be treated as reliable merely because it is detailed.

The Shunda case presents a particularly useful model for discussion with Thai police professionals because it shows Thailand functioning as an investigative platform rather than merely a transit state. The compound was located outside Thai territory, but the proximity of the border, the movement of recovered evidence and witnesses, and the presence of foreign law-enforcement personnel created a situation in which Thai cooperation was operationally decisive. The arrangement also raises legitimate questions concerning jurisdiction, evidence handling, foreign-agent access and the division of responsibility between Thai and overseas investigators.

Disruption of Digital Infrastructure

The investigation of transnational scams increasingly extends beyond arrest, prosecution and asset seizure to the removal of the technical infrastructure through which fraud is conducted. Fraudulent investment platforms, social-media accounts, mobile applications, messaging channels and domain names are not merely communications tools. They are operational assets that allow criminal networks to acquire victims, imitate legitimate institutions, display false account balances and control the victim's understanding of the supposed investment.

On 2 December 2025, the United States Department of Justice announced the seizure of the domain tickmilleas.com, which it alleged had been used by operators connected to the Tai Chang compound, also known as Casino Kosai, in Kyaukhat village, Myanmar. According to the supporting affidavit, the site was designed to resemble a legitimate investment platform and displayed fictitious profits and transactions. Victims were instructed to download linked mobile applications from the Apple App Store and Google Play. The FBI notified Apple and Google, after which several applications were voluntarily removed. Meta also removed more than 2,000 accounts after receiving information from the FBI concerning the Tai Chang network.

The operation illustrates a disruption model in which law enforcement, prosecutors and private companies act against different components of the same infrastructure. The domain seizure prevented continued use of a specific website and replaced it with a law-enforcement notice. Removal of mobile applications reduced access to the platform through official application stores. Deletion of social-media accounts disrupted recruitment and victim-contact channels. None of these measures alone dismantled the wider organisation, and criminal operators could attempt to rebuild under new names. Collectively, however, they increased costs, interrupted current fraud activity, protected potential victims and generated further intelligence.

This model was expanded through the United States Scam Center Strike Force, formally established in November 2025. On 23 April 2026, the Department of Justice announced that the task force had seized 503 fraudulent investment domains, restrained more than USD 700 million in cryptocurrency alleged to be connected to scam-related money laundering, and seized a Telegram channel allegedly used to recruit trafficking victims for work in a Cambodian scam compound. The same announcement included the charges arising from the Shunda investigation.

The 503 domains were identified through Operation Level Up, an FBI and United States Secret Service initiative established in January 2024 to identify and warn active victims of cryptocurrency investment fraud. By March 2026, the programme had reportedly contacted 8,935 victims or

potential victims. Seventy-seven per cent were unaware that they were being defrauded when contacted, and the authorities estimated that intervention prevented more than USD 562 million in additional losses. Ninety-three individuals were referred to FBI victim specialists for suicide intervention. These figures illustrate that victim notification itself can be treated as a disruption operation rather than simply a public-awareness function.

The approach is important because long-duration investment scams depend on keeping victims psychologically engaged. A victim may continue transferring money because the fraudulent platform displays apparent profits, because the supposed adviser claims that additional deposits are necessary to release existing funds, or because an online relationship has created emotional dependence. Proactive intervention by police can break that cycle before the criminal organisation extracts the maximum possible value.

Sanctions, Designations and the Expansion Beyond Criminal Prosecution

Foreign agencies have increasingly supplemented criminal investigations with sanctions, financial restrictions, diplomatic measures and rewards programmes. These tools can impose costs on persons and entities that may be difficult to arrest or prosecute, particularly where they operate in territories beyond the practical reach of the investigating state.

On 8 September 2025, the United States Department of the Treasury's Office of Foreign Assets Control imposed sanctions on a network of entities and individuals associated with scam operations in Myanmar and Cambodia. The action included nine targets connected to Shwe Kokko and ten targets based in Cambodia. Treasury stated that the Shwe Kokko network operated under the protection of the Karen National Army and described Yatai New City as a major scam hub. Treasury also stated that the same action targeted ownership and support structures rather than only frontline operators.

On 12 November 2025, Treasury designated the Democratic Karen Benevolent Army, four senior leaders, Trans Asia International Holding Group Thailand Company Limited, Troth Star Company Limited and Thai national Chamu Sawang. Treasury alleged that the designated persons and entities supported the development or operation of scam compounds near Myawaddy, including Tai Chang, Huanya and KK Park. The action was coordinated with the FBI's San Diego Field Office, the United States Attorney's Office for the District of Columbia, the Department of Justice Criminal Division, the United States Secret Service and the Drug Enforcement Administration.

Sanctions designations are administrative measures and should not be described as criminal convictions. They rely on the designating government's legal authorities and evidential standards, which differ from those required in a criminal trial. Nevertheless, they can have significant operational effect by restricting access to the United States financial system, exposing corporate relationships, discouraging counterparties and providing foreign governments with intelligence leads.

The use of sanctions also illustrates the growing involvement of agencies that would not traditionally be considered part of a police investigation. Treasury departments, foreign ministries, financial regulators and intelligence services may contribute information or authorities unavailable to conventional investigators. A criminal investigation may therefore develop into a broader government campaign involving prosecution, asset restraint, sanctions, immigration controls, diplomatic engagement and public attribution.

This whole-of-government approach creates benefits but also requires discipline. Intelligence suitable for administrative action may not be admissible in court. Public attribution may alert suspects or complicate an undercover investigation. Foreign sanctions may affect Thai companies or nationals before domestic proceedings have concluded. Effective cooperation therefore requires a clear understanding of each agency's objective and legal threshold.

The Foreign Agency Dimension in Thailand

Thailand's role as a regional transport, financial and diplomatic centre makes sustained foreign law-enforcement engagement inevitable. The FBI maintains personnel in Bangkok, and recent United States cases show agents being deployed to Thailand specifically to investigate scam compounds in Myanmar. Singapore, Malaysia, Hong Kong, Canada, the Republic of Korea, Indonesia, Brunei, the Maldives and other jurisdictions also maintain increasingly direct anti-scam relationships with Thai authorities through FRONTIER+ and bilateral channels.

Foreign agency involvement can provide specialist capabilities, access to overseas victim reports, blockchain intelligence, foreign legal process and evidence concerning criminal infrastructure outside Thailand. In the Shunda investigation, United States authorities possessed information concerning American victims, while Thai authorities provided the operational environment in which seized devices and witnesses could be examined. In FRONTIER+ operations, participating anti-scam centres were able to send urgent financial requests through established counterparts rather than beginning each case through unfamiliar diplomatic procedures.

The relationship must nevertheless remain grounded in Thai sovereignty and domestic law. Foreign officers operating in Thailand do not possess independent police powers unless a specific legal arrangement provides otherwise. Interviews, searches, arrests and seizures ordinarily require Thai authority. Evidence gathered for overseas prosecution must also be handled in a manner that preserves its admissibility and does not compromise Thai investigations or the rights of affected persons.

This creates a delicate but manageable balance. A restrictive approach that limits foreign cooperation may prevent access to essential evidence and allow criminal networks to exploit jurisdictional separation. An overly permissive approach may create legal, political or institutional concerns regarding foreign operational activity. The most sustainable model is structured cooperation in which Thai authorities retain control of activity conducted inside Thailand while foreign partners provide intelligence, technical expertise and lawful access to evidence held overseas.

Experienced Thai police officers are particularly well placed to assess how this balance operates in practice. Formal agreements may establish the legal basis for cooperation, but the speed and quality of an investigation often depend on professional trust between individual officers, liaison personnel, prosecutors and financial institutions. Relationships built before a major case can determine whether an urgent request is recognised, prioritised and acted upon in time to make a difference.

Measuring Success Beyond Arrest Numbers

Large operations frequently report arrests because they provide an easily understood measure of activity. Arrest figures, however, do not necessarily reveal whether a criminal network has been dismantled. A raid may detain hundreds of low-level operators while leaving the leadership,

financial managers, recruiters and technical infrastructure intact. In trafficking-based compounds, a high arrest total may also include coerced workers whose culpability requires careful assessment.

A more meaningful evaluation should consider whether an operation identified and removed senior organisers, recovered assets, protected victims, disrupted communications infrastructure, exposed corporate support structures and reduced the organisation's ability to regenerate. It should also examine whether prosecutions were ultimately successful, whether victims received compensation and whether criminal activity relocated elsewhere.

Operation FRONTIER+ III provides a useful example of broader measurement. Its reported results included arrests, investigations, account freezes, funds seized and specific cross-border recoveries. Operation First Light 2026 similarly combined arrests with account blocking, wallet intervention, victim identification and INTERPOL notices. The Scam Center Strike Force reported domain seizures, asset restraint, victim warnings, sanctions coordination and criminal charges. These measures present a more complete picture of disruption than any single arrest figure.

The central analytical point is that modern scam investigations should be judged against the structure of the criminal enterprise. If the organisation depends on continuous recruitment, access to bank accounts, fraudulent domains and cryptocurrency conversion, an operation that disrupts those functions may achieve strategic value even before senior leaders are arrested. Conversely, an operation producing numerous arrests may have limited long-term impact if the organisation can rapidly recruit replacements and reopen its digital infrastructure.

Implications for Future Investigative Practice

The emerging model of transnational scam investigation is not a rejection of traditional policing. Witness interviews, search warrants, forensic examination, surveillance, arrest, prosecution and courtroom evidence remain indispensable. The change lies in how those functions are connected and prioritised.

The investigation must begin earlier, often while victimisation is still occurring. Financial institutions and cryptocurrency providers must be integrated into urgent response mechanisms. Digital evidence must be examined not only for proof of individual offences but for information revealing command structure and network relationships. Foreign partners must be engaged before the case reaches the extradition or prosecution stage. Victim identification must account for persons who may have been coerced into offending. Success must be measured through disruption of capacity as well as punishment of individuals.

For Thailand, the principal opportunity is to strengthen its position as a regional investigative and coordination centre. The country's proximity to Myanmar, Cambodia and Laos, its established relationships with international agencies and its participation in mechanisms such as FRONTIER+ provide a foundation for this role. The Shunda investigation demonstrates that Thai cooperation can be central even when the principal compound and most victims are located outside Thailand. Operation First Light 2026 shows that Thai authorities are also capable of identifying sophisticated cryptocurrency laundering activity with international significance.

The principal challenge is institutional integration. Scam networks do not separate cybercrime, trafficking, money laundering, immigration crime and organised crime into different investigative categories. Police and government structures often do. Where relevant information

is divided between specialised units without rapid fusion, the criminal organisation retains the advantage.

The future investigative model will therefore depend on the creation of mechanisms that allow specialised agencies to retain their expertise while sharing information through a common operational picture. Cyber investigators must understand the financial network. Financial investigators must understand the recruitment and trafficking process. Border and immigration officers must recognise indicators of forced criminality. Foreign liaison officers must be able to translate overseas intelligence into action that is lawful and operationally useful inside Thailand.

The most defensible conclusion is not that traditional policing has failed. It is that traditional policing, acting alone and within a single jurisdiction, cannot fully address a criminal enterprise designed to distribute its functions across borders, technologies and legal systems. The emerging response is a hybrid model combining criminal investigation, intelligence analysis, financial intervention, digital disruption, victim protection and international cooperation. Recent operations indicate that this model can produce substantial results, but its effectiveness depends on speed, trust, lawful information sharing and the ability to maintain pressure after the immediate raid or arrest has concluded.

PRIVATE-SECTOR ROLE

Private Companies as Operational Partners: Banks, Telecommunications Providers, Technology Platforms and the Redistribution of Investigative Responsibility

The Emergence of Private-Sector Gatekeepers

The growth of transnational scam networks has altered the relationship between police organisations and private companies. In conventional criminal investigations, private firms were commonly treated as third parties holding evidence. A bank might provide account records under lawful authority, a telecommunications company might identify the subscriber associated with a telephone number, and an internet service provider might preserve connection data. The investigation remained primarily state-led, with private entities responding to requests after an offence had been reported.

That distinction is becoming increasingly difficult to maintain. Banks, telecommunications providers, social-media platforms, payment processors, cryptocurrency exchanges and application-store operators now control many of the systems through which scams are initiated, maintained and monetised. They may detect suspicious conduct before a victim reports it and, in some circumstances, before police are aware that an offence has occurred. A bank can identify unusual movement across linked accounts; a mobile operator can recognise bulk activity associated with suspicious subscriber identity module cards; a platform can detect coordinated creation of false profiles; an application store can remove malicious software; and a cryptocurrency exchange can freeze assets before they are transferred beyond practical recovery.

These companies have therefore become operational gatekeepers. They do not possess the arrest, search or prosecution powers of the state, but they control critical points within the criminal process. Their decisions can determine whether a fraudulent account remains active,

whether a suspicious transaction is completed, whether a malicious application remains available and whether investigators receive actionable information before criminal infrastructure is abandoned.

This development provides strong support for the central hypothesis of this paper. Traditional policing remains legally and institutionally indispensable, but it no longer controls all of the capabilities required to disrupt transnational scam networks. The most immediate indicators of criminal conduct may exist inside private systems that law enforcement cannot independently observe. Effective action consequently depends on whether public authorities and private companies can convert commercial data into operational intelligence while preserving legality, evidential integrity, privacy and accountability.

The issue is more significant than ordinary public-private cooperation. It represents a redistribution of investigative responsibility. Private firms are increasingly expected not merely to comply with police requests but to design products against criminal abuse, identify suspicious behaviour proactively, interrupt transactions, preserve evidence, report suspected offences and compensate victims where mandated controls were not applied. The controversial question is no longer whether companies should assist police. It is how far responsibility for preventing crime should be transferred to organisations whose primary role is commercial rather than governmental.

Information Advantage and the Problem of Fragmented Visibility

Transnational scam networks deliberately distribute their activity across multiple services. Initial contact may occur through a social-media platform, the conversation may move to an encrypted messaging application, a victim may be directed to a fraudulent investment website, and payment may then be made through a bank transfer or cryptocurrency platform. The recruitment of workers may occur through employment websites or messaging groups unrelated to the systems used to target victims. Each company sees only a portion of the activity.

This fragmentation creates both a criminal advantage and an investigative weakness. A social-media provider may identify a group of false accounts but may not know that the same operators are using a separate messaging service to continue conversations. A bank may identify suspicious transactions but lack access to the communications that induced them. A cryptocurrency exchange may observe transfers between wallets without knowing that the funds originated from a victim deceived through a false romantic relationship. Police may receive individual reports from victims but not possess the aggregated platform data necessary to identify the common infrastructure.

The resulting problem is not simply that information is unavailable. It is that relevant information exists in disconnected institutional systems governed by different laws, commercial policies, technical standards and disclosure procedures. The criminal organisation benefits when no participant has a complete picture.

The joint report on illicit financial flows from cyber-enabled fraud produced by the Financial Action Task Force, INTERPOL and the Egmont Group identified this fragmentation as a central operational problem. The report concluded that the speed and volume of fraud-related financial movement require strong domestic coordination, centralised investigative mechanisms and cooperation between public authorities and private entities. It specifically identified social-media

platforms, telecommunications companies, internet service providers, financial institutions and virtual-asset service providers as relevant participants in a coordinated response.

This analysis suggests that the most effective public-private model is not one in which companies separately submit large quantities of information to police. Unstructured data transfer can overwhelm investigative capacity and create legal and privacy risks without generating useful intelligence. The more effective model is one in which authorities and private partners agree in advance on priority indicators, reporting thresholds, standardised data fields and urgent escalation procedures.

The distinction is critical. More information does not automatically produce better investigations. A police unit receiving millions of platform records without suitable analytical systems may be less effective than a smaller unit receiving carefully structured information identifying links between accounts, devices, payment channels and previously reported victims.

The strategic requirement is therefore information fusion rather than information accumulation.

The Bangkok Joint Disruption Model

A recent example of this approach occurred through a series of joint disruption activities centred in Bangkok. On 11 March 2026, Meta announced the results of a second Joint Disruption Week led by the Royal Thai Police Anti-Cyber Scam Center, the United States Federal Bureau of Investigation, the United States Department of Justice Scam Center Strike Force and other participating agencies. Representatives from the United Kingdom, Canada, the Republic of Korea, Japan, Singapore, the Philippines, Australia, New Zealand and Indonesia joined the initiative, while personnel from the messaging service LINE participated in discussions. Meta reported that information exchanged during the operation resulted in the removal of more than 150,000 accounts associated with scam-centre networks and that the Royal Thai Police arrested 21 people in connection with scam activity.

Meta stated that the initiative followed an earlier pilot operation in December 2025. According to the company, intensive live information sharing during that pilot led to the removal of approximately 59,000 accounts, pages and groups and contributed to the issuance of six arrest warrants. These figures were published by Meta and should be treated as company-reported operational results rather than independently audited statistics. The available public information does not provide a complete breakdown of the offences associated with the arrested individuals, the jurisdictions in which every suspect operated, the number of accounts later restored following appeal, or the extent to which the removals permanently degraded the underlying criminal networks.

Despite those limitations, the Bangkok initiative is analytically significant. It appears to have moved beyond the conventional model in which police send individual preservation or disclosure requests to a platform. Instead, officers and company investigators exchanged information during a concentrated operational period, allowing separate indicators to be compared while the investigation remained active.

The value of such a process lies in speed and correlation. Police may possess names, telephone numbers, bank accounts and witness statements. Meta may possess account-registration details, device indicators, behavioural links, content-policy violations and relationships between seemingly unrelated accounts. A foreign agency may possess victim reports and cryptocurrency

wallet information. Examined in isolation, each dataset may be incomplete. Examined collectively, it may identify a coordinated cluster of activity.

The operation also demonstrates Thailand's potential role as a regional coordination platform. Bangkok offers proximity to the principal mainland Southeast Asian scam environments, established international law-enforcement representation and a sufficiently developed domestic investigative system to host multinational activity. This does not mean that foreign agencies should direct Thai operations. Rather, it means that Thai authorities are positioned to convene partners, retain control of domestic enforcement action and use foreign technical or evidential contributions to strengthen Thai-led investigations.

The professional judgement of experienced Thai investigators would be especially valuable in assessing whether these disruption weeks generate lasting investigative value. The number of accounts removed may be impressive, but the more important questions concern what happened afterwards. It would be necessary to establish whether removed accounts were connected to senior organisers, whether retained data was converted into admissible evidence, whether affected networks re-established themselves on new platforms, and whether the operation generated further arrests, asset seizures or victim identification.

This distinction reflects a recurring theme throughout the paper: visible disruption is not necessarily structural dismantlement.

Platform Enforcement as a Form of Non-Judicial Disruption

Technology companies can act against suspicious accounts more rapidly than courts or police because they enforce contractual terms and internal policies rather than criminal law. A platform generally does not require proof beyond reasonable doubt before suspending an account. It may act when behaviour violates its rules or when technical indicators suggest coordinated abuse.

This creates an important operational advantage. Scam accounts can be removed before investigators have completed a criminal case, thereby reducing immediate harm. It also creates a significant governance concern. Platform enforcement may resemble a form of private sanction imposed without the procedural safeguards associated with criminal proceedings.

Meta stated in November 2024 that it had removed more than two million accounts linked to scam centres in Cambodia, Myanmar, Laos, the Philippines and the United Arab Emirates during that year. The company said that it had designated certain scam-centre organisations under its Dangerous Organizations and Individuals policy, allowing it to prohibit associated entities and apply broader enforcement measures against attempts to re-establish activity. Meta also described information sharing with the Royal Thai Police and other law-enforcement partners. The figures and organisational assessments were provided by Meta itself and were not independently verified in the company's publication.

The use of a dangerous-organisation designation is analytically important because it demonstrates how private companies are developing their own organisational intelligence assessments. The company is not simply evaluating whether a single message is fraudulent. It is determining whether accounts are associated with a wider criminal entity and then applying network-level restrictions.

This resembles intelligence-led policing in method, although not in legal authority. The platform maps relationships, identifies affiliated infrastructure and attempts to suppress reconstitution. The difference is that the process occurs under private policy, with limited public visibility into the evidential standard, analytical methodology or appeal arrangements.

There are valid reasons for confidentiality. Full disclosure of detection methods could allow criminals to evade them. Nevertheless, excessive opacity creates risks. Police may rely on company assessments that cannot be fully tested in court. Legitimate users may be incorrectly associated with a criminal network. Accounts used by victims, journalists, investigators or humanitarian organisations may display technical connections to criminal infrastructure without participating in criminal conduct.

The most defensible approach is therefore to distinguish operational leads from legal conclusions. A platform's designation or account suspension may provide grounds for further investigation, but it should not by itself establish criminal guilt. Police must independently corroborate identity, intent, control and participation before coercive state action is taken.

This distinction protects both the integrity of criminal proceedings and the credibility of public-private cooperation.

Product Design as Crime Prevention

The role of a technology company is not limited to detecting criminal accounts after they have been created. Product architecture can shape whether common scam techniques succeed.

In its March 2026 announcement, Meta described warnings for suspicious Facebook friend requests, alerts for potentially fraudulent WhatsApp device-linking attempts and expanded scam detection in Messenger. The Messenger feature was described as identifying patterns associated with common scam approaches, including suspicious employment offers, and offering users the option of submitting recent messages for automated review.

Google's June 2026 fraud advisory similarly described measures directed at adversary-in-the-middle phishing, abuse of trusted cloud services, malicious post-installation application behaviour and impersonation of police or government agencies. Google stated that its security teams were using technical controls, developer verification, behavioural analysis and legal action against phishing infrastructure. The advisory was produced by Google and reflects the company's own threat assessment rather than an independent law-enforcement finding.

These interventions show that the platform itself has become part of the crime-prevention environment. A warning displayed at the moment a user receives an unusual friend request may prevent a relationship scam before a police report is ever required. A delay imposed on a suspicious account change may frustrate an attempt to take over a victim's banking profile. Restrictions on application permissions may prevent remote-control malware from accessing financial services.

The broader implication is that the design of commercial systems can determine the scale of criminal opportunity. When security protections are optional, difficult to understand or activated only after loss has occurred, the platform may unintentionally support criminal scalability. When systems incorporate friction at high-risk moments, criminals must invest more time and resources in each victim.

This creates a tension between commercial convenience and security. Digital services are designed to make communication, account creation and payments rapid and accessible. The same qualities reduce friction for criminals. Stronger identity verification, transaction delays and behavioural monitoring may reduce fraud but also inconvenience legitimate users, increase operating costs and exclude individuals who lack conventional documentation or technological literacy.

There is no risk-free design. The policy question is how risk should be allocated and who should bear the cost when commercial convenience creates predictable criminal vulnerability.

Banks as Investigative and Preventive Actors

Financial institutions occupy a particularly important position because scam networks ultimately depend on the movement and conversion of value. A social-media account can create the deception, but a bank account, payment service or cryptocurrency wallet is usually required to realise the financial benefit.

Banks traditionally treated fraud prevention primarily as a customer-protection and compliance function. In the transnational scam environment, they increasingly perform an intelligence role. Transaction monitoring can identify links between victims who have never met, accounts spread across several institutions and recurring payment patterns associated with laundering networks.

The Bank of Thailand announced enhanced mule-account measures on 30 January 2025. The measures shifted attention from individual suspicious accounts towards the persons controlling them. Banks were directed to consider transfer patterns and transaction values, take action against high-risk accounts even where a victim complaint had not yet been filed, block incoming funds to identified mule accounts, warn customers attempting to transfer funds to those accounts and exchange information concerning individuals displaying suspicious behaviour. The Bank of Thailand also emphasised cooperation with the Securities and Exchange Commission and digital-asset businesses to close financial pathways used by scam networks.

This approach represents a significant conceptual change. Traditional account control was reactive: a victim reported a loss, the account receiving the funds was identified, and authorities or the institution attempted to freeze it. The newer model attempts to predict misuse before a confirmed victim report exists.

That predictive approach is necessary because the first reported victim may not be the first person defrauded. An account may receive funds from multiple victims over a short period and transfer them almost immediately. Waiting for a formal complaint can allow the laundering chain to move beyond recovery.

The approach nevertheless creates risks. A person may be incorrectly classified as a mule because of unusual but legitimate activity. A small business receiving payments from multiple unfamiliar customers may superficially resemble a laundering account. A migrant worker sending funds through informal patterns may trigger indicators developed around conventional banking behaviour. If one institution’s risk designation is automatically shared across the entire financial system, an error can result in broad exclusion.

For this reason, moving from account-level to individual-level intervention requires strong safeguards. Risk classifications should distinguish between intelligence indicators, temporary restrictions and confirmed criminal involvement. Affected persons should have access to a rapid

review process. Authorities should monitor whether particular communities or occupations are disproportionately affected by automated detection.

The value of predictive prevention depends on public confidence that the system can distinguish risk management from punishment.

Shared Responsibility and the Reallocation of Loss

A major policy development has been the movement towards shared-responsibility frameworks. These frameworks challenge the assumption that the victim should bear the entire loss whenever they were technically responsible for authorising a transaction.

Singapore's Shared Responsibility Framework took effect on 16 December 2024. It applies to specified banks, payment providers and mobile-network operators and defines particular duties intended to reduce the risk of certain phishing-related transactions. The framework allocates responsibility where a regulated institution or telecommunications company fails to comply with its prescribed obligations. Its scope is deliberately limited and does not apply to every type of scam, investment fraud or voluntarily authorised transfer.

The significance of the Singapore framework lies less in its immediate scope than in the principle it establishes. It recognises that fraud losses may result from multiple failures across an ecosystem. A victim may have been deceived, but a bank may also have failed to provide required warnings or controls, and a telecommunications provider may have failed to apply a mandated filter.

Thailand has moved in a similar policy direction. On 30 January 2025, the Bank of Thailand stated that sustainable prevention required defined responsibilities for banks, telecommunications providers, other relevant agencies and the public. It further stated that non-compliance with regulatory standards should result in accountability and compensation for resulting damage. On 8 April 2025, the Cabinet approved draft measures under which financial institutions, telecommunications operators and social-media platforms could be responsible for damage resulting from negligence in preventing technology-related crime. The official announcement stated that the measures would take effect following publication in the Royal Gazette. The cited announcement records Cabinet approval of the draft at that date and should not, by itself, be treated as confirmation of the final wording or judicial interpretation of the enacted law.

The development of shared responsibility is mildly controversial because it alters the incentive structure of fraud prevention. If companies bear no financial consequence when known vulnerabilities are exploited, prevention may remain subordinate to speed, growth and customer convenience. Liability creates a commercial reason to invest in controls.

However, an excessively broad liability regime could produce defensive behaviour. Banks may block legitimate transfers, platforms may remove accounts on weak suspicion, and telecommunications companies may impose burdensome identity checks. Smaller firms may struggle to comply, reducing competition and concentrating data in a small number of powerful institutions.

A sound framework must therefore define specific duties rather than impose unlimited responsibility for all criminal use of a service. Liability should depend on whether the company failed to apply a reasonable, prescribed control, not simply on whether a scam occurred.

This distinction preserves incentives without making private firms insurers against every act of deception.

Telecommunications Providers and the Control of Criminal Connectivity

Telecommunications infrastructure remains central to scam activity despite the increased use of internet-based messaging. Criminal networks depend on subscriber identities, mobile devices, data connections, one-time-password interception, caller-number manipulation and large-scale communication with potential victims.

Telecommunications providers may detect patterns that are invisible to police, including repeated registration of subscriber cards using common identity information, unusual concentrations of calls, rapid movement between devices and geographical anomalies inconsistent with normal use.

Thailand's policy announcements during 2025 gave regulators and telecommunications companies a more direct role in suspending suspected services. The Cabinet-approved draft announced in April 2025 authorised the National Broadcasting and Telecommunications Commission to direct temporary suspension of telephone services found to be connected to criminal activity. An earlier government announcement in January described proposed authority for relevant agencies and operators to suspend suspected subscriber identity module cards.

Such authority can produce immediate disruption. A telephone number used to impersonate a police officer can be disabled more quickly through cooperation with the provider than through a conventional prosecution. The limitation is that numbers and subscriber cards are replaceable. Criminal networks may also use foreign services, internet calling, stolen identities or virtual numbers.

Telecommunications disruption is therefore most effective when combined with intelligence exploitation. Before a suspicious service is terminated, investigators should consider whether monitoring, subscriber analysis or device correlation may identify additional network members. Immediate suspension protects potential victims, but premature action may alert the organisation and destroy a wider investigative opportunity.

This creates a familiar tension between prevention and investigation. The decision to disable a service should be based on the risk of continued harm, the value of intelligence collection and the likelihood that delay will produce a more significant enforcement outcome.

Cryptocurrency Exchanges and Virtual-Asset Service Providers

Cryptocurrency exchanges and other virtual-asset service providers occupy a position broadly comparable to banks, although the technical and jurisdictional environment is different. Public blockchain transactions may be visible, but the identity of the person controlling a wallet may remain unknown until the assets interact with a regulated service.

Exchanges can link wallet activity to account-registration records, identity documents, device information, login locations and bank transfers. They may therefore hold the information that converts blockchain intelligence into personal attribution.

The joint FATF, INTERPOL and Egmont report identified virtual-asset service providers as relevant participants in anti-fraud and anti-money-laundering cooperation. It recommended risk-based

monitoring, customer verification, analysis of device and network indicators, and rapid private-sector intervention when illicit funds are detected.

The investigative challenge is that exchanges operate under different national licensing regimes. A provider may respond rapidly to a lawful request from one jurisdiction but have no meaningful presence in another. Decentralised services may have no conventional compliance department. Criminals can also move assets across tokens and networks in an effort to exploit differences in monitoring capability.

Foreign law-enforcement and private analytics firms may possess valuable blockchain intelligence, but reliance on proprietary tools creates evidential questions. An investigator must be able to explain how a transaction path was identified and distinguish mathematical blockchain records from assumptions generated by a commercial attribution database. A company's label associating a wallet with a particular group is an intelligence lead, not necessarily proof of control.

For Thai investigators, the strongest model would integrate domestic financial intelligence, regulated Thai exchanges, overseas service providers and foreign blockchain expertise while retaining an auditable evidential process. The objective should be to benefit from commercial analytical capability without allowing the criminal case to depend on an opaque conclusion that cannot be independently tested.

The Risk of Privatised Surveillance

The operational advantages of public-private cooperation are substantial, but they must be balanced against the risk of excessive surveillance.

Banks, telecommunications companies and technology platforms collect data for commercial and service purposes. Using that data to identify criminal behaviour may be justified, particularly where it prevents immediate harm. However, the integration of multiple private datasets can create a level of visibility into individual behaviour that no single agency previously possessed.

A system combining banking history, device identifiers, telephone records, platform relationships, location information and identity documents could identify criminal networks with considerable precision. It could also expose the lawful activities of large numbers of people who are not under legitimate suspicion.

The risk is particularly significant when information is exchanged internationally. A foreign company may provide information directly to a foreign agency concerning activity involving Thai nationals or occurring partly within Thailand. Even where the objective is legitimate, poorly structured cooperation can create the appearance that foreign authorities or multinational companies are conducting investigations beyond Thai oversight.

The appropriate response is not to reject cooperation but to establish clear governance. Thai authorities should define the circumstances in which information can be shared, the purpose for which it may be used, the retention period, the evidential process and the mechanism for review. Foreign agency access should occur through identified liaison arrangements rather than informal or unrecorded transfer of personal data.

The operational need for speed should not eliminate accountability. Indeed, sustained international cooperation is more likely when agencies and companies can demonstrate that information is handled lawfully and proportionately.

Corporate Metrics and the Problem of Measuring Disruption

Private companies often report the number of accounts, pages, domains or applications removed. These figures demonstrate activity but require careful interpretation.

Removing 150,000 accounts does not necessarily mean that 150,000 individual offenders were disrupted. A single operator may control hundreds of accounts, while some accounts may be dormant or only indirectly connected to criminal activity. Conversely, the removal of a small number of high-value administrator accounts may have greater effect than a much larger mass suspension.

Company metrics may also serve reputational and regulatory objectives. A platform has a commercial interest in demonstrating that it is addressing abuse. This does not make the figures false, but it means they should be evaluated as self-reported performance information.

Law enforcement should therefore assess platform disruption using additional measures. Investigators should consider how quickly criminal actors reappeared, whether removed accounts were linked to known compounds, whether the action preserved evidence, whether victims were identified and whether the removal affected financial activity.

The more meaningful measure is not the amount of content removed but the reduction in criminal capability.

Dependency and the Possibility of Corporate Withdrawal

A further strategic risk is that police capability may become dependent on voluntary corporate cooperation. A platform may currently provide specialist analysts, expedited disclosure channels or financial support for joint initiatives. Corporate priorities can change. A company may withdraw from a market, restructure its safety teams, alter its policies or become involved in a legal dispute with the government.

Core investigative capability should therefore not be outsourced. Police require their own expertise in digital evidence, financial analysis, open-source intelligence and blockchain tracing. Private partners can provide access, scale and specialist knowledge, but the state must retain sufficient independent capability to evaluate their information and continue investigations when cooperation is reduced.

This principle applies equally to foreign agencies. External support may be essential in a major international investigation, but Thai authorities should remain able to understand the methodology, retain relevant evidence and develop domestic expertise from the cooperation.

The best partnership is one that strengthens national capacity rather than creating permanent dependence.

Analytical Assessment

Private-sector involvement supports the paper’s central hypothesis because it demonstrates that the modern scam investigation cannot be contained within the traditional boundaries of police work. Criminal networks operate through privately owned systems, and the organisations controlling those systems often possess earlier and more detailed visibility than public authorities.

However, the evidence does not support the conclusion that private companies should replace police or exercise unrestricted investigative authority. Their commercial incentives, contractual powers and evidential standards differ from those of the state. Platform enforcement can interrupt harm, but only public authorities can lawfully arrest, prosecute and impose criminal punishment.

The emerging model is therefore one of distributed responsibility. Police retain legal authority and strategic control. Financial institutions interrupt and trace money. Telecommunications companies restrict criminal connectivity. Platforms identify and remove digital infrastructure. Cryptocurrency providers connect blockchain activity to identifiable users. Foreign agencies contribute overseas evidence and specialist capabilities.

This model can operate effectively only when responsibilities are clearly defined. Private companies should be expected to maintain reasonable controls, preserve evidence and act rapidly against credible threats. They should not be expected to determine criminal guilt. Police should use commercial intelligence to guide investigation but must independently establish the facts required for coercive action and prosecution.

The deeper implication is that the criminal ecosystem is now being confronted by an enforcement ecosystem. The central contest is no longer between an individual detective and an individual fraudster. It is between two networks: one criminal, operating across borders and technologies, and one institutional, combining police powers, financial controls, communications infrastructure, private data and international cooperation.

The success of the institutional network will depend on whether it can act with the speed and integration of the criminal network without abandoning the legal safeguards that distinguish legitimate enforcement from private or arbitrary power.

ARTIFICIAL INTELLIGENCE & FUTURE THREAT

Artificial Intelligence, Synthetic Identity and the Automation of Transnational Fraud

Artificial Intelligence as a Criminal Force Multiplier

Artificial intelligence is unlikely to create an entirely new category of transnational crime. Fraud, impersonation, extortion, identity theft and deceptive recruitment existed long before generative artificial intelligence became widely available. The more significant development is that artificial intelligence reduces the cost, time and specialist skill required to conduct these crimes at scale. It allows established criminal methods to be executed more quickly, in more languages, against more carefully selected victims and with more convincing supporting material.

This distinction is important to the central hypothesis of the paper. The challenge facing law enforcement is not simply the arrival of a novel technical tool. It is the integration of that tool into already mature criminal ecosystems possessing recruitment networks, physical compounds, money-laundering services, corrupt facilitators, digital infrastructure and international financial access. Artificial intelligence strengthens each stage of that system without removing the continuing need for human organisers, financial channels, telecommunications access and physical operating environments.

The criminal value of artificial intelligence lies primarily in its ability to industrialise deception. A human scam operator can research a limited number of victims, maintain a limited number of conversations and communicate effectively only in languages in which the operator possesses sufficient skill. Generative systems can assist with target research, translate conversations, produce natural responses, imitate particular communication styles and generate supporting documents, photographs, audio and video. The operator can consequently manage a larger number of victims while maintaining the appearance that each conversation is personal.

INTERPOL's Global Financial Fraud Threat Assessment, released on 16 March 2026, described artificial intelligence as a central factor in what it termed the industrialisation of fraud. INTERPOL reported that AI-enhanced fraud was 4.5 times more profitable than traditional methods and warned that emerging "agentic AI" systems could plan and execute significant parts of a fraud campaign, including reconnaissance and victim engagement. The public summary did not publish the full methodology underlying the profitability comparison, and the figure should therefore be treated as an INTERPOL threat-assessment finding rather than a universally established measurement. Nevertheless, the assessment reflects the judgement of an international police organisation drawing upon information from multiple member countries and should not be dismissed as speculative.

The scale of reported losses in the United States provides one indication of the emerging financial impact, although US complaint data should not be assumed to represent the exact situation in Thailand or Southeast Asia. The Federal Bureau of Investigation's Internet Crime Complaint Center received 22,364 complaints containing reported artificial-intelligence indicators during 2025, with adjusted losses of USD 893,346,472. Investment-related complaints with an identified AI connection accounted for more than USD 632 million of those losses. Business email compromise cases involving AI produced reported losses exceeding USD 30 million, while confidence and romance cases with a likely AI connection exceeded USD 19 million. Distress scams, including schemes using cloned voices to impersonate relatives or close friends, caused more than USD 5 million in reported losses.

These figures almost certainly do not measure the complete role of artificial intelligence in fraud. Victims may recognise that they were deceived but remain unaware that an AI-generated photograph, translated script, cloned voice or automated conversation formed part of the deception. The FBI itself noted that total investment-scam losses during 2025 exceeded USD 8 billion, substantially more than the USD 632 million attached to complaints in which an AI connection was reported. This suggests that AI-related statistics will remain partly dependent on what victims and investigators are able to recognise after the event.

Artificial intelligence should therefore be understood less as a separate crime type and more as an enabling layer that can be incorporated into numerous offences. A single scam may use AI-generated advertising to identify a potential victim, automated translation to begin a conversation, a synthetic identity to establish credibility, a cloned voice to overcome suspicion and an artificially generated investment dashboard to display false returns. The laundering of the resulting funds may then be identified by a separate AI system operated by a bank or law-enforcement partner.

The conflict is consequently developing into a contest between criminal and defensive automation.

The Removal of Language and Labour Constraints

Language has historically limited the geographic reach of many fraud networks. A criminal organisation targeting Japanese, Thai, Korean, English-speaking or European victims required operators capable of communicating naturally in the relevant language. Poor grammar, unfamiliar cultural references and unnatural conversation could expose the scam.

Generative AI substantially reduces that limitation. Automated systems can translate text, adapt tone, correct grammar and suggest culturally appropriate responses. They can also retain information from earlier conversations and use it to construct the impression of continuity and personal attention. This is especially valuable in long-term investment and romance scams, where success depends on sustained emotional engagement rather than a single deceptive message.

INTERPOL's Asia and South Pacific Cyber Threat Assessment for 2025–2026 warned that AI-generated audio, visual material, messages and automated interactions were being incorporated into large-scale scam ecosystems involving fake employment offers, investment schemes, romance baiting and identity fabrication. The report assessed that AI was increasing the speed, scope, accuracy and impact of cybercriminal operations and allowing criminal networks to automate phishing and produce realistic deepfakes.

The removal of language constraints has important implications for scam compounds. A compound no longer requires one suitably skilled worker for every language group it intends to target. Less experienced operators can use automated translation and prepared AI-assisted scripts to communicate with victims whose language they do not speak fluently. More capable staff can supervise multiple conversations, intervene at key stages and concentrate on victims assessed as likely to produce high returns.

This may increase the productivity of coerced labour. A trafficked worker who would otherwise possess limited value to the criminal organisation can be equipped with tools allowing that individual to manage more accounts and target a broader range of victims. Artificial intelligence may therefore increase the revenue produced by forced criminality without reducing the need for trafficked workers in the immediate term.

Over a longer period, however, automation may change the internal structure of scam compounds. Routine conversations can increasingly be generated by software, while human operators concentrate on emotional manipulation, credibility testing and closing high-value transactions. The likely outcome is not the complete replacement of human workers but a division of labour in which automation performs repetitive engagement and selected human operators manage the most sensitive interactions.

This matters for police planning. Raiding a facility containing fewer visible operators may not indicate that the criminal network has become smaller. It may instead indicate that the organisation has increased its technological efficiency.

Synthetic Identities and the Collapse of Visual Trust

Synthetic media alters one of the most basic assumptions underlying human communication: that hearing a familiar voice or seeing a recognisable face provides meaningful evidence of identity.

A deepfake does not need to be technically perfect to succeed. It needs only to be sufficiently convincing in the circumstances in which it is presented. A short voice message received during an apparent emergency may not be examined critically. A low-quality video call with poor lighting and an unstable connection may conceal visual defects. A victim who already believes that they are speaking to a trusted person will interpret ambiguous information in a way that supports that belief.

The criminal method therefore combines technical fabrication with psychological preparation. The victim is frequently primed before synthetic media is introduced. Earlier messages establish a relationship, create urgency or explain why communication quality is poor. The voice or video then serves as confirmation of a narrative the victim has already accepted.

The Thai experience demonstrates that seniority and familiarity with government do not provide immunity. On 15 January 2025, Prime Minister Paetongtarn Shinawatra publicly disclosed that scammers had used an AI-generated voice purporting to be that of an unnamed ASEAN leader. According to her account, the contact began through voice messages on a chat application and included a call placed at approximately 23:00, which she did not answer. A later voice message requested a donation and claimed that Thailand was the only ASEAN state that had not contributed. She became suspicious because of the request and because the provided bank account did not belong to the neighbouring government. The incident was reported by Thai media, and the full technical details of any subsequent investigation were not publicly released.

The significance of this incident lies less in the unsuccessful request than in the targeting process. The offender apparently possessed contact information capable of reaching the head of government and selected the identity of a foreign leader whose communication would plausibly receive attention. The scam was not based on random bulk messaging. It appears to have combined access to personal contact data, knowledge of regional relationships and synthetic voice technology.

This form of targeting demonstrates how artificial intelligence can enhance traditional social engineering. The synthetic voice creates credibility, but the success of the operation still depends upon intelligence concerning the victim's role, professional contacts and expected behaviour. The underlying offence therefore retains an intelligence-gathering component.

An official Thai government warning issued on 26 June 2026 described two further examples reported to the Anti-Online Scam Operation Center, known as AOC 1441. In one case, a victim received a call from a person claiming to be the victim's younger brother. The voice reportedly resembled that of the genuine relative, and the victim transferred THB 79,000 before confirming that the brother had not made the request. In a separate case, scammers allegedly impersonated telecommunications staff, Anti-Money Laundering Office personnel and senior police officers. The victim was shown documents resembling court papers and participated in a video interview with a person appearing to be a senior police officer before transferring a total of THB 11,497,998. The government publication presented the case within a warning concerning AI and deepfake impersonation, but it did not disclose a forensic report establishing precisely which portions of the video or audio were synthetically generated. The case should therefore be described as an officially reported suspected deepfake-enabled impersonation rather than a technically proven example in every detail.

That qualification is important because public discussion of deepfakes can itself create analytical errors. Not every convincing impersonation requires advanced synthetic media. Criminals may

use recorded video, carefully selected camera angles, conventional voice actors, stolen photographs or actual corrupt participants. Investigators should not assume that an incident involved AI merely because the victim believed a video call was authentic.

The correct investigative question is not whether the media “looked fake”. It is how the communication was produced, transmitted and controlled.

Artificial Intelligence Across the Full Scam Cycle

Artificial intelligence is commonly discussed only at the point where a scammer communicates with a victim. Its relevance is broader. It can support target selection, recruitment, operational management, money laundering and counter-surveillance.

A Bank of Thailand analysis published on 3 August 2026 described AI use across the wider scam cycle. It referred to criminal networks using social-media information to identify people experiencing financial or employment vulnerability, deepfakes and real-time face overlays to impersonate officials or financial institutions, and fraudulent employment advertisements to recruit people into job scams or scam compounds. The same analysis noted that financial institutions were using graph neural networks to identify relationships between mule accounts that might otherwise appear unrelated.

This assessment highlights the dual role of data. Information publicly disclosed through social media can allow criminals to identify an individual’s occupation, family relationships, travel, financial aspirations and emotional vulnerabilities. AI systems can process this information at a scale that would be impractical for a human research team.

A criminal network could use automated tools to rank potential victims according to apparent wealth, loneliness, age, employment insecurity or interest in investment. Different scripts could then be assigned according to the characteristics of each target. A recently unemployed person might receive a job offer. A business executive might receive a supplier or corporate impersonation approach. An older victim might receive a family-emergency call. A person engaging with investment content might be directed toward a fraudulent trading platform.

This represents an important transition from mass fraud to mass personalisation.

Traditional bulk scams succeeded by sending the same message to very large numbers of people and accepting a low success rate. AI-assisted fraud can preserve the scale of bulk activity while making each message appear individually prepared. The criminal organisation can therefore increase both volume and conversion probability.

Artificial intelligence can also support the recruitment of trafficking victims. INTERPOL reported in June 2025 that AI-generated job advertisements were being used to attract people into scam-centre networks and that deepfake photographs and profiles were being used in romance scams and sextortion.

The use of synthetic recruiters may make attribution more difficult. A trafficked worker may believe that they communicated with a genuine human-resources employee, when the profile, photograph and messages were generated or managed by multiple people. The identity presented during recruitment may not correspond to any real person.

This weakens the value of traditional witness descriptions. A victim may provide an accurate account of the identity they encountered while that identity itself is entirely artificial.

The Potential Development of Agentic Fraud

The term “agentic AI” refers broadly to systems capable of performing a sequence of tasks with a degree of autonomy rather than responding only to individual prompts. In a criminal context, such a system might search for targets, gather personal information, generate an approach, maintain a conversation, identify signs of interest and escalate promising victims to a human operator.

INTERPOL’s March 2026 assessment warned that agentic systems could autonomously plan and execute complete fraud campaigns. This should be treated as an emerging capability assessment rather than evidence that fully autonomous criminal campaigns have already replaced conventional scam operations at scale.

The immediate threat is likely to be partial autonomy. A criminal organisation may use different systems for target research, language translation, message generation, image creation and conversation management. Human supervisors remain responsible for campaign objectives, financial decisions and the handling of valuable victims.

Even partial autonomy would alter the economics of crime. An automated system does not require rest, salary, accommodation or physical coercion. It can maintain large numbers of simultaneous conversations and identify which victims warrant human attention.

This could reduce the cost of unsuccessful approaches. At present, every conversation consumes some amount of human labour. Under an automated model, criminals could contact vastly more potential victims without a corresponding increase in staff.

The long-term implication is that the number of attempted scams may rise even where the number of criminal organisations remains stable. Police complaint systems, banks and platforms could face a volume of activity disproportionate to the number of people directly involved in producing it.

This weakens traditional metrics. Counting offenders or physical workstations may no longer accurately indicate criminal capacity.

Artificial Intelligence and the Victim-Offender Relationship

AI may also complicate the distinction between voluntary and coerced participation inside scam networks.

A trafficked worker may use an AI system that automatically generates much of the fraudulent conversation. The worker may perform only limited functions, such as selecting a response, entering victim information or following instructions from a supervisor. Establishing the worker’s knowledge, intent and level of control may become more difficult.

At the opposite end of the hierarchy, senior organisers may attempt to distance themselves from operational conduct by arguing that automated systems generated the relevant communications. This does not remove criminal responsibility where the system was deliberately deployed for fraud, but it may complicate proof concerning authorship and intent.

Investigators will need to distinguish between the person who physically sent a message, the person who configured the automated system, the person who supplied victim data and the person who controlled the criminal campaign. These roles may be distributed across different countries.

The resulting inquiry resembles investigation of a corporate or command structure more than attribution of an isolated fraudulent message.

This again supports the central hypothesis. The appropriate investigative target is not merely the visible operator. It is the decision-making and technical system through which the fraud was designed, financed and controlled.

The Evidential Challenge: Authenticity, Attribution and Intent

Synthetic media creates three separate evidential questions.

- The first concerns authenticity. Investigators must determine whether an image, audio recording, document or video has been generated or materially altered.
- The second concerns attribution. Even where manipulation is established, it remains necessary to identify who produced, commissioned or distributed the material.
- The third concerns intent. Synthetic media has legitimate uses in entertainment, translation, accessibility, education and privacy protection. Criminal responsibility depends on demonstrating that it was knowingly used to deceive, extort, impersonate or facilitate another offence.

Deepfake detection software may assist with authenticity, but detection alone cannot resolve attribution or intent. A forensic tool may identify anomalies suggesting that a video was manipulated, but it may not identify the person who created it. Conversely, platform logs and device evidence may connect a suspect to the production process even where the synthetic content is visually convincing.

Evidence collection must therefore extend beyond the media file. Investigators may require the original message, platform metadata, account-registration details, device logs, cloud-storage records, model-access history, payment records and communications discussing production or intended use.

The preservation of original files is particularly important. Media forwarded through messaging applications may be compressed or stripped of metadata. A screen recording of a video call may preserve what the victim saw but not the underlying data necessary to determine how the video was generated.

Police first responders and victim-reporting systems will increasingly need to collect technical context at the earliest opportunity. The relevant evidence includes the application used, account identifiers, exact date and time, links, telephone numbers, transaction instructions and whether the victim retains the original media.

The more times content is copied, converted or reposted, the more difficult forensic analysis may become.

The “Liar’s Dividend” and the Denial of Genuine Evidence

The most serious long-term evidential effect of deepfake technology may not be the creation of false evidence. It may be the weakening of confidence in genuine evidence.

INTERPOL has warned that artificial intelligence can be used both to create fabricated evidence and to portray authentic evidence as false.

A suspect confronted with an authentic recording may claim that the material was synthetically generated. A public official may dismiss genuine audio as a voice clone. A trafficking victim's recorded evidence of abuse may be challenged as fabricated. The mere existence of convincing deepfakes creates an alternative explanation that did not previously carry the same credibility.

This effect places additional pressure on chain-of-custody procedures. A video obtained directly from a seized device, supported by metadata, witness testimony and platform records, will carry greater evidential weight than a copy downloaded from social media.

Police agencies will increasingly need to prove not only that evidence supports the allegation but that the evidence itself is authentic.

The practical consequence is an increase in the cost and complexity of prosecution. Digital-media authentication may become routine in cases where it was previously unnecessary. Courts, prosecutors and defence lawyers will require greater technical understanding. Competing experts may interpret detection results differently.

Law-enforcement agencies that lack access to reliable forensic capability may become dependent on foreign agencies or private companies. This dependency reinforces the need for international cooperation but also raises questions concerning sovereignty, disclosure and the ability of a domestic court to examine the underlying methodology.

Why Visual Warning Signs Are an Incomplete Defence

Government warnings frequently advise the public to look for unnatural blinking, mismatched lip movement, unusual voice rhythm or inconsistent lighting. These indicators can be useful, and Thailand's AOC 1441 included similar guidance in its June 2026 warning.

They should not, however, be treated as a durable defence. Synthetic-media quality is improving, and communication conditions often conceal imperfections. A low-bandwidth video call may naturally display delayed lip movement. A genuine speaker may pause unnaturally because of stress. Compression can alter audio quality. Criminals may deliberately claim that a poor connection explains irregularities.

Training the public to identify technical defects risks creating false confidence. A victim may conclude that a call is genuine because none of the familiar warning signs is present.

A stronger approach is procedural verification. Identity should be confirmed through a separate, previously established channel. An unexpected financial request from a family member should be checked by calling a known number. A request from an executive should be confirmed through an internal approval process that does not depend on voice or video recognition alone. A person claiming to be a police officer should be verified through the relevant station or official contact system.

This approach treats media as information rather than proof of identity.

The shift is conceptually significant. Society has historically relied upon sight and sound as basic authentication tools. Deepfakes require institutions and individuals to replace intuitive recognition with process-based verification.

Biometric Security and the Risk of Synthetic Presentation

Financial institutions have responded to impersonation by expanding biometric verification, including facial comparison and liveness detection. Thailand's banking standards require facial comparison combined with presentation-attack detection for specified high-risk mobile-banking actions. Measures include additional verification for transfers of THB 50,000 or more in a single transaction, aggregate daily transfers reaching THB 200,000 and increases in daily transfer limits to THB 50,000 or above. The Bank of Thailand also requires controls intended to identify application tampering and prevent mobile-banking use while high-risk remote-control or accessibility applications are operating.

These controls show how the defensive system is adapting to synthetic identity threats. A conventional facial comparison asks whether the presented face resembles the registered customer. Presentation-attack detection asks whether a genuine live person is physically present rather than a photograph, replayed video or manipulated biometric input.

The continuing risk is that biometric security can become an arms race. As detection improves, criminals develop more sophisticated injection methods, real-time face replacement or compromised devices capable of bypassing the normal camera process. Defensive systems must therefore evaluate not only the image but the integrity of the device, application and transaction context.

No single biometric should be treated as conclusive. Strong protection is more likely to result from combining identity, device, behavioural and transaction indicators.

This principle has direct investigative relevance. A successful facial-authentication event does not necessarily prove that the genuine customer knowingly authorised the transaction. Investigators must consider whether the device was compromised, whether remote-control software was active and whether the customer was manipulated into completing the biometric check.

Artificial intelligence does not merely create fake identities. It can also manipulate genuine people into authenticating fraudulent activity.

AI-Assisted Policing

The scale of AI-enabled fraud makes some form of defensive automation unavoidable. Human analysts cannot manually examine every suspicious transaction, social-media account, telephone number and cryptocurrency wallet.

Banks already use machine learning to detect abnormal transactions and networks of mule accounts. Platforms use automated systems to identify coordinated behaviour. Police agencies can use AI to cluster complaints, identify common infrastructure, translate seized communications and prioritise high-risk leads.

INTERPOL and the United Nations Interregional Crime and Justice Research Institute have developed a Toolkit for Responsible AI Innovation in Law Enforcement. The toolkit emphasises readiness assessment, risk evaluation, governance, ethics and human-rights considerations when police organisations develop or deploy AI systems.

INTERPOL has also established Project SynthWave to develop law-enforcement capability to detect AI-generated synthetic media. The project reflects recognition that deepfake detection cannot be left solely to commercial platforms or individual national agencies.

For Thailand, AI-assisted complaint analysis could be particularly valuable because scam reports may be distributed across police stations, online reporting systems, AOC 1441, banks and foreign agencies. Automated link analysis could identify recurring telephone numbers, accounts, phrases, web domains and device indicators.

The danger is that AI systems can reproduce errors at scale. A flawed risk model may incorrectly associate innocent people with mule-account networks. An opaque facial-recognition system may produce false matches that investigators are unable to explain. Automated translation may misinterpret coded language or cultural nuance.

AI-generated leads should therefore be treated as investigative indicators rather than proof. Human investigators must review the basis of the result, seek corroboration and remain accountable for any coercive action.

The principle should be straightforward: automation may prioritise attention, but it should not determine guilt.

The Foreign Agency Requirement

Synthetic-media investigations will frequently exceed the capability or jurisdiction of a single national police organisation. The model provider may be based in one country, the cloud server in another, the suspect in a third and the victim in Thailand. The relevant platform may preserve information under a foreign legal regime, while the cryptocurrency payment used to purchase the service may pass through several exchanges.

Foreign agencies may possess specialist laboratories, platform relationships or intelligence concerning tools already linked to other investigations. Sharing synthetic-media indicators can allow Thai investigators to determine that a voice model, face-swapping service or technical signature has appeared in cases elsewhere.

The involvement of foreign agencies must nevertheless remain structured. A foreign conclusion that material is synthetic should not be accepted without sufficient information concerning the analytical method. If the conclusion is to support prosecution in Thailand, Thai investigators and courts must be able to understand and test it.

International cooperation should therefore focus not only on exchanging conclusions but on developing common forensic standards, preservation procedures and evidential terminology.

The absence of common standards creates the risk that one jurisdiction will classify content as manipulated while another regards the finding as insufficiently reliable for court use.

Strategic Assessment

Artificial intelligence strengthens the overall hypothesis because it increases the mismatch between nationally organised policing and internationally distributed criminal networks. It allows scam organisations to operate across language barriers, automate victim engagement, create convincing identities and process larger volumes of personal information.

However, AI does not eliminate the physical and financial dependencies of organised crime. Scam networks still require access to victims, communications infrastructure, accounts, devices, payment systems and persons capable of controlling the proceeds.

These dependencies remain investigative opportunities.

The correct strategic response is therefore not to focus exclusively on detecting deepfakes. Synthetic media is one component of a broader criminal system. Removing a single fake video will not dismantle the organisation that produced it. Arresting the operator who sent it may not affect the manager, recruiter, platform administrator or money launderer.

AI makes the network-disruption model more necessary, not less.

The future investigation must identify how the synthetic identity was created, how targets were selected, which infrastructure distributed the material, how the victim was directed to pay and where the proceeds ultimately moved.

The mildly controversial conclusion is that audio and video can no longer be treated as inherently reliable forms of identification. Police organisations, companies and the public must move from recognition-based trust toward verification-based trust.

This change will impose additional cost and inconvenience. Transactions will require more checks. Police will require more forensic resources. Companies will be expected to preserve more information. International evidence requests will become more technically complex.

Those costs are likely unavoidable.

The central threat is not that artificial intelligence will make fraud impossible to investigate. It is that AI will allow criminal networks to generate deception more quickly than complaint-led police systems can recognise and connect it.

The law-enforcement response must consequently become more anticipatory, more technically capable and more internationally integrated. It must combine AI-assisted analysis with human judgement, private-sector visibility with public accountability, and rapid disruption with evidence capable of surviving judicial scrutiny.

The decisive advantage will not necessarily belong to the side possessing the most advanced artificial intelligence. It will belong to the side able to combine technology, intelligence, lawful authority and international cooperation into the more coherent operational network.

CONCLUSION

Conclusion

Transnational scam networks have developed beyond the investigative assumptions traditionally associated with online fraud. They are neither exclusively cybercriminal organisations nor conventional organised-crime groups that happen to use the internet. They combine physical control, digital reach, financial concealment and cross-border mobility in a single operating model. Their strength lies in the ability to distribute criminal functions across people, technologies and jurisdictions while ensuring that no single victim, investigator, financial institution or government initially sees the complete organisation.

The paper’s hypothesis is therefore supported, with an important qualification. Traditional policing has not become ineffective or obsolete. Arrest, interview, search, forensic examination, prosecution and judicial process remain essential. The limitation arises when these methods are applied in isolation, after the event and within the boundaries of a single jurisdiction. The scam network is designed to survive precisely that form of response.

The core investigative change is a movement from offence-focused investigation towards system-focused disruption. The relevant question is no longer limited to identifying who sent a fraudulent message or received a particular transfer. Investigators must determine how victims were selected, how the deception was maintained, which infrastructure supported it, where funds were consolidated and who exercised strategic or financial control. This broader analysis is necessary because the visible offender may be replaceable, coerced or operationally insignificant compared with the organisers and facilitators sustaining the enterprise.

This does not mean that every scam investigation should become an extensive multinational operation. Individual complaints must still be assessed proportionately. However, complaint systems should be designed so that recurring accounts, telephone numbers, websites, devices, cryptocurrency wallets and methods can be connected across cases. The strategic value of the initial report may lie not in resolving that single offence but in revealing a node within a larger network.

Financial intervention is likely to remain the most immediate and measurable method of reducing harm. Scam networks depend on rapid movement of proceeds. The ability to freeze or recall funds before they are dispersed is therefore not secondary to the investigation; it is part of the operational response itself. This requires cooperation that operates faster than traditional international evidence processes, while ensuring that temporary intervention is followed by proper legal authority and review.

The same reasoning applies to digital infrastructure. Removing accounts, applications and fraudulent domains can protect potential victims and increase the operating costs of criminal groups. Such actions should nonetheless be assessed according to their structural effect. The removal of a large number of low-value accounts may achieve less than the disruption of a small number of administrator accounts, payment channels or recruitment systems. The emphasis should remain on reduction of criminal capability rather than the production of impressive but potentially misleading activity statistics.

The human-trafficking dimension requires equal attention. The presence of forced criminality means that enforcement cannot rely on a simple distinction between offender and victim. Some individuals will have knowingly participated, some will have been coerced from the beginning, and others may have moved between roles over time. Effective investigation must identify decision-making authority and economic benefit rather than assuming that the person operating a device occupies the same position as the person controlling the organisation.

This has direct implications for raids and repatriation activity. Removing large numbers of people from a compound may end immediate confinement, but it does not automatically dismantle the network. The evidential opportunity presented by rescued workers, seized devices and operational records must be used to identify recruiters, managers, financial controllers and protectors. Without that follow-through, the physical facility may be closed while the criminal system survives.

Foreign-agency involvement is likely to remain a permanent feature of these investigations. The international distribution of victims, infrastructure and proceeds makes external cooperation unavoidable. The challenge is not whether foreign agencies should be involved, but how that involvement should be structured.

Thailand has a legitimate interest in preserving control over activity undertaken within its territory, protecting domestic legal processes and ensuring that foreign partners operate through recognised channels. At the same time, overly restrictive cooperation would deprive Thai investigations of overseas evidence, technical support and rapid access to foreign financial systems. The appropriate balance is a Thai-led model of cooperation in which external agencies contribute capability without displacing Thai authority.

This model also presents an opportunity. Thailand's location, institutional relationships and operational experience position it to function as a regional coordination centre for investigations involving mainland Southeast Asian scam networks. Such a role would not require Thailand to assume responsibility for criminal activity occurring in neighbouring states. It would involve strengthening the ability to combine border intelligence, financial reporting, digital evidence and international liaison into a common investigative picture.

Private-sector involvement further reinforces the need for a networked enforcement model. The systems enabling transnational scams are largely privately owned. Banks, telecommunications providers, online platforms and cryptocurrency exchanges therefore occupy points of intervention that police cannot independently control.

The case for requiring reasonable preventive action by these companies is strong. A service provider that repeatedly observes known criminal patterns cannot be regarded as a purely neutral conduit. Companies should maintain proportionate controls, act on credible indicators, preserve evidence and provide urgent channels for lawful cooperation.

The limits are equally important. Private companies should not become unaccountable police organisations. Their decisions may be based on contractual rules, commercial risk models and proprietary technology rather than criminal evidential standards. Their findings should guide investigation and immediate risk reduction but should not, without corroboration, determine criminal responsibility.

Shared-responsibility frameworks reflect a broader recognition that scam losses often result from failures across an ecosystem rather than from one victim's decision alone. Their effectiveness will depend on careful design. A framework that imposes no consequence for preventable institutional failure may provide insufficient incentive for security investment. A framework imposing unlimited liability may produce excessive blocking, exclusion and surveillance. The more sustainable approach is to define clear duties and link responsibility to failures to perform those duties.

Artificial intelligence will accelerate these pressures. It will allow criminal networks to conduct more personalised and linguistically convincing fraud at lower cost. It will also make the apparent identity of the speaker or caller less reliable. This is not merely a technical problem. It changes the basis on which individuals and institutions establish trust.

The practical response is procedural rather than intuitive. Identity must increasingly be verified independently of the communication being received. An executive instruction should be checked through established corporate authorisation procedures. A family emergency should be confirmed through a known contact. A person claiming official authority should be verified through an official institution. Familiarity of voice, image or writing style is no longer sufficient.

Police evidence procedures will require similar adaptation. Synthetic-media detection may assist, but successful prosecution will depend on establishing provenance, control, intent and

distribution. Original files, device data, platform records and transaction evidence will be more important than subjective judgements concerning whether content appears genuine.

AI-assisted policing will be required to manage the scale of the threat, but its role must remain controlled. Automated systems can identify relationships, prioritise complaints and expose suspicious financial patterns. They cannot replace legal judgement, contextual understanding or responsibility for coercive decisions. The principle that automation may direct attention but should not determine guilt must remain central.

The overall conclusion is that transnational scam networks have exposed a structural weakness in traditional law-enforcement organisation: criminal systems integrate functions that governments and companies continue to manage separately. The solution is not the elimination of specialisation. Cyber investigators, financial analysts, trafficking specialists, border police and prosecutors require distinct expertise. The solution is the ability to combine that expertise rapidly around a shared understanding of the network.

The most effective future model will therefore be intelligence-led, financially focused, technologically capable and internationally connected. It will intervene while crime is occurring rather than relying entirely on retrospective prosecution. It will treat victim protection, asset restraint and infrastructure disruption as operational outcomes. It will preserve domestic authority while drawing on foreign and private-sector capabilities. It will use automation without surrendering human judgement or procedural accountability.

The central strategic contest is between two types of network. The criminal network seeks to exploit fragmentation, delay and uncertainty. The institutional network must overcome those weaknesses through trust, lawful information sharing and coordinated action.

Transnational scam networks are unlikely to disappear. Enforcement pressure may displace them geographically, encourage technological adaptation or alter their internal labour structures. Success should therefore not be defined as the permanent elimination of fraud. A more realistic objective is to make the operating environment progressively more hostile: to reduce access to victims, increase the difficulty of moving funds, expose organisational leadership, protect coerced workers and shorten the period during which criminal infrastructure remains effective.

The central hypothesis is ultimately confirmed. Conventional policing can address individual offences and offenders, but dismantling modern transnational scam ecosystems requires something broader. It requires a coordinated enforcement system capable of acting across the same borders, technologies and financial channels that the criminal organisation itself exploits.

The challenge for Thailand and its international partners is to develop that system without weakening sovereignty, legality or public trust. That balance will determine not only the effectiveness of anti-scam enforcement, but the legitimacy of the wider international policing model now emerging in response.

SOURCE BASE

References

Official, Government and Institutional Sources

- Bank of Thailand (2025), 'Bank of Thailand Enhances Measures to Manage Mule Accounts and Promotes a Shared Responsibility Framework', 30 January 2025. Available at: https://www.bot.or.th/en/news-and-media/news/news-20250130.html
- Bank of Thailand (2025), Notification No. 19/2568: Standards and Measures to Prevent Technological Crime for Financial Institutions [Thai-language regulatory notification], effective 8 August 2025. Available at: https://www.bot.or.th/content/dam/bot/fipcs/documents/FPG/2568/ThaiPDF/25680154.pdf
- Bank of Thailand (2026), 'แรงงาน กับ การเงิน ในยุค AI' ['Labour and Finance in the Age of AI'], 3 August 2026. Available at: https://www.bot.or.th/th/research-and-publications/articles-and-publications/articles/article-20260803.html
- Federal Bureau of Investigation (2026), 2025 Internet Crime Report, Internet Crime Complaint Center. Available at: https://www.fbi.gov/file-repository/2025_ic3report.pdf
- Federal Bureau of Investigation (2026), 'Cryptocurrency and AI Scams Bilk Americans of Billions', 6 April 2026. Available at: https://www.fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions
- Financial Action Task Force, INTERPOL and Egmont Group of Financial Intelligence Units (2023), Illicit Financial Flows from Cyber-Enabled Fraud, November 2023. Available at: https://www.interpol.int/content/download/20483/file/Final_Illicit-financial-flows-from-cyber-enabled-fraud.pdf
- Google (2026), 'Our Latest Fraud and Scams Advisory', 8 June 2026. Available at: https://blog.google/innovation-and-ai/technology/safety-security/fraud-scams-advisory-june-2026/
- Infocomm Media Development Authority and Monetary Authority of Singapore (2024), Guidelines on Shared Responsibility Framework, issued 24 October 2024 and effective from 16 December 2024. Available at: https://www.imda.gov.sg/-/media/imda/files/regulations-and-licensing/regulations/consultations/2024/shared-responsibility-framework-for-phishing-scams/guidelines-on-shared-responsibility-framework.pdf
- INTERPOL (2023), Artificial Intelligence Toolkit: Toolkit for Responsible AI Innovation in Law Enforcement, developed with the United Nations Interregional Crime and Justice Research Institute. Available at: https://www.interpol.int/en/How-we-work/Innovation/Artificial-Intelligence-Toolkit
- INTERPOL (2025), 'INTERPOL Releases New Information on Globalization of Scam Centres', 30 June 2025. Available at: https://www.interpol.int/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres
- INTERPOL (2025), INTERPOL Asia and South Pacific Cyber Threat Assessment: Report 2025/2026. Available at: https://www.interpol.int/content/download/24327/file/CYBER_ASP%20Cyber%20Threat%20Assessment%20Report_2025_2026_v4.pdf
- INTERPOL (2025), 'USD 439 Million Recovered in Global Financial Crime Operation', concerning Operation HAECHI VI, 24 September 2025. Available at: https://www.interpol.int/News-and-Events/News/2025/USD-439-million-recovered-in-global-financial-crime-operation
- INTERPOL (2025–2026), 'Project SynthWave', a programme developing law-enforcement capability to detect and respond to AI-generated synthetic media. Available at: https://www.interpol.int/How-we-work/Innovation/Projects/Project-SynthWave
- INTERPOL (2026), 'INTERPOL Report Warns of Increasingly Sophisticated Global Financial Fraud Threat', 16 March 2026. Available at: https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat
- INTERPOL (2026), 'Over 5,800 Arrests, USD 293 Million Intercepted in Global Fraud Bust', concerning Operation First Light 2026, 9 July 2026. Available at: https://www.interpol.int/News-and-Events/News/2026/Over-5-800-arrests-USD-293-million-intercepted-in-global-fraud-bust
- INTERPOL (undated), 'Spotlight Cybercrime Innovation: Fighting AI with AI'. Available at: https://www.interpol.int/Resources/INTERPOL-Spotlight/Spotlight-Issue-2-Cybercrime/Spotlight-Cybercrime-Innovation

- Meta (2024), 'Cracking Down on Organized Crime Behind Scam Centers', 21 November 2024, updated 14 July 2025. Available at: https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers/
- Meta (2026), 'Global Law Enforcement Agencies, With Support From Meta, Disrupt Major Criminal Scam Networks Based in Southeast Asia', 11 March 2026, updated 30 March 2026. Available at: https://about.fb.com/news/2026/03/meta-global-law-enforcement-disrupt-major-southeast-asia-criminal-scam-networks/
- Royal Thai Government (2026), 'หน้าใช่ เสียงคุ้น อาจไม่ใช่ตัวจริง! AOC ชวนเช็ก 7 จุดสังเกต AI ปลอมตัว ก่อนโดนหลอกโอนเงินไม่รู้ตัว' ['The Face and Voice May Be Familiar but May Not Be Genuine: AOC Identifies Seven Warning Signs of AI Impersonation'], 26 June 2026. Available at: https://www.thaigov.go.th/th/news/165660
- Singapore Police Force (2026), 'Operation FRONTIER+ III: Joint Two-Month Crackdown on Transnational Scams Resulted in More Than 3,000 Arrests Across Ten Jurisdictions', 20 May 2026. Available at: https://www.police.gov.sg/media-hub/news/2026/05/20260520_operation_frontier_iii_joint_two_month_crackdown_on_transnational_scams
- Thailand Government Public Relations Department (2025), 'Two Draft Bills on Cybercrime and Digital Asset Businesses Win Cabinet Approval', 9 April 2025. Available at: https://thailand.prd.go.th/en/content/category/detail/id/48/iid/380287
- United Nations Office on Drugs and Crime (2025), Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia. Available at: https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf
- United States Department of Justice (2025), 'Justice Department Announces Seizure of Tai Chang Scam Compound Domain Used in Cryptocurrency Investment Fraud', 2 December 2025. Available at: https://www.justice.gov/opa/pr/justice-department-announces-seizure-tai-chang-scam-compound-domain-used-cryptocurrency
- United States 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
- United States Attorney's Office for the District of Columbia (2026), 'Investigations into Cryptocurrency Scams Result in Seizure of More Than USD 25 Million', 21 July 2026. Available at: https://www.justice.gov/usao-dc/pr/investigations-cryptocurrency-scams-result-seizure-more-25-million
- United States Department of the Treasury (2025), 'Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams', 8 September 2025. Available at: https://home.treasury.gov/news/press-releases/sb0237
- United States Department of the Treasury (2025), 'Treasury Sanctions Burma Armed Group and Companies Linked to Organized Crime Targeting Americans', 12 November 2025. Available at: https://home.treasury.gov/news/press-releases/sb0312
- United States Secret Service (2020), 'Secret Service Announces Creation of the Cyber Fraud Task Force', July 2020. Available at: https://www.secretservice.gov/newsroom/releases/2020/07/secret-service-announces-creation-cyber-fraud-task-force
- United States Secret Service (undated), 'Digital Assets and Cryptocurrency Investigations'. Available at: https://www.secretservice.gov/investigations/digitalassets

Media and Supplementary Reporting

- Farge, E. (2026), 'UN Says Human Trafficking into Asian Scam Centres Is Surging', Reuters, 28 July 2026. Available at: https://www.reuters.com/legal/government/un-says-human-trafficking-into-asian-scam-centres-is-surging-2026-07-28/
- Naing, S. (2025), 'Over 200 Foreigners Rescued from Scam Centres Still Stranded Along Thai-Myanmar Border', Reuters, 24 June 2025. Available at:

https://www.reuters.com/world/asia-pacific/over-200-foreigners-rescued-scam-centres-still-stranded-along-thai-myanmar-2025-06-24/

- Reuters (2025), 'China to Fly Back 200 Nationals Rescued from Myanmar Scam Centres', 18 February 2025. Available at: https://www.reuters.com/world/asia-pacific/myanmar-detains-270-foreigners-scam-compounds-thai-border-2025-02-18/
- Reuters (2025), 'Chinese Extricated from Myanmar Scam Centres Fly Home via Thailand', 20 February 2025. Available at: https://www.reuters.com/world/asia-pacific/chinese-extricated-myanmar-scam-centres-fly-home-thailand-2025-02-20/
- Reuters (2025), 'Thousands in Limbo on Thai-Myanmar Border after Scam Centre Crackdown', 24 February 2025. Available at: https://www.reuters.com/world/asia-pacific/thousands-limbo-thai-myanmar-border-after-scam-centre-crackdown-2025-02-24/
- Reuters (2025), 'Some Foreigners Pulled out of Myanmar Scam Centres Face Struggle to Get Home', 28 February 2025. Available at: https://www.reuters.com/world/asia-pacific/some-foreigners-pulled-out-myanmar-scam-centres-face-struggle-get-home-2025-02-28/
- Reuters (2025), 'Scam Hubs on Thai-Myanmar Border Still Have Up to 100,000 People, Thai Police Says', 18 March 2025. Available at: https://www.reuters.com/world/asia-pacific/scam-hubs-thai-myanmar-border-still-have-up-100000-people-thai-police-says-2025-03-18/
- The Nation Thailand (2025), 'Even I Was Almost Fooled, Says Paetongtarn on AI Scam Encounter', 15 January 2025. Available at: https://www.nationthailand.com/news/general/40045195