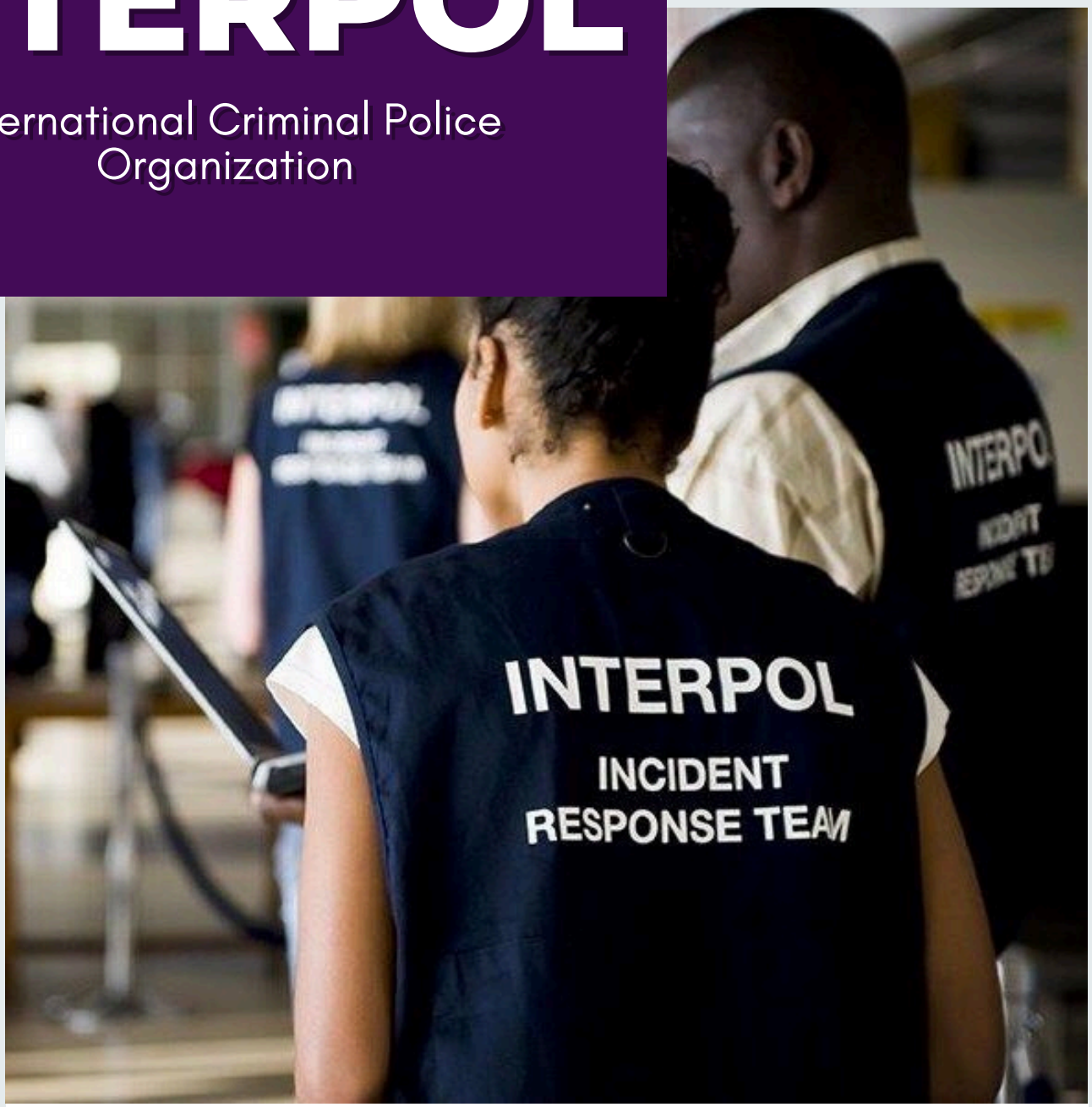
NIMUN' 26

INTERPOL

International Criminal Police Organization

STUDYGUIDE



INTERNATIONAL CRIMINAL POLICE ORGANIZATION

Topic: Combating Cyber-Enabled Financial Crime and Cryptocurrency Laundering

Table of Content

1. Glossary & Key Terms 4

2. Committee Overview 6

2.1 Mandate and Responsibilities 6

2.2 Structure and Coordination Mechanism 6

3. Introduction to the Agenda 7

3.1 Digital Transformation & Erasure of Boundaries 7

3.2 Cryptocurrency-Enabled Money Laundering 7

3.3 Why It's Among the Fastest-Growing Threats 7

3.4 Scale, Global Impact & Multi-Jurisdictional Nature 8

4. Background of the Agenda 8

4.1 Evolution of Online Fraud & Cyber-Financial Crime 8

4.2 Shift from Fiat Laundering to Crypto Schemes 8

5. International Cooperation & Past Operations 9

6. Case Studies 10

6.1 Past Implications 10

6.1.1 Case Study 1: Global Cyber-Enabled Financial Crime Crackdown

6.1.2 Case Study 2: Cryptocurrency Mixing Services and Large-Scale Money Laundering

6.2 Present Implications 11

6.2.1 Case Study 3: Systemic Financial Harm Through Online Investment Fraud

7. Challenges to Combating Cyber-Financial Crime 13

8. INTERPOL Tools, Systems & Mechanisms (Crypto/Financial Crime) 14

9. State Responses to Cyber-Enabled Financial Crime 15

10. Questions A Resolution Must Answer (QARMA) 15

11. Bibliography 16

Authors & Contributions

Editorial Oversight: Zainab Fawad - Director Publications

Editors

Safa Nasar – Deputy Director Publications

Saifullah Shamim – Deputy Director Publications

Coordinators

Mahad Saeed – Director Secretariat Affairs

Contributing Authors

Team	Authors
Publications	***Muhammad Abdul Wasey***
Secretariat Affairs	***Ayesha Usman***
	Gul Sheh Bano

1. Glossary & Key Terms

1. **Cryptocurrency (Virtual Asset)** is defined as a digital representation of value, such as Bitcoin or Ether, that can be transferred or exchanged electronically using blockchain technology. Cryptocurrencies enable peer-to-peer transactions without reliance on a central bank and often provide pseudonymity rather than full anonymity.
2. **Virtual Asset Service Providers (VASPs)** are entities that conduct activities involving cryptocurrencies, including exchanges, custodial wallets, brokers, and transfer services. Under Financial Action Task Force (FATF) standards, VASPs are required to implement Anti-Money Laundering (AML) and Know Your Customer (KYC) obligations.
3. **Money Laundering** refers to the process of disguising the illegal origin of funds to make them appear legitimate. In cryptocurrency ecosystems, laundering commonly occurs through mixers, cross-chain transfers, layered conversions, and unregulated exchanges.
4. **Mixer / Tumbler** is a service that blends cryptocurrency from multiple users to obscure the transaction trail between sender and receiver, significantly complicating forensic analysis and often facilitating the laundering of illicit funds.
5. **The FATF "Travel Rule"** is an international AML standard requiring VASPs to collect and transmit accurate information about the sender and recipient of cryptocurrency transfers above a specified threshold, aiming to reduce anonymity while balancing privacy and compliance concerns.
6. **Privacy Coins** are cryptocurrencies, such as Monero or Zcash, that obscure transaction details including the sender, recipient, and transaction amount, thereby making blockchain tracing extremely difficult for regulators and law enforcement.
7. **Decentralized Finance (DeFi)** refers to financial services operating on blockchain networks without centralized intermediaries, including decentralized exchanges, lending platforms, and liquidity pools, which present significant regulatory and enforcement challenges.
8. **Cross-Chain Bridges** are protocols that allow the transfer of digital assets between different blockchain networks, fragmenting transaction histories and frequently enabling fund layering during laundering processes.
9. **On-Chain Transactions** are cryptocurrency transfers that are permanently recorded on a public blockchain ledger, while Off-Chain Transactions involve transfers conducted

through private databases, fiat systems, or exchange accounts, often used as exit points by criminal networks.

10. **Wallet Clustering and Chain Analytics** are blockchain forensic techniques used to group multiple wallet addresses believed to be controlled by a single entity and trace suspicious transaction patterns, though such methods may occasionally result in false positives.
11. **Suspicious Transaction Reports (STRs)** are formal disclosures submitted by financial institutions and VASPs to regulatory or law enforcement authorities when transactions appear to involve money laundering, fraud, or other illicit activity.
12. **I-GRIP (Global Rapid Intervention of Payments)** is INTERPOL's real-time payment-freezing mechanism designed to rapidly block suspicious fiat and cryptocurrency transactions before funds can be transferred across borders.
13. **Custodial Wallets** are services in which a third party, usually an exchange, controls users' private keys, allowing regulatory oversight and potential asset seizure, whereas Non-Custodial Wallets give users full control over their assets, limiting enforcement reach.
14. **Sanctions Evasion** via Cryptocurrency refers to the use of digital assets to transfer value around sanctioned individuals, entities, or jurisdictions, raising international compliance, security, and geopolitical concerns.
15. **Smurfing** is a money laundering technique in which large illicit sums are divided into numerous smaller transactions to evade AML detection thresholds and reporting mechanisms.
16. **Off-Ramps (Fiat Conversion Points)** are exchanges, over-the-counter desks, or payment providers where cryptocurrencies are converted into traditional fiat currencies, often representing the final stage of the laundering process.
17. **Decentralized Autonomous Organizations (DAOs)** are blockchain-based entities governed by smart contracts and collective token-holder voting, with unclear legal status and accountability frameworks.
18. **Wrapped Assets and Synthetic Tokens** are digital representations of assets issued on alternative blockchains, complicating asset provenance, tracing, and enforcement actions.
19. **Seizure vs. Forfeiture** distinguishes the temporary control of assets during investigations from the permanent transfer of ownership to the state following judicial proceedings.
20. **Mutual Legal Assistance (MLA)** refers to formal international cooperation mechanisms through which states request evidence, extradition, or asset recovery assistance, a process that is essential but often time-consuming.

21. Artifact Evidence includes non-blockchain materials such as server logs, metadata, exchange records, and KYC documentation that support attribution, tracing, and prosecution.
22. **Privacy-Preserving Anti-Money Laundering (PP-AML)** refers to emerging compliance techniques, such as zero-knowledge proofs, that seek to balance user privacy with regulatory oversight and financial transparency.

2. Committee Overview

The International Criminal Police Organization (INTERPOL) is a global police-cooperation body linking 196 member countries.

Headquartered in Lyon, France, INTERPOL facilitates information-sharing and coordination among national law enforcement agencies to combat transnational crime. Its central hub, the General Secretariat, supports a National Central Bureau (NCB) in each member state as the point of contact.

INTERPOL's mandate covers major crime areas – terrorism, organized crime, human trafficking, cybercrime, financial crime, etc. – but it has no power to arrest or prosecute on its own. Instead, it relies entirely on member states: it issues alerts (such as color-coded Notices), shares intelligence, and coordinates joint operations, but arrests and enforcement are carried out by national authorities. INTERPOL's strength lies in its global reach and information networks, not in direct enforcement.

2.1 Mandate and Responsibilities

INTERPOL's core mission is to enable international police cooperation by maintaining secure communications networks and global crime databases for member countries. Through its General Assembly and Executive Committee, it sets priorities and policy, and works with public–private partnerships to combat emerging threats such as cyber-enabled financial crime and money laundering.

To support this coordination, INTERPOL uses a system of color-coded Notices and Diffusions: Red Notices request the provisional arrest of fugitives, Blue Notices seek additional information, Orange Notices warn of new threats, Purple Notices share criminal modus operandi, and the Silver Notice traces and recovers criminal assets.

These Notices and databases significantly expand INTERPOL's global reach, but they also highlight a core limitation: INTERPOL cannot arrest, detain, or seize assets itself. Every action must be executed by national authorities.

2.2 Structure and Coordination Mechanism

INTERPOL's structure is federal, consisting of the General Secretariat, Regional Bureaus, and National Central Bureaus in each member country. The Command and Coordination Centre operates 24/7.

Specialized units include the Cybercrime Directorate and the Financial Crime & Anti-Corruption Centre. The I-24/7 secure communications network enables real-time data sharing across all NCBs. INTERPOL also maintains extensive databases on stolen documents, fingerprints, DNA, wanted persons, and known criminals.

3. Introduction to the Agenda

3.1 Digital Transformation & Erasure of Boundaries

The financial world has undergone a digital transformation: banking, payments and commerce have largely moved online, and cryptocurrencies offer new, borderless ways to transfer value. This blurs traditional boundaries: crimes like fraud and money laundering that used to require physical banks or local shell companies can now occur entirely over the internet. Organized crime groups exploit this shift. INTERPOL's recent assessments warn that AI, large language models and crypto enable more sophisticated fraud without advanced skill.

In effect, criminals can target victims globally via phishing, deepfake scams, romance baiting and other schemes, using digital tools to scale operations across countries. One INTERPOL official calls it an "epidemic" of financial fraud powered by new technologies.

In this context, cyber-enabled financial crime has become a pervasive global threat, requiring transnational response.

3.2 Cryptocurrency-Enabled Money Laundering

Cryptocurrencies add to the risk. Virtual assets (Bitcoin, Ether, stablecoins, etc.) offer pseudonymity and instantaneous cross-border transfers. Criminals use tools like mixers/tumblers and privacy coins to obfuscate transactions. (FATF notes that "tumblers and mixers are services that use various methods to conceal the connection between the address sending VA and the address receiving VA".)

Illicit funds can be moved through decentralized exchanges (DEXs) and cross-chain bridges, making tracing difficult. Criminals also exploit regulatory gaps: some crypto exchanges and Virtual Asset Service Providers (VASPs) operate in low-regulation jurisdictions or without KYC. The global reach of crypto means that once laundered, tainted funds can flow anywhere, undermining all borders.

3.3 Why It's Among the Fastest-Growing Threats

Experts highlight how quickly these crimes can spread. INTERPOL reports that criminals are fusing "cryptocurrencies with phishing- and ransomware-as-a-service" to run advanced fraud at low cost. A fraud campaign that might once have hit one country can now victimise thousands worldwide in minutes. Unlike older schemes, an algorithmic or automated fraud does not burn out easily. INTERPOL Secretary-General Jürgen Stock warns that, with AI and crypto, "the situation is only going to get worse without urgent action".

In addition, these crimes often generate high profits: law enforcement is seizing ever-larger sums (see below), which in turn attracts more investment by criminals. Thus cyber-enabled financial crime is not only prolific but growing rapidly in scale.

3.4 Scale, Global Impact & Multi-Jurisdictional Nature

A defining feature of this agenda is scale: a single international syndicate can defraud, extort or launder money on multiple continents simultaneously. For example, one single cyberattack or scam might involve hackers in country A, servers in country B, exchanges in C, and victims globally. This complexity means no single state can tackle it alone. Moreover, many victims are ordinary people: as INTERPOL notes, vulnerable individuals worldwide have lost millions to online scams like romance fraud and business email compromise.

These crimes can destabilize economies (e.g. large-scale Ponzi schemes), fund terrorism or organized crime, and undermine trust in financial systems. Because the networks are

global and continually shifting servers and currencies, dismantling them requires constant international coordination.

4. Background of the Agenda

4.1 Evolution of Online Fraud & Cyber-Financial Crime

Online fraud has evolved dramatically since the early 2000s. Initially, cybercrime meant simple phishing emails or fake websites. Today, schemes are highly sophisticated and global. Criminals now run networked fraud rings (often using call centers) that operate 24/7 in multiple countries. They combine techniques – for instance, "romance baiting" scams on dating apps, sextortion, spear-phishing, and business email compromise – often aided by AI (e.g. deepfake voices or chatbots).

INTERPOL's 2024 assessment warns that criminals are deploying AI and large language models to craft convincing scams, and using hybrid methods (like combining romance fraud with cryptocurrency investment fraud) to better target victims. Similarly, malware and ransomware attacks have surged; victims often pay ransoms in crypto and then rely on mixers to launder it. These trends reflect the co-evolution of technology and crime: just as legitimate finance becomes digital, criminals harness the same tools to expand their reach.

4.2 Shift from Fiat Laundering to Crypto Schemes

Traditionally, money launderers relied on banks, shell companies, trade-based schemes, or physical cash smuggling. Now, many turn to crypto-enabled laundering. Common crypto laundering techniques include: using mixers/tumblers to break links between origin and destination; converting crypto through unregulated exchanges or OTC brokers; employing privacy coins (like Monero) that obscure sender/receiver; and moving funds across cross-chain bridges to muddy the trail. These methods can be layered: for example, a criminal might convert stolen fiat to crypto, send it through several mixers or hops, cash out to another cryptocurrency, and finally off-ramp it via an exchange in a jurisdiction with lax checks. Each step can span countries, making the money trail almost invisible. These innovations have outpaced regulators. In response, bodies like the Financial Action Task Force (FATF) have updated guidelines for Virtual Assets and VASPs (e.g. the 2019–2021 "travel rule"), but many countries still lag. The result: jurisdictions with weak regulation or enforcement become safe havens for crypto laundering. As FATF warns, "without proper regulation, virtual assets also risk becoming a safe haven for the financial

transactions of criminals and terrorists". In effect, global regulatory gaps create "significant loopholes" that criminals exploit.

5. International Cooperation & Past Operations

INTERPOL has conducted several major operations targeting cyber-financial crime. The HAECHI series (I–VI, 2020–2025) are international crackdowns on fraud and crypto laundering. For example, HAECHI VI (Apr–Aug 2025) spanned 40 countries, uncovering seven fraud types (phishing, romance scams, sextortion, investment fraud, gambling ML, BEC, e-commerce fraud). This operation blocked 68,000 bank accounts and froze 400 crypto wallets, recovering over USD 439 million (342M in fiat, 97M in cash/crypto). Another earlier operation (Dec 2023) resulted in ~3,500 arrests and USD 300 million in seized assets.

These successes relied on rapid data-sharing: INTERPOL's Global Stop-Payment tools like I-GRIP (launched 2022) enable member banks to freeze suspect transactions in real time. Since I-GRIP's launch, INTERPOL reports intercepting over USD 500 million in illicit proceeds.

Beyond INTERPOL, Europol (EU police agency) has led major busts in Europe. Europol coordinated a June 2025 probe that dismantled a crypto fraud ring in Spain which had laundered €460 million ($540M) through a worldwide network. Other national efforts (e.g. the UK's "Operation Destabilise") have disrupted laundering networks tied to drugs and even sanctions evasion.

UN bodies also support this fight: the UN Office on Drugs and Crime (UNODC) promotes adoption of international AML conventions and trains police in digital forensics. Tech companies and banks now frequently partner with law enforcement – for example, INTERPOL's African "Contender" operation (Sept 2025) against romance scams involved private-sector data analysis from firms like Group-IB and Trend Micro. These collaborations and policy frameworks (FATF standards, UN conventions) form a growing architecture for tackling cyber-financial crime.

6. Case Studies

6.1 Past Implications

6.1.1 Case Study 1: Global Cyber-Enabled Financial Crime Crackdown (INTERPOL Operation HAECHI Series, 2020–2025)

Between 2020 and 2025, INTERPOL conducted a series of multinational enforcement operations collectively known as the Operation HAECHI initiative, aimed at combating cyber-enabled financial crimes such as online investment fraud, romance scams, business email compromise (BEC), phishing schemes, and cryptocurrency laundering. These operations were designed to address the rapid growth of online financial fraud during and after the COVID-19 pandemic, which saw criminal networks increasingly exploit digital platforms and cross-border payment systems.

Operation HAECHI relied on cooperation between national law enforcement agencies, financial intelligence units, banks, Virtual Asset Service Providers (VASPs), and cybersecurity firms across more than 40 countries. The operational strategy focused on identifying fraudulent payment flows, freezing suspicious bank and cryptocurrency accounts, dismantling criminal infrastructure, and arresting high-value suspects. The scale of the operation was unprecedented in INTERPOL's financial crime mandate, reflecting the transnational and highly networked nature of cyber fraud.

By the sixth phase of the operation (HAECHI VI, 2025), law enforcement authorities had blocked over 68,000 bank accounts and frozen hundreds of cryptocurrency wallets, recovering an estimated USD 439 million in stolen assets. The operation revealed that many cybercrime syndicates operated hybrid financial models—combining traditional bank transfers, shell companies, and cryptocurrencies to rapidly move stolen funds across jurisdictions before victims or authorities could respond.

Despite its success, the operation demonstrated critical structural challenges. Freezing accounts often required rapid responses from national authorities, and delays in mutual legal assistance allowed criminals to dissipate funds. The case highlights both the effectiveness and limitations of INTERPOL's coordination role, illustrating the urgent need for real-time cross-border payment interruption mechanisms and standardized regulatory cooperation across jurisdictions.

6.1.2 Case Study 2: Cryptocurrency Mixing Services and Large-Scale Money Laundering (Cryptomixer.io Takedown, 2016–2025)

Cryptocurrency mixers, also known as tumblers, have emerged as a central infrastructure for laundering illicit digital assets. One of the most prominent examples was cryptomixer.io, a Bitcoin mixing service that operated internationally for nearly a decade. The service allowed users to obscure the origin of cryptocurrency funds by pooling transactions and redistributing them, severely limiting blockchain traceability.

Cryptomixer.io became heavily associated with ransomware groups, darknet markets, and large-scale online fraud operations. Investigations later revealed that billions of euros in illicit cryptocurrency had passed through the platform. Law enforcement agencies in Switzerland and Germany, supported by Europol and INTERPOL-linked intelligence sharing, coordinated a multi-year investigation that culminated in the seizure of cryptomixer.io's servers, domains, and associated infrastructure in December 2025.

Authorities confiscated significant volumes of data—including transaction logs and internal records—along with over €25 million worth of cryptocurrency. This digital evidence enabled investigators to de-anonymize previous transactions and trace funds linked to ransomware, drug trafficking, and online scam networks. While the takedown severely disrupted money-laundering operations, experts warned that mixers are easily replaceable and can rapidly reappear under new identities.

This case illustrates how decentralized financial tools, when left unregulated, can enable industrial-scale money laundering. It also exposes legal gaps, as mixer services often operate in jurisdictions with unclear legal classification, raising complex questions about criminal liability, encryption rights, and freedom of software development.

The takedown of cryptomixer.io exposed the scale of mixer-enabled laundering and legal gaps surrounding decentralized services.

6.2 Present Implications

By 2024–2025, cyber-enabled financial crime had evolved into a systemic global crisis affecting individuals, corporations, and governments alike. Cybercriminal organizations increasingly rely on automated tools, artificial intelligence, and cryptocurrencies to

conduct fraud at unprecedented scale. Phishing campaigns now target thousands of victims simultaneously across continents, while deepfake technology is used to impersonate executives and manipulate payment systems.

In the financial sector, cryptocurrency investment scams—often advertised through social media and messaging platforms—have resulted in billions of dollars in losses worldwide. Victims are lured into fake trading platforms and persuaded to move funds through multiple crypto wallets, making recovery increasingly difficult. These losses disproportionately affect elderly individuals, migrant populations, and first-time digital finance users.

At the same time, underserved regions—particularly parts of Africa, Southeast Asia, and Latin America—have been affected by the emergence of cybercrime "call centers" where organized groups conduct romance scams and investment fraud targeting victims in wealthier countries. These operations exploit regulatory asymmetries, limited cybersecurity capacity, and slow international cooperation mechanisms, allowing criminal networks to thrive across borders with limited consequences.

The rapid digitization of financial services has also placed enormous pressure on law enforcement agencies, many of which lack the technical expertise to conduct blockchain forensics or the legal authority to compel cryptocurrency platforms to cooperate. As a result, enforcement often lags behind innovation, allowing criminal networks to adapt faster than regulatory frameworks.

6.2.1 Case Study 3: Systemic Financial Harm Through Online Investment Fraud (Global Crypto Scam Networks, 2019–Present)

Large-scale cryptocurrency investment fraud schemes represent one of the most damaging forms of cyber-enabled financial crime. Since 2019, transnational scam networks have operated fraudulent investment platforms that imitate legitimate cryptocurrency exchanges and trading applications. Victims are recruited through social media advertisements, dating platforms, and messaging applications, where scammers cultivate trust before directing funds into controlled wallets.

Investigations indicate that many of these networks operate from physical compounds in Southeast Asia, West Africa, and Eastern Europe, employing hundreds of individuals to manage victim communications. Once funds are

deposited, victims are shown false "profits" through manipulated dashboards, encouraging further deposits. When withdrawal is attempted, accounts are blocked and funds are laundered through mixers, cross-chain bridges, and offshore exchanges.

The long-term consequences have been severe. Victims often lose life savings, pensions, or borrowed funds, leading to debt, mental health crises, and social hardship. Law enforcement responses remain fragmented due to jurisdictional boundaries, while asset recovery rates remain extremely low once funds are moved into decentralized finance ecosystems

This case highlights the human cost of cyber-enabled financial crime and underscores the importance of preventive regulation, global awareness campaigns, and rapid-response financial interdiction mechanisms. It also raises ethical questions about platform accountability, especially where social media companies profit from advertisements used to perpetrate fraud.

7. Challenges to Combating Cyber-Financial Crime

7.1 Jurisdictional Fragmentation and Legal Inconsistencies

A core obstacle is the patchwork of national laws governing cybercrime, crypto-assets, and financial investigations. Criminals exploit this fragmentation: evidence, servers, or suspects located in one country may be legally unreachable from another. Many regions lack clear crypto-asset regulations or strong anti–money laundering (AML) enforcement, effectively creating "safe havens" for cyber-financial criminals. As a result, even when INTERPOL issues alerts or coordinates operations, inconsistent legal frameworks limit the speed and scope of action.

7.2 Rapid Technological Evolution Outpacing Regulation

Technology in the cyber-financial space evolves far faster than national regulatory systems. Criminals adopt privacy coins, decentralized finance (DeFi) protocols, AI-driven laundering methods, and automated obfuscation tools long before lawmakers can respond. Decentralized services—such as unhosted wallets, cross-chain bridges, and mixers—lack centralised control points, making traditional investigative techniques ineffective. This

regulatory lag allows criminals to innovate constantly while law enforcement remains reactive.

7.3 Limited Technical Capacity and Operational Gaps

Many countries, particularly in the developing world, lack the technical expertise, digital forensics units, and blockchain-analytics tools needed to investigate cyber-financial crimes. Without strong stop-payment systems, blockchain tracing capabilities, or trained cyber units, local police may be unable to act on INTERPOL intelligence. Time lags in detection and response intensify the problem—by the time a fraudulent scheme is identified, criminals have typically already moved funds offshore, converted them into cash, or layered them across multiple chains.

7.4 Weak Operational Coordination and Dependence on National Action

INTERPOL facilitates information-sharing and can coordinate freezes or alerts, but final action always depends on national authorities. If local police, banks, or prosecutors do not act immediately—whether on a Red Notice, a diffusion, or an I-GRIP alert—illicit funds can disappear within minutes. Slow domestic procedures, bureaucratic delays, or limited institutional capacity allow suspects to escape and assets to dissipate. Victim underreporting further reduces available intelligence, making coordinated responses even more difficult.

7.5 Trust Deficits and Insufficient Cross-Border Information-Sharing

Cyber-financial crime is inherently transnational, yet many jurisdictions remain hesitant to share data or rely on foreign agencies. Differences in privacy laws, institutional mistrust, or geopolitical tensions hinder smooth cooperation. INTERPOL's Secretary-General emphasized the need to "close existing gaps and ensure information sharing… is the norm, not the exception." Without consistent cross-border trust, even the best technological or legal tools fail to achieve meaningful impact against sophisticated criminal networks.

8. INTERPOL Tools, Systems & Mechanisms (Crypto/Financial Crime)

1. **Notices & Diffusions:** INTERPOL continues to use its notice system (Red, Blue, Orange, Purple, Silver, etc.) to alert all members about wanted persons, new fraud methods, threats to victims, and assets to trace. The new Silver Notice (2025) specifically targets criminals'

assets (bank accounts, properties, vehicles) enabling police to locate and seize laundered funds.

2. **I-24/7 Secure Network:** The real-time I-24/7 network connects all NCBs for instant communication. Through it, officers can swiftly exchange alerts (e.g. flagging suspect IP addresses, wallet addresses or phone numbers), vastly increasing responsiveness.
3. **Cyber and Financial Crime Units:** INTERPOL's specialized units (e.g. Cybercrime Directorate, IFCACC) analyze data from operations and issue intelligence products on emerging trends. They coordinate task forces against cyber-enabled fraud and maintain centralized watchlists of stolen virtual assets.
4. **Stop-Payment & Asset-Freeze (I-GRIP/ARRP):** INTERPOL's Global Rapid Intervention of Payments (I-GRIP) and Anti-Money Laundering Rapid Response Protocol (ARRP) allow member states to freeze suspect bank or crypto transactions in real time. Since its launch in 2022, I-GRIP helped intercept over USD 500 million in proceeds from cyber fraud. These mechanisms let police "hit the brakes" on illicit transfers instantly, working across borders with partner banks.
5. **Public–Private Collaboration:** Law enforcement increasingly partners with financial and tech companies. For example, in the Pan-African cybercrime operation described above, INTERPOL cited cooperation with cybersecurity firms (Group-IB, Trend Micro) which provided data that helped identify suspects. Similarly, analysts from blockchain intelligence companies often assist investigations by tracing crypto flows.
6. **National Central Bureaus (NCBs):** Each member's NCB serves as the pivot for that country's participation. Some NCBs have deployed liaison officers to work directly with cryptocurrency exchanges, banks and regulators. INTERPOL also provides training and capacity-building through its networks, helping member states improve KYC enforcement and digital forensics.

9. State Responses to Cyber-Enabled Financial Crime

FATF-aligned / Developed Countries (e.g. EU, USA, UK): These countries generally have robust AML/CFT regimes and strict regulation of VASPs. Exchanges must register, conduct KYC ` checks. Ideally, these hubs aim to balance innovation and regulation: allowing fintech growth while enforcing transparency rules to prevent abuse. Developing Regions (e.g. parts of Africa, South Asia): Many face capacity gaps. Regulatory frameworks may be incomplete or just emerging. Law enforcement often lacks expertise or tools for crypto tracing. As a result, criminals

sometimes target these regions as safe channels: for example, using unregulated peer-to-peer crypto markets or informal money changers to launder funds. These countries therefore rely heavily on capacity-building support from organizations like UNODC and INTERPOL, as well as guidance from FATF-style regional bodies. High-Risk Jurisdictions (e.g. certain West African states, parts of Southeast Asia): In places where supervision is weak and oversight sparse, there is a higher risk of hosting both scammers and laundering operations. For example, illicit "call centers" conducting romance scams or fake investment schemes have been found in some West African nations. Similarly, digital nomad hubs in Southeast Asia have attracted cybercriminal forums. International partners often focus on these areas with targeted training and law-enforcement missions to address the vulnerabilities. Major Victim Countries (e.g. large EU economies, USA): Wealthy countries with advanced economies tend to be targets of ransomware and investment fraud. They have more resources for enforcement and victim assistance, but also more at stake in securing their financial systems. Such countries often lead global initiatives (funding INTERPOL projects, pushing for Asset Recovery protocols, sanctioning foreign facilitators) because they suffer significant losses and see themselves as first responders.

10. Questions A Resolution Must Answer (QARMA)

1. Should INTERPOL be empowered to request temporary cross-border crypto asset freezes?
2. Should global AML/KYC standards be mandated for all VASPs?
3. Should cross-border MLA for crypto be fast-lane prioritized?
4. Should VASPs integrate standardized chain-analytics sharing with INTERPOL?
5. Should INTERPOL establish a global Crypto Asset Registry?

11. Bibliography

1. Europol. (2025). Europol supports dismantling of global cryptocurrency fraud ring. Europol Press Release.
2. Europol. (2025). Cryptomixer.io taken offline in coordinated European operation. Europol Newsroom.
3. Financial Action Task Force (FATF). (2019). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF, Paris.
4. Financial Action Task Force (FATF). (2023). Targeted Update on Implementation of the FATF Standards on Virtual Assets. FATF.
5. INTERPOL. (2023). Global Rapid Intervention of Payments (I-GRIP) Factsheet. INTERPOL.
6. INTERPOL. (2024). Global Financial Fraud Assessment. INTERPOL Strategic Analysis Report.
7. INTERPOL. (2025). Operation HAECHI VI disrupts global cyber-enabled financial crime. INTERPOL News.
8. INTERPOL. (2025). INTERPOL introduces the Silver Notice for asset tracing. INTERPOL Press Release.
9. INTERPOL. (n.d.). About INTERPOL. INTERPOL Official Website.
10. National Crime Agency (United Kingdom). (2025). Operation Destabilise: disrupting international money laundering networks. NCA Press Release.
11. United Nations Office on Drugs and Crime (UNODC). (2022). Cybercrime and Anti-Money Laundering Strategies. UNODC.
12. United Nations Office on Drugs and Crime (UNODC). (2023). Global Programme on Cybercrime. UNODC.
13. Reuters. (2025). European police dismantle €460 million cryptocurrency fraud ring. Reuters Investigations.
14. Reuters. (2025). Germany and Switzerland shut down major bitcoin mixing service. Reuters World News.
15. INTERPOL. (2024). Financial Fraud Assessment: A global threat boosted by technology. – Global assessment of cyber-enabled fraud trends, including crypto-enabled scams.
16. INTERPOL. (2025, June 30). INTERPOL releases new information on globalization of scam centres. – On global spread of scam centers, human-trafficking-fueled fraud, use of cryptocurrencies and AI.

17. INTERPOL. (2025). USD 439 million recovered in global financial crime operation. (Operation HAECHI VI) — Seizure of fiat & virtual assets; freezing crypto wallets; cross-border cooperation.
18. INTERPOL. (2024, November 27). Financial crime operation makes record 5,500 arrests, seizures worth over USD 400 million. (Operation HAECHI V) — Demonstrates scale of enforcement against cyber-enabled fraud / money laundering.
19. Europol / Eurojust / European & Swiss-German authorities. (2025, December 1). Crypto-mixing service used to launder money taken down (Cryptomixer.io). — Official takedown of a major mixer; seizure of servers, crypto assets, data.
20. Europol. (2025). Europol seizes $29M bitcoin laundering "cryptomixer". — Details of seizure; underscores ongoing crackdown on mixers used for illicit flows.
21. Europol & partners. (2025). Authorities seize $1.51B Bitcoin-mixing service ("Cryptomixer") after long-running laundering operations. — Highlights the historic scale of mixer-enabled laundering since 2016.
22. (2025). "Bitcoin Mixer Tied to €1.3 Billion in Illicit Flows Taken Down by European Authorities." — Academic/industry-oriented report summarizing mixer shutdown and laundering volume.
23. (2025). Analysis of selected cryptocurrency mixers: behavior analysis and law-enforcement challenges. — Research exploring mixer behavior and implications for AML efforts.
24. (2025, April 16). Topological Analysis of Mixer Activities in the Bitcoin Network — Uses blockchain-graph analysis to identify structural patterns of mixer operations; relevant to your technical discussion of mixers.
25. (2025). MPOCryptoML: Multi-Pattern based Off-Chain Crypto Money Laundering Detection — Recent ML-based model for detecting off-chain crypto laundering patterns, shows academic advance in detection technology.
26. (2025). A Graph Machine Learning Approach for Detecting Topological Patterns in Transactional Graphs — Graph-ML framework proposing improved detection of complex laundering schemes in both crypto and fiat networks.
27. (2025). Beyond Static Datasets: Behavior-Driven Entity-Specific Simulation to Train Effective Crypto AML Models — Addresses data scarcity in crypto-AML research; proposes simulation-based dataset generation for training detection models.

28. (2025). Cryptocurrencies as a Tool for Money Laundering: Risk Perceptions and Regulatory Implications — Examines how financial-sector professionals perceive crypto risk and laundering, offering insight into regulatory/policy dimensions.
29. (2023). Internet Organised Crime Threat Assessment (IOCTA) 2024 by Europol — Offers systemic overview of how cryptocurrencies and crypto-enabled laundering appear in broader organised crime and financial-crime trends.
30. (2024). Article: "Technology boosting global financial crime" — summarizing how new technologies (crypto, AI) have amplified global fraud and money laundering risks.
31. (2024). As part of UNODC / global crime studies: use of crypto & mixing services in organized financial crime (see UNODC issue papers referencing mixer risks) — relevant for background on international regulatory context and global crime convergence.
32. (2025). News: major cross-border crypto investment fraud ring dismantled (2025, Spain) — laundering of €460 million ($540 M) via crypto and traditional banking/exchange channels; arrests made.
33. (2023). Shutdown of another mixer, ChipMixer — evidence of long-standing mixer crackdowns; highlights persistence of laundering tools and law-enforcement efforts.
34. (2024). News on global "scam centres" and human-trafficking-fueled crypto fraud, showing geographic expansion into West-Africa, Middle East, etc. — underscores multi-regional threat.
35. (2024). Public-private cooperation emphasised by INTERPOL's Global Fraud Summit (March 2024) — highlights need for cross-sector collaboration, data sharing, regulatory harmonization.
36. (2025). Research on mixers and tumblers — technical and forensic challenges for law enforcement and compliance communities.
37. (2025). Statistical and ML-based analysis of crypto-asset laundering risks and detection, pointing toward emerging detection tools and methods.
38. (2025). Comparative analysis of cryptocurrency risk perceptions in the financial sector vs. actual illicit-finance use — useful for policy discussion and regulatory design.
39. (2024–2025). Multiple Europol / INTERPOL operations (HAECHI V & VI, mixer takedowns, global fraud assessments) together illustrating evolving legal and enforcement landscape — useful for your "Background," "Challenges," and "Tools & Mechanisms" sections.