Committee: INTERPOL
Topic: International Cooperation Against Cryptocurrency Fraud and Money Laundering.
Chair: Cesar Eduardo Martínez Garza
Moderator: Maria Regina Medrano Duque

Overview of the Problem

Criminals exploit borderless cryptocurrencies, such as Bitcoin, and digital wallets to transfer illicit funds across the globe. Victims may lose substantial sums before proceeds are moved through exchanges, intermediary services, or bank accounts in multiple jurisdictions. Individual law enforcement agencies cannot effectively combat these networks on their own. Countries affected by cryptocurrency-related fraud and laundering include Myanmar, Cambodia, Laos, Nigeria, Ghana, China, Canada, Russia, the UAE, Germany, France, U.S.A., Madagascar, Peru, and Colombia.

These countries can be grouped according to the role they may play in a particular scheme: places where scams originate or are organized, jurisdictions through which illicit funds are transferred or laundered, and countries where victims reside. These roles can overlap and may change as criminal networks relocate. The United States and Canada have reported substantial financial losses, particularly from “pig butchering” scams involving fraudulent investment platforms (FBI,2022). Key obstacles include the use of pseudonymous wallets, obfuscation techniques, cross-chain transfers, inconsistent regulations, delays in mutual legal assistance, and AI-enabled fraud.

Introduction

With the rise of cryptocurrencies, the global financial system is experiencing dramatic changes. Cryptocurrencies allow people and businesses to send money without fully depending on the conventional banking system. Although cryptocurrencies create new financial opportunities for people and organizations, their popularity has attracted criminal groups that exploit them for illegal purposes, including committing fraud, concealing illicit profits, and making illegal transfers.

Currency fraud occurs when people or businesses use dishonest methods to obtain the digital assets of others. Several examples of cryptocurrency fraud include fake investment websites, romance scams, impersonation scams, and fraudulent internet businesses. Another important concept is money laundering, which is the process of concealing illegal origins of money to make it appear that it was obtained legitimately. Money laundering consists of three stages: placement, layering, and integration. Criminals may use cryptocurrency exchanges, digital wallets, and transactions between different blockchain networks to make these activities more difficult to investigate.

One of the most concerning developments is the expansion of organized online scam centres. These facilities are frequently connected to international criminal networks that operate fraudulent investment schemes and other online scams. In certain cases, individuals working inside these compounds have been trafficked or forced to participate in criminal activities. This demonstrates that cryptocurrency-related crime is not exclusively a financial problem, since it can also be connected to human trafficking, cybercrime, and organized criminal activity (INTERPOL, 2026a; United Nations Office on Drugs and Crime [UNODC], 2025).

The international community should be concerned because these operations affect individuals, governments, and financial institutions around the world. Victims can lose substantial amounts of money, while criminal organizations use their profits to expand their activities. Furthermore, the movement of illicit funds between countries makes it difficult for national authorities to investigate these crimes without the assistance of other jurisdictions. In the United States alone, the Federal Bureau of Investigation reported approximately USD 11.366 billion in losses associated with cryptocurrency-related complaints during 2025 (Federal Bureau of Investigation [FBI], 2026).

The international criminal police organization (INTERPOL) is an intergovernmental organization responsible for facilitating cooperation between police authorities in its 196 member countries. Its main purpose is to connect national law enforcement agencies, allowing them to exchange information, coordinate investigations, and respond to

crimes that extend beyond national borders. Through resources such as its secure I-24/7 communication system, international police databases, and financial cooperation mechanisms, INTERPOL helps countries strengthen their investigative capabilities (INTERPOL, n.d.-a).

Addressing this issue through INTERPOL is particularly important because the organization can help connect countries that may otherwise struggle to investigate the same criminal network independently. However, it is important to understand that INTERPOL is not an international police force and cannot independently arrest individuals or impose financial regulations on member countries.

Its responsibilities are focused on facilitating cooperation and supporting national authorities. In this background paper, delegates will examine the current situation, the countries and organizations involved, and the obstacles that prevent effective international action. They will also consider how cooperation between governments, law enforcement agencies, and private companies can contribute to reducing cryptocurrency fraud and money laundering.

Historical Background

Bitcoin's first block, known as the genesis block, was created on January 3, 2009. Silk Road, an early large-scale darknet marketplace that used Bitcoin for transactions, began operating in approximately January 2011 and was seized by law enforcement on October 2, 2013. The case demonstrated how cryptocurrency could be used in illicit online markets (Blockstream, n.d.; European Union Agency for Drugs, n.d; U.S. Department of Justice, 2014). Early gaps in oversight of some cryptocurrency services also created challenges for identifying users and tracing illicit proceeds.

Over the following years, governments and international standard-setting bodies developed anti-money-laundering and counter-terrorist-financing expectations for virtual-asset service providers. FATF's guidance and later assessments have encouraged risk-based controls, customer due diligence, and information-sharing requirements for certain transfers (FATF, 2026a, 2026b). The United States has also

applied existing financial-crime laws to cases involving virtual currencies (Bank Secrecy Act, 1970; Money Laundering Control Act, 1986).
Strategies have included requiring major cryptocurrency exchanges to strengthen AML and KYC controls, as well as establishing partnerships with stablecoin issuers to freeze suspected criminal funds. These efforts have benefited from blockchain-forensic tools that can trace transactions long after they occur. By contrast, outright prohibitions on cryptocurrency transactions or mining, and attempts to eliminate decentralized privacy tools and smart contracts, have had limitations. Restrictions may push some activity out of regulated channels and into jurisdictions with less developed oversight.

The Situation Today

Cryptocurrency-related crime has become an increasingly important international concern because of the financial resources involved and the growing sophistication of criminal organizations. According to Chainalysis (2026), addresses associated with the illicit cryptocurrency activity received at least USD 154 billion during 2025, representing a 162% increase compared with its revised estimate for 2024. TRM Labs (2026) reported approximately USD 158 billion in illicit cryptocurrency flows during the same year.

These figures are estimates rather than direct measurements of money stolen from individual victims. They also reflect different analytical methodologies. Nevertheless, both organizations identify an increase in cryptocurrency-related criminal activity. At the same time, Chainalysis estimates that illicit activity represents less than 1% of overall cryptocurrency transaction volume, showing that most cryptocurrency activity remains legitimate.

An important development is the increasing use of stablecoins. Although these digital currencies provide a relatively stable way to transfer money internationally, criminals may exploit them to move and conceal illicit funds. Chainalysis (2026) estimates that stablecoins represented approximately 84% of identified illicit cryptocurrency transaction

volume during 2025. FATF (2026) has also warned about the risks associated with stablecoins and transactions involving privately controlled digital wallets.

The financial consequences are particularly evident in the United States. The FBI's 2025 Internet Crime Report recorded 181,565 complaints involving cryptocurrency and approximately USD 11.366 billion in associated losses. Individuals aged 60 and older experienced more than USD 4.4 billion in cryptocurrency-related losses, demonstrating how these schemes can affect ordinary people, particularly vulnerable populations (FBI, 2026).

Another major concern is the expansion of online scam centres, especially in Southeast Asia. Criminal organizations frequently use fraudulent employment advertisements to recruit individuals from different countries. Some victims are transported to compounds where their documents are confiscated and they are forced to conduct online scams. INTERPOL (2026a) identifies these operations as a growing international threat connected to financial fraud and human trafficking.

UNODC estimated that online scam operations across East Asia, Southeast Asia, Australia, and New Zealand caused losses between USD 88.3 billion and USD 114.1 billion during 2025, according to Reuters (McPherson, 2026). These figures refer to online scams generally, not exclusively cryptocurrency fraud. Criminal organizations have also relocated their operations when authorities increased enforcement efforts, making isolated national actions insufficient.

Money laundering networks have also become increasingly organized. Criminal groups use cryptocurrency exchanges, offshore companies, intermediary services, and different blockchain networks to conceal the origins of their funds. One example is Cambodia-based Huione Group. In October 2025, the US Financial Crimes Enforcement Network (FinCEN) restricted the group's access to the American financial system because of its connections to illicit financial activity (FinCEN, 2025).

Despite these difficulties, international operations have demonstrated the importance of cooperation. In 2025, INTERPOL's Operation HAECI VI involved 40 countries and

territories, resulting in approximately USD 439 million in recovered assets. Authorities also blocked more than 68,000 bank accounts and froze nearly 400 cryptocurrency wallets (INTERPOL, 2025).

Another important initiative was Operation First Light 2026, which involved 97 countries and territories. The operation resulted in 5,811 arrests, approximately USD 293 million in intercepted assets, more than 142,000 identified victims, and 31,014 blocked bank accounts (INTERPOL, 2026a).

In March 2026, INTERPOL also announced Operation Shadow Storm, supported by the United Kingdom's Home Office. Its objective is to investigate the financial networks behind scam centres and identify connections involving fraud, money laundering, and human trafficking (INTERPOL, 2026a).

Different regions face different challenges. Southeast Asia continues to experience the presence and relocation of scam centre operations, while North America reports substantial financial losses. European countries have established regulatory frameworks such as MiCA and rules concerning information accompanying certain crypto-asset transfers. Meanwhile, countries across Africa, Latin America, and the Pacific may face limitations in investigative resources and technological infrastructure. (European Union, 2023a, 2023b)

FATF’s 2026 assessment found that 83% of surveyed jurisdictions had introduced legislation implementing the Travel Rule, compared with 73% in 2025. However, several countries continue to experience difficulties enforcing these requirements effectively (FATF, 2026a). This demonstrates that international cooperation requires not only legislation but also the resources and institutional capabilities necessary to apply it.

Key Stakeholders and Their Positions

INTERPOL’s member nations participate in international operations against cryptocurrency fraud and money laundering. However, their priorities differ according to

their financial systems, economic influence, and enforcement capabilities. They can be divided into three main groups.

1. Heavily Regulated Financial Destination Nations: United States, the United Kingdom, Singapore, Japan, South Korea are major financial destinations seeking stricter cryptocurrency regulations, stronger transaction monitoring, harsher penalties, and the recovery of illicit funds. These countries are pushing for monetary security and transparency, and backed heightened scrutiny of digital transactions to track financial crime. However, this focus on monitoring is a source of contention between privacy advocates and nations leaning toward less stringent regulations on cryptocurrency.

2. Financial Transit and Regional Hubs: Thailand and other countries serving as regional financial transit points face challenges involving the movement of illegal money across borders. The principal objectives in this regard are improving cross-border cooperation, enhancing reporting capabilities, and preventing crime syndicates from using loopholes between the jurisdictions. However, the problem faced by the authorities is that tightening restrictions may impede their economic objectives related to the accessibility of financial services and foreign investments.
3. Capacity-Constrained and Vulnerable States: Eswatini, Uganda, Nigeria, and Palau face challenges in introducing advanced financial oversight systems because of insufficient technical resources and enforcement capabilities. Their priorities include getting international technical support, bolstering the legislation, recovering misappropriated assets, and fighting human trafficking and other crimes linked to illegal financial networks. However, their interests may conflict with those of nations subject to strict regulations: the demands imposed by the international norms for the provision of requisite resources are difficult to fulfill.

These categories represent different regulatory priorities rather than formal political alliances. Heavily regulated financial destinations generally support stronger KYC

requirements, transaction monitoring, and rapid asset recovery. In contrast, financial transit hubs may prioritize maintaining accessible financial services and attracting international investment while preventing criminal exploitation. Capacity-constrained states tend to emphasize financial assistance, technical training, and gradual implementation of international standards. These differences create competing interests regarding financial privacy versus government surveillance, immediate asset freezing versus judicial due process, and international regulatory obligations versus national sovereignty. Understanding these differences is essential for developing solutions that can be accepted by countries with different economic and institutional capabilities.

INTERPOL does not act alone. It relies on extensive work of various international organizations fighting the same crimes. For instance, the UNODC trains judges and prosecutors worldwide in digital forensics to handle complex cryptocurrency laundering cases. The World Bank and the IMF develop risk assessment models to help countries establish appropriate legislation. The World Bank also analyzes the opportunities for taking advantage of public and open blockchain technology in order to minimize losses from public bribery.

These international organizations focus on maintaining institutional stability, global integrity, and a coherent international legal system. They regard cryptocurrency crimes as a systematic threat to worldwide advancement because fraud takes public funds, facilitates tax evasion, and finances terrorism and drug trafficking, thus undermining economies of developing countries.

A number of fintech companies and banks collaborate with the FBI to eliminate phishing networks and coordinate removing fraudulent applications. Moreover, cryptocurrency exchanges and companies developing blockchain and AI technologies create software to track transactions in real time and cooperate with banks and law enforcement agencies in assigning a risk level to wallets and compliance scores. As a result, suspicious transactions can be tracked and frozen once transferred into a bank system

through off-ramps. Such companies seek to minimize the risk of legal and financial liability.

The Basel Institute on Governance holds international meetings with Europol and the United Nations in order to enhance cooperation between anti-money laundering professionals and the NGO field. Moreover, in their work, charities stick to rigorous internal cryptocurrency policies, making use of custodial wallets and automated software for donation verification and assessment of the involvement of donations in unlawful activities.

Finally, victims of cryptocurrency scams and money laundering demand justice and compensation for their financial losses. Meanwhile, ordinary people desire a safer financial environment in which they conduct transactions without fear of being scammed.

Past Attempts and Existing Frameworks

International organizations have implemented a variety of conventions, operational task forces, and regulatory frameworks to fight these crimes. Those actions are based on a coordinated approach that combines INTERPOL's law enforcement networks, United Nations legal frameworks, and FATF compliance rules.

The United Nations Convention against Transnational Organized Crime (UNTOC), and adopted by the General Assembly on November 15, 2000, provides a framework for international cooperation against organized crime (United Nations General Assembly, 2000). On March 28, 2019, the Security Council adopted Resolution 2462, which addresses the prevention and suppression of terrorist financing (United Nations Security Council, 2019). UNODC's October 2024 regional report also examines criminal networks that exploit digital technologies and underground banking in Southeast Asia (UNODC, 2024).

The United States has applied existing financial laws, including the Bank Secrecy Act and the Money Laundering Control Act of 1986, to financial activity involving digital assets (Bank Secrecy Act, 1970; Money Laundering Control Act, 1986). Blockchain analytics and digital-forensic tools can help investigators trace transactions and identify suspects. However, criminal activity may shift toward less-regulated over-the-counter (OTC) desks, peer-to-peer (P2P) networks, and decentralized-finance (DeFi) platforms, where enforcement can be more difficult because there may be no centralized operator (UNODC,2024)

In Southeast Asia, initiatives like HAECHI VI and First Light 2026, in combination with INTERPOL's I-GRIP system, have aided international efforts with cross-border investigations and have helped some countries, including Singapore and Thailand, to freeze illicit funds fairly quickly. However, the existence of loopholes in the legislation, political instability, corruption, and lack of resources available to law enforcement agencies made way for large scam networks, which are sometimes connected to human trafficking and organized criminal activities. For example, in the Golden Triangle Special Economic Zone in Laos, weak enforcement procedures give criminals the opportunity to move their operations when authorities attempt to intervene.

Cooperation between Europol, Eurojust, and regional authorities has helped dismantle large-scale deepfake advertising networks and cryptocurrency fraud platforms across several European countries, including Belgium, Bulgaria, Germany, and Spain. Efforts to bolster anti-money laundering and counter-terrorist financing frameworks in countries such as Georgia, Moldova, and Ukraine have been further supported by an OSCE-UNODC partnership. Bureaucratic delays are still a major hurdle as formal international judicial cooperation, such as MLA Treaties, could take weeks or even months. Furthermore, by the time cross-border orders are issued, stolen funds may have passed through several blockchain bridges and decentralized mixers, making those funds harder to trace and recover.

In Latin America, the governments of Brazil and Chile have clearly increased the reporting requirements for fiat money and cryptocurrency by expanding KYC rules to

local OTC trading venues, making it easier to identify illicit funds. However, inadequate institutional stability, diverging judicial rulings, and dependence on conventional banking laws have complicated the regulation of decentralized cryptocurrencies. These shortcomings have allowed large drug cartels to create financial networks that use cryptocurrency to launder their money through commercial front companies.

These international initiatives still have many gaps when it comes to dealing with this issue. First of all, there is no unified international viewpoint on how to treat decentralized protocols such as DAOs, smart contracts, and decentralized software. Second, the absence of any international standards in blockchain intelligence tools and definitions creates complications in international investigation and prosecution, while the lack of specialized training leads law enforcement to confuse fraud with money laundering. Finally, the pace of criminal procedures is still way too slow in comparison to the rapid pace of the token economy.

Challenges and Complications

International law enforcement faces institutional barriers, even with arrests being made. Cooperation can be weakened by political conflicts and competing national interests. One documented example of state-linked cryptocurrency activity concerns the Democratic People's Republic of Korea (DPRK). In a report dated October 22, 2025, the Multilateral Sanctions Monitoring Team (MSMT), a group of 11 participating governments, reported that its members contributed at least USD 1.19 billion from January through September 2025. The latter figure included the February 2025 theft of approximately USD 1.4 billion from the Bybit exchange. The report stated that DPRK actors used cryptocurrency services in multiple jurisdictions to launder stolen assets before attempting to convert them into traditional currency (MSMT, 2025). These findings concern identified state-linked actors and should not be generalized to the populations or businesses of the jurisdictions mentioned in the report.

Some nations that may not have extradition treaties with the requesting state, and INTERPOL Red Notices do not themselves require a country to arrest or extradite an individual. National authorities decide what action to take under domestic laws.

Many law enforcement agencies lack the resources, trained personnel, and advanced technologies needed to investigate these crimes. Often, blockchain investigators and cybersecurity specialists work for private companies that pay much higher wages than government agencies do. On top of that, the expensive blockchain-tracking software is still unavailable for many developing countries as well as local law enforcement agencies.

Criminal organizations continuously take advantage of technological advances to hide stolen money. Cross-chain bridges allow cryptocurrency to move from one blockchain to another, complicating investigations. Self-hosted wallets are not managed by a centralized service provider, which can limit the ability of authorities to obtain information or request action from an intermediary. Artificial intelligence can also make fraud more convincing, while law enforcement agencies may lack the tools and training to respond.

Hawala, associated particularly with South Asia, and Fei Ch'ien, associated with China, are examples of informal value-transfer systems discussed in research on remittances and cross-border transfers (Kapur, 2004). UNODC's 2024 report describes informal settlement arrangements in East and Southeast Asia, including offsetting arrangements similar to Hawala, and explains that criminal networks may misuse such systems (UNODC, 2024). These systems also serve legitimate communities and should not be treated as inherently criminal. Legal approaches to cryptocurrency differ among countries; delegates should consult specific national laws and authoritative legal interpretations rather than generalize about entire regions or religious communities.

Finally, the fear of being blamed for fraudulent actions prevents victims from reporting scams, limiting the information available to authorities and complicating investigations.

The Committee's Role and Powers

INTERPOL's main responsibility is to facilitate cooperation between national police authorities. Its 196 member countries are connected through National Central Bureaus, which communicate with INTERPOL's General Secretariat. Through its secure I-24/7 network, countries can exchange information and access international police databases (INTERPOL, n.d.-a).

Regarding cryptocurrency fraud and money laundering, INTERPOL can coordinate investigations, provide technical assistance, exchange intelligence, support international operations, and use I-GRIP to help countries respond to suspicious financial transfers. It can also issue Notices and Diffusions when the applicable requirements are met. (INTERPOL, 2025)

However, INTERPOL cannot independently arrest suspects, impose financial regulations, or force governments to freeze assets. FATF establishes anti-money laundering standards, UNODC supports efforts against organized crime and human trafficking, and national governments remain responsible for enforcing their laws and prosecuting offenders. (FATF, 2026a).

During this Model United Nations committee, delegates must represent their assigned countries, research their national policies, and participate in formal debate. They will work together to develop a resolution containing practical recommendations within INTERPOL's responsibilities. All proposals should respect national sovereignty, international law, human rights, and the political neutrality of the organization.

Guiding Questions for Debate

1. In what ways can global entities formulate a cohesive legal framework for offenses related to cryptocurrencies without violating the independence of each country?
2. Do decentralized organizations and smart contracts need to answer for their part in criminal offenses, and if so, who is responsible when no overseeing body is present?

3. What measures can countries adopt to unify the usage of tools for tracking blockchain transactions and accessing digital evidence?
4. What action can international organizations take to improve judicial education and prevent misunderstanding and misclassification of cryptocurrency fraud crimes?
5. What options do countries have to halt, seize, and return the assets derived from crime prior to their being transferred through many blockchains by criminals?
6. How can international structures such as INTERPOL foster cross-border investigations without compromising the sovereignty of nations?
7. Is it necessary to provide financial and technical assistance to countries with less effective regulatory systems, and if so, which coordination strategies are to be employed?
8. In what ways are governments able to monitor decentralized financial (DeFi) sectors without hindering the technological progress and privacy of their clients?

Conclusion and Call to Action

Cryptocurrency fraud and money laundering have become serious international challenges affecting financial security, national institutions, and ordinary individuals. Although digital financial systems provide opportunities for innovation, criminal organizations continue to exploit them to expand their operations across national borders. Recent investigations demonstrate that these activities cannot be effectively addressed without cooperation between governments, police institutions, and private companies.

INTERPOL provides an important opportunity for countries to exchange information and coordinate investigations. However, international action must also consider differences in national legislation, resources, and political priorities. Strengthening investigative capabilities, protecting victims, and improving financial information-sharing procedures are essential steps toward an effective response.

Delegates must understand that the objective is not to restrict legitimate cryptocurrency use, but to prevent criminal organizations from exploiting digital financial systems. Through research, diplomatic negotiation, and international cooperation, they have the opportunity to develop practical solutions that respect national sovereignty and human rights. Building a safer international financial environment requires countries to work together, ensuring that technological progress does not become an advantage for organized crime.

References

INTERPOL. (2025, September 24). *USD 439 million recovered in global financial crime operation.*https://www.interpol.int/en/News-and-Events/News/2025/USD-439-million-recovered-in-global-financial-crime-operation

Financial Action Task Force. (2026, March 3). *Targeted Report on Stablecoins and Unhosted Wallets.* https://www.fatf-gafi.org/en/publications/Virtualassets/targeted-report-stablecoins-unhosted-wallets.html

United Nations Office on Drugs and Crime (UNODC). (n.d.). *Annual Report 2025.* https://www.unodc.org/documents/AnnualReport/UNODC_REPORT_2025_web_15_June.pdf

Europol. (n.d.). *International takedown of cryptocurrency fraud network laundering over EUR 700 million.* https://www.europol.europa.eu/media-press/newsroom/news/international-takedown-of-cryptocurrency-fraud-network-laundering-over-eur-700-million

INTERPOL. (n.d.). *INTERPOL report warns of increasingly sophisticated global financial fraud threat.* https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat

McPherson, P., & Perry, M. (2026, July 21). *Crime gangs snare more than $88 billion in scams in Asia-Pacific, UN says.* Reuters. https://www.reuters.com/legal/government/crime-gangs-snare-more-than-88-billion-scams-asia-pacific-un-says-2026-07-21/

United Nations Office on Drugs and Crime (UNODC). (2026). *Non-Punishment of Victims of Trafficking.*

https://www.unodc.org/documents/human-trafficking/ICAT/19-10800_ICAT_Issue_Brief_8_Ebook.pdf

INTERPOL. (2026, July 9). *Over 5,800 arrests, USD 293 million intercepted in global fraud bust.* https://www.interpol.int/en/News-and-Events/News/2026/Over-5-800-arrests-USD-293-million-intercepted-in-global-fraud-bust

European Union. (2023, May 31). *Regulation (EU) 2023/1113.* EUR-Lex. https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng

Financial Action Task Force (FATF). (2026, July 16). *Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs.* https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtualassets-vasps-2026.html

TRM Labs. (n.d.). *Tackling Crypto Crime 2023 Survey of Law Enforcement – Report.* https://www.trmlabs.com/reports-and-whitepapers/tackling-crypto-crime-2023-survey-of-law-enforcement

United Nations Office on Drugs and Crime (UNODC). (2024, October 16). *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape.* https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

TRM Labs. (n.d.). *2026 Crypto Crime Report – Illicit Crypto Trends & Typologies.* https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report

TRM Labs. (2026, January 28). *2026 Crypto Crime Report – Illicit Crypto Trends & Typologies.* https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report

Chainalysis. (2026, January 8). *2026 Crypto Crime Report Introduction.* https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/

Chainalysis. (n.d.). *2026 Crypto Crime Report: Scams.* https://www.chainalysis.com/blog/crypto-scams-2026/

Europol. (n.d.). *Cryptocurrencies: Tracing the Evolution of Criminal Finances.* https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

INTERPOL. (2025). *What Is INTERPOL?* https://www.interpol.int/en/Who-we-are/What-is-INTERPOL

Office of the United Nations High Commissioner for Human Rights (OHCHR). (2026, February 20). *Wicked Problem: Seeking Human Rights-Based Solutions to Trafficking for Cyber Scam Operations.* https://bangkok.ohchr.org/reports/wicked-problem-seeking-human-rights-based-solutions-trafficking-cyber-scam-operations

Federal Bureau of Investigation (FBI). (2022, October 3). *[Cryptocurrency investment schemes].* https://www.ic3.gov/PSA/2022/PSA221003

INTERPOL. (2025, September 24). *USD 439 million recovered in global financial crime operation.* https://www.interpol.int/en/News-and-Events/News/2025/USD-439-million-recovered-in-global-financial-crime-operation

Financial Crimes Enforcement Network (FinCEN). (2025, October 14). FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System

https://www.fincen.gov/news/news-releases/fincen-issues-final-rule-severing-huione-group-us-financial-system

United Nations Office on Drugs and Crime (UNODC). (n.d.). *Annual Report 2025.* https://www.unodc.org/documents/AnnualReport/UNODC_REPORT_2025_web_15_June.pdf

Global Initiative Against Transnational Organized Crime. (2025, May 29). *Compound Crime: Cyber Scam Operations in Southeast Asia.* https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/

Europol. (n.d.). *International Takedown of Cryptocurrency Fraud Network Laundering over EUR 700 Million.* https://www.europol.europa.eu/media-press/newsroom/news/international-takedown-of-cryptocurrency-fraud-network-laundering-over-eur-700-million

INTERPOL. (2026, March 16). *INTERPOL Report Warns of Increasingly Sophisticated Global Financial Fraud Threat.* https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-th

McPherson, P., & Perry, M. (2026, July 21). *Crime Gangs Snare More Than $88 Billion in Scams in Asia-Pacific, UN Says.* Reuters. https://www.reuters.com/legal/government/crime-gangs-snare-more-than-88-billion-scams-asia-pacific-un-says-2026-07-21/

United Nations Office on Drugs and Crime (UNODC). (2026). *Non-Punishment of Victims of Trafficking.* https://www.unodc.org/documents/human-trafficking/ICAT/19-10800_ICAT_Issue_Brief 8_Ebook.pdf

INTERPOL. (2026, July 9). *Over 5,800 Arrests, USD 293 Million Intercepted in Global Fraud Bust.* https://www.interpol.int/en/News-and-Events/News/2026/Over-5-800-arrests-USD-293-million-intercepted-in-global-fraud-bust

European Union. (2023, May 31). *Regulation (EU) 2023/1113.* EUR-Lex. https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng

Financial Action Task Force (FATF). (2026, July 16). *Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs.* https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtual ssets-vasps-2026.html

TRM Labs. (n.d.). *Tackling Crypto Crime 2023 Survey of Law Enforcement – Report.* https://www.trmlabs.com/reports-and-whitepapers/tackling-crypto-crime-2023-survey-of-law-enforcement

United Nations Office on Drugs and Crime (UNODC). (2024, October 16). *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape.* https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

TRM Labs. (n.d.). *2026 Crypto Crime Report – Illicit Crypto Trends & Typologies.* https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report

Chainalysis. (2026, January 8). *2026 Crypto Crime Report Introduction.* https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/

Chainalysis. (n.d.). *2026 Crypto Crime Report: Scams.* https://www.chainalysis.com/blog/crypto-scams-2026/

Europol. (n.d.). *Cryptocurrencies: Tracing the Evolution of Criminal Finances.* https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf