INTERPOL

GLOBAL FINANCIAL FRAUD THREAT ASSESSMENT

SECOND EDITION

MARCH 2026

Disclaimer

All reasonable precautions have been taken by INTERPOL to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall INTERPOL be liable for damages arising from its use. INTERPOL takes no responsibility for the continued accuracy of that information or for the content of any external website.

This report has not been formally edited. The content of this publication does not necessarily reflect the views or policies of INTERPOL, its Member Countries, its governing bodies or contributory organizations, nor does it imply any endorsement. The boundaries and names shown and the designations used on any maps do not imply official endorsement or acceptance by INTERPOL. The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of INTERPOL concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

INTERPOL General Secretariat
200, quai Charles de Gaulle
69006 Lyon
France
Telephone + 33 4 72 44 70 00
Fax + 33 4 72 44 71 63
Web: www.INTERPOL.int
E-mail: info@INTERPOL.int

Contents

Secretary General's Foreword

Fraud is now a part of everyday life. It could start with an unsolicited text message, a convincing request by email or an online offer that seems too good to be true.

As digital technologies become increasingly central to how we live and work, opportunities for fraud have expanded, making it a shared challenge for individuals, businesses and governments worldwide.

Today, fraud is one of the most significant threats facing law enforcement. It increasingly sits at the centre of polycriminality, intersecting with organized crime, human trafficking and cybercrime.

The proceeds of fraud are often laundered and used to finance other serious offences, directly impacting global security and economies. Addressing fraud therefore requires a clear understanding of its scale, impact and role within wider criminal networks and financial systems.

This second edition of the INTERPOL Global Financial Fraud Threat Assessment examines how the fraud landscape has evolved over the past two years, highlighting key trends and emerging threats. It places particular focus on artificial intelligence, reflecting its growing influence on the scale and nature of fraud.

Fraud causes harm on a vast scale, with estimated losses reaching hundreds of billions of US dollars per year. But its impact is not just financial, with victims also commonly suffering lasting emotional harm.

A compassionate response is essential to encourage reporting and support recovery.

Because fraud crosses borders and sectors, collective action is critical. INTERPOL remains committed to supporting our global membership to address this global fraud epidemic through stronger international cooperation, intelligence sharing and coordinated action.

I invite you to read this report as a call to awareness and action. Together, we can strengthen our response, reduce fraud and prevent harm. Together, against financial crime.

Valdecy Urquiza
INTERPOL Secretary General

Acknowledgement

This report has been produced following analysis of information gathered from a variety of sources, including INTERPOL member countries, international organizations, academia, and private sector partners. Additionally, intelligence drawn from INTERPOL systems and datasets have been leveraged to inform and enrich the report, ensuring a comprehensive understanding of the complex dynamics and challenges related to financial fraud. We gratefully acknowledge the financial support from the United Kingdom as well as all the contributions of member countries and all external organizations that have provided valuable insights to inform this report.

CITY OF LONDON POLICE

EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS

GASA Global Anti-Scam Alliance

GLOBAL COALITION TO FIGHT FINANCIAL CRIME

ISEC Connecting experts

Meta

UNIVERSITY OF PORTSMOUTH

WORLD ECONOMIC FORUM

Key Findings

The second edition of the INTERPOL Global Financial Fraud Threat Assessment highlights that since 2024 financial fraud targeting individuals and businesses has continued to increase in volume, innovate in modus operandi, and expand globally.

The key findings include:

- **Law enforcement authorities collaborating more effectively against financial fraud.** Since 2024, the number of fraud-related Notices and Diffusions has increased by 54 per cent, the majority issued by European member countries. Over the same period, INTERPOL has supported member countries in more than 1,500 transnational fraud cases in lost assets valued at USD 1.1 billion.
- **Significant global and human costs due to financial fraud.** Global losses related to financial fraud in 2025 alone have been estimated at USD 442 billion.[1] Beyond financial damage, individual victims commonly experience shame and psychological trauma. INTERPOL assesses the overall global risk related to financial fraud as HIGH and expects the scale of offending to escalate significantly over the next three to five years, mainly due to increased availability of AI technology and low barriers to entry.
- **Global spread of scam centres.** Initially, scam centres emerged as a regional phenomenon. However, the trend has now evolved into a global threat, with centres discovered across multiple regions. These centres engage hundreds of thousands of people, many of whom are forced to perpetrate online frauds. To date victims from nearly 80 countries have been trafficked into online scam centres, with no continent left untouched.
- **Fraud increasingly enabled by artificial intelligence tools.** Dark Web marketplaces offer applications which can clone voices and faces from mere seconds of genuine audio or video samples, enabling criminals to impersonate celebrities or associates of intended victims. "Agentic AI" can autonomously plan and execute fraud campaigns from start to finish. INTERPOL reports a global surge in these AI-enhanced fraud schemes, notably sextortion, intertwined with investment scams, as well as impersonation frauds, including fake kidnappings for ransom.
- **Criminal networks cooperating globally, sharing expertise and technology.** Criminal networks perpetrating fraud adapt their illicit business models to optimize efficiency, including through collaboration with specialized money laundering networks. INTERPOL assesses these offenders as highly organized, skilled and agile.
- **An increasing nexus between financial fraud and terrorist financing across the African region.** Terrorist groups operating in the African region have been found to rely on fraud schemes for resource generation, especially via crypto-based scams.

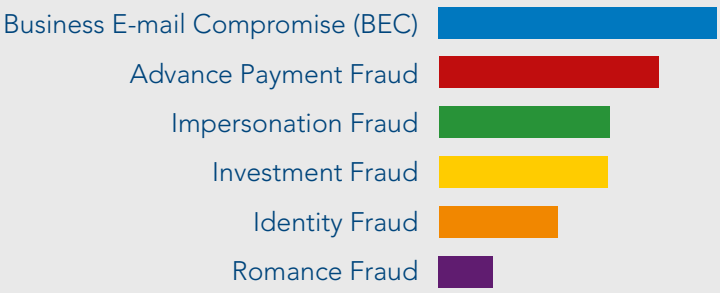
1 According to the 2025 estimate provided by the Global Anti-Scam Alliance.


12 021 3801 12 021 3801
12 021 3801
021 3801 12 021 3801

Global Trends in Financial Fraud

Financial Fraud among the TOP 5 Global Crime Threats

Top Global Financial Fraud Threats Facing Law Enforcement in 2024 and 2025



77% of global business leaders reported rising fraud in 2025

73% personally affected or impacted through their network

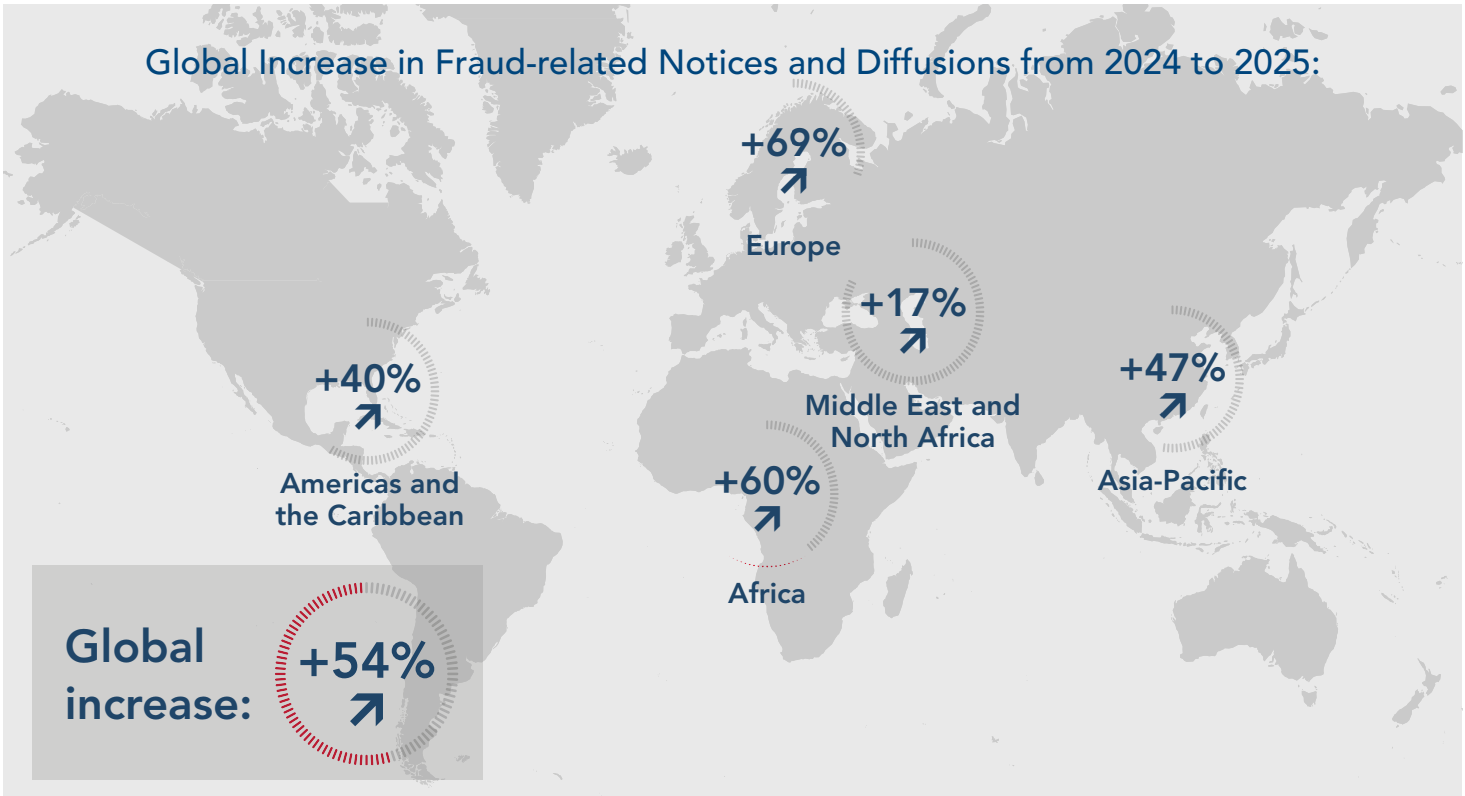
World Economic Forum, 2025

I-GRIP

More than **1,000** requests per year in 2024 and 2025.

HUNDREDS OF THOUSANDS of victims from more than 80 nationalities worldwide trafficked for the purpose of forced online financial fraud.

Global Increase in Fraud-related Notices and Diffusions from 2024 to 2025:



Global increase: +54%

Introduction

While digital innovation is empowering individuals and businesses globally, it is also increasing the effectiveness and efficiency of offenders who commit transnational crime. As this report details, the digital revolution has had a particular impact on the scale and nature of financial fraud, resulting in this crime becoming one of the most serious faced by INTERPOL member countries today.

The increasing technological sophistication of transnational crime syndicates enables them to obscure the origin of funds, effectively circumventing established regulatory oversight and complicating international asset recovery efforts. This shift requires unprecedented levels of cross-border law enforcement cooperation and intelligence sharing to disrupt the flow of illicit capital.

In particular, the proliferation of generative AI has lowered the barriers for entry into fraud, with criminal actors utilizing deepfake technology and automated models to execute hyper-realistic social engineering and synthetic identity fraud at scale. These advancements have rendered traditional detection methods and prevention messaging largely ineffective, necessitating a pivot towards adaptive, AI-driven defence mechanisms.

Drawing on INTERPOL's own intelligence, data from member countries, information from a global network of trusted partners and publicly available information from trusted sources where appropriate, this Assessment offers updated analysis on the global threat posed by contemporary financial fraud. This report identifies the top fraud threats targeting individuals and institutions, how fraud trends are currently evolving, the impact on victims and systemic vulnerabilities enabling these crimes. In addition to assessing the threat, this report also aims to set a strategic foundation for coordinated, technologically proficient, cross-border action to dismantle the criminal infrastructures underpinning this global crisis.

Financial Fraud Types and Trend Updates

Advance-payment Fraud

Advance-payment Fraud involves a financial transaction for fraudulent products or services. Perpetrators may use online commercial website, social media platforms, or other means for promoting sales of in-demand goods and services at sub-market prices. Payment is requested up front and prior to the reception of any product or service, which may either be non-existent or significantly sub-standard.

Information indicates increases in employment fraud, inheritance fraud, and "lottery" fraud, all of which involve deceiving victims into paying fees upfront, under the false pretence of registering for a job, claiming an inheritance, or unlocking a non-existent prize. INTERPOL data indicates that the African region is a primary target for this fraud trend.

Business Email Compromise

Business Email Compromise (BEC), also known as Chief Executive Officer (CEO) fraud, is a prevalent form of impersonation fraud, whereby criminals use social engineering techniques to target businesses. By compromising email accounts and impersonating executives, the fraudsters manipulate employees into transferring funds to suspect accounts in order that the diverted funds can be quickly laundered.

Globally, BEC was the most frequently reported fraud type to INTERPOL through operations and requests for investigative support from member countries. The majority of these reports originated from the Asia and Pacific and European regions, supporting the assessment that individuals and entities in these two regions are highly impacted and most frequently targeted for this type of fraud.

Impersonation Fraud

Impersonation Fraud occurs when an offender poses as a person or an institution with whom the victim has, or could have, a pre-existing, real relationship. For example, the offender might impersonate a public official, a service provider (such as a tech support assistant), or an acquaintance (in the case of extortion fraud). Impersonation fraud typically relies on eliciting fear or worry to deceive their victim.

Over the past two years, INTERPOL has observed a rising form of impersonation fraud involving fake kidnapping scams, where criminals use AI-generated images and videos of victims' loved ones to demand ransoms.

Another rising trend known as "quishing," relies on malicious QR codes, exploiting the convenience and trust associated with QR technology to bypass traditional security measures. Fraudsters distribute tampered QR codes via email, SMS, public posters, digital ads, or online marketplaces, presented as legitimate links to trusted service providers—such as banks, payment platforms, or government portals. When scanned, these codes redirect victims to fraudulent websites designed to mimic authentic interfaces, luring them to enter personal data, download malware, or approve fraudulent transactions.

The framework for assessing financial fraud in this report stems from an operational, law enforcement definition of the crime, encompassing a wide array of "illegal activities that have the aim of financial gain through deceptive actions against and to the detriment of an individual or entity."[2] As society, technology, and regulations evolve, so do the tactics and methodologies of fraudsters, requiring continuous understanding and adaptation by law enforcement. The following is an overview of the financial fraud types observed by INTERPOL and a highlight of current and emerging crime trends over 2024 and 2025.[3]

2 This Assessment focuses on the commission of financial fraud against individuals and private entities, thus excluding fraud committed against the government or public administration.

3 For consistency, the typologies used to categorize financial fraud from INTERPOL operational data are based on the agreed definitions set in the 2024 report.

Identity Fraud

Identity Fraud refers to the unauthorized acquisition and use of an individual's personal information (usernames, passwords, credit card credentials, biometric data, etc.) for illicit financial gain. Fraudsters can gain access to personal information through social engineering (such as phishing, smishing, vishing, spoofing, etc.), system intrusion (via the use of malware or hacking techniques) and physical theft. Identity fraud is therefore comprised of two elements: on the one hand, the manipulative technique to obtain a victim's personal data and, on the other hand, the fraud tactic by which this data will be misused. Identity fraud can be perpetrated without the direct involvement of the victim, for example when personal data has been obtained through theft. In addition to stealing funds, fraudsters often sell victims' personal information through online dark markets for further exploitation by criminals.

INTERPOL has detected an increase in synthetic identity fraud facilitated by AI in reports from member countries. Synthetic identity fraud results in the creation of a "new" identity based on real and fake information generated by AI. In this context, child identity theft for financial fraud is a particularly concerning new trend. Fuelled by childhood photos and personal details unknowingly shared by parents, the theft and exploitation of a minor's identity to commit fraud often goes undetected until the victim reaches adulthood.[4]

PHISHING:
A fraudulent attempt to steal sensitive data by disguising as a trustworthy entity via email or fake websites.

SMISHING:
A form of phishing conducted via deceptive text messages (SMS).

VISHING:
A voice-based phishing where scammers use phone calls to deceive victims.

SPOOFING:
The act of falsifying communication identifiers (like caller ID, email address, or website URL) to appear as a trusted source.

Insurance Fraud

Insurance Fraud involves any intentional act designed to deceive an insurance company during the application or claims process, or to mislead an insurer regarding the denial of a legitimate claim. It encompasses various forms, including, false claims, misrepresentation, premium fraud and staged accidents.

Information strongly suggests that this type of fraud, notably involving car or medical insurance claims, has been escalating globally, greatly aided by digital technologies. INTERPOL data suggests that Western and Eastern Europe are the regions most targeted by insurance fraud.

For instance, the UK saw a 25 per cent spike in motor insurance fraud driven by false applications and identity theft in early 2025.[5] In France, the detection of fraud cases increased significantly in 2024, accounting for nearly USD 1 billion.[6] Similarly, insurers in Germany flagged 10 per cent of claims as suspicious, with annual losses exceeding USD 7 billion, mainly targeting motor insurance.[7]

4 'It Takes an Industry: Combatting the Rise of Child Identity Theft', LSEG Risk Intelligence,June 2025, https://thesource.lseg.com/thesource/getfile/index/c56dadae-7a0e-49c5-af0e-9ac2c3c71908 (Accessed 23 November 2025)

5 'AI fuels surge in identity fraud, as people sell their personal information - Fraudscape six-month report', CIFAS, 5 August 2025, https://www.cifas.org.uk/newsroom/fraudscape-2025-6monthupdate (Accessed 5 February 2026)

6 'Fraude à l'assurance, Agence de Lutte contre la Fraude à l'assurance', ALFA, 20 August 2025, www.alfa.asso.fr/fraude-a-lassurance/#chiffres-cles (Accessed 6 February 2026)

7 'Insurance fraud causes damage of over six billion euros a year', GDV, 2 May 2024, https://www.gdv.de/gdv/medien/medieninformationen/versicherungsbetrug-verursacht-schaeden-von-ueber-sechs-milliarden-euro-im-jahr-176852 (Accessed 6 February 2026)

Investment Fraud

Investment Fraud consists of manipulating people into investing money in fake or misleading ventures, usually through online platforms, for example investment/trading applications controlled by perpetrators, resulting in significant financial losses for the victims. Fraudsters use various deceptive tactics, including promising high returns, misrepresenting investments and creating a sense of urgency. Investment fraud schemes often adopt operating models such as pyramid and Ponzi schemes. Additionally, in many investment fraud schemes, victims do not incur losses at the outset. Fraudsters often return the initial capital along with purported profits to build credibility and trust. Once the victim increases their investment, believing the scheme to be legitimate, the fraudster withdraws access and absconds with the funds.

Investment fraud results in some of the highest financial losses to individual victims. Current trends involve investing in phoney virtual assets (crypto-investment scams) or fictitious real estate. Victims of investment fraud are often doubly victimized: after losing money through a fake investment, offenders often re-contact victims—posing as international law firms, recovery agents, or law enforcement agencies—with false promises of retrieving their stolen funds.

Romance Baiting

Romance Baiting combines romance and crypto-investment frauds. Offenders initiate contact with potential victims via social media, dating apps, or direct messages akin to romance fraud. After establishing trust and confidence, criminals subsequently motivate victims to invest in fraudulent investment schemes, promising high returns. For example, victims may be provided with fraudulent applications controlled by perpetrators, which manipulate cryptocurrency trades and display inflated profits, to motivate victims to invest. Romance baiting victims have also reported being subsequently targeted for "recovery fraud," a form of re-victimization by yet another fraudster, aggravating both financial loss and psychological trauma.

Romance baiting modus operandi presents unique challenges to law enforcement, particularly due to the use of cryptocurrencies. INTERPOL analysis indicates that this fraud-type, which was initially primarily linked to organized crime syndicates from Eastern Asia, emerged in Southeast Asia but has since spread globally to Africa, Latin America and Europe.

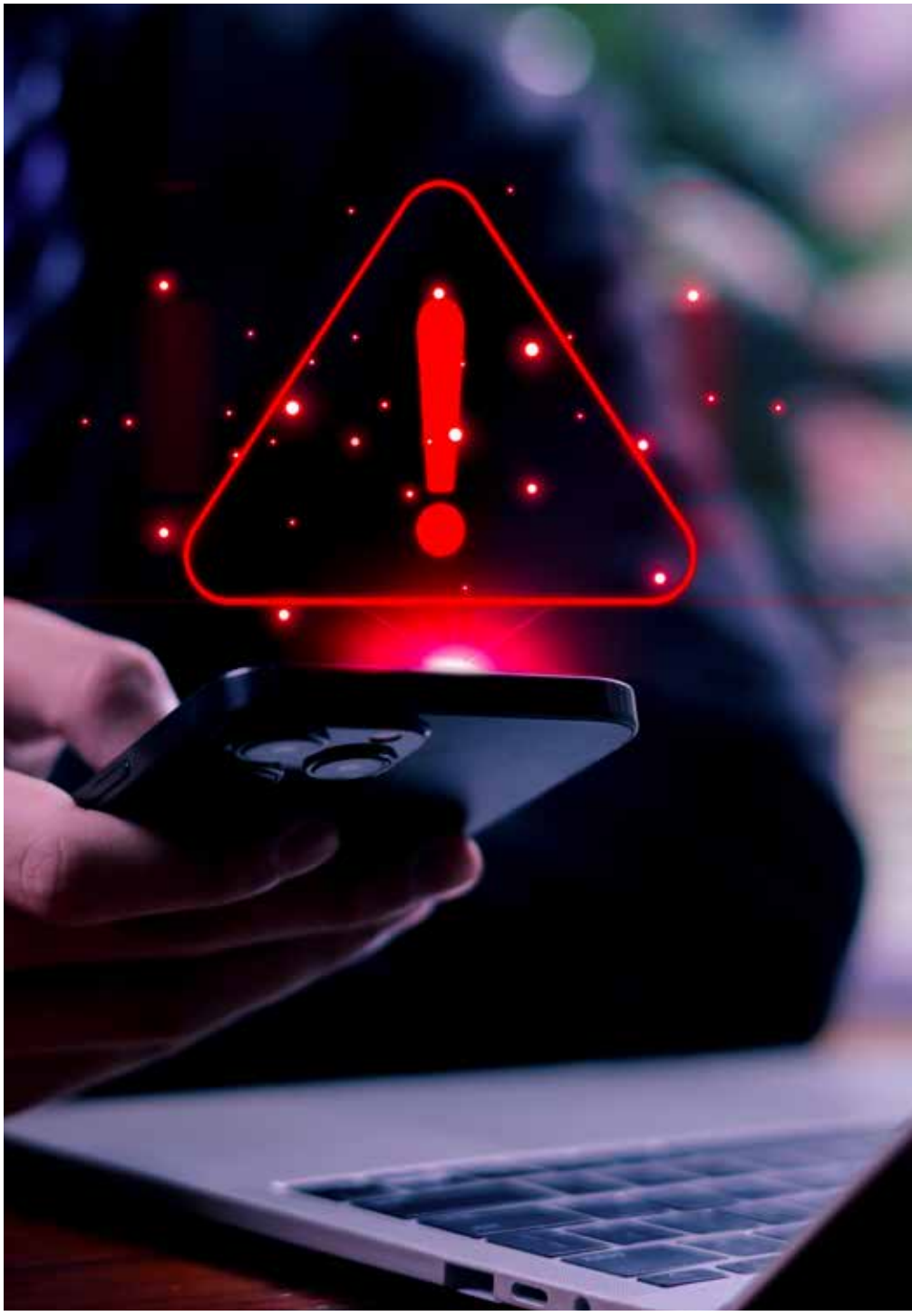
Romance Fraud

Romance Fraud is a type of fraud perpetrated by criminals, who develop a "relationship" of trust and /or intimacy with victims, often commencing through social media, dating apps and messaging platforms. Victims are gradually persuaded, under the guise of love and commitment, to provide financial assistance to the offender, frequently in response to fabricated emergencies such as travel complications, business setbacks, or medical crises involving a child or parent. As one of the earliest documented forms of deception, romance fraud remains among the most challenging to address, as victims often suffer not only financial losses but also profound emotional and psychological harm.

Sextortion

Sextortion, a form of blackmail, refers to the practice of extorting money from someone by threatening to publish or distribute real or AI-generated explicit images, videos, or information about victims to their family and personal and professional contacts.

INTERPOL detects a global increase in sextortion, with offenders increasingly integrating sextortion into other complex fraud schemes. Reports from trafficked victims forced to work in scam centres reveal that while fraud strategies and scripts typically follow investment fraud tactics, if these prove to be unfruitful, instructions are to pursue methods of sextortion. Member countries have reported notable increases of this phenomenon targeting victims in the African and MENA regions. Reports from all regions also indicate the use of AI-generated imagery and deepfakes in recent sextortion cases.



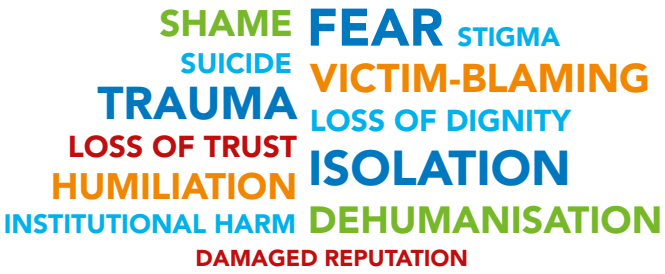
Extremely High Levels of Pervasiveness, Financial Loss and Harm

Assessing global pervasiveness, volume and impact, INTERPOL ranks financial fraud among the most threatening crimes globally, alongside drug trafficking and money laundering.[8] In 2025, the World Economic Forum found that 77 per cent of business leaders surveyed worldwide reported an increase in fraud over the past year, with 73 per cent of respondents indicating that they, or someone in their business network, had been personally affected by cyber-enabled fraud during that year.[9]

Further highlighting the global scale of the crisis, INTERPOL data indicates a 54 per cent year-to-year increase in financial fraud-related Notices and Diffusions[10] issued by member countries between 2024 and 2025. European member countries issued 38 per cent of these Notices and Diffusions, followed by 28 per cent from countries in the Asia and Pacific region. In this same period, the number of fraud-related messages received by the INTERPOL Financial Crime and Anti-Corruption Centre (IFCACC) continued to increase significantly. Between 2024 and 2025, IFCACC supported member countries in over 1,500 financial fraud cases amounting to USD 1.1 billion in reported lost assets.

The Scale of Fraud

Estimating the financial cost of fraud is challenging for a number of reasons, including significant levels of under-reporting. However, a range of data points indicate that the cost is very high and growing. For instance, one estimate suggests that global losses in 2025 totaled USD 442 billion.[11] National statistics can also help to evaluate the scale and monetary loss due to financial fraud schemes. In the United Kingdom, the Office for National Statistics[12] reported that fraud accounted for 43 per cent of all estimated crime in 2025. The City of London Police further highlighted a year-on-year rise of 33 per cent of losses linked to financial fraud, representing approximately USD 3.5 billion.[13] The United States has seen a steady increase of financial loss due to fraud, from nearly USD 4 billion in 2020 to USD 16.6 billion in 2024.[14] In the Asia and Pacific region, the Singapore Police Force highlighted that, despite a decrease from 2024, financial fraud remained a major security concern with losses estimated at approximately USD 721 million in 2025.[15]



The Human Cost

Beyond the immediate and often devastating financial losses suffered by individuals and organizations, research clearly shows the harm from financial fraud is much more than monetary. Victims of fraud often experience profound emotional distress, psychological trauma and social isolation due to an erosion of trust, the consequences of which can endure long after a fraud scheme has ended. In the most severe cases, victims of fraud have resorted to suicide.

Research focusing on romance scams, in particular, highlights that beyond financial ruin, victims commonly experience guilt and shame, which frequently deter them from reporting the crime due to fear of being blamed, as evidence points to a culture of judgment and criticism in many cases. These factors exacerbate the issue of under-reporting mentioned above and result in fewer opportunities for agencies in the public sector to investigate fraud or support victims.

8 INTERPOL strategic findings in 2024 and 2025. Global and regional threat rankings for transnational organized crimes are obtained through a threat actor-driven methodology that evaluates and weights criminal capability, reach, and impact using data from member countries, INTERPOL databases, and law enforcement operations.

9 Information provided by the World Economic Forum.

10 The assessment included all valid Notices and Diffusions published in either 2024 or 2025 with the offence code for "Banking/Financial Fraud" and/or "Commercial Fraud"

11 Global Anti Scam Alliance (GASA) and Freedzai, Global State of Scams 2025 Report, https://www.gasa.org/post/global-scams-on-the-rise-over-half-of-adults-worldwide-report-scam-encounters (Accessed 10 October 2025).

12 'Crime in England and Wales, Year Ending 2024', Office for National Statistics, 24 April 2025, https://www.ons.gov.uk/releases/crimeinenglandandwalesyearendingdecember2024 (Accessed 26 January 2026)

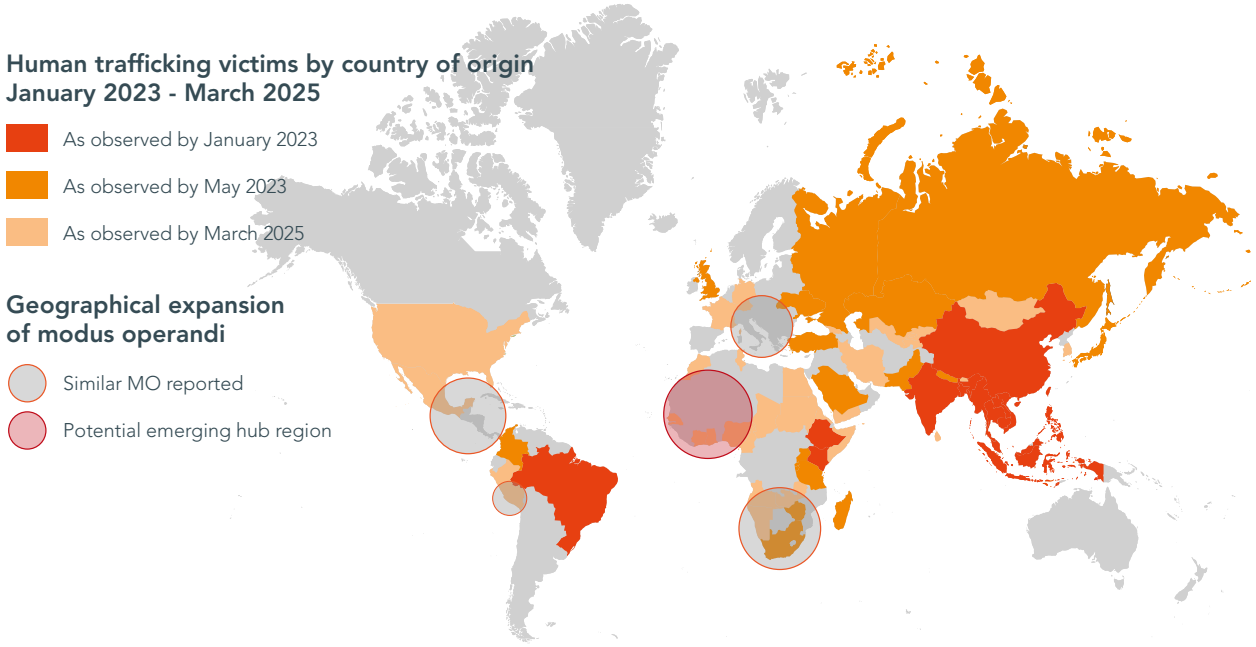
13 'Fraud and Cybercrime Annual Assessment 2024-2025', National Fraud Intelligence Bureau (City of London Police), 2025 (Accessed 12 December 2025)

14 'Internet Crime Report 2024,' United States Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), 20 April 2025, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf (Accessed 14 February 2026)

15 Singapore Police Force, Annual Scam and Cybercrime Brief 2025

The Continued Expansion of Scam Centres

Since 2022, INTERPOL has been closely monitoring a trend that began regionally but has since evolved into a global threat, often involving human trafficking for the purpose of forced online fraud. This threat is based on a dual-victim model: on the one hand, individuals who are usually lured by fake online job offers, trafficked and held in scam centres where they are forced to commit fraud; and on the other hand, another set of victims who are defrauded, generally in other jurisdictions.[16] Operational information has shown that despite intensified law enforcement efforts, scam centres continue to grow more dangerous, sophisticated and widespread.



Map of the global expansion of human trafficking for forced online financial fraud, June 2025.

By late 2025, trafficked victims spanned nearly 80 nationalities — up from 66 in the first quarter of 2025 — reflecting a truly global footprint.[17] Initially, these scam centres were concentrated in Southeast Asia, and most human trafficking victims were Chinese-speaking and sourced from Asia. Since 2022, consistent reports have shown that victims have been trafficked to Southeast Asia from distant regions, including South America, Western Europe and Eastern Africa. Moreover, new scam centres have been reported in the MENA, Central American, and in West African regions, with an indication that those working in these centres may include trafficked victims.

The geographical expansion of this criminal model reflects the growing influence of transnational organized crime groups linked to Asia, as well as local and regional groups employing similar methods.[18]

According to reports shared by member countries, financial frauds launched from scam centres include schemes such as investment fraud (including Ponzi schemes, romance baiting, cryptocurrency and Forex frauds), fake art or precious metals sales, romance scams, impersonation fraud, and unauthorized online gambling.

Information suggests that trafficked individuals held captive in compounds located in Southeastern Asia are also increasingly engaging in sextortion schemes, using AI-manipulated images to blackmail victims. Reports indicate that if a fraud approach is unsuccessful, criminals may resort to obtaining sexually explicit images and using these to extort the victim.[19]

16 'Crime trend update: Human Trafficking-fueled Scam Centres', INTERPOL, June 2025.

17 INTERPOL Human Trafficking and Smuggling of Migrants Unit

18 'Crime trend update: Human Trafficking-fueled Scam Centres', INTERPOL, June 2025.

19 'AI-aided sextortion, 'punishment rooms' & cyber slaves: Inside Cambodia's billion-dollar scam industry', ThePrint, 1 April 2024, https://theprint.in/india/ai-aided-sextortion-punishment-rooms-cyber-slaves-inside-cambodias-billion-dollar-scam-industry/2022322 (Accessed 14 January 2026)

Specific West and Central African Human Trafficking for Fraudulent Schemes. Over the past two years, INTERPOL has been monitoring specific human trafficking networks in West and Central Africa. These networks operate under the guise of multi-level marketing (MLM) companies, manipulating victims with false promises of a better life. Victims are required to pay upfront fees related to fake jobs or business opportunities. They are subsequently retained and coerced into recruiting relatives, turning them into both "sales agents" and new victims. These pyramid schemes primarily generate illicit proceeds through fees paid by newly recruited victims. Trafficking networks appear to be local, recruiting locally or regionally. They use low-tech tools like messaging applications, mobile money and in-person recruitment to exploit trust within families and communities.

OPERATION LIBERTERRA III

Operation LIBERTERRA III targeted criminals engaged in human trafficking and migrant smuggling and was a joint effort between INTERPOL, partner organizations and national law enforcement agencies. One of the key successes of the operation was the dismantling of human trafficking-fuelled scam centres in Asia, as well as pyramid-style human trafficking networks in West Africa. Over 3,700 arrests were made and 4,414 victims identified by the 119 participating countries.

Over 3,700
arrests

4,414
Victims identified

119
Participating countries

Technology and Artificial Intelligence A Force Multiplier

Over the past two years, technology has continued to enable and enhance financial fraud, empowering criminal networks to scale operations exponentially with minimal investment. Digital technology and AI, in particularly, have dramatically transformed social engineering techniques and victim profiling, enabling fraudsters to construct highly persuasive fraud environments. The proliferation of AI-driven tools, large language models (LLMs), cryptocurrencies, and the rapid expansion of the Fraud-as-a-service (FaaS) platforms have collectively lowered barriers to entry, enabling widespread access to sophisticated fraud capabilities, elevating the generation of financial gain through fraud schemes to an efficient, global industry.

Criminal Use of "Agentic" AI Today, AI agents can autonomously plan and execute entire fraud schemes through reconnaissance of victims, harvesting of credentials, infiltration of systems, selection of high-value data, calculation of optimal ransom amounts based on financial analysis, and generation of psychologically tailored, visually alarming ransom notes.[20]

Deepfake-as-a-Service has been identified in Dark Web marketplaces which offer "synthetic identity kits," complete with AI-generated video avatars, voice clones, and biometric data at affordable prices. Attackers are now able to create highly convincing digital clones using just 10 seconds of audio harvested from public sources such as social media posts or private information, enabling them to bypass authentication systems and impersonate individuals with accuracy.[21]

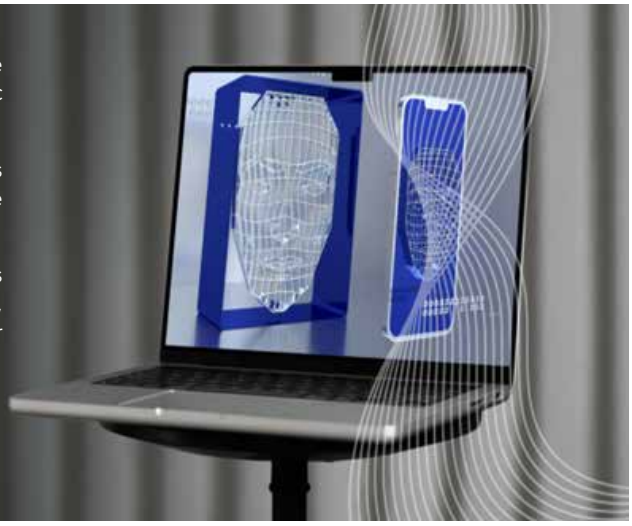
Criminal peer-to-peer (P2P) marketplaces provide full-service hubs for financial fraud syndicates. These networks offer end-to-end criminal infrastructure including phishing tools, fake trading platforms, AI-powered chatbots for victim grooming and encrypted communication channels. They also provide integrated money laundering services designed to obscure transactions and cash out illicit funds with minimal trace. Information indicates cross-regional criminal transactions involving networks operating in Eastern Europe selling phishing kits to criminal groups running scam centres out of Southeast Asia and, subsequently, turning to networks in South Asia to launder the illicit proceeds.

AI-enabled financial fraud schemes are very likely to further expand and escalate, as they are estimated to be 4.5 times more profitable than non-enhanced fraud tactics. AI greatly boosts both efficiency and effectiveness, enabling fraudsters to target more victims while making each interaction more convincing, accelerating the industrialization of fraud.[22]

Project SynthWave is led by the INTERPOL Innovation Centre and addresses rising threats from AI-generated synthetic media in Southeast Asia through regional collaboration.

It brings together law enforcement, experts, and academics from Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, Timor-Leste, and Vietnam.

Supported by the Government of Japan, the initiative aims to build regional capacity through knowledge-sharing, collaborative research, and tailored INTERPOL guidelines for detecting and responding to synthetic media abuse.



20 For an example see - 'Threat Intelligence Report: August 2025', Anthropic, August 2025, https://www-cdn.anthropic.com/b2a76c6f6992465c09a6f2fce282f6c0cea8c200.pdf (Accessed 1 February 2026)

21 'Weaponised AI Is Powering the Fifth Wave of Cybercrime, Group-IB Warns', Group-IB, 20 January 2026, https://www.group-ib.com/media-center/press-releases/weaponised-ai-cybercrime/ (Accessed 1 February 2026)

22 'Record $17 Billion Estimated Stolen in Crypto Scams and Fraud in 2025 as Impersonation Tactics and AI Enablement Surge', Chainalysis, 13 January 2026, https://www.chainalysis.com/blog/crypto-scams-2026 (Accessed 20 January 2026)

Increasingly Hybrid Fraud Tactics and the Rise in Sextortion

Over the last two years, INTERPOL has observed an escalation in the reporting of financially motivated sextortion across all regions of the world. The recent surge in sextortion is likely a result of the ease of execution and effectiveness of this fraud type, when facilitated by AI. With the use of generative-AI to create sexually explicit content and deepfakes, fraudsters can more effectively exploit a victim. Any individual with accessible online visual content is a potential victim of sextortion.

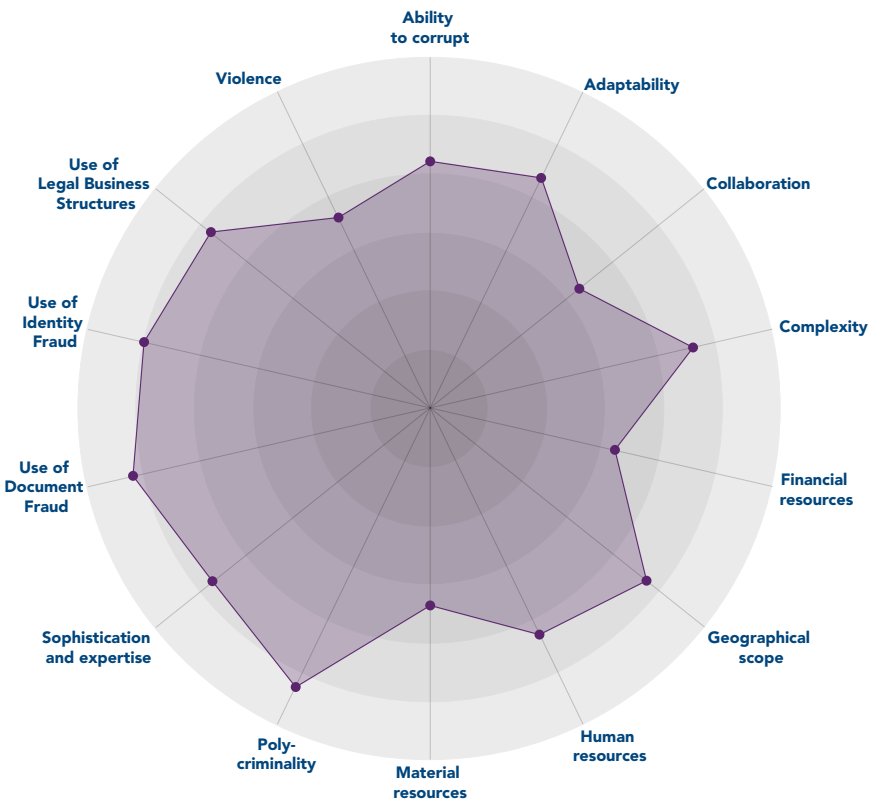
The combination of sextortion with other fraud types, notably investment fraud – represents a relatively low-effort tactical evolution that significantly increases the probability of success for offenders. As previously mentioned, this tactical shift has already been observed in scam centres located in Southeast Asia. A similar evolution has also been observed in scam centres operating out of Africa, with sextortion no longer an opportunistic afterthought, but systematically embedded in fraud schemes.

The methodological inclusion of sextortion in romance-based fraud scams has been the subject of recent research, with findings that suggest organized criminal groups may be using scripts, in particular to manage the sextortion phase.[23, 24] AI-generated personas, deepfake images, and scripted emotional manipulation make it easier to escalate from flirtation to intimacy. These so-called hybrid fraud schemes, notably involving sextortion, which are more likely to yield returns, are almost certain to further intensify in the near future. While these crimes primarily target adults, member countries have also reported the victimization of minors.

23 Marasa, Marie-Helen, and Ives, Emily R., 'Deconstructing a form of hybrid investment fraud: Examining 'pig butchering' in the United States', Journal of Economic Criminology, 2024.

24 Cross, C., Holt, K., and O'Malley, R., 'If U Don't Pay They Will Share the Pics": Exploring Sextortion in the Context of Romance Fraud', Victims & Offenders, 19 May 2022. https://www.tandfonline.com/doi/full/10.1080/15564886.2022.2075064 (Accessed 20 January 2025)

Financial Fraud Offender Profile



Building threat actor profiles helps law enforcement to better understand the behaviour and capabilities of criminal groups, and to adopt counter strategies or redirect investigative efforts to address intelligence gaps. Based on data from member countries and operational support units, the radar chart above displays the different threat actor attributes assessed by INTERPOL.

The data available suggests that criminals and crime groups conducting financial fraud are poly-criminal, highly-organized, skilled and adaptable. Information also indicates that these offenders, not surprisingly, use document fraud, identify fraud as well as using legal business structures.

Data submitted by member countries further suggests mid-level collaboration among criminal groups and moderate access to financial and material resources. This likely reflects the low barriers to entry into fraud, as offenders face low "start up" costs, making this type of criminality attractive for people from a wide range of economic backgrounds.

Finally, it is noteworthy that the assessment of violence is also moderate, and almost surely points to the need for further awareness-raising among law enforcement on the suffering inflicted by perpetrators of financial fraud.

Sophisticated Financial Fraud Scheme in South America

Authorities in South America exposed a highly sophisticated financial fraud operation conducted by a local organized crime group, which leveraged advanced technical expertise and a coordinated division of labor to systematically compromise victims' financial accounts. Using stolen personal and banking data, they ported victims' mobile phone lines to intercept two-factor authentication codes, enabling them to bypass bank security protocols. They then altered delivery addresses and ordered new credit cards in victims' names.

To circumvent biometric security measures, a technician used laser equipment to forge fingerprints. Meanwhile, recruiters identified and impersonated victims, while storekeepers acted as cash-out points—purchasing goods or services to launder stolen funds. This multi-role, tightly coordinated network enabled the group to steal and monetize credit lines on a large scale, demonstrating a high level of organizational sophistication and technical capability.

INTERPOL OPERATION CATALYST

INTERPOL Operation Catalyst – Financial Fraud and Terrorism Nexus in Africa

Beyond the known convergence with human trafficking, intelligence suggests a growing nexus between financial fraud and terrorism financing across the African region. One example of this is drawn from Operation Catalyst, a transnational case involving a massive cryptocurrency-based Ponzi scheme, which claimed to be a legitimate online trading platform, affecting at least 17 countries around the world, including Cameroon, Kenya, and Nigeria. The scheme affected more than 100,000 victims with an estimated loss to victims of USD 562 million. The investigations found that several large-valued wallets were potentially linked to terrorism financing activities in Central Africa.[25]

Geographic hubs of concern in relation to this terrorism-fraud nexus include:

West and Central Africa (Nigeria, Cameroon): primary sources of funding for terrorist groups via crypto-fraud schemes.

East Africa (Kenya, Tanzania): funds used for the recruitment and radicalization traced through a cryptocurrency trading platform.

South Africa (Angola): informal value transfer systems identified as connected to potential terrorist financing and money laundering.

25 '83 arrests in landmark African operation against terrorism financing', INTERPOL, 22 October 2025, https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2025/83-arrests-in-landmark-African-operation-against-terrorism-financing (Accessed 5 November 2025)

Global Risk Projections

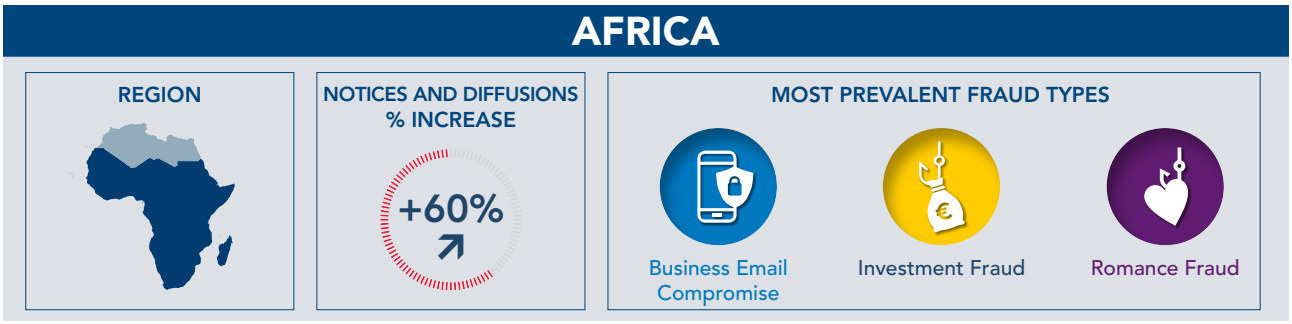
In order to assess the projected risk of financial fraud, INTERPOL requested member countries to provide a national assessment of how fraud is expected to evolve over the next three to five years. In response, member countries indicated whether fraud was expected to no longer exist, significantly diminish, slightly diminish, stabilize, increase or increase significantly at the national level. They also anticipated if the degree of harm from fraud would be none, minor, moderate, major or severe, respectively across five key domains, including economic, social, health, governance and security.

Based on the responses from member countries and using a weighted analytical methodology, the overall global risk of financial fraud over the next three to five years is HIGH, with projections of a significant escalation in financial fraud-related crimes at the global level.

The data further forecasts that this significant rise in the global threat from financial fraud will most negatively impact the economic, social, and security domains, where the global risk is also assessed as HIGH, with a major degree of harm anticipated. In contrast, global risk to the governance and health sectors is assessed by member countries as MODERATE.

RISK PROJECTIONS

Regional Financial Fraud Threats and Trends



Fraud-related INTERPOL Notices and Diffusions

Between 2024 and 2025, there was a 60 per cent increase in the publication of fraud-related Notices and Diffusions by member countries in the African region. The majority of the offenders targeted by these Notices and Diffusions were nationals from countries within the region, mainly from West Africa. There were also offenders with nationalities from Europe, the Asia and Pacific, and MENA regions.

Top Regional Fraud Types and Trends

Member countries in the African region indicated that financial fraud posed a HIGH threat, with financial fraud ranking among the top five crimes in the region, along with terrorism and illicit drug trafficking. While most fraud types have surged over the previous two years, INTERPOL identifies BEC, investment fraud and romance fraud as the top three most prevalent fraud types in the African region.

BEC

BEC remains one of the most financially detrimental crime threats in the African region. Available data reveals that BEC has shifted from simple spoofing to sophisticated, multi-stage attacks driven by AI and "stealer" malware. While the primary threat actors—highly organized criminal syndicates—are predominantly based in West Africa, their operations are rapidly expanding into Eastern and Southern Africa, exploiting the region's growing digital infrastructure to launch global campaigns, targeting high-value organizations in sectors including finance, energy, education and healthcare.

Investment Fraud

Investment frauds represent a highly professionalized, transnational threat to the African region, one that has shifted into an industrialized "hybrid" model. Often originating from scam centres in Southern and West Africa, these schemes increasingly utilize AI-driven advertising and polished mobile apps to target "high-value" victims primarily in North America and Europe. The rise in this fraud type has coincided with the expansion of romance baiting, where victims are groomed over time before being coerced into fraudulent cryptocurrency platforms. This evolution has led to large-scale campaigns; for example, a single operation in Zambia uncovered 65,000 victims having been defrauded of an estimated USD 300 million.[26]

Romance Fraud often Evolving into Sextortion

Often linked to organized syndicates mainly active in West Africa, romance fraud schemes involve fabricating financial emergencies or promoting fraudulent cryptocurrency schemes, resulting in massive financial losses and psychological harm to victims across Africa, as well as in other targeted regions. Consistent with global trends, information from African member countries indicates that, in recent years, offenders start off with romance fraud before pivoting to sextortion or romance baiting, increasingly making use of AI-generated content to facilitate these crimes. This shift includes teenage victims across the continent, most notably in Southern Africa.[27, 28]

26 'African authorities dismantle massive cybercrime and fraud networks, recover millions', INTERPOL, 22 August 2025, https://www.interpol.int/en/News-and-Events/News/2025/African-authorities-dismantle-massive-cybercrime-and-fraud-networks-recover-millions (Accessed 16 January 2026)

27 'INTERPOL Africa Cyberthreat Assessment Report 2024', INTERPOL, April 2024

28 'INTERPOL Africa Cyberthreat Assessment Report 2025', INTERPOL, May 2025

OPERATION RED CARD 2.0

African Threat Actors Leveraging Technology and Tools

Threat actors operating in the African region, notably in Western and Southern Africa are increasingly leveraging AI, deepfake technology, and automated phishing tools to commit a range of fraud offences at scale. With some online vendors offering FaaS, even less tech-proficient criminals can now launch sophisticated AI-powered frauds with minimal effort. The convergence of technology and organized crime is driving more sophisticated, efficiently coordinated financial fraud and fuelling a sustained rise in this crime area across the African region.

Emergence of New Model of Human Trafficking for Fraudulent Schemes in Central, West Africa

INTERPOL has recently uncovered a new trend in Central and West Africa involving human trafficking for the purpose of fraudulent schemes, including pyramid schemes and clandestine Multi-Level Marketing (MLM) operations. Unlike the high-tech, foreign-operated scam centres of Southeast Asia—which rely on technological advancements, encrypted platforms, and cryptocurrency to defraud strangers abroad—the West African fraud model is low-tech, locally driven, and deeply embedded in community networks. Led by actors from countries in the region, these operations use mobile messaging to recruit mainly students and unemployed youths aged 16 to 25, then mobile money platforms to exploit and extort them. These individuals are targeted with enticing promises of quick income, international education, career advancement, entrepreneurial success, and immigration pathways, etc. They are then forced to deceive their own families and friends under the guise of legitimate MLM businesses, with revenue generated not through external theft but through fees extracted from new recruits and pressure to sell overpriced or fake products. This creates a self-sustaining cycle of exploitation rooted in social trust, economic desperation, and the absence of formal employment opportunities.

Regional Risk Projections for Africa

African member countries assess the risk level of financial fraud in the region as HIGH, with projections of a significant escalation in financial fraud-related crimes over the next three to five years.

The data received further forecasts that the expected rise in the regional threat from financial fraud will most negatively impact the economic domain, where the risk is also assessed as HIGH, with a major degree of harm anticipated. The regional risks to society, security and governance are likewise assessed by member countries as HIGH, however, with projected harm expected to be moderate. In contrast, the regional risk to the health sector is assessed as MODERATE, with a minor degree of harm anticipated by African member countries.

RISK PROJECTION - AFRICA

Overall Level of Risk	Economic Risk	Governance Risk	Health Risk	Security Risk	Social Risk
HIGH	HIGH	HIGH	MODERATE	HIGH	HIGH

OPERATION SERENGETI 2.0

Operation SERENGETI 2.0 (June - August 2025) specifically targeted ransomware, BEC, and other cyber-enabled fraud. This joint operational effort involved INTERPOL, partner organizations, private sector partners, and law enforcement agencies from 19 African countries and resulted in 1,209 arrests and the identification of 88,000 victims, with USD 97.4 million recovered by national authorities.

19
Participating countries

1,209
Arrests

88,000
Victims identified

With
USD 97,4 MILLION
recovered by national authorities

AMERICAS AND THE CARIBBEAN

REGION

NOTICES AND DIFFUSIONS % INCREASE

MOST PREVALENT FRAUD TYPES

Investment Fraud

Business Email Compromise

Impersonation Fraud

Fraud-related INTERPOL Notices and Diffusions

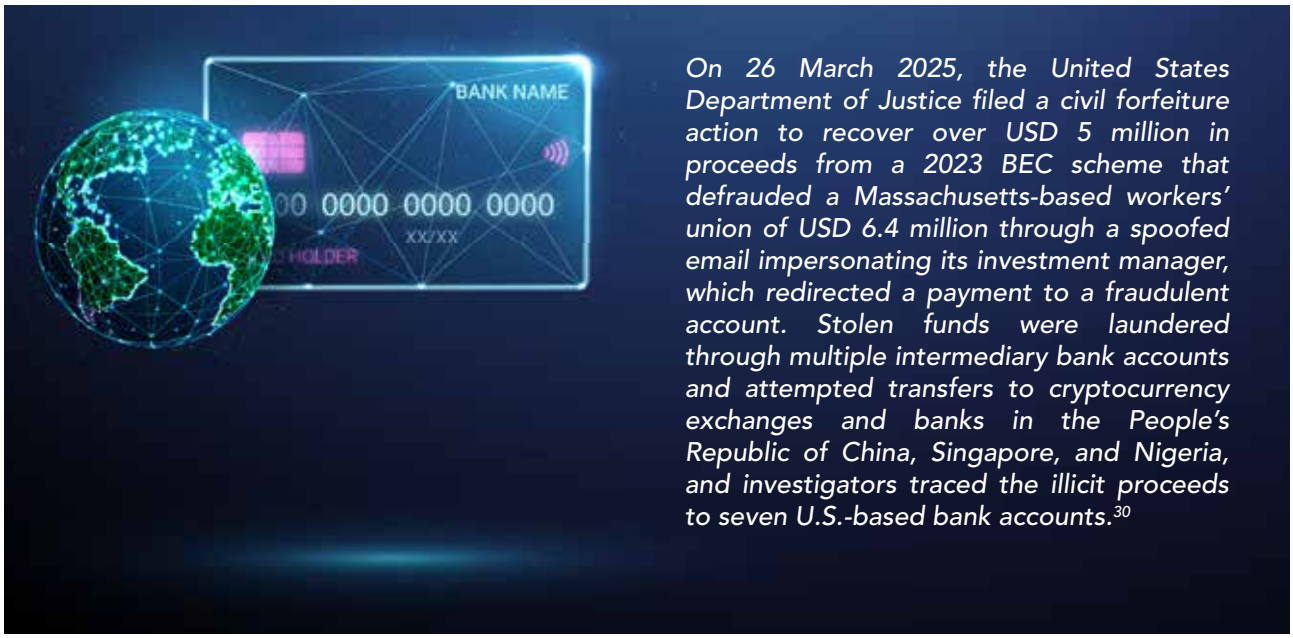
Between 2024 and 2025, there was a 40 per cent increase in the publication of fraud-related Notices and Diffusions by member countries in the Americas and Caribbean region. The majority of the offenders targeted by these Notices and Diffusions were nationals from countries within the region, particularly South America.

Top Regional Fraud Types and Trends

Closely aligning with crime threats in other regions, member countries from the Americas and Caribbean region assessed financial fraud as a high-level regional crime threat inflicting huge financial losses on businesses and individuals. Reporting from member countries in the region indicates that investment fraud, BEC, and impersonation fraud are the fraud types that pose the greatest threat.

Increasingly Tech-enabled Investment Frauds and BEC

Over the past two years, member countries in the Americas and Caribbean region have reported soaring financial losses from increasingly sophisticated investment frauds, primarily fuelled by the misuse of virtual asset payment and investment systems, the proliferation of fake or cloned cryptocurrency investment platforms, and the deliberate manipulation of returns by fraudsters. These crimes are compounded by fraudulent real estate schemes and BEC attacks. Driven by global technological trends, these scams have evolved into hybrid attacks fuelled by phishing, social engineering, and FaaS tools. The North American sub-region remains the primary target for BEC with financial losses estimated in USD billions over the past year.[29]



On 26 March 2025, the United States Department of Justice filed a civil forfeiture action to recover over USD 5 million in proceeds from a 2023 BEC scheme that defrauded a Massachusetts-based workers' union of USD 6.4 million through a spoofed email impersonating its investment manager, which redirected a payment to a fraudulent account. Stolen funds were laundered through multiple intermediary bank accounts and attempted transfers to cryptocurrency exchanges and banks in the People's Republic of China, Singapore, and Nigeria, and investigators traced the illicit proceeds to seven U.S.-based bank accounts.[30]

29 '2024 Internet Crime Report', Federal Bureau of Investigation, 23 April 2025, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf Accessed 2 February 2026)

30 'United States Files Forfeiture Action to Recover Over $5M of Funds Traceable to Business Email Compromise Scheme Targeting Massachusetts Workers Union', U.S. Department of Justice, 5 June 2024, https://www.justice.gov/archives/opa/pr/united-states-files-forfeiture-action-recover-over-5m-funds-traceable-business-email (Accessed 5 February 2026)

Impersonation Fraud

Over the past two years, impersonation fraud has surged across the Americas and the Caribbean. Fraudsters have increasingly exploited digital platforms, social engineering, and compromised personal data to pose as government officials, bank representatives, or even family members, manipulating victims into sending money or disclosing sensitive information. In North America, fraudulent calls from tax or social security authorities have spiked, while in South America and the Caribbean, impersonation of utility companies, mobile providers, and law enforcement has led to significant losses—particularly among elderly and less digitally literate populations. The Caribbean region, with its growing digital adoption and fragmented regulatory frameworks, has seen a rise in "grandparent scams" and phishing schemes tied to remittance channels.

Surges in Sextortion following Global Trends

Similar to other regions of the world, sextortion is reportedly on the rise in the Americas and Caribbean region. In Latin America, financially motivated sextortion has recently targeted business executives demanding high ransom payments in cryptocurrency. In North America, member countries have recently reported sextortion trends targeting teenage boys aged between 14 and 17 with fraudsters extorting money through threats of exposing intimate AI-generated deepfake images.

Scam Centres Expanding in South America

Over the past two years, scam centres have expanded into and increasingly targeted countries in the Americas and Caribbean region, notably South America.[31] Member countries report the detection of scam centres in several South American countries, where victims are mainly lured through fake job advertisements.[35] Reports from member countries further indicate that transnational organised crime groups—particularly those based in the Asia and Pacific region—are increasingly targeting South America, driving a growing demand for Spanish- and Portuguese-speaking labour in scam centres across Southeast Asia.[32] This mirrors a trend observed over the past three years, where victims have been trafficked from South America into these operations.[33]

Organized Crime linked to Financial Fraud in South America

South American crime syndicates, traditionally linked to drug trafficking, arms trafficking, money laundering and criminal violence at the national and regional levels, are also known for their involvement in the commission of financial fraud. The recent arrest of a suspect, with alleged links to Tren de Aragua, in connection with a USD 150 million cryptocurrency fraud scheme used to launder proceeds from drug trafficking and extortion across Chile, Colombia, Venezuela and the Iberian Peninsula, highlights the convergence of financial fraud and other crimes in this region.[34]

Regional Risk Projections for the Americas and the Caribbean

Member countries in the Americas and Caribbean region assess the risk level of financial fraud as MODERATE, despite their anticipation for these crimes to increase over the next three to five years.

According to member country responses, in the near future, financial fraud will most negatively impact the economic and social domains, where the regional risk is assessed as HIGH, with a major degree of harm anticipated. In contrast, the regional risk projections for governance, health and security are assessed by member countries as MODERATE, with projected harm to be moderate to governance, and minor to health and security.

RISK PROJECTION - AMERICAS AND THE CARIBBEAN

31 'Crime trend update: Human Trafficking-fueled Scam Centres', INTERPOL, June 2025.

32 'Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia', United Nations Office on Drugs and Crime, April 2025, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf (Accessed 13 January 2026)

33 'Crime Trend Update: Human Trafficking-Fueled Scam Centres', INTERPOL, June 2025

34 'International fugitive hunt leads to 85 arrests', INTERPOL, 29 December 2025, https://www.interpol.int/News-and-Events/News/2025/International-fugitive-hunt-leads-to-85-arrests (Accessed 2 February 2026)

INTERPOL Uncovers Fraudulent Vehicle Export Scheme in the Americas

In North America, a growing, sophisticated transnational fraud scheme was first detected in early 2024. Criminal networks use identity theft and "straw buyers" to obtain financed vehicles from car dealerships, then export them overseas before lenders can detect fraud. To secure loans, perpetrators submit forged employment records, and falsified income and revenue statements, making minimal initial payments to establish credibility—only to default after export, leaving lenders or financial institutions with unrecoverable losses.

The scheme exploits delays between loan default and fraud detection, allowing vehicles to be removed from the region before law enforcement can intervene. By the time vehicles are flagged as stolen, they have often bypassed national databases, making them untraceable in INTERPOL's system. The trend is spreading, exposing critical gaps in cross-border verification and fraud response.

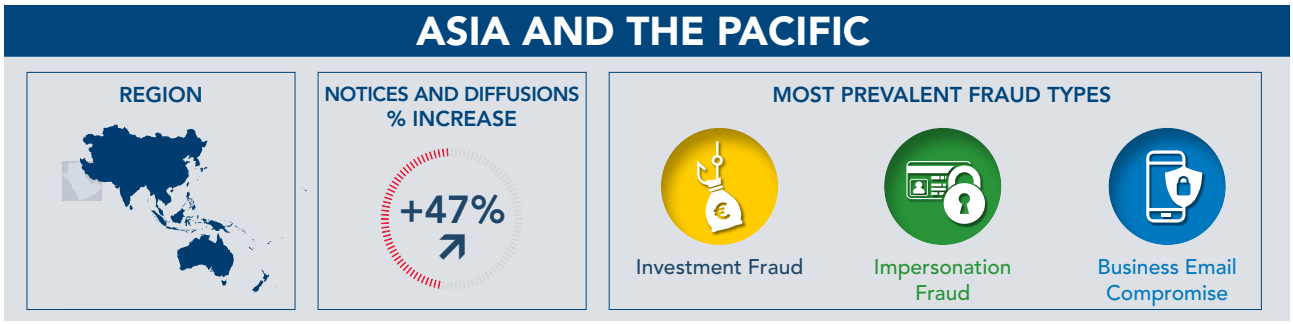
OPERATION FIRST LIGHT

Operation FIRST LIGHT (March–May 2024) was a globally coordinated law enforcement initiative led by INTERPOL, targeting widespread online scams including phishing, investment fraud, fake e-commerce websites, romance fraud, and impersonation fraud. The operation brought together four regional law enforcement organizations and agencies from 61 countries, resulting in nearly 4,000 arrests and assets valued at USD 257 million being seized.

61
Participating countries

4,000
Arrests

Value of Assets Seized:
USD 257 MILLION



Fraud-related INTERPOL Notices and Diffusions

Between 2024 and 2025, there was a 47 per cent increase in the publication of fraud-related Notices and Diffusions by member countries in the Asia and Pacific region. The majority of the offenders targeted by these Notices and Diffusions were nationals from countries within the region – particularly Eastern and Central Asia. There were also offenders with nationalities from the European region – notably from Eastern European countries.

Top Regional Fraud Types and Trends

Financial fraud is assessed as a high-level threat to the Asia and Pacific region, due to the dense concentration of sophisticated criminal actors and the region's growing attractiveness as a prime target for fraudulent activities. According to INTERPOL data, the types of financial fraud that represent the greatest threat to the Asia and Pacific region are investment fraud, impersonation fraud, and BEC.

Investment Fraud: A Multifaceted Threat Combining Financial Deception, Cultural Exploitation, and Sextortion

Investment fraud has become a sophisticated, global menace combining financial deception, cultural manipulation, and digital blackmail. Fraudsters use social media to lure victims with fake cryptocurrencies, Ponzi schemes, and sham Forex platforms, bolstered by AI-generated dashboards and forged credentials. They tailor pitches to exploit religious, ethnic, or national identities in victims' native languages. Defrauded funds are frequently laundered through cryptocurrencies across Southeast Asia, South Asia, MENA, Europe, and Africa, making recovery nearly impossible. Hybrid investment-sextortion schemes now use deepfakes to blackmail victims, marking a new frontier in financial crime.

Impersonation Fraud: From Remote Calls to Physical Theft

Impersonation fraud, often beginning with a phone call, is evolving into a dangerous hybrid threat that bridges virtual deception and real-world crime. Criminals pose as law enforcement, bank representatives, or government officials to manipulate victims into believing they are under investigation or facing legal penalties, sometimes instructing victims to leave cash at their doorsteps, where accomplices later appear in person to collect it. INTERPOL has documented such schemes targeting victims in Eastern Asia, highlighting a shift from purely remote telecom fraud to coordinated physical theft. This evolution underscores the growing sophistication of criminal networks that exploit trust, fear, and geographic distance to maximize impact and evade detection.

BEC Fraud: Leveraging Technology for Sophisticated Deception

BEC fraud across the Asia and Pacific region has become increasingly sophisticated, exploiting advanced technologies to target regional businesses with precision. Fraudsters use email spoofing, phishing kits, and AI-generated, hyper-personalized messages to impersonate executives or trusted partners, often manipulating employees into authorizing fraudulent wire transfers. In high-value cases, perpetrators now employ deepfake audio to mimic the voices of CEOs or Chief Financial Officers (CFOs) during real-time phone calls, bypassing traditional verification protocols. Compounding the threat is the rise of "Fraud-as-a-Service" platforms — powered by generative AI and large language models — which have enabled widespread adoption of cybercrime. These platforms enable low-skill actors to launch professional-grade BEC campaigns with minimal effort, providing ready-made tools such as automated phishing websites, fake payment gateways, and bot-generated fake testimonials that mimic legitimate business communications.[40]

35 'Asia and South Pacific Cyberthreat Assessment Report', INTERPOL, August 2024.

Expansion of Scam Centres into the Pacific Region

Member countries have reported scam centres across the Pacific, targeting individuals through telecom fraud and romance scams. Victims in these schemes suffer average losses of USD 25,000 per telecom fraud incident and up to USD 83,000 in romance baiting cases. The model is now expanding into Pacific Island nations, with evidence of East Asian-linked scam operations exploiting weak regulatory oversight and fraudulent visa arrangements. Similar illicit networks are suspected in abusing Special Economic Zones in the region, where shell companies and citizenship-by-investment programmes are being weaponized to facilitate fraud and obscure criminal activity.[36]

A Connected and Diverse Criminal Ecosystem

Fraud networks today span a broad spectrum of actors — from individual offenders, often unemployed youth serving as recruiters or money mules, to highly organized, transnational criminal syndicates. In the Asia and Pacific region, major fraud hubs are firmly entrenched in Southeast Asia and South Asia. Criminal networks, often originating from East Asia, dominate these hubs, leveraging coordinated infrastructure and multilingual staffing to target victims globally. Meanwhile, Central Asian criminal groups are rapidly expanding through an affiliate-based model — outsourcing day-to-day operations to local actors while retaining centralized control over technology, funding, and command structures. Increasingly, these actors are collaborating across borders, with operational ties extending between East and Southeast Asia and Eastern Europe, creating a fluid, resilient, and hard-to-disrupt global fraud ecosystem.

Regional Risk Projections for the Asia and Pacific Region

Member countries in the Asia and Pacific region assess the overall regional risk level of financial fraud as MODERATE, despite anticipation that these crimes will increase over the next three to five years.

The data further forecasts that the regional threat from financial fraud will most negatively impact the economic and social domains, where the regional risk is assessed as HIGH, with a major degree of harm anticipated.

In contrast, the projected regional risks to governance, health and security are assessed by Asia and Pacific member countries as MODERATE, with projected harm to be moderate to governance and security, and minor to health.

RISK PROJECTIONS ASIA AND PACIFIC

Overall Level of Risk	Economic Risk	Governance Risk	Health Risk	Security Risk	Social Risk
MODERATE	HIGH	MODERATE	MODERATE	MODERATE	HIGH

OPERATION HAECHI VI

40
Participating countries

32,835
Arrests

68,000
Bank accounts blocked

Amount recovered:
USD 439 MILLION
(USD 342 million in government-backed currencies and USD 97 million in physical and virtual assets)

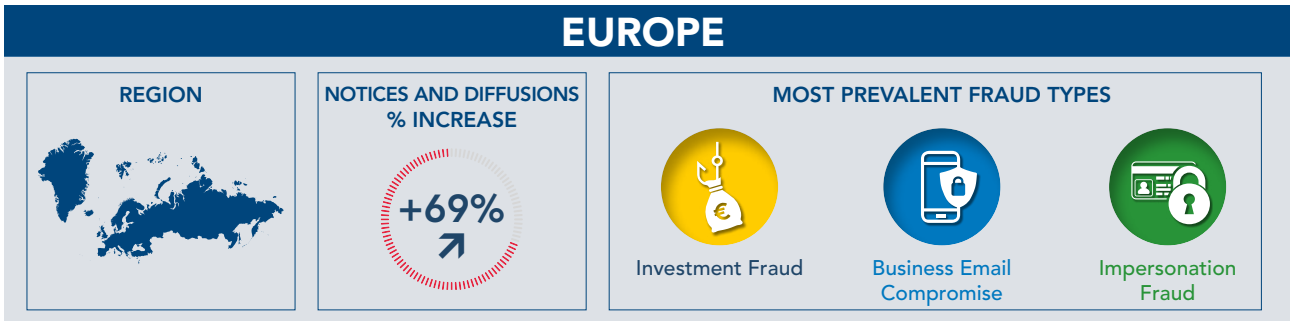
Operation HAECHI VI (April - August 2025), targeted seven types of financial crimes: voice phishing, romance scams, online sextortion, investment fraud, money laundering associated with illegal online gambling, BEC and e-commerce fraud. The 40 countries involved successfully made 32,835 arrests, blocked 68,000 bank accounts and recovered USD 439 million.

36 'Southeast Asia and the Pacific Organized Crime Threat Alert Strategic infiltration of vulnerable jurisdictions through criminal foreign direct investments: the case of Timor-Leste', United Nations Office on Drugs and Crime, September 2025, https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Alert_Strategic_infiltration_of_vulnerable_jurisdictions_through_criminal_foreign_direct_investments.pdf (Accessed 3 December 2025)

Between February and December 2025, China, Myanmar and Thailand conducted coordinated operations against cyber-enabled fraud networks operating in scam compounds in Myanmar. The crackdown led to the demolition of 635 buildings hosting scam centres in KK Park and the full evacuation of Yatai New City, with 14,000 foreign nati onals from 54 countries detained.

I-GRIP Mechanism Helps Facilitate Record Recovery of Over USD 40 Million

In July 2024, Singaporean authorities made a record recovery of over USD 40 million thanks to cooperation with Timor-Leste through INTERPOL. A significant BEC campaign resulted in a Singaporean firm manipulated into wiring USD 42.3 million to a fraudulently disguised account in Timor-Leste after receiving a spoofed email from a fake supplier. INTERPOL swiftly activated its I-GRIP mechanism to facilitate cooperation between Singapore and Timor-Leste to help trace and intercept the stolen funds. Thanks to this cooperation, Timor-Leste authorities initially intercepted USD 39 million, and, after further investigations, arrested seven suspects and recovered an additional USD 2 million.



Fraud-related INTERPOL Notices and Diffusions

Between 2024 and 2025, there was a 69 per cent increase in the publication of fraud-related Notices and Diffusions by member countries in the European region. Most of the offenders targeted by these Notices and Diffusions were nationals from countries within the region – particularly Eastern and Western Europe. There were also offenders with nationalities from the Asia and Pacific region – notably from Central Asian countries, and West Africa.

Top Regional Fraud Types and Trends

Financial fraud is assessed as representing a high threat to the European region. Heavy reliance on digital payments, financial technology, and e-commerce—combined with robust economies and sophisticated financial systems—makes Europe an attractive target for financial fraudsters. According to INTERPOL data, the types of financial fraud that represent the greatest threat to the European region are investment fraud, BEC, and impersonation fraud, which is often combined with identity fraud.

Investment Fraud – The Costliest Crime

Investment frauds in Europe are among the most financially detrimental, targeting primarily older adults and inexperienced investors, particularly across Western and Northern Europe, through emotionally manipulative tactics on social media, dating apps, and vishing campaigns. Fraudsters promote deceptive platforms offering unrealistic returns on cryptocurrencies, renewable energy, or luxury assets, with victimisation sometimes lasting for years. Victims are not only defrauded of savings but are often re-victimized by fraudsters posing as recovery agents, or law enforcement, and may also be coerced into becoming money mules or involved in blackmail-based fraud.

Sophisticated BEC Attacks

European countries have identified BEC schemes as a persistent and evolving threat. Offenders are increasingly leveraging cybercriminal tools and tactics to infiltrate victim organizations—such as deploying malware to exfiltrate sensitive data from corporate servers or tampering with internal systems. To evade detection, fraudsters are also making greater use of locally opened bank accounts, often facilitated by money mules within the target country, thereby reducing the likelihood of triggering red flags for international financial transactions. European authorities have emphasized the high level of sophistication in these attacks, noting that perpetrators conduct extensive reconnaissance on their targets, including studying corporate hierarchies, communication styles, and transaction patterns, before initiating carefully staged interactions to build trust.

The Convergence of Impersonation and Identity Fraud

Impersonation fraud and identity fraud have grown increasingly sophisticated across Europe, often occurring in tandem as part of coordinated, multi-channel social engineering campaigns. Fraudsters predominantly exploit vishing, smishing, and increasingly quishing to manipulate victims into transferring money or disclosing sensitive personal information. Common impersonation tactics reported by European member states include posing as trusted entities such as banks, law enforcement agencies, telecommunications providers, or major tech support services. In addition, fraudsters increasingly exploit familial trust through emotionally manipulative scenarios—commonly known as "grandparent scams" or "shock calls." These involve fabricated emergencies, such as claims that a relative has been involved in a serious accident, arrested, or requires urgent surgery, often accompanied by a plea for money. These messages are designed to trigger urgency and suppress rational decision-making, pressuring victims into making immediate financial transfers.

New QR Code Scam Targeting Online Sellers in Europe

A European Member country reported a new modus operandi: fraudsters impersonate buyers on online marketplaces before manipulating victims into moving communications to a mobile messaging application using a local phone number. They then claim payment was sent to a local post office, providing a fake QR code. Scanning the code leads to a fraudulent website impersonating the local post office, where victims are then instructed to click "Receive Money" and select their bank—redirecting them to a fake bank login page. Entering credentials grants the fraudsters access, which is secured by adding a new two-factor authentication device to block victim notifications. Funds are then drained via mobile money transfer. In one case, over USD 110,000 was stolen.

European Scam Centres

According to police reports from European member countries, scam centres have been identified in several European nations located in Central, Eastern and Southern Europe, as well as in the Western Balkans region. These centres more closely resemble "boiler rooms[37]" and are not frequently associated with human trafficking. Fraudsters operating out of these centres are predominantly engaged in investment frauds.

Organized crime groups in Europe are highly specialized and transnationally networked

Eastern European networks dominate telecom and investment fraud, using Russian-speaking operators to target elderly populations through police impersonations and romance scams. These same criminal groups also operate scam centres. Highly organized criminal groups comprising nationals and dual nationals from Europe and the Middle East run sophisticated, multi-layered scams with strong ties to European financial systems, with important hubs in Eastern Europe and the MENA region. West African criminal networks, residing and operating within the European region, tend to specialize in advance-fee and romance frauds.

Illicit Financial Flows from Europe Moving East

Stolen illicit funds originating in Europe are predominantly moved across international borders, with very few cases remaining within domestic systems. These funds typically pass through a series of intermediary bank accounts, often located in Southwestern and Southeastern Europe, before being funnelled toward financial hubs in East Asia and the Middle East. In recent years, cryptocurrencies have become an increasingly common vehicle for moving these proceeds, frequently transiting through Eastern European jurisdictions exploiting regulatory gaps and digital infrastructure.

Regional Risk Projections for the European Region

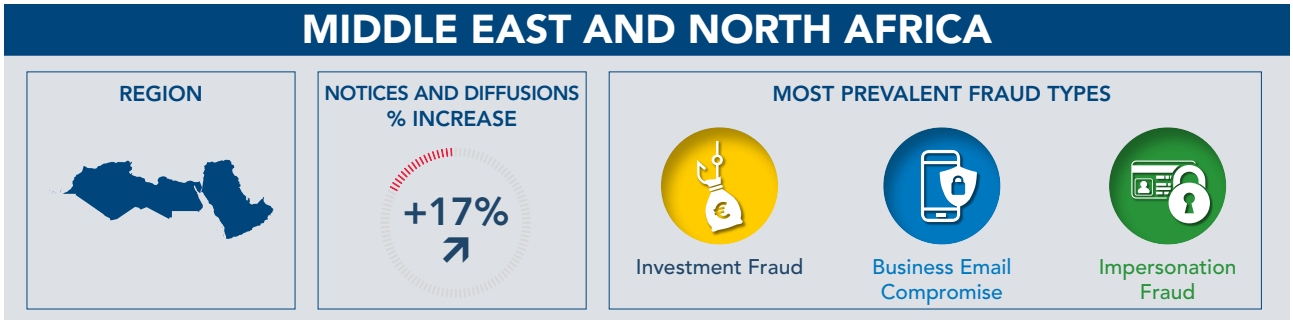
European member countries assess the overall risk level of financial fraud over the next three to five years as HIGH, with member countries projecting an escalation in the volume of such crimes.

The data further forecasts that this rise in the regional threat from financial fraud will most negatively impact the economic, security and social domains, where the regional risk is assessed as HIGH, with a major degree of harm anticipated. Regional risk projections for governance and health are also assessed by European member countries as HIGH, but with anticipated harm to be moderate to both of these sectors.

RISK PROJECTION - EUROPE

Overall Level of Risk	Economic Risk	Governance Risk	Health Risk	Security Risk	Social Risk
HIGH	HIGH	HIGH	HIGH	HIGH	HIGH

37 A boiler room is an operation where salespeople use high-pressure, often deceptive tactics—typically over the phone or online—to persuade people to invest in fraudulent or highly speculative schemes. These setups commonly involve scripted pitches, fake credentials, and aggressive persistence to extract money from victims.



Fraud-related INTERPOL Notices and Diffusions

Between 2024 and 2025, there was a 17 per cent increase in the publication of fraud-related Notices and Diffusions by member countries in the MENA region. Most of the offenders targeted by these Notices and Diffusions were nationals from countries within the region. There were also offenders with nationalities from the Asia and Pacific region – notably from South Asia.

Top Regional Fraud Types and Trends

Member countries from the MENA region assessed the threat related to financial fraud as MODERATE to HIGH in the region. As in other regions, rapid digitalization across the MENA region has not only created a widely connected online ecosystem, but also rendered it an attractive target for cyberattacks and online fraud. According to INTERPOL data, the types of financial fraud that represent the greatest threat to the MENA region are investment fraud, BEC, and impersonation fraud.

Investment Fraud: How Fake Returns Turn Victims into Money Mules

Investment fraud — particularly Ponzi schemes — is one of the most prevalent and financially damaging forms of fraud in the MENA region. Perpetrators impersonate legitimate fintech firms or investment platforms on social media and messaging applications, luring victims into closed groups with promises of high, quick returns for completing simple digital tasks or investing in crypto projects. Victims are then persuaded to deposit money into the offender's digital wallet, believing they are participating in genuine, profitable opportunities. Perpetrators initially pay victims small returns to build trust, then coerce them into larger investments. Victims from the region have also been coerced into acting as money mules, allowing their bank accounts to be used as transit hubs for funds stolen from other victims, thereby facilitating money laundering and expanding the perpetrator's operational reach.

Business Email Compromise: Manipulating Victims and Deceiving Businesses

BEC, another prevalent trend in the MENA region, exploits trust in business communications and digital vulnerabilities — including email systems, the internet, and electronic stock trading platforms — to defraud individuals and businesses through sophisticated social engineering tactics. According to member countries in the region, BEC shows convergence with impersonation fraud by exploiting established trust in vendor communications, blending technical intrusion with psychological manipulation to bypass internal financial controls without requiring direct system compromise. Data shows that BEC attacks on the MENA region originate from criminal networks in West and North Africa.

Impersonation Fraud: Exploiting Emotional Vulnerability to Deceive Victims

In the MENA region, perpetrators often impersonate banks, financial institutions, or delivery services through spoofed calls, phishing emails, or deceiving social media profiles, using fear-based narratives — such as risks of account suspension — to manipulate victims. Other schemes involve impersonating money transfer agents with forged identity documents to manipulate people into wiring funds under false pretences. Additional schemes include emergency scams, in which fraudsters impersonate family members or friends and fabricate false claims of urgent crises to manipulate victims into sending money. This trend frequently converges with investment and identity fraud.

The Smuggling Scam: How Financial Fraud is Fuelling Human Trafficking

Scam centres have been detected in several countries across the MENA region. Criminal networks target refugees from Syria via social media, luring them with false promises of safe passage to Europe and fraudulent employment offers, extracting up to USD 5,000 per victim under the guise of smuggling fees.

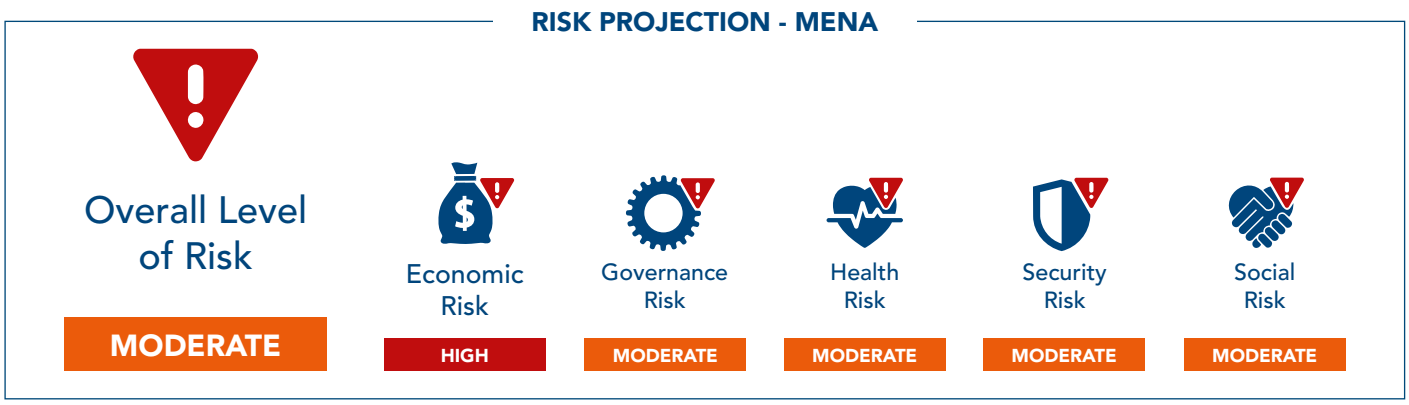
Once paid, victims are transported via Lebanon or Türkiye to Cyprus and Italy, where they are forced into labour or abandoned. This trend highlights a hybrid digital-physical enterprise where financial fraud directly funds and enables human exploitation. Stolen funds finance the victims' own captivity, while their personal data fuels further fraud.

Regional Risk Projections for the MENA Region

Member countries from the MENA region assess the overall risk level of financial fraud over the next three to five years as MODERATE, notably projecting stabilization in crimes related to financial fraud.

Member countries nonetheless forecast that the regional threat from financial fraud will most negatively impact the economic domain, where the regional risk is assessed as HIGH, with a major degree of harm anticipated.

In contrast, regional risks to governance, health, society and security are assessed by member countries as MODERATE, with projected harm to be moderate to governance and society, and minor to health and security.



Recommendations

Intelligence-Led Coordination and International Cooperation

- Strengthen interagency police cooperation, including with financial intelligence units, regulatory bodies and customs authorities, and address fraud as a networked, transnational threat rather than a series of isolated incidents.
- Direct analytical resources to map the criminal networks that enable and sustain fraudulent activity, including their cross-border operations, illicit financial flows, and the technological infrastructure on which they depend.

Operational Support and Rapid Response

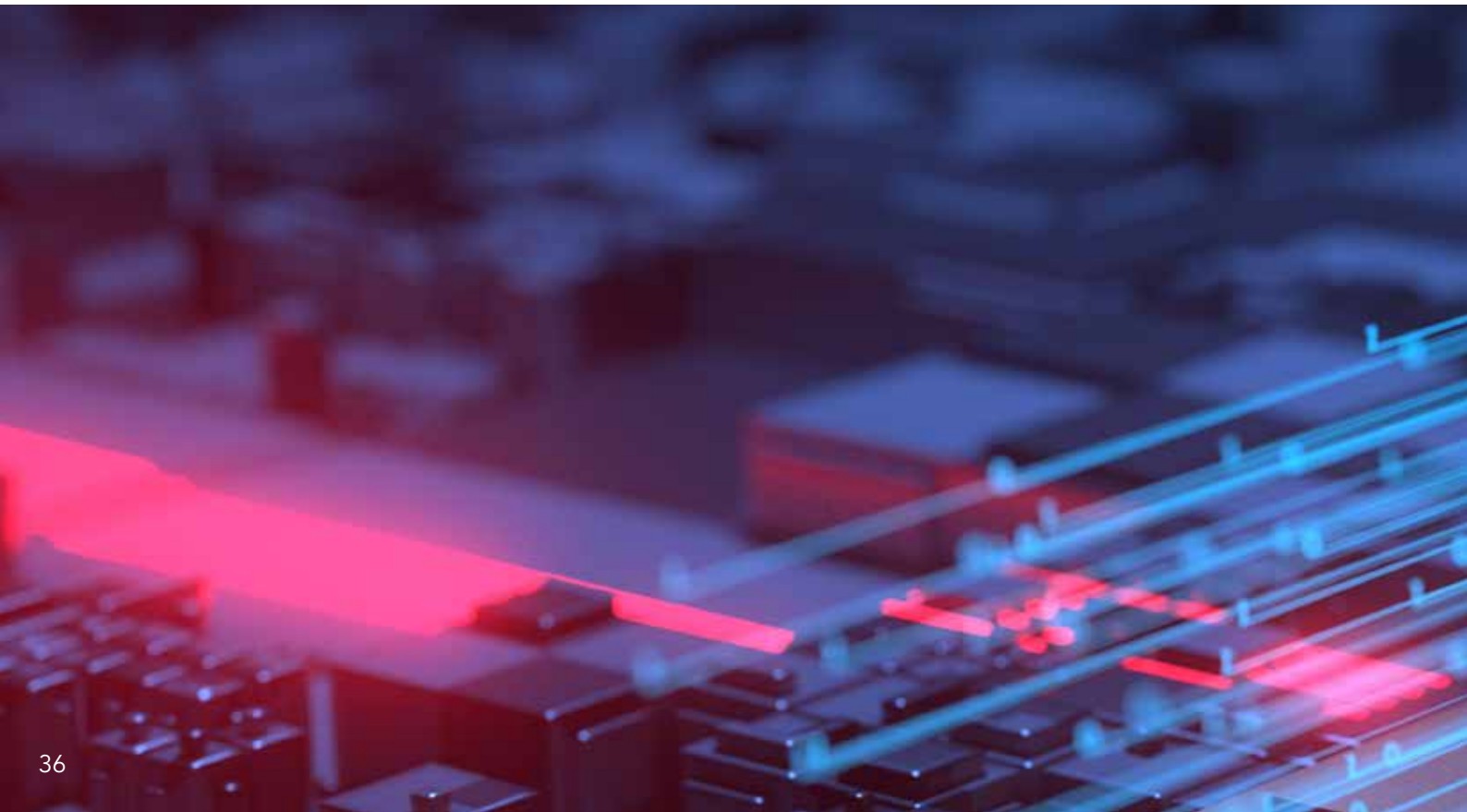
- Increase routine cooperation among member countries leveraging INTERPOL's secure communications system, global databases, and Notices and Diffusions framework, to facilitate coordinated intelligence exchange and the tracing of illicit assets across jurisdictions.
- Promote the implementation of coordinated rapid stop-payment and asset-freezing measures to intercept stolen funds before they can be moved or laundered, in particular INTERPOL's I-GRIP stop payment mechanism, which enables authorities to trace, intercept and block criminal proceeds across borders.

Build Capacity amongst Investigators

- Enhance investigators' capabilities to address the evolving nature of fraud and financial crime by utilizing appropriate training resources. Priority areas should include financial investigation techniques, cryptocurrency tracing, AI-generated content detection (e.g. recognizing AI-enabled fraud schemes, deepfakes, and understanding indicators that support the identification or attribution of AI-produced materials), and intelligence analysis.
- Leverage INTERPOL capabilities for the deployment of specialized tools for processing large datasets and tracing digital payment flows, in order to improve data collection and the timely exchange of actionable intelligence among competent authorities.

Strengthen Legal and Regulatory Frameworks

- Improve legal frameworks as a response to the growing threats of AI-driven and cryptocurrency-based fraud, criminalizing the malicious use of generative AI for impersonation, voice cloning, and associated social engineering large-scale operations.
- Improve the regulatory oversight of virtual asset service providers, update KYC/AML procedures, real-time transaction monitoring mechanisms, and standardized reporting requirements.



Partnerships and Information Sharing

- Encourage structured and routine collaboration among banks, technology companies, telecommunications operators, and law enforcement agencies, recognizing that each sector holds complementary insights into the fraud threat landscape.
- Develop formal mechanisms for timely information sharing on suspicious transactions and fraudulent platforms, supported by appropriate legal and data-protection safeguards.

Fraud Reporting

- Develop crime reporting mechanisms as a strategic priority. A significant proportion of fraud and related crimes remain unreported. Reporting mechanisms should therefore be simple and accessible while also being highly visible to the public.
- Centralize collected data to enable the rapid identification of patterns, particularly recurring tactics such as impersonation schemes, investment fraud, and AI-enabled attacks.

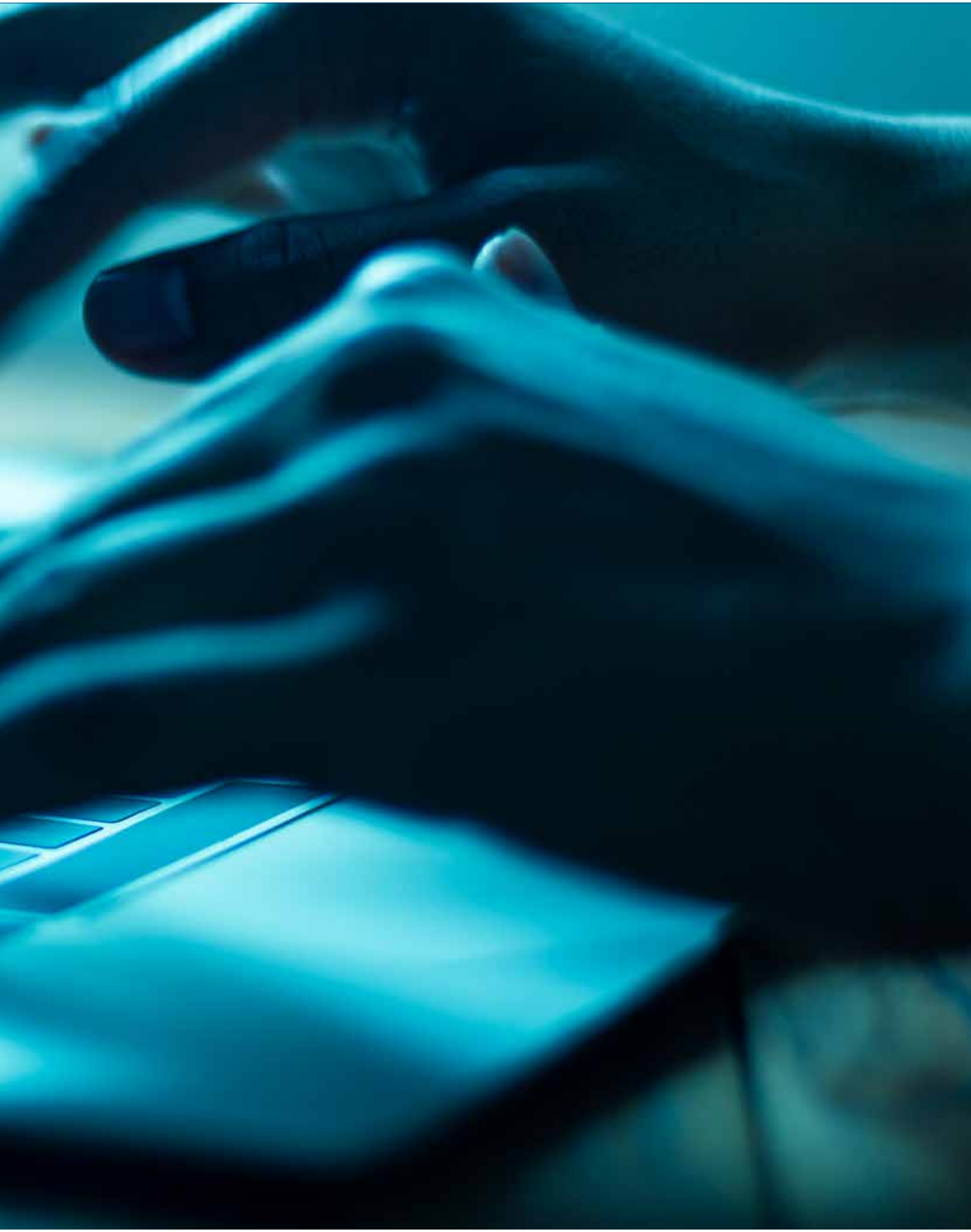
Prevention and Public Awareness

- Deliver clear and timely public warnings that include practical examples of current fraud schemes, such as scams involving AI-generated voices, fraudulent investment applications, romance manipulation, and malicious QR codes.
- Prioritize outreach to the most exposed groups, through targeted and accessible communication channels.

Victim Care

- Ensure appropriate support for the victims of fraud, noting in particular the prevalence of repeat victimisation of individuals. The provision of expert support to help victims, and those close to them, to understand what has happened and why, will promote recovery and resilience to future fraud attempts.
- Raise awareness and cultivate compassion among relevant authorities for the harm inflicted on victims of fraud, positively impacting their willingness to report crime and support future investigations. This includes avoiding the use of language which minimizes the crime or inadvertently assigns blame to victims.


connect to address 192.168.1.1
username: **********
password: **********
Access granted...
exited after 0.006146 seconds with return value
any key to continue . . .



INTERPOL

ABOUT INTERPOL

INTERPOL's role is to enable police in our 196 member countries to work together to fight transnational crime and make the world a safer place. We maintain global databases containing police information on criminals and crime, and we provide operational and forensic support, analysis services and training. These policing capabilities are delivered worldwide and support four global programmes: financial crime and corruption; counter-terrorism; cybercrime; and organized and emerging crime.

OUR VISION: "TOGETHER AGAINST CRIME"

In a world where crime knows no borders, it is clear that collective action is essential to combating crime effectively. INTERPOL serves as a unifying force that brings together police and stakeholders from around the globe with a shared aim: to tackle crime and create a safer world.

www.interpol.int | INTERPOL | @INTERPOL_HQ | INTERPOL_HQ | INTERPOL HQ | INTERPOL