INTERPOL

INTERPOL GLOBAL FINANCIAL FRAUD ASSESSMENT

MAY 2024

Disclaimer

This publication must not be reproduced in whole or in part and in any form without special permission from the copyright holder. When the right to reproduce this publication is granted, INTERPOL would appreciate receiving a copy of any publication that uses it as a source.

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

Executive Summary – Key Findings

Financial fraud has increased and diversified significantly, both in terms of the volume of fraud offences and the methods deployed to perpetrate them. Today, financial fraud represents a pervasive, global threat.

Understood as an umbrella category, encompassing those activities that "aim at the procurement of a financial gain through deliberate, deceitful actions against individuals and to their detriment," fraud does not only wreak major financial losses on individuals and businesses, but also undermines domestic and global economies by eroding trust and weakening the integrity of financial systems.

The INTERPOL Global Financial Fraud Assessment constitutes an in-depth analysis of INTERPOL data holdings on offences and offenders related to financial fraud, which has been perpetrated against individuals and/or businesses, including INTERPOL Notices and/or Diffusions linked to financial fraud offences. The key findings from this assessment include:

- The most prevalent types of financial fraud at the global level are investment fraud, advance-payment fraud, romance fraud and business email compromise;
- Financial fraud is increasingly dependent on information and communication technologies, which by their nature are globalized, meaning that fraud operations are transnational and often transcontinental;
- Offenders are making use of emerging technology, particularly Artificial Intelligence (AI) such as deepfakes, to deceive their victims and conceal their identities;
- Information suggests that the use of "scam centres" or compounds are increasingly prevalent, including those which depend on human trafficking for forced criminality with this trend detected in Southeast Asia, West, East and Southern Africa, Eastern Europe and Latin America;
- The so-called "pig-butchering" fraud scheme, a hybrid modus operandi combining romance fraud and investment fraud, often using cryptocurrencies, is escalating and expanding and victims hesitant to come forward.
- Financial fraud is most often perpetrated by a network of co-offenders, where the degree of organization varies from highly structured to loosely organized crime groups;
- Crime convergence frequently occurs around financial fraud where cybercrimes-as-a-service and money-laundering-as-a-service are important in empowering fraudsters, both individual offenders and crime groups.
- While modi operandi may be understood, less is known about fraud offenders and "how fraud is organized," and there is an urgent need to strengthen data collection and analysis on financial fraud in order to develop more informed and effective counter strategies.

Financial fraud is a predatory crime which is perpetrated in anonymity and across borders. INTERPOL remains engaged to support member countries in the global fight against financial fraud, from data collection and crime analysis to operational support.

The findings in this report are part of an of an ongoing analytical initiative to assess current and emerging crime threats in order to produce the INTERPOL Global Crime Threat Assessment, which will be available to law enforcement in INTERPOL member countries in November 2024.

Introduction

In an increasingly digitalized and interconnected world, financial fraud has become a pervasive and costly threat to individuals and businesses alike. The economic impact of fraud is staggering. As technology evolves, so do the modi operandi used by fraudsters, who are quick to exploit new vulnerabilities and adapt their tactics to circumvent security measures, staying one step ahead of law enforcement agencies.

Identifying and assessing the threat posed by various fraud types (i.e. offence methods) as well as the factors driving its growth and the threat actors involved are crucial to countering this multifaceted threat. However, due to the reluctance of its victims to come forward, financial fraud is largely underreported to law enforcement, resulting in the true extent and impact of this crime almost certainly not being fully appreciated.

In addition, where information and research on financial fraud does exist, it often focuses on modi operandi whereas much less is known about the different profiles of fraud offenders and, more importantly, "how fraud is organized." It is clear that financial fraud requires varying degrees of collaboration between co-offenders but the nature and scope of crime convergence needs to be better understood.

Assessing the information available to INTERPOL, the purpose of this report is to present an assessment of global financial fraud trends, how they manifest at the regional and global levels and who are the threat actors, in order to develop informed and effective strategies for collective action against individuals and organized crime groups engaged in perpetrating financial fraud.

Methodology

The INTERPOL Global Financial Fraud Assessment has been elaborated following an all-sources methodology. Most of the data analyzed has been extracted from INTERPOL data holdings, including INTERPOL's Notices and Diffusions with offences related to financial fraud, direct contributions from INTERPOL member countries and partners, operational messages from member countries and responses to the 2022 and 2024 INTERPOL Global Crime Trend Questionnaires for financial fraud. Where appropriate, this data was complemented with open-source documentation produced by international partners in the public and private sectors.

Analytical framework

The conceptualisation of financial fraud in this report stems from an operational, law enforcement perspective. As such, this report refers to financial fraud as an umbrella term 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[1]."

From this point of view, financial fraud is fundamentally an interplay of two elements: motive (obtaining a financial gain) and means (deception in various forms) with an effective combination resulting in an unjust advantage or benefit that is detrimental to another. Consequently, fraud types encountered by law enforcement are dynamic and evolve with changes in the social, economic, technological and legal environment.

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

Offence Methods for Financial Fraud (Modi Operandi)

Impersonation fraud

Impersonation fraud involves an offender posing as a person or an institution with whom the victim has, or could have, a pre-existing, real relationship, either personal, official, or business. For example, the offender might impersonate a tax or police authority, a service provider which the victim uses, or a distant acquaintance. Impersonation fraud typically relies on eliciting fear or worry to deceive their victim.

Business Email compromise

Business Email Compromise (BEC)[2] is an increasingly prevalent form of impersonation fraud, whereby fraudsters use social engineering techniques to target businesses by compromising email accounts and impersonating executives and business lawyers to trick employees to transfer funds to accounts owned by the fraudsters, who then quickly launder the funds. Criminals, sometimes operating out of scam centres, are capable of launching large-scale impersonation frauds targeting millions of businesses and individuals via emails, text messages, social media and robocalls.

Investment fraud

Investment fraud involves deceiving people into investing money in fake or misleading ventures, resulting in significant financial losses for the victims. This modus operandi represents a prolific threat as victims often experience the highest losses compared to other types of individual fraud. 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, which provides fraudsters with a wider base of victims, thereby maintaining the flow of investment and increasing criminal profits. Fraudsters often target potential victims or investors via social media, fraudulent websites or applications, tele-marketing campaigns (mostly conducted out of call centres or boiler rooms) and in-person. Fraudsters effectively deploy these communication techniques at various stages of the investment fraud scheme. Criminal groups or networks involved in investment fraud commonly adopt the mannerisms of a legitimate business entity to perpetrate their crime. The rise of cryptocurrency has created new opportunities for investment fraud. Market manipulation and financial grooming are some of the techniques used to perpetrate cryptocurrency investment fraud. Fraudsters use fraudulent crypto-investment platforms and "rug pulls" to persuade then later defraud investors.

RUG PULL

IN 2023, INTERPOL IDENTIFIED "RUG PULL" AS ONE OF THE GROWING DIGITAL INVESTMENT FRAUD PRACTICES. THIS MODUS OPERANDI INVOLVES THE SUDDEN ABANDONMENT OF CRYPTOCURRENCY PROJECTS BY THE DEVELOPERS CAUSING INVESTORS TO LOSE THEIR MONEY[3].

[2] Although a sub-type of impersonation fraud, BEC has been assessed independently in this Report due to the volume/frequency of this method of financial fraud reported across regions.

[3] INTERPOL, "USD 300 Million Seized and 3,500 Suspects Arrested in International Financial Crime Operation", 19 December 2023, https://www.interpol.int/en/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation

Among the many modi operandi which are used to perpetrate financial fraud, INTERPOL has detected that impersonation fraud, investment fraud, romance fraud, advance-payment fraud and identity fraud are the most globally pervasive threats.

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. The victims are ultimately manipulated by the offender, often multiple times, who is motivated by financial gain, causing both emotional and financial harm to the victim.

Advance-payment fraud

Advance-payment fraud, one of the most prevalent fraud types, 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 goods and services which are in demand 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 from how it was advertised.

Identity fraud

Identity fraud refers to the unauthorized acquisition and use of an individual's personal information (username and passwords, credit card credentials, biometric data, etc.) intended for obtention of an illicit financial gain. Identity 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, an enabler, which refers to the technique employed for the acquisition of personal data intended for the obtention of an illicit financial gain and, on the other hand, the use of these data for such purposes[4]. Fraudsters can perpetrate identity fraud without the direct involvement of the victim, whose identity has been stolen. In addition to stealing funds, fraudsters often sell compromised personal information on online criminal markets. This personal information can be further exploited by criminals to commit identity fraud, revictimize targets and facilitate the deceptive techniques used in other fraud types such as romance fraud.

OPERATION NERVONE

In July 2023, INTERPOL and its partners targeted a criminal group believed to have launched over **30 SOPHISTICATED SPEAR** phishing campaigns across

15 countries in Africa, Asia and Latin America, stealing potentially as much as

USD 30 MILLION from financial institutions and mobile banking services since 2019.

[4] Hereafter, the assessment of identity fraud will focus on the threat posed by phishing as well as other social engineering and intrusion techniques.

INTERPOL Data and Trends in Financial Fraud

According to the 2022 INTERPOL Global Crime Trend Report, financial fraud constitutes one of the highest threat concerns among INTERPOL membership. When surveyed, a majority of respondents, from all regions of the world, indicated that they expected financial crimes, including financial frauds, to increase or significantly increase in the next three to five years.

Between 2022 and 2023, 85 per cent of Red Notices and Diffusions issued by INTERPOL member countries were related to fraud,. These Red Notices and Diffusions were mostly issued by European countries, followed by countries from the Asia and Americas region.

According to reports from INTERPOL member countries, the commission of financial fraud has a transnational component in most cases, with individuals being the most frequent victim over private sector entities. In 2023 alone, INTERPOL Financial and Anti-Corruption Centre (IFCACC) supported over 700 financial fraud cases initiated by member countries, which concerned approximately USD 1.2 billion. At the global scale, BEC and investment fraud constituted the most prevalent types of financial fraud reported to INTERPOL, followed by impersonation fraud, advance-payment fraud, romance fraud and phishing. Despite financial fraud being ubiquitous throughout the globe, different trends can be identified across regions.

In the **Asian** region[5], impersonation fraud, romance fraud and phishing are the most frequent forms of fraud. While half of the cases reported in 2023 by Asian countries originated within the region, financial fraud is not an endogenous threat, as INTERPOL has also identified cases of BEC committed from Europe and the Americas, and romance fraud from Africa, all of them targeting Asian countries.

For the case of **Africa**[6], advance-payment fraud constitutes the most concerning form of financial fraud, followed by investment fraud, BEC and romance fraud. Fraud cases reported by African member countries during 2023 were committed from Asia, Africa and Europe. However, Africa (especially West African countries) remains an important source of financial fraud within the continent and beyond, which was recently confirmed by INTERPOL-led Operations Contender and Killerbee.

Investment fraud constitutes the most concerning type of fraud in the **European** region, followed by BEC, romance fraud and telecom fraud. Regarding the **Americas**, phishing schemes, BEC and advance-payment fraud are an emerging concern, although there remain significant intelligence gaps that prevent a thorough assessment of the threat in the Americas.

[5] In this Assessment, the Asian region includes countries in the Middle East and Pacific countries unless stated otherwise.

[6] Similarly, the African region includes countries in the North of Africa unless stated otherwise.

Emerging Trends in Financial Fraud

Capitalizing on Technological Advancements

Within financial fraud, technology has emerged as the key enabling factor for criminal groups. The use of AI, large language models (LLM) and cryptocurrencies can scale up certain types of financial fraud exponentially with low levels of investment.

The use of synthetic content generated through AI, also known as "deepfakes," for the purpose of online fraud, is an emerging trend and an increasing concern for member countries. The barrier to entry for using generative AI and deepfakes is ever decreasing as technology becomes more user-friendly and accessible.

The business models of as crime-as-a-service (CaaS), phishing-as-a-service (PaaS) and ransomware-as-a-service (RaaS) continue to lower the barrier of entry for new and less technologically proficient cybercriminals, facilitating more online fraud and enabling threat actors to conduct more sophisticated fraud campaigns without the need for advanced technical skills. These models allow for skill-sharing and distribution of complex criminal software or stolen personal data on the darknet or deepweb where trusted parties openly trade in data, hosting services and software. The CaaS model also helps organized crime groups to recruit and expand their network of money mules. In combination with these elements, a rapidly growing population of online users worldwide constitutes the breeding ground for a rapid expansion of financial fraud across regions.

INTERPOL data confirms that cryptocurrencies and cryptocurrency service providers are widely used in investment and romance fraud and, to a lesser extent, in advance-payment and telecom fraud. While the use of Bitcoin in financial fraud schemes is common throughout the world, Tether (also known as USDT) and Altcoins have been reported by member countries in Africa, Southeast and East Asia, and the Pacific, and Etherium for the case of Europe. Services offered by Virtual Asset Service Providers (VASPs) such as Binance, and virtual payment and investment service systems such as Skrill, Perfect Money, Netteller, Altcoin Trader and Luno Trading have also been reported to be misused by fraudsters to facilitate acts of financial fraud with a cryptocurrency component, especially in Africa, Asia and Europe. In some cases, criminals set up, or outsource the setting up of, their own fake investment app as part of their deception strategies. Criminals have also been reported to create mirror investment platforms, mimicking reputable investment companies or services. The criminals manipulate trades and display inflated profits on these cloned platforms, creating the illusion of success and encouraging victims to invest more money in the fraudulent schemes.

The adoption of deepfakes and LLMs further benefit criminal networks. There have been recent cases within member countries where deepfake photographs have been created for opening online bank accounts to expand money mule networks. Whereas LLMs have been used for investment and job scam purposes in online forums and using widely available instant messaging applications. It should be noted that in each instance the technology was relatively crude in application, but it showed immense potential for sophistication.

Financial Fraud and Forced Criminality

INTERPOL research and analysis brought to light a trend involving human trafficking for the purpose of forced online fraud. This trend refers to a modus operandi involving, on the one hand, Victims (A) - those who are trafficked and forced to conduct online fraud in so-called scam call centres or compounds and, on the other hand, Victims (B) - those who are defrauded of large sums of money by the trafficked victims. In the framework of Operation STORM MAKERS I & II, INTERPOL's Human Trafficking and Smuggling of Migrants (HTSM) Unit identified large-scale, cyber-enabled human trafficking operations perpetrated by Asian crime syndicates for the purpose of forced online fraud across several Southeast Asian countries[7]. Whilst originally, trafficked individuals were mostly Chinese-speaking victims, as the trend spread, both recruitment and defrauding strategies further evolved to include victims from across the world[8].

OPERATIONS STORM MAKERS I AND II

In 2022, during Operation STORM MAKERS, INTERPOL's HTSM Unit started receiving reports of trafficked victims trapped in scam centres in South East Asia. In 2023, Operation STORM MAKERS II, which was aimed at identifying and dismantling criminal organizations engaged in human trafficking and smuggling of migrants, entailed a unique focus on the trend of human trafficking for the purpose of online fraud in Southeast Asia and other impacted regions.

Although it is important to note that not all scam centres depend on the use of forced criminality, information recently shared by member countries with INTERPOL suggests that scam centres or compounds that do exploit trafficked victims have begun to emerge across the globe. In Latin America, INTERPOL member countries have reported the identification of a similar modus operandi where Victims (A), who typically originate from the region, are recruited through fake job advertisements, sometimes in public spaces. Once in the compounds, their identity documents are taken and they are forced to commit online financial fraud, mostly in the form of advance-payment fraud, telecom fraud and impersonation fraud. These schemes tend to involve relatively small sums of money (between USD 100 and USD 500), but they are replicated on a large-scale through social media platforms and online marketplaces. The fact that small sums are involved often discourages victims from reporting the fraud, which prevents the identification of the criminal structures behind these fraud schemes.

Furthermore, INTERPOL has been notified of the existence of similar scam centres in African countries, targeting not only individuals and businesses in the African region, but also worldwide.

Regarding Europe, and based on cases shared with INTERPOL, scam centres were reportedly active since the 2010s in European countries among other member countries. Moreover, and although intelligence gaps remain, there are reports pointing at the existence of human trafficking-fuelled scam centres in Eastern European countries, where local groups are believed to be collaborating with foreign criminal organizations. In these cases, Victims (A) are reportedly from the Middle East.

As this modus operandi continues to expand and the profiles of Victims (A) become more diversified, with victims from Asia, Africa and Latin America being held in scam centres, it is highly likely that the pool of targeted Victims (B) will further enlarge. In addition, the emergence of AI-generated content will likely increase the reach, sophistication and capacity of fraud schemes conducted through trafficking-driven scam centres, resulting in the expansion of fraud worldwide.

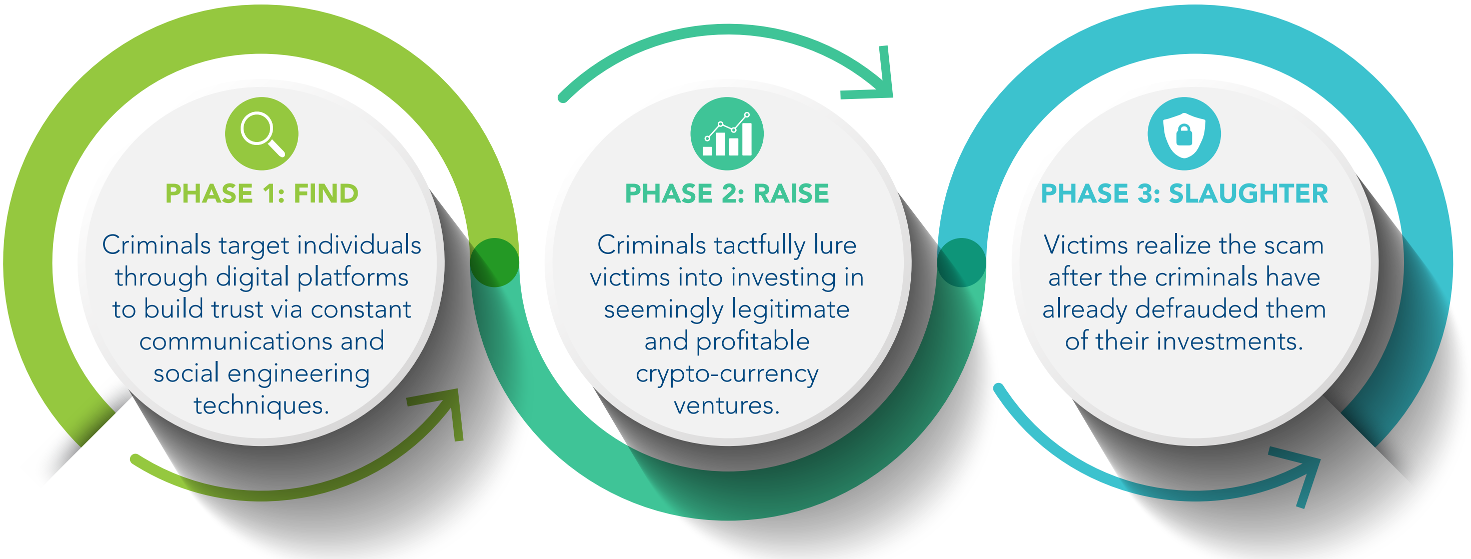
[7] INTERPOL. Online Scams and Human Trafficking in South East Asia. 25 October 2022. Public Version. INTERPOL for Official Use Only.

[8] INTERPOL. Online scams and Human Trafficking in South East Asia / Update 2 – From Regional to Global Threat (PUBLIC Version). 06 July 2023. INTERPOL for official use only.

Hybrid Methods of Financial Fraud – The Escalation of Crypto Investment Fraud

Since 2022, INTERPOL has not only observed a notable escalation in cases but also the growing complexity and sophistication of online financial frauds. One trend, which is sometimes known as "pig butchering[9]," has rapidly emerged as a major concern for law enforcement with victims from across the globe losing millions to savvy financial fraudsters. This fraud is a hybrid method that combines elements of romance fraud and crypto-investment fraud where criminals manipulate cryptocurrency trades and display inflated profits to motivate victims to invest more money in fraudulent schemes.

Crypto investment fraud frequently commences as a type of romance fraud, with skilled fraudsters targeting victims via social media platforms, dating applications, and often even sending direct messages to phone numbers. The phenomenon of re-victimization is a relevant aspect of this crime type. Re-victimization does not only increase the financial damage, but it also aggravates the psychological and emotional trauma experienced by the victims. This modus operandi, beyond its immediate financial implications, poses significant challenges due to its international scale and the utilization of cryptocurrencies.



PHASE 1: FIND

Criminals target individuals through digital platforms to build trust via constant communications and social engineering techniques.

PHASE 2: RAISE

Criminals tactfully lure victims into investing in seemingly legitimate and profitable crypto-currency ventures.

PHASE 3: SLAUGHTER

Victims realize the scam after the criminals have already defrauded them of their investments.

The phases of "Crypto Investment Fraud" (Source: IGCR 2023)[10]

Recent INTERPOL research demonstrates the expanding geographical footprint of this trend. There is evidence that the trend is increasingly spreading beyond its original hub in Southeast Asia and is being replicated in other regions such as Africa and Latin America, where call centres similar to the ones in Southeast Asia have emerged. INTERPOL information confirm that Asian organized crime syndicates were recruiting youths, mainly students, to conduct online fraud out of call centres in Southern Africa. These criminals lure their victims, who are primarily based in the North America to invest in cryptocurrency fraud schemes. INTERPOL expects online fraud schemes, including romance and investment frauds linked to cryptocurrencies, to increase in the near future as the emergence of this hybrid modus operandi will add another layer of complexity to these fraud types.

[9] INTERPOL prefers to not use this terminology to refer to this financial fraud modus operandi out of respect to its victims and due to other possible sensitivities.

[10] INTERPOL, 2023 INTERPOL Global Crime Report, November 2023, p.19

Regional Trends in Financial Fraud

OPERATIONS DELILAH, FALCON II, AFRICA CYBER SURGE I & II, CONTENDER

BETWEEN 2022 AND 2023, INTERPOL CONDUCTED SEVERAL OPERATIONS, INCLUDING OPERATION DELILAH, OPERATION FALCON II, AFRICA CYBER SURGE OPERATION I & II, AND OPERATION CONTENDER, ACROSS THE AFRICAN CONTINENT TARGETING CRIMINAL GROUPS AND ACTORS ENGAGED IN BEC, ROMANCE FRAUDS, CRYPTOCURRENCY FRAUDS, PHISHING AND OTHER CYBERCRIMES[11].

Africa

The African financial sector has rapidly digitalized and the region is among global leaders in the use of mobile banking and money transactions. This has opened up a multitude of opportunities to criminals to perpetrate financial fraud.

According to INTERPOL's 2023 African Cyberthreat Assessment Report, BEC, phishing and other online frauds are a growing concern in Africa due to the rapid transition to an increasingly digitalized economy[12]. Expanding Internet access coupled with poor levels of digital literacy make many Africans easy targets for fraudsters and cybercriminals.

BEC remains one of the most prevalent trends in Africa, causing major financial losses for individuals and businesses. Many actors carrying out BEC fraud have been found to be based in West Africa, but their victims are often based in other jurisdictions. These criminals often have connections with larger criminal networks worldwide, which allow them to target large numbers of victims on a global scale.

Online frauds include a wide range of fraudulent activities in the digital sphere. Advance-payment/non-delivery frauds, e-commerce fraud, romance fraud, tech support fraud and cryptocurrency (investment) fraud are among the most common online fraud and they are becoming increasingly prevalent in the African region.

Also of concern is the increasing use of hybrid crypto investment fraud in Africa. Cases of this fraud type have been identified in West and Southern Africa targeting victims in other jurisdictions beyond the continent.

CaaS is becoming an increasingly popular trend in Africa. It has lowered the entry barrier for new, less technology-savvy cyber-criminals, and facilitates cyber-criminals' malicious activities by enabling them to carry out sophisticated attacks without the need for advanced technical skills.

INTERPOL information suggests that certain West African criminal groups continue to grow more transnational and are well-established in countries and regions across the globe. These West African organized crime groups, which are engaged in polycriminality, are known to be involved in and have extensive skills in online financial fraud such as romance fraud, investment fraud, advance fee fraud, and cryptocurrency fraud.

[11] INTERPOL (Cybercrime Directorate), AFJOC - African Joint Operation against Cybercrime, 2023, https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime (accessed 13 February 2024)

[12] INTERPOL (Cybercrime Directorate), African Cyberthreat Assessment Report 2023: Cyberthreat Trends, March 2023, (accessed 12 February 2023)

OPERATION JACKAL

INTERPOL's Operation Jackal, launched in May 2023, targeted West African crime groups in 21 countries across the world resulting in over

100 ARRESTS

THE OPERATION ALSO LED TO THE BLOCKING OF OVER 200 BANK ACCOUNTS LINKED TO PROCEEDS OF ONLINE FINANCIAL CRIME.

Americas

In line with global trends, online financial frauds, many exploiting increased demands for medical supplies and other vulnerabilities heightened by the pandemic, escalated considerably across the Americas region, particularly targeting private citizen and businesses in North America. The 2022 INTERPOL Global Crime Trend Report indicated that some of the most common types of fraud were impersonation, romance, tech support, advance-payment and telecom frauds[13].

Businesses and citizens in this region have incurred huge financial losses through online financial fraud. These threats have been reported to emanate mainly from Africa and Asia where organized crime groups like the West African criminal confraternities and Asian crime syndicates operate respectively. The rise in financial losses through financial fraud also poses an increased money laundering threat.

Human trafficking-fuelled fraud continues to be a growing crime phenomenon. An INTERPOL-coordinated operation, Operation Turquesa V, revealed that hundreds of victims were trafficked out of the region after being lured via messaging apps and social media platforms and coerced to commit fraud, including investments frauds in boiler rooms run by crime syndicates in Southeast Asia[14].

There is emerging evidence that Latin American crime syndicates are also involved in the commission of financial fraud, a trend that presumably took off more vigorously following the COVID-19 outbreak. While these groups have been traditionally linked to drug trafficking, arms trafficking, money laundering, kidnapping and episodes of heightened criminal violence at the national and regional levels.

Crime service providers are making financial fraud relatively easy, low-risk and lucrative. Digital tools and technology increase the scale of operations, ensure the anonymity of offenders, and facilitate the laundering of criminal proceeds. For these reasons, it is very likely that more criminal organizations will take on new financial fraud ventures.

[13] INTERPOL, 2022 INTERPOL Global Crime Trend Report, October 2022

[14] INTERPOL, Americas: 257 suspected migrant smugglers and human traffickers arrested, 11 December 2023, https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2023/Americas-257-suspected-migrant-smugglers-and-human-traffickers-arrested

OPERATION HAECHI IV

In December 2023, INTERPOL concluded a transcontinental police operation against cyber-enabled frauds and other cybercrimes (romance fraud, investment fraud, BEC, e-commerce fraud, voice phishing, online sextortion and money laundering associated with online gambling), which resulted in almost 3,500 arrests and seizures of USD 300 million worth of assets across 34 countries in Africa, the Americas, Asia, Europe and Oceania.

The Operation also alerted member countries to an emerging cryptocurrency fraud technique called "rug pull" or exit fraud, where developers create a new token and promote it to investors, only to suddenly abandon the project causing investors to lose their money. HAECHI IV also uncovered the increasing use of AI and deep fake technology to defraud, harass and extort victims, particularly through impersonation, romance and investment frauds.

3,500 ARRESTS

USD 300 MILLION

34 COUNTRIES

Asia

Financial fraud is a fast-evolving threat in the region. Member countries in the region have become prime targets of financial fraud given their position among the fastest-growing digital economies in the world. The COVID-19 pandemic accelerated the digitalization of the services and behaviours of private citizens and businesses in the Asian region. As a consequence, financial frauds, largely cyber-enabled, have escalated and are expected to continue to escalate. Member countries in the Asian region frequently indicated that financial fraud was the crime trend that posed a very high threat.

INTERPOL recently identified the pig butchering fraud scheme, which is a variation of the traditional romance fraud that involves a cryptocurrency investment element. These schemes were first initiated in Asia in 2019 and expanded during the COVID-19 pandemic. Subsequently, Asia has emerged as a focal point, with criminal organisations in poorer countries across the region employing business-like structures, in some cases exploiting victims of human trafficking to perpetrate these fraudulent activities. Research indicates that this modus operandi is fast expanding to other jurisdictions beyond Asia.

Another fraud type that has experienced a surge in recent years in Asia is a telecommunication fraud whereby perpetrators use local and international lines from their hubs in some countries in the region to impersonating law enforcement officers or bank officials to trick victims to disclose their credit card or bank account credentials or to hand over huge amounts of money.

According to the 2021 ASEAN Cyberthreat Assessment, BEC, phishing and e-commerce fraud are some of the crime trends that continue pose a very high threat to member countries in the region. INTERPOL anticipates that these trends will continue to grow in the next few years[15]. Evidence from Southeast Asia indicate that one member country lost over USD 500 million to fraud in 2023 with over 30 per cent of that amount lost to investment fraud[16].

While data available to INTERPOL reveals that all age groups are vulnerable to fraud, the majority of victims in the Asian region are aged 30 to 49. The victims are mainly targeted through social media and messaging platforms. Financial fraud in the region shows no signs of slowing down or decreasing as fraudsters and cybercriminals continue to embrace technology.

[15] INTERPOL (Cybercrime Directorate), ASEAN Cyberthreat Assessment 2021: Key Cyberthreat Trends Outlook From The ASEAN Cybercrime Operations Desk, 21 January 2021, https://www.interpol.int/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia (accessed 13 February 2024)

[16] Singapore Police Force, Annual Scams and Cybercrime Brief 2023, 18 February 2024, p.8

Europe

European countries have indicated that financial fraud poses a very high threat to individuals, companies and public institutions in the region. Similar to other regions, the use of online tools by criminals to perpetrate financial fraud schemes has also rapidly expanded since the pandemic. There is evidence that cyber-enabled fraud even accounts for over 80 per cent of reported frauds in some countries in the region. Money laundering related to fraud is prevalent, with modi operandi that are subject to less severe financial controls likely being exploited, including the use of cryptocurrency to launder illicit proceeds.

Online investment frauds, phishing, and other online financial fraud schemes have escalated on carefully selected targets to maximize profits. Mobile phone apps are also being targeted by cybercriminals. Based on available information, investment fraud and BEC are the most prolific fraud types causing the highest financial losses in the region[17]. Online fraud schemes represent a fast-growing threat as fraudsters increasingly target individuals, companies and public institutions across Europe. The criminal networks involved in these online schemes often display sophisticated and complex modi operandi, which are usually a combination of different fraud types.

Frauds exploiting major crisis or emergency situations, such as the conflict in Ukraine and the deadly earthquake in Türkiye have been detected increasingly in the last few years[18]. Fraudsters posing as genuine organizations or celebrities pretending to raise funds for humanitarian efforts thereby tricking victims to make financial payments often in the form of cryptocurrency.

Crypto investment frauds, predominantly conducted from boiler rooms in Southeast Asia, is also on the rise. Based on available data, call centres such as the ones run by Southeast Asian organized crime syndicates have been identified in Europe, though this is rare. INTERPOL analysis has also identified the existence of organized crime groups led by nationals from countries in the Middle East that specialize in impersonation fraud (CEO fraud), foreign currency (Forex) fraud, telecom fraud and romance fraud, often in call centres. While there is emerging evidence pointing at cooperation between European organized crime groups cooperating with these crime groups for the commission of financial fraud in different forms, these centres are believed to be located -at least- in Eastern Europe and presumably in some African countries.

However, the main threat of online fraud schemes, including investment, impersonation and romance frauds, remains from lone criminals and crime groups operating from West Africa, often with a European element and a wide network of associates, who facilitate elements of the fraud at the international level. Fraud operations in the region have established links to West African criminal confraternity.

Fraudsters have a good knowledge of banking protocols and access to a sophisticated and complex network of money mules making it difficult to follow the proceeds of fraud. The shift away from mainstream banks towards online banks, cryptocurrency, money transfer apps and gift cards to launder the proceeds of fraud make it difficult to identify its origin. Nonetheless, some countries have indicated that these laundered funds sometimes end up in other jurisdictions in West Africa and Southeast Asia.

Available evidence indicates that fraudsters and cybercriminals typically use social media and messaging apps to target individuals from European countries, both male and female aged between 30 and 80. Victims of fraud, especially in the case of romance fraud, are often vulnerable.

The growing presence of enablers, including phishing kits, remote administration tools, card dumps, databases of personal data, and manuals on fraud methods on dark web forums, is also facilitating the activities of criminals.

Online fraud schemes are expected to further increase in the near future as fraudsters and cybercriminals will likely continue to embrace new technologies and tools, including deepfakes and other generative AI variants to lure more victims. The growth of new technologies will add to the complexity of the evolving threat.

[17] EUROPOL, Online Fraud Schemes: A Web of Deceit (IOCTA 2023), 19 December 2023, https://www.europol.europa.eu/publication-events/main-reports/spotlight-report-online-fraud-iocta-2023

[18] EUROPOL, Online Fraud Schemes: A Web of Deceit (IOCTA 2023), 19 December 2023, https://www.europol.europa.eu/publication-events/main-reports/spotlight-report-online-fraud-iocta-2023

Organized Financial Fraud

Organized crime groups are major threat actors in the world of financial fraud. Their resources, structure, and predatory nature make them particularly dangerous. Although research is lacking on transnational organized crime groups that engage in financial fraud, INTERPOL data suggests that these networks of offenders are empowered by technology and partnerships that make them major threat actors in the financial fraud ecosystem and beyond. In fact, INTERPOL has observed that financial fraud and the laundering of its proceeds tend to converge with other criminal activities besides human trafficking, such as trafficking in drugs, counterfeit products and other illicit commodities. This convergence or networking effect is likely to be related to the establishment of said collaborative ties among criminal actors.

Crime groups involved in financial fraud often establish networks that not only cross national borders, but regional and continental borders as well. Collaboration with other co-offenders often ensures different aspects of criminal operations. Examples of roles played by financial fraud collaborators include:

- **Recruitment of skilled and/or knowledgeable accomplices:** identifying persons, including crime service providers with specific skillsets (e.g., tech experts, financial advisers, etc.) to fill crucial roles in their operations, including developing complex investment schemes.

- **Identifying targets and victims:** researching and determining which demographics or targets will be most susceptible to manipulation, or depending on the offence method being used, purchasing "lead" lists from persons how have access to information about potential targets.

- **Laundering illicit proceeds:** the transfer and laundering of criminal proceeds is fundamental to the sustained engagement of crime groups in financial fraud. This could be done by collaborating with legitimate business owners or seeking out other individuals or networks offering money-laundering-as-a-service. Criminal networks are moving the illicit proceeds of fraud at an increasing rate across physical and virtual borders using complex money laundering schemes. INTERPOL has established a stop-payment mechanism to curtail the laundering of millions of dollars generated from financial fraud (See table below).

I-GRIP CASE STUDY

A company based in Country A fell victim to impersonation fraud, involving criminals purporting to be the national bank. The victim transferred EUR 1.2 million to an account in Country B and EUR 2 million to another account in Country C.

The NCB of Country A alerted the victim's bank to request that the payment be blocked, if possible, and contacted the INTERPOL Financial Crime and Anti-Corruption Centre (IFCACC) for further coordination with Countries B and C to stop the payments and further dissipation of funds. In close coordination with IFCACC, the NCBs of Countries B and C requested that beneficiary banks in their respective jurisdictions stop the payments. The total loss of EUR 3.2 million was recovered within a day and returned to the victim.

Organized crime invests heavily in technology to create fake websites, social media profiles, and phishing emails that appear genuine. They can also develop automated tools to launch large-scale cyberattacks. The emergence of the CaaS model has greatly expanded opportunities for organized criminal groups to collaborate, sell and share resources. As mentioned earlier in this report, this criminal model does not only present a profitable enterprise for criminal entrepreneurs but it also lowers the barriers of entry to criminal groups with fewer technical skills.

Organized criminal structure

Financial fraud does not fundamentally require criminal collaboration depending on the offence method being used. However, some types of large-scale, cyber-enabled fraud are more likely to be perpetrated by transnational organized crime groups or syndicates. Although difficult to investigate, known syndicates appear to operate in both hierarchical structures and decentralized cells.

INTERPOL has observed that West African organized crime syndicates or confraternities generally respect a hierarchical model, with each member fulfilling a specific role and defined responsibility. However, sources have indicated to INTERPOL that these organization often intentionally try to confound police investigations by using misleading titles to distinguish their leadership. In the case of the West African confraternities, the hierarchical structure may also vary from country to country.

Other organized crime groups involved in financial fraud also operate in a more decentralized manner that provides services under the CaaS model. Groups operating in this model are less rigid and criminal relationship may be more ephemeral. According to a report co-authored by INTERPOL and partners, a criminal group was observed to operate under this model offering money laundering services to cyber-enabled fraudsters[19].

In the framework of this report, INTERPOL and its partners have identified several criminal organizations known for perpetrating financial frauds operating from different regions. Available data indicates that crime groups from East Asia, Latin America, West Africa, and Europe are involved in different forms of financial fraud and money laundering. The use of globalized information and communication technologies to perpetrate cyber-facilitated frauds means that these crime groups are capable of targeting victims in any jurisdiction across the world.

INTERPOL GLOBAL RAPID INTERVENTION OF PAYMENTS (I-GRIP)

INTERPOL introduced a global stop-payment mechanism to facilitate communication between member countries to intercept illicit money flows and help victims recover the funds stolen by criminal groups through cyber-enabled financial crimes. The coordination across jurisdictions increases the likelihood that swift and appropriate actions, to the extent authorized by national laws, can be taken before illicit payments are made, cash is withdrawn and/or assets transferred further. Since the launch of I-GRIP in 2022, INTERPOL helped member countries intercept more than USD 500 million in criminal proceeds stemming largely from cyber-enabled fraud.

[19] FATF, INTERPOL, EGMONT GROUP, Illicit Financial Flows from Cyber-Enabled Fraud, November 2023

Conclusions

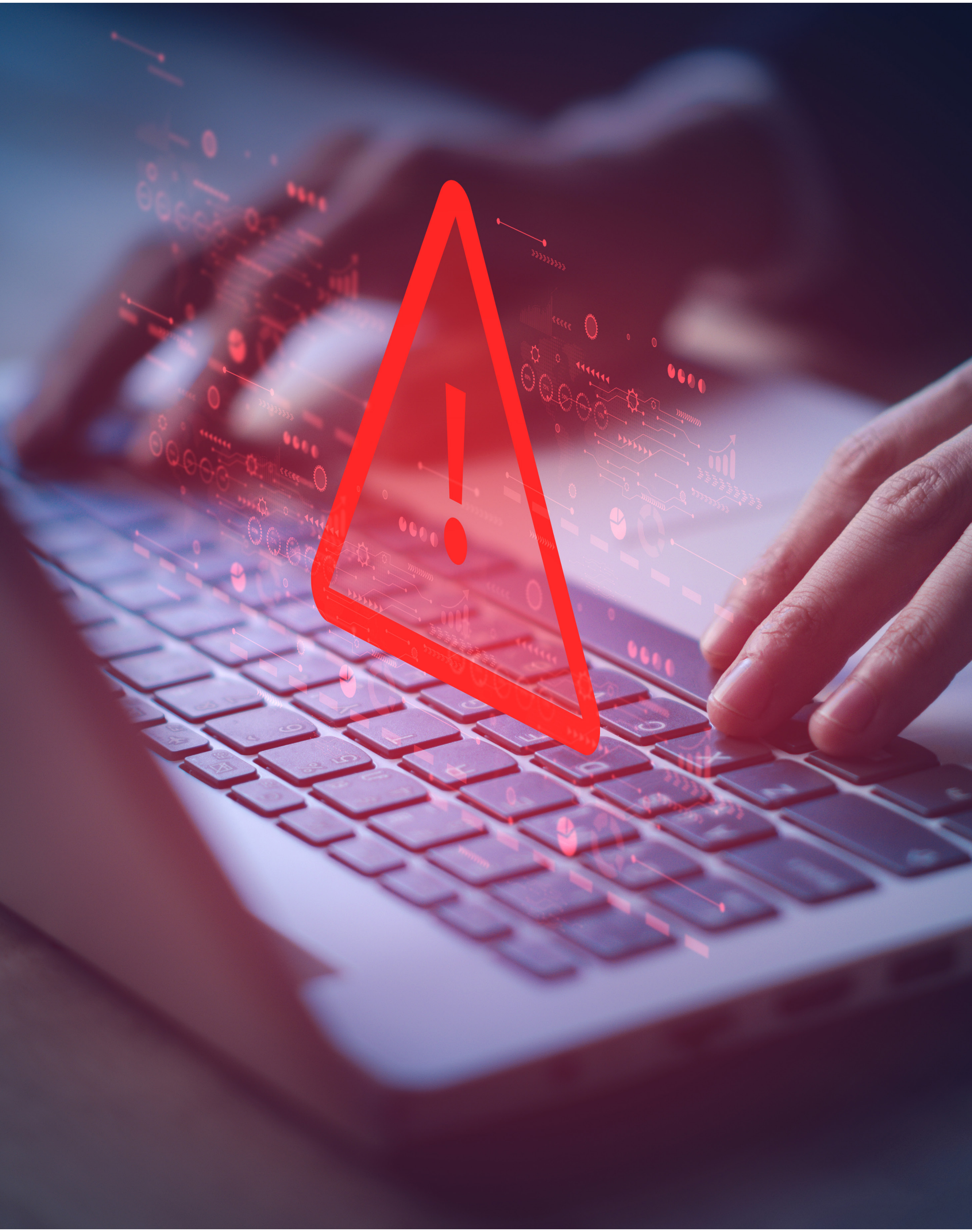
This report aims to assess INTERPOL data in order to understand how financial fraud trends are evolving, as well as to identify which trends are posing the highest threats to individuals and businesses in each region and globally. The report also examines the convergence between financial fraud and other crimes, specifically human trafficking and money laundering, and the dynamics of organized crime groups that are involved in perpetrating financial fraud.

According to INTERPOL data, investment fraud and BEC remain the dominant modi operandi at the global level. Although financial fraud remains ubiquitous across the globe, fraud trends vary from region to region: while impersonation fraud and romance fraud are the most prominent types of fraud in Asia, advanced-payment fraud is the most prevalent type of fraud in Africa, followed by BEC and romance fraud. In the case of Europe, it is BEC, telecom fraud and romance fraud. While phishing, BEC and advance-payment fraud dominate in the Americas.

Member countries expect the scale and magnitude of financial fraud to grow in tandem with technological advancements and the expansion of virtual services across the globe. New trends deploying AI and cryptocurrencies have already emerged and faudsters are also using "hybrid" techniques, combining romance frauds with investment schemes. However, the sophistication of new fraud techniques is hardly a barrier for less technologically savvy criminals. Crime service providers have become important enablers of largescale financial fraud, notably cybercrimes-as-a-service and money-laundering-as-a-service.

Financial fraud, especially cyber-enabled fraud, which is by default globalized and anonymous, is most often perpetrated by transnational organized crime groups. While more information needs to be collected to better understand the dynamics and extent to which organized crime groups are engaged in perpetrating financial fraud, the crime groups identified in this report indicate that organized fraud offenders do operate globally, appear to share criminal experiences and know-how, and most likely collaborate in order to optimize criminal opportunities and profits.

INTERPOL's efforts to assess the degree of threat posed by financial fraud, perpetrated by both individuals and groups, at the regional and global levels is ongoing and data from the Organization's 196 member countries remains critical to producing accurate assessments. The findings in this report will inform the Organization's strategy to support member countries in the fight against financial fraud and will also be further developed for inclusion in the INTERPOL Global Crime Threat Assessment, which will be published in November 2024.



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: "CONNECTING POLICE FOR A SAFER WORLD"

Our vision is that of a world where each and every law enforcement professional will be able through INTERPOL to securely communicate, share and access vital police information whenever and wherever needed, ensuring the safety of the world's citizens. We constantly provide and promote innovative and cutting-edge solutions to global challenges in policing and security.

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