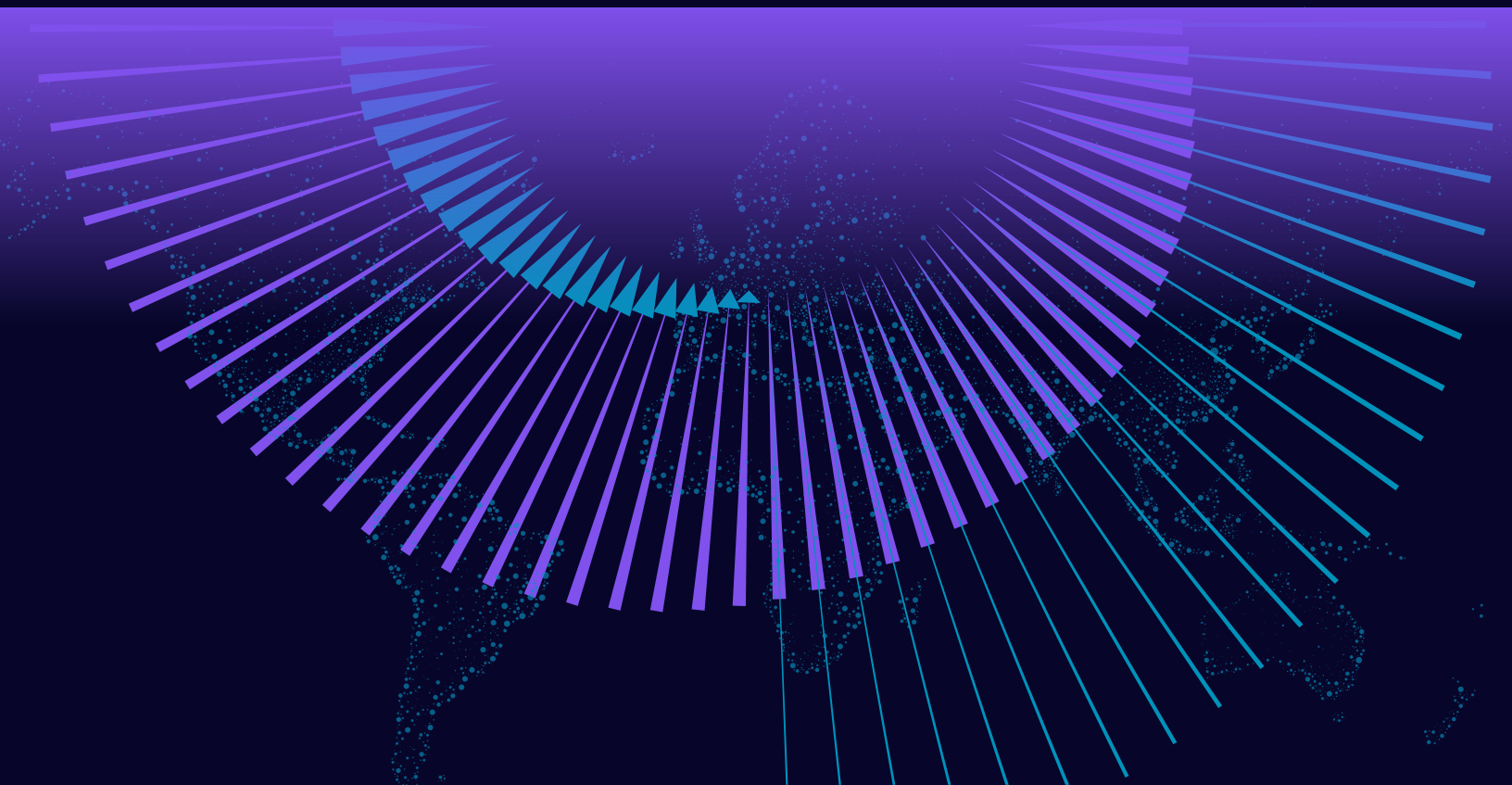
Nasdaq
Verafin

2026

Global Financial Crime Report

Inspiring Collective Action in a New Era of Evolving Threats



Message from Stephanie Champion

Executive Vice President, Head of Nasdaq Verafin

Stephanie Champion
EVP & Head of Nasdaq Verafin, Financial Crime Management Technology, Nasdaq

Today, the financial crime landscape is more complex and resistant to traditional defenses than ever before. The use of artificial intelligence (AI) by bad actors has boomed. Criminals have been quick to adopt the latest advances in AI to perfect their scam playbooks and maximize illicit profits. These aren't isolated cases — 90% of financial professionals we surveyed as a part of this report noted an increase in AI-driven attacks over the past two years.

AI alone isn't pushing the financial crime crisis to new heights. Criminal networks are orchestrating sophisticated schemes with the scale and coordination of multinational corporations. Troubling reports from around the world detail the rise of scam compounds, revealing new layers in the deeply interconnected worlds of human trafficking and fraud. In the two years since we published Nasdaq Verafin's inaugural Global Financial Crime Report, it is abundantly clear there has been a step change in the nature and scale of criminal threats.

> "In the wrong hands, AI is an accelerant for criminal activity, but in the hands of financial crime-fighters, it can be a true force for good."

A closer look at the numbers reveals a staggering surge in criminal activity. In just two years, global illicit financial activity has risen by $1.3 trillion, reaching an estimated $4.4 trillion in 2025 and outpacing GDP growth by a significant margin. Fraud totals surged to more than a half a trillion dollars, with losses estimated at $579.4 billion in 2025. These figures are not merely statistics, but represent significant institutional risk and immeasurable human cost.

Financial institutions are on the front lines of this fight, but they cannot defeat criminal threats in isolation. Increasingly, financial institutions are turning to external sources such as law enforcement or leveraging their peer financial institutions to aid in identifying new and emerging threats. However, while the industry has made great strides in developing channels for collaboration, significant gaps remain. The complexity of today's threats, coupled with increasingly faster payment channels and porous borders, demands a coordinated response across the public and private sectors, and across industries.

In this report, we have featured several organizations demonstrating what the future of coordinated action against financial crime looks like. These insights serve as a blueprint for driving stronger partnerships across the public and private sector, while delivering real protection for citizens around the globe.

If AI represents our biggest challenge, it is also presenting us with an opportunity to truly get ahead in the fight against financial crime. We are in the midst of a paradigm shift and the industry is investing heavily to strengthen its collective defenses. Three-quarters of anti-financial crime professionals we surveyed plan to increase their use of AI for financial crime detection, and the world's largest banks plan to increase their spend on AI technologies by 20% over the next year. In the wrong hands, AI is an accelerant for criminal activity, but in the hands of financial crime-fighters, it can be a true force for good.

The latest advances in AI technology and the collective intelligence of the public and private sector stand as our most powerful tools in the current financial crime epidemic. The convergence of cutting-edge technology and network-level insights offers us a unique opportunity to get ahead of financial crime for good. Ultimately, no single entity can solve the problem of financial crime alone. Addressing this growing crisis requires a coordinated effort, to disincentivize and disrupt criminal networks and prevent financial crimes from happening in the first place. Together, we can safeguard and strengthen the integrity of the global financial system and better protect individuals and communities worldwide.

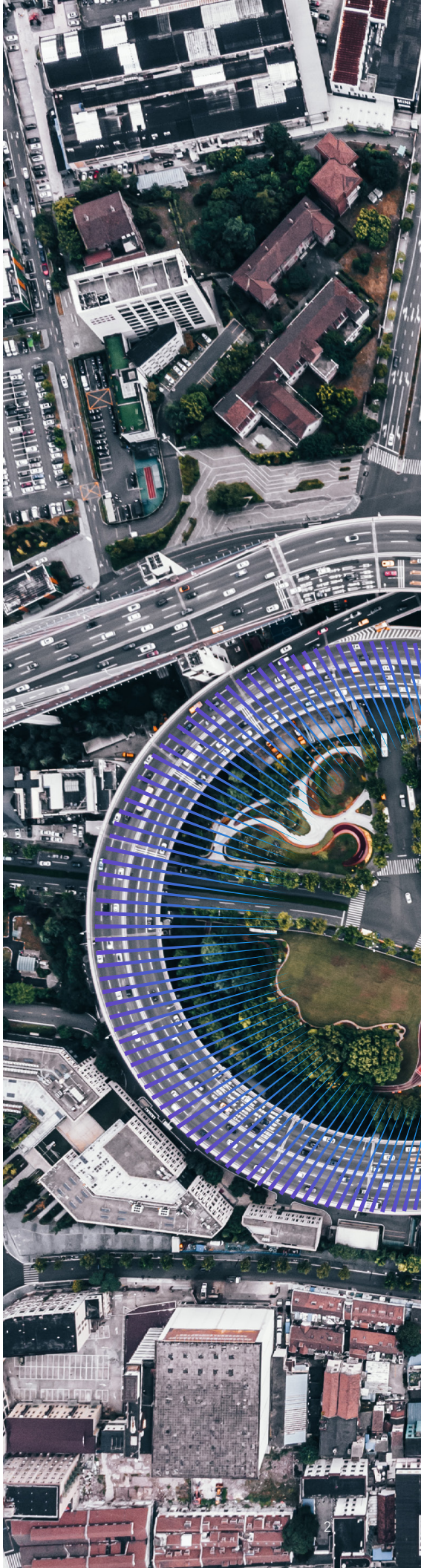


Table of Contents

About this Report

Last Updated **March 11, 2026**

The Global Financial Crime Report is based on data collection, research and analysis performed by Celent Research and Oliver Wyman, as outlined in the methodology. Unless otherwise stated, the currency used in this report is shown in US dollars (USD), and percentages represent two-year compound annual growth rates from 2023 to 2025. Compound annual growth rate (CAGR) is the annualized rate at which a value would grow over a specified period, assuming the growth occurs at a constant rate and is compounded each year.

A custom model was developed to determine the global estimate of financial crime, grounded in the best available industry data from public and private sources, market knowledge, and global economic patterns and indices. While the analysis is presented at a broad regional level, the following countries and territories were excluded due to limited data availability and/or inconsistent economic reporting coverage: Aruba, Greenland, Iran, Iraq, Russia, Syria.

Interpreting Scale and Loss Metrics

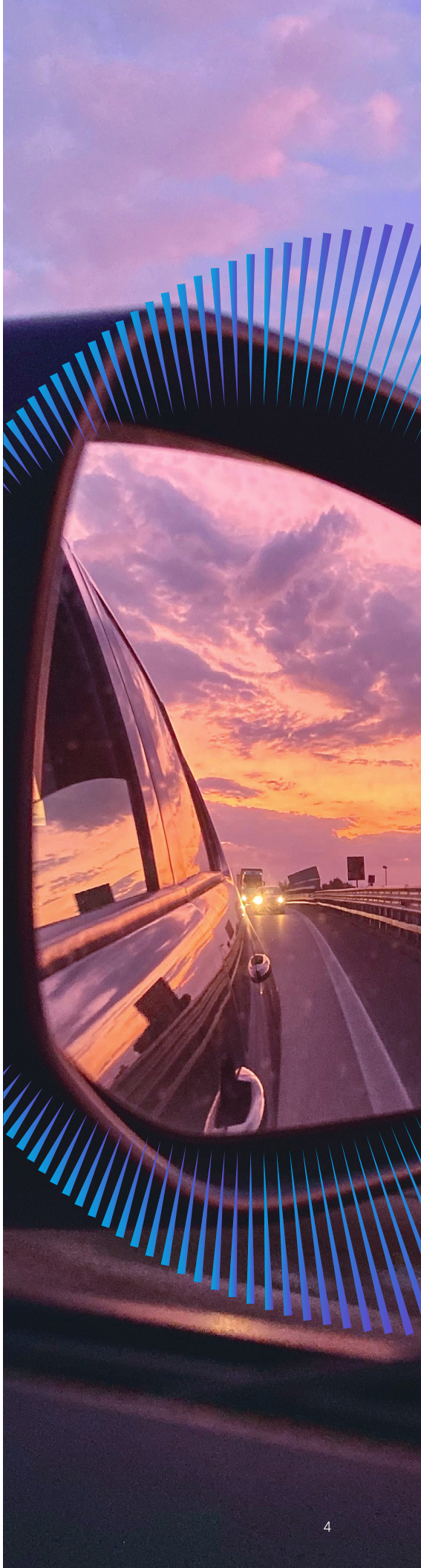
Estimates of total illicit financial flows reflect the overall scale of the illicit value moving through the global financial system, across a wide range of criminal activities, including corruption, money laundering, tax evasion, trafficking, sanctions evasion, movement of the proceeds of fraud, and other predicate offenses.

By contrast, fraud loss statistics represent an estimate of confirmed and reported losses from identified fraud incidents within a given period. As a result, fraud loss figures capture only a subset of the impact of financial crime and should not be interpreted as a measure of the full scale of illicit activity. The two metrics are complementary but not directly comparable, differing in scope, methodology, and intent.

For this report, Celent Research and Oliver Wyman also conducted a survey of 505 anti-financial crime professionals from financial institutions, as well as deep-dive interviews with senior executives, to inform the industry insights within this report.

Notwithstanding this expert research, we recognize that the scope of the model is not inclusive of all financial crime typologies and data is limited to current global detection and reporting capabilities and/or law enforcement interdiction — these numbers can only represent a part of criminal activity and victims of financial crime.

We also share our gratitude to the innovators and advocates who contributed expert perspectives to the spotlights in this report, broadening its insight and value to the industry.



Methodology

Global Estimates of Financial Crime

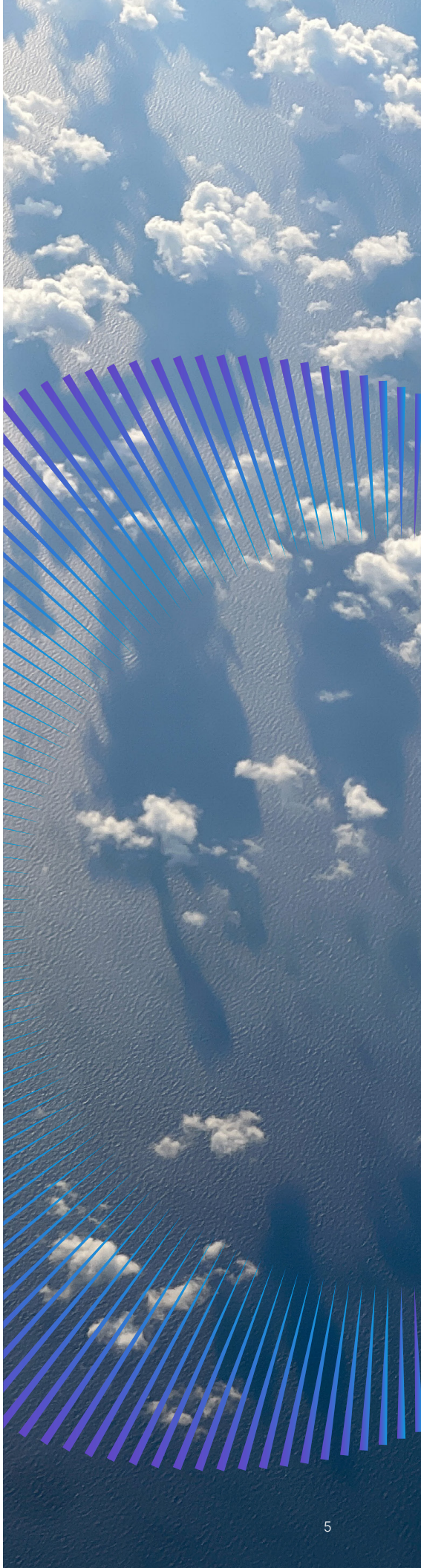
Financial crime estimates for fraud and money laundering were developed by Celent Research as a global model. Estimates were built using a bottom-up amalgamation of regional and country-level estimates, which were then compared with top-down estimates from global sources. Global indices and data were used to create the regional and country-level estimates for countries where there were no primary financial crime sources. Data sources include governments, international agencies, non-governmental organizations (NGOs), law enforcement agencies, interviews with industry experts, and news media.

The three-stage approach to developing these global estimates of financial crime included:

1. Bottom-Up Modeling

The foundation of the model was built on more than 500 global, regional, and country-level estimates and reports of fraud, financial crime and money laundering activity. These individual data points were combined and then extrapolated to fill in country-level and regional gaps. Estimates from prior years were adjusted to 2025 estimates. Data sources for bottom-up modeling include, but are not limited to:

- **Governments and Law Enforcement** *(e.g., Australian Financial Crimes Exchange (AFCX), Australian Taxation Office (ATO), Canadian Anti-Fraud Centre (CAFC), European Union Drugs Agency (EUDA), Europol, French Anti-Fraud Centre, Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3), Interpol, Japan's National Police Agency (NPA), Singapore Police Force (SPF), South Africa's Special Investigating Unit (SIU), South African Banking Risk Information Centre (SABRIC) Report, the United Kingdom's Department of Health and Social Care, the United Kingdom's Home Office, United States Department of Justice (DOJ), United States Department of the Treasury)*
- **Private Sector** *(e.g., Celent, Deloitte, Euromonitor, FICO, GlobalData, McKinsey & Company, Oliver Wyman, LSEG Data & Analytics, S&P Global Data & Analytics)*
- **NGOs and Trade Groups** *(e.g., Association of Certified Fraud Examiners (ACFE), Identity Theft Resource Center (ITRC), Ponemon Institute, World Bank, United Nations Office on Drugs and Crime (UNODC))*
- **Media Sources** *(e.g., Financial Times, Forbes, AML Intelligence)*



2. Top-Down Modeling

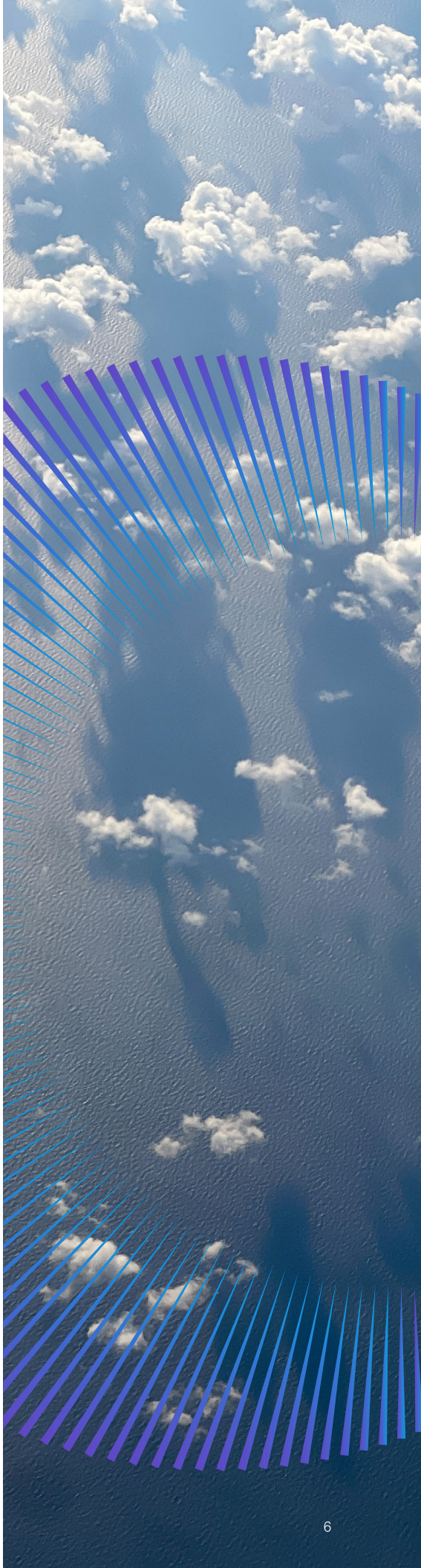
The next step of the modeling process considered global estimates of fraud and money laundering to build a broader framework for the model. These data provided global totals for specific types of financial crime (e.g., human trafficking), different methods (e.g., trade-based money laundering) or for a category of financial crime as a whole (e.g., payment fraud). Any data sets that were reported in a previous year were adjusted to 2025 levels for both economic growth and technological advances that abet financial crime. The data sources used for top-down modeling were primarily international agencies and NGOs *(e.g., Bank for International Settlements (BIS), International Monetary Fund (IMF), World Bank, United Nations)*.

3. Reconciliation with Global Patterns

The final step in building the model was to reconcile the country, region, and global data. Global data and indices were used to rebalance country-level and regional estimates using economic data, financial data and global indices of criminal activity. Data for this part of the methodology were sourced from international agencies *(e.g., Global Initiative Against Transnational Organized Crime's Global Organized Crime Index and the Basel Institute on Governance's AML Index)*.

Scope

Please note that the fraud loss estimates do not include tax evasion, corruption, bribery, embezzlement, business lost to counterfeit goods or industrial espionage. The regional allocations of loss to fraud victims represent the location of the victim, not that of the perpetrator. Money laundering estimates are estimates of money flowing into and out of the banking system, and do not reflect the value of funds moved physically or through digital currencies. In addition to the financial modeling, Celent collected primary data on top priorities, concerns and approaches to fighting financial crime from an online survey of 505 anti-financial crime executives globally from financial institutions ranging from $10 billion to over $500 billion in assets.



Executive Summary

Since 2023, illicit financial activity has surged by $1.3 trillion, pushing the scale of global financial crime to an estimated $4.4 trillion at a 19.2% compound annual growth rate (CAGR). This growth in the scope, scale and evolution of financial crime fundamentally threatens the integrity of the financial system, fueling some of the world's most insidious and destabilizing crimes such as human trafficking, terrorism, and elder abuse. How the industry responds to this new reality will prove critical to ensuring the safety and stability of the world's economy.

The 2026 Global Financial Crime Report combines expert research and data with industry perspectives to illustrate how challenges and opportunities have evolved from 2023 to 2025.

In 2025, as trillions of dollars in illicit funds flowed through the global financial system, there was alarming growth across every measured typology. Illicit flows reached:

- **$1.1 trillion** in drug trafficking activity, with annualized growth of 17.1%
- **$528.5 billion** in human trafficking, with annualized growth of 23.5%
- **$16.2 billion** in terrorist financing, with annualized growth of 18.8%

In addition, fraud scams and bank fraud schemes **totaled $579.4 billion** in losses globally in 2025, representing 9.2% annualized growth since 2023, including:

- **$62 billion** in losses from fraud scams, with annualized growth of 19.3%
- **$517.4 billion** in losses from bank fraud, with annualized growth of 8.2%

Despite the scale of this research, these estimates represent a fraction of the true scope of financial crime given the sheer volume of obfuscated, undetected or unreported illicit activity.

AI presents both the biggest challenge and opportunity in stopping illicit activity. Criminals have always been on the forefront of adopting new technology, and AI is no exception. By and large, the industry recognizes that winning the technology arms race will be critical to protect the financial system from the criminals that look to exploit it. Financial institutions are investing heavily in both the technology expertise and the tools themselves to future-proof their defenses, improving detection while removing layers of complexity through automation.

$4.4T
in illicit flows in 2025

↑19.2%
2023–2025 CAGR

Drug trafficking
$1.1T | ↑17.1%

Human trafficking
$528.5B | ↑23.5%

Terrorist financing
$16.2B | ↑18.8%

$579.4B
in fraud losses in 2025

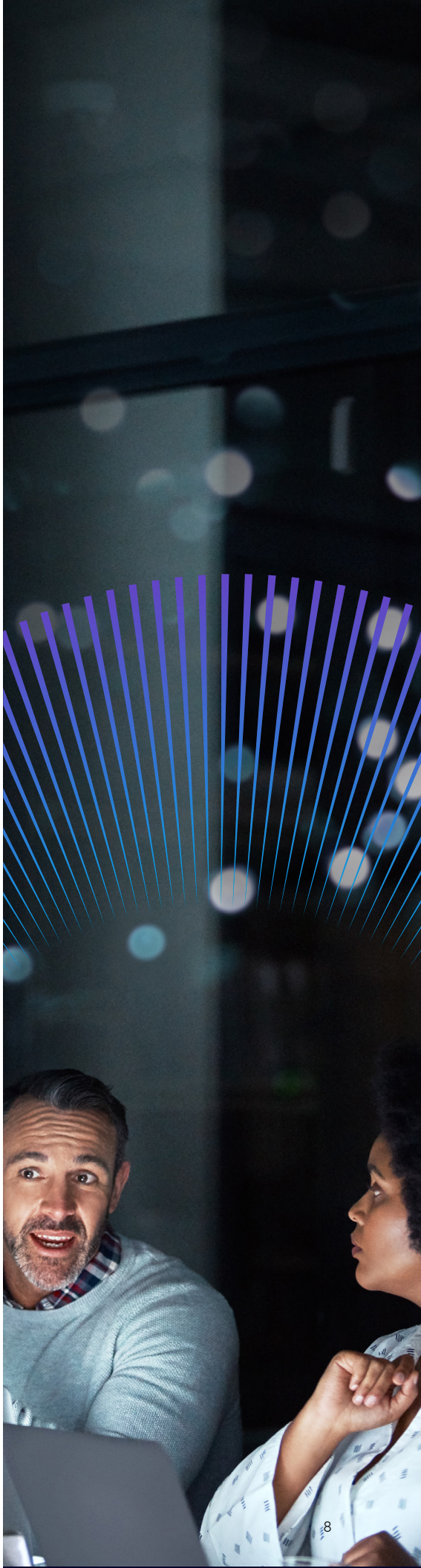
↑9.2%
2023–2025 CAGR

Fraud scams
$62B | ↑19.3%

Bank fraud schemes
$517.4B | ↑8.2%

Collaboration will be critical to successfully removing criminals from the financial system. As threats evolve, financial institutions are increasingly looking for intelligence from law enforcement and other financial institutions to stay ahead of emerging trends. Despite improved collaboration efforts with regulators, law enforcement, and between institutions, gaps remain. Throughout this report, we spotlight the innovators and advocates that exemplify what coordinated action looks in practice, serving as models for what the next generation of collaborative frameworks looks like.

With the financial crime crisis reaching new heights, the industry is sitting at an inflection point. The actions we take next will define the future of the fight against financial crime. If we can bring together the tools at our disposal — advanced AI technology, collaborative frameworks, and regulatory alignment — we can turn the tide against criminals, protecting consumers and making the financial system safer for all.

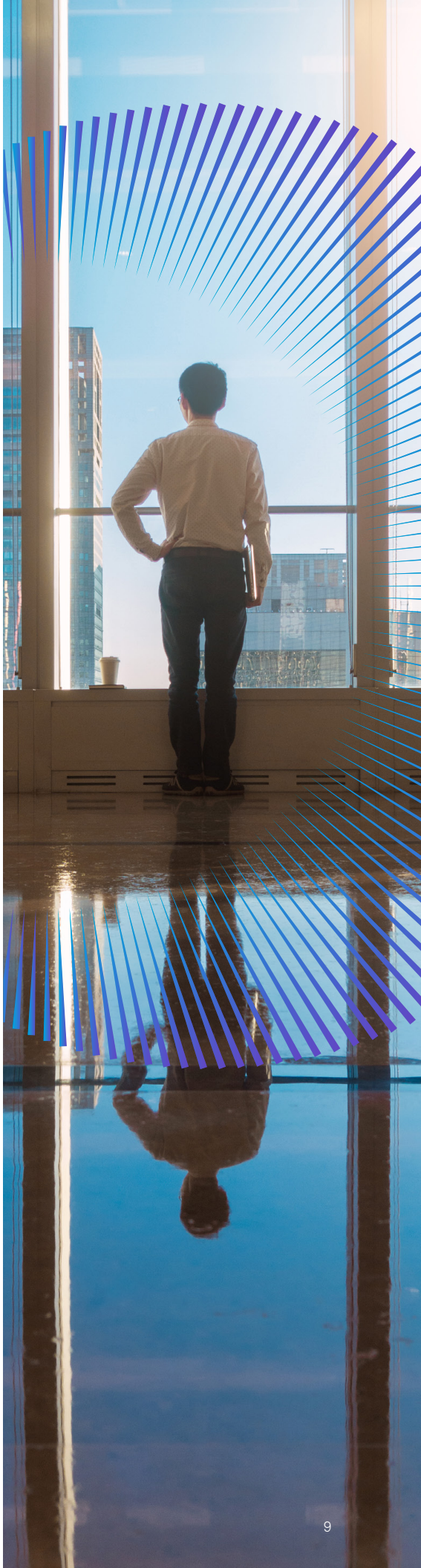


The Global Scale of Financial Crime

Financial crime is increasing at a staggering pace, growing by more than a trillion dollars since 2023 and pushing the global financial crime crisis to an estimated $4.4 trillion. Between 2023 and 2025, this surge amounted to 19.2% growth — far outpacing the 3.6% GDP growth of the global economy.[1]

Financial crime now represents the equivalent of 3.8% of global GDP, underscoring the scale of the crisis. The impact of crime is immense, with fraud losses alone surging past a half a trillion dollars — banks bore losses of $517.4 billion and scams targeting consumers and businesses surged to $62.0 billion.

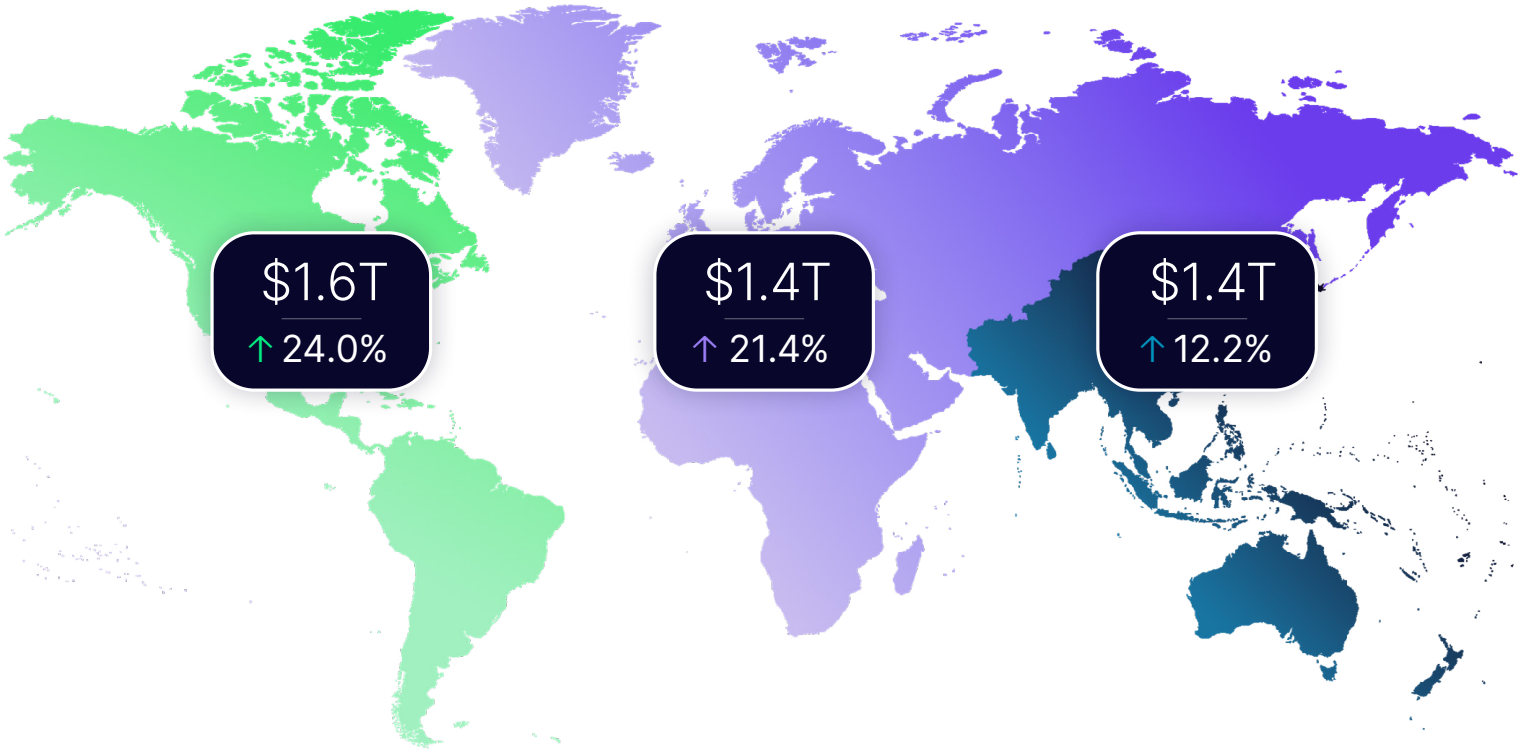
However, these numbers do not reflect the immeasurable human cost borne by victims at the hands of fraudsters, human traffickers, drug traffickers, terrorist networks, and other illicit enterprises.



$4.4 Trillion in Illicit Funds

Global estimate of terrorist financing, money laundering and the proceeds of underlying crimes including human trafficking, drug trafficking, corruption, organized crime, fraud and other illicit activity.

↑19.2% 2023–2025 Compound Annual Growth Rate



Americas

Other *(Organized crime, fraud, corruption, etc.)*	**$1.0T**	↑24.1%
Drug Trafficking	**$428.0B**	↑22.0%
Human Trafficking	**$181.4B**	↑29.0%
Terrorist Financing	**$7.5B**	↑21.5%

EMEA[2]

Other *(Organized crime, fraud, corruption, etc.)*	**$908.1B**	↑21.6%
Drug Trafficking	**$322.0B**	↑19.2%
Human Trafficking	**$167.2B**	↑24.7%
Terrorist Financing	**$5.3B**	↑19.4%

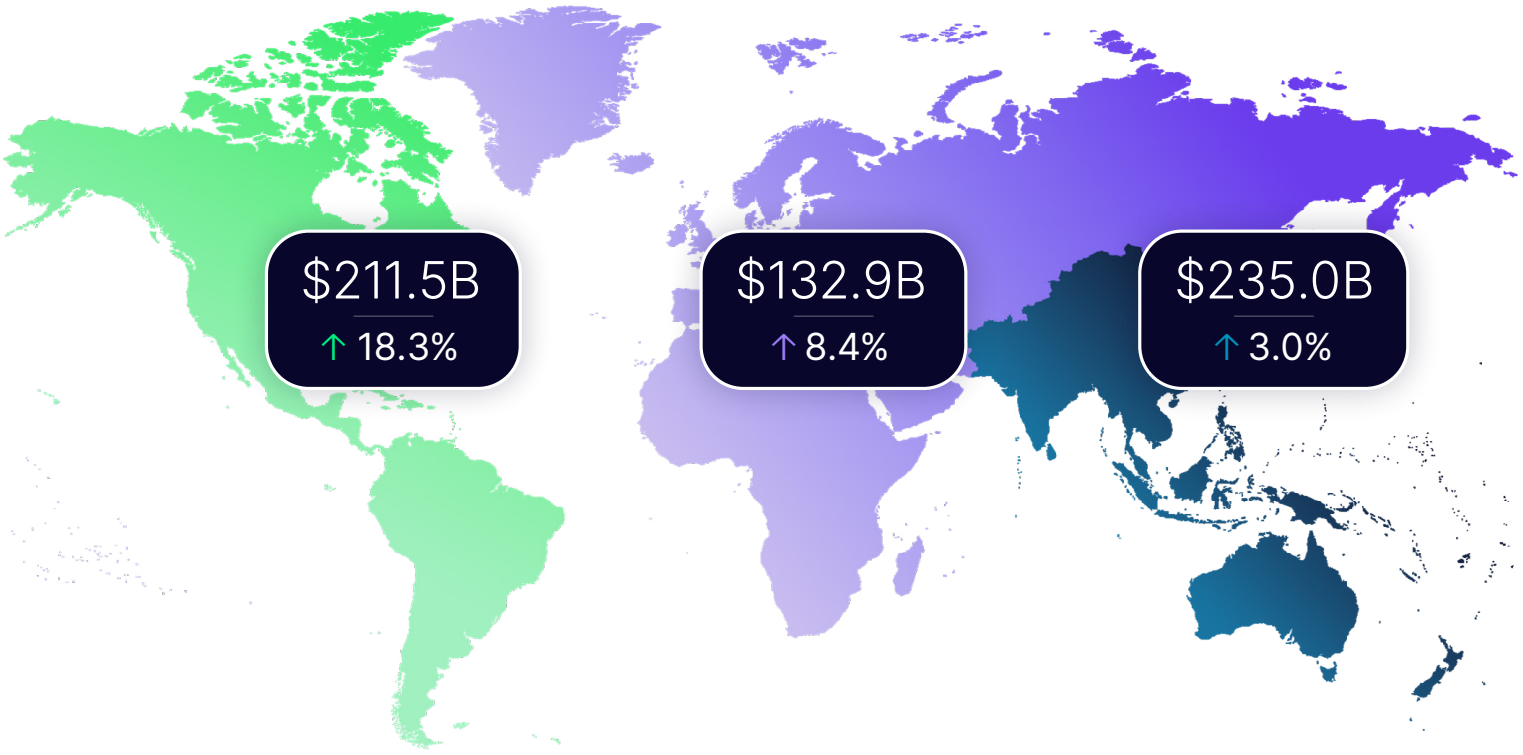
Asia-Pacific

Other *(Organized crime, fraud, corruption, etc.)*	**$869.3B**	↑12.2%
Drug Trafficking	**$323.5B**	↑9.7%
Human Trafficking	**$179.9B**	↑17.6%
Terrorist Financing	**$3.4B**	↑12.7%

$579.4 Billion in Scams & Schemes

Global losses to consumers and businesses from impersonation, confidence, advance fee, employment, and cyber-enabled scams, as well as bank fraud losses from payments, check and credit card fraud.

↑ 9.2% 2023–2025 Compound Annual Growth Rate



	Americas	EMEA[2]	Asia-Pacific
Bank Fraud (First-Party/ Unauthorized) **↑8.2%**	Account to Account Payments **$132.7B** ↑13.7% Check **$34.2B** ↑27.5% Credit Card **$23.8B** ↑32.2%	Account to Account Payments **$107.5B** ↑6.9% Credit Card **$3.8B** ↑11.6% Check **$376.0M** ↓9.7%	Account to Account Payments **$199.1B** ↑2.3% Credit Card **$11.9B** ↑0.3% Check **$4.0B** ↓11.8%
Consumer & Business Fraud Scams (Third-Party/ Authorized) **↑19.3%**	Cyber-Enabled **$7.7B** ↑24.4% Advance Fee **$6.8B** ↑20.2% Employment **$2.5B** ↑27.1% Impersonation **$2.3B** ↑21.0% Confidence **$1.4B** ↑22.2%	Advance Fee **$11.5B** ↑18.4% Cyber-Enabled **$4.1B** ↑15.6% Employment **$2.2B** ↑13.8% Impersonation **$1.9B** ↑15.9% Confidence **$1.6B** ↑16.6%	Advance Fee **$9.0B** ↑20.3% Impersonation **$5.4B** ↑18.6% Cyber-Enabled **$2.4B** ↑12.9% Confidence **$2.2B** ↑14.6% Employment **$927.2M** ↑19.8%

Industry Insights

The 2026 Global Financial Crime Report delivers our most rigorous analysis of industry threats, priorities, and opportunities to date. Drawing on world-class data modeling, in-depth executive interviews, and a survey of 505 senior industry leaders across the globe, it provides unprecedented insight into the scale and complexity of financial crime, and how the industry is responding to the rapidly evolving risk landscape.

To better understand what makes collaborative frameworks for fighting financial crime successful, we have worked with several organizations to showcase what coordinated action looks like in practice. Their stories are featured throughout this report to provide real-life examples of successful models for collective action through partnerships across the public and private sectors.

Industry Insights: Threats & Trends

Financial crime is growing rapidly in scale, driven by illicit criminal networks that are leveraging sophisticated tactics to circumvent controls. Adding fuel to the fire are increasingly faster payment channels and a world that grows more interconnected every day, providing endless paths for criminals to move funds across borders and beyond detection.

Criminals are often on the leading edge of innovation, being among the first to adopt new technologies in their efforts to exploit the financial system for their own gain. AI is no exception and is currently being leveraged by criminal networks to enhance existing playbooks. At the same time, the technology is producing new threats, such as AI-enabled hyper scams and scams-as-a-service.

Human Trafficking

Globally, human trafficking generated an estimated $528.5 billion in 2025, reflecting a staggering illicit market built on the lifelong trauma inflicted on millions[3] of men, women, and children forced into labor or sex work. Since 2023, funds linked to this heinous crime have risen with a growth rate of 23.5%, driven by emerging forms of exploitation, the growing use of AI and digital technologies to groom and deceive victims, and, above all, the immense profits that continue to fuel perpetrators' operations. As the Organization for Security and Cooperation in Europe (OSCE) emphasizes, combating human trafficking requires a whole-of-society response — one that recognizes this crisis as a social, economic, and security threat that transcends borders and demands coordinated global action.

Terrorist Financing

In 2025, an estimated $16.2 billion funded terrorist acts and organizations worldwide, from arms trafficking to foreign and domestic terrorism, and domestic violent extremism — a growth rate of 18.8% from 2023. These financial flows can be tied to lone extremists, cell operations, or massive international networks and pose a significant risk to the integrity of the global financial system, threatening the security and safety of communities worldwide.

Financers of these nefarious activities often leverage low-dollar transactions and multiple evasion techniques to obfuscate the source or destination of these funds. The sheer scale and speed of transactions flowing through global financial institutions and payment systems makes these flows incredibly difficult to detect.

At the same time, terrorist financing has increasingly expanded beyond traditional banking channels. Cryptocurrency has emerged as a prominent vehicle for moving funds, with frequent crossover between crypto exchanges and the traditional financial system.

In 2025 an estimated

$16.2B

funded terrorist acts

> We need to pay attention to how financial crime is becoming more industrial strength organized crime.
>
> - SVP Chief AML and Sanctions Officer at a National Monoline in North America

Money Laundering Risks of Greatest Concern

Terrorist groups also continue to exploit trusted structures such as nonprofit organizations (NPOs) and crowdfunding platforms, shifting from vague charitable causes toward the misuse of legitimate NPOs, front organizations, and formal fundraising campaigns. Compounding these risks, more sophisticated networks increasingly rely on professional enablers — including lawyers, accountants, and complex corporate structures — to formalize and conceal financial flows.

Drug Trafficking

In 2025, $1.1 trillion in illicit funds flowed to drug trafficking and Drug Trafficking Organizations (DTOs), representing 17.1% annualized growth from 2023.

The UNODC *2025 World Drug Report*[4] indicates that the drug trade accounts for the bulk of illicit proceeds generated by organized criminal groups. Illegal drug production, trafficking and distribution is a major source of income for criminal organizations, operating in virtually all drug markets around the globe[4]. As organized crime and illicit proceeds grow, so does drug-trafficking associated violence — in countries of origin, transit and destination markets.

Transnational criminal organizations (TCOs) are significant threats, enabling a wide range of illicit activities, from drug and weapons trafficking to human trafficking and smuggling.[5]

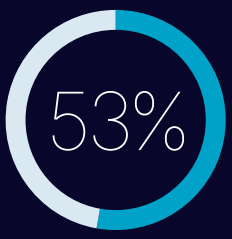
TCOs engaged in drug trafficking operations employ a variety of complex money laundering schemes to avoid detection, including the use of front companies, money mules and professional money laundering networks.[5]

Cross-Border Illicit Activity

As payments become more connected globally, criminals are exploiting international transfers to obscure the flows of illicit funds, creating cross-border dirty money trails that are increasingly difficult to track.

Globally, $482.9 billion flowed across international borders in 2025 — an estimated 11% of total illicit flows globally. Cross-border movement of illicit funds is a core mechanism of money laundering and a critical enabler of the broader criminal ecosystem.

Cross-border illicit flows may also be orchestrated by professional money laundering networks as part of massive schemes. In our survey, 63% of respondents cited these networks as their top money laundering concern. In our deep-dive interviews, experts emphasized that modern criminal groups are increasingly operating like legitimate corporate enterprises, utilizing global structures and industrialized recruitment, with massive scam compounds functioning as multi-crime hubs and linking large-scale fraud directly to violent predicate crimes.



of respondents ranked **laundering through crypto assets** as a top concern

In 2025

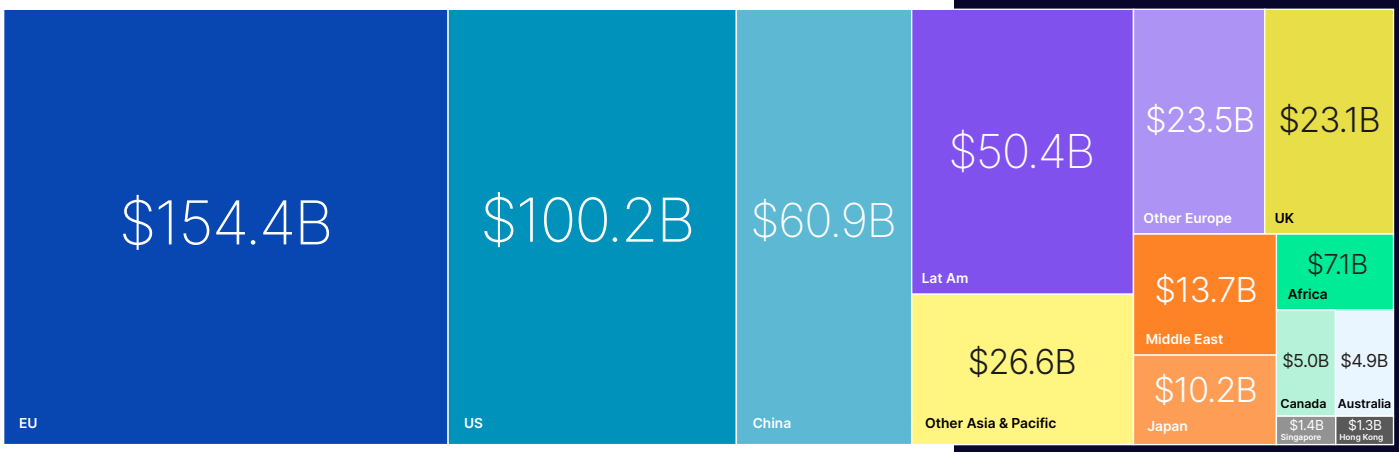
$1.1T

in illicit funds connected to drug trafficking and DTOs

$482.9B

in global cross-border illicit activity

Global Cross-Border Illicit Flows



Cross-Border Flows in the European Union

In 2025, the European Union recorded $154.4 billion in cross-border illicit flows, with Germany and France accounting for nearly half of the total for the region.

As discussed in Financial Crime Insights: Europe,[6] the region is advancing innovation and interoperability of payments across member states, making payments faster and more accessible. Representing nearly a third of all global cross-border illicit activity, the EU's financial industry has a unique opportunity to set new standards of leadership in combating financial crimes across borders, by taking collective, decisive action against cross-border scams, fraud and associated money laundering.

Money Mules

Money mules and money mule networks are critical enablers of the global criminal economy, acting as the connective tissue that allows proceeds from fraud, organized crime, drug trafficking, human trafficking, and terrorist financing to move through legitimate financial institutions.

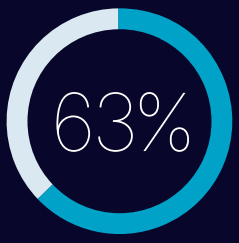
In 2025, money mules moved an estimated $284 billion in dirty money — 6.5% of all illicit funds globally. By routing funds through multiple mule-controlled accounts in different jurisdictions, launderers deliberately exploit regulatory fragmentation, increasing the distance from the originating crime and significantly complicating detection and recovery efforts.

This threat is recognized by financial institutions. Nearly a third of survey respondents identified money mules as the greatest risk to their customers, reflecting awareness that mules are often customers themselves — either knowingly engaging in criminal activity or unknowingly manipulated as victims of scams.

In deep-dive interviews, experts noted that criminal groups have professionalized the recruitment of money mules, specifically targeting students, migrants, and gig workers, often through online channels and scams, as a deliberate strategy to scale mule networks rapidly.

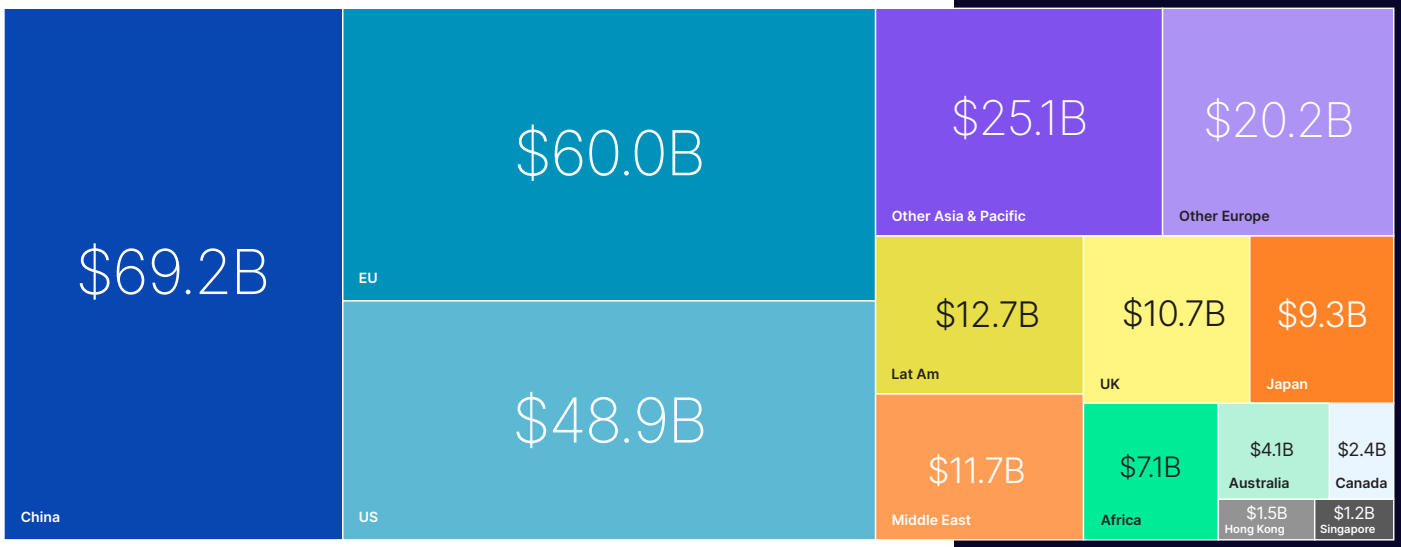
Money mule networks are often integrated with international professional money laundering organizations. These criminal enterprises take advantage of regulatory gaps across jurisdictions, using cross-border transactions to multiple mule accounts to evade detection, complicate investigations, and materially reduce the likelihood of recovery.

> Disrupting mule networks was framed by interviewees as one of the most effective leverage points in financial crime prevention, simultaneously impacting multiple predicate crimes, and underscoring the need for network-level detection, cross-institutional collaboration, and faster payments monitoring.



of survey respondents ranked **Professional Money Laundering Networks** as their top money laundering concern

Total Estimated Volumes of Illicit Funds Moved by Money Mules



Spotlight: The Convergence of Fraud and Human Trafficking — An OSCE Perspective on Collective Global Action

> "Technology is today's most powerful tool — we must use it to strengthen our response and protect victims."
>
> - Dr. Kari Johnstone, *OSCE Special Representative and Coordinator for Combating Trafficking in Human Beings*

Human trafficking remains one of the world's most urgent and complex challenges, and today its scale, sophistication, and financial impact are accelerating at a pace that demands new ways of thinking. What was once primarily a crime of physical exploitation has expanded into a digitally enabled ecosystem of coercion, profit, and transnational criminal enterprise.

Tarana Baghirova
OSCE Programme Officer and Technology and Financial Investigations Programme Lead

Dr. Kari Johnstone
OSCE Special Representative and Coordinator for Combating Trafficking in Human Beings

As our conversations with the Organization for Security and Co-operation in Europe (OSCE) made clear, the world is confronting a form of trafficking that is evolving alongside — and intertwined with — the broader surge in global fraud.

The OSCE plays a uniquely influential role in this space. With a mandate that spans research, technical assistance, financial investigations, capacity building, and cross-border coordination, the organization provides critical guidance to governments, financial institutions, civil society groups, and law enforcement bodies working to understand and disrupt trafficking. In our discussion with Dr. Kari Johnstone, the OSCE Special Representative and Coordinator for Combating Trafficking in Human Beings, and Tarana Baghirova, Programme Officer and Technology and Financial Investigations Programme Lead, one message resonated throughout: **trafficking cannot be solved in isolation. And no single institution — financial, governmental, or law enforcement — can combat it alone**.

The scope and scale of human trafficking is growing and its links with other crimes, including financial crimes are growing, because it is fundamentally a financially motivated crime. Traffickers generate extraordinary profit by exploiting vulnerable people in increasingly diverse and technologically sophisticated ways. Technology accelerates and scales crime but does not create it. As Dr. Johnstone emphasized, **"Technology is today's most powerful tool — we must use it to strengthen our response and protect victims."** What criminals have done is leverage digital platforms, large-scale communication tools, and AI-powered techniques to reach victims more efficiently, expand their operations across borders, and conceal illicit proceeds with unprecedented agility.

One of the most concerning evolutions highlighted by the OSCE is the emergence of large-scale scam compounds, which now represent a new frontier for both trafficking and fraud, as traffickers leverage forced criminality to power large-scale scam operations and sustain illicit financial flows.

Across Southeast Asia and now increasingly within the OSCE region, people are lured by deceptive job offers, often facilitated by AI-generated messaging, multilingual outreach, and digital grooming techniques. Upon arrival, they find themselves trapped in industrial-scale fraud factories where they are coerced into defrauding others. Victims who fail to meet financial quotas face brutality, torture, or being sold into other forms of exploitation. These are not isolated cases — they are highly organized, transnational operations built on coercion, with a scale that mirrors legitimate multinational enterprises.

This dynamic illustrates why a financial lens is crucial. **Financial investigation remains one of the most powerful tools available to expose trafficking operations.** Following financial patterns and indicators — payments to recruiters, digital asset movements, transactions linked to scam facilities, and a victim's financial behavior — enables detection of illicit activity and allows investigators to build strong cases against traffickers. Yet the OSCE stressed that many countries still underutilize financial intelligence. National risk assessments frequently overlook trafficking altogether, or they rely on minimal criminal justice data rather than proactively examining financial flows. The result is a diagnostic gap: trafficking is everywhere, but often invisible within financial systems that are not primed to detect it.

Both Johnstone and Baghirova underscored the urgent need for a whole-of-society approach to close the gap. Financial institutions hold insights into illicit flows. Law enforcement holds intelligence on perpetrators. NGOs understand victim vulnerabilities and traffickers' recruitment tactics earlier than anyone else. Technology companies possess visibility into online grooming, platform misuse, and scam typologies. Social services, educators, and medical professionals are often the first to encounter victims. Without mechanisms that connect these stakeholders in real time, our collective ability to intervene early and effectively remains sharply limited.

A critical part of building this shared defense is fostering network-level intelligence. Criminal groups have already embraced the network model. They share best practices and successful fraud scripts, replicating methods across jurisdictions. They leverage professionalized mule networks, payment facilitators, and money laundering channels. They diversify exploitation models, moving seamlessly between forced labor, sex trafficking, forced criminality, online fraud, and extortion. And crucially, they do this at speed. As Baghirova observed, criminals are moving at "the speed of transactions," while the systems designed to stop them still move at "the speed of legislation."

The OSCE's message is clear: **fraud and human trafficking share an ecosystem.** You cannot solve one without understanding and intervening in the other. Every time a fraud typology works, it is scaled and repeated across institutions. Disrupting these cycles requires disincentivizing criminals through earlier detection, shared intelligence, stronger public-private partnerships (PPPs) and a unified industry response.

The call to action has not changed — but the urgency has. In a world that's continuously evolving, advocates must match that pace through rapid, coordinated action. The OSCE's work provides a model for how this can be done. By bringing together financial intelligence units, regulators, private sector partners, law enforcement, civil society, and survivor leaders, they demonstrate what a modern anti-trafficking response must look like: inclusive, interconnected, nimble, and driven by a clear understanding that no one can succeed in isolation.

Ultimately, the OSCE reminds us that behind every trendline are human lives — people who are exploited, coerced, and often repeatedly victimized across multiple stages of criminal activity. By approaching trafficking as both a human and financial crime, and by embracing a whole-of-society approach rooted in information sharing and collective action, we can build a future in which trafficking and the ecosystems it fuels are confronted by a global network that is as coordinated, adaptive, and determined as the criminals themselves.

A Surging Global Fraud Landscape

Fraud is a massive threat to the integrity of the financial system as industrialized criminal schemes and fraud scams grow in scale and sophistication. By 2025, estimated global losses exceeded half a trillion dollars, rising to $579.4 billion with an annualized growth rate of 9.2% since 2023 — as criminals leveraged AI at scale to enhance their tactics and effectiveness. Fraud and other predicate crimes also contributed to trillions of dollars in downstream money laundering activity. These illicit proceeds continue to fuel broader nefarious operations, amplifying systemic risk well beyond financial loss. The result is a fraud landscape defined not only by its volume, but by its velocity, complexity, and connection to larger criminal enterprises.

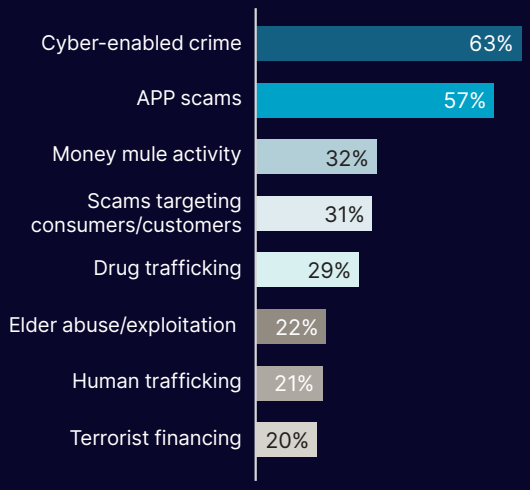
Scams & Authorized Push Payment Fraud

In 2025, fraud scams were a $62 billion drain on the financial system, up 19.3% since 2023 — more than double the annualized growth rate of bank fraud losses, which rose 8.2% to $517.4B in the same two-year period. This growth reflects a core truth in the fight against financial crime — fraudsters always take the path of least resistance. As banks strengthen controls at the institution level, fraudsters have readily adapted by targeting customers with scams such as authorized push payment (APP) fraud.

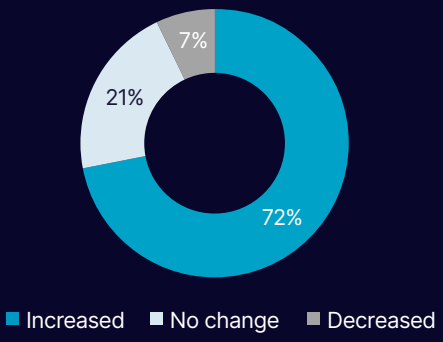
APP fraud occurs when a victim is manipulated into transferring funds to a fraudster they believe to be a legitimate payee, often through social engineering. This tactic encompasses schemes such as Business Email Compromise (BEC), confidence scams, and investment scams, and has emerged as one of the most significant fraud threats in the financial industry. Respondents identified APP fraud as a leading concern, with more than half citing it as a major industry threat and nearly three-quarters reporting an increase in such attacks since 2024.

When asked which forms of APP fraud were currently responsible for the greatest increase in customer attacks, respondents pointed to investment scams as the top challenge. Often leveraging an intricate sales pitch showing fabricated profits, fraudsters will convince the victim to invest in stocks, commodities, digital assets, real estate, or other investment vehicles. In reality, the investment is non-existent or worthless, and the

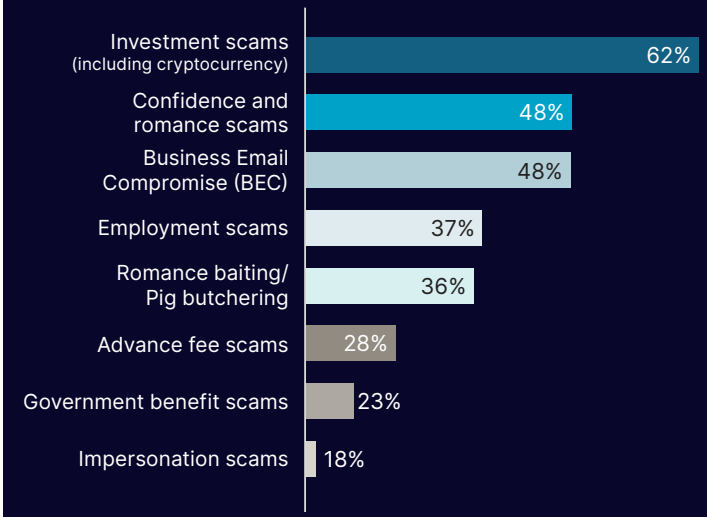
Financial Crime Posing Greatest Risk to Customers



Change in Volume of APP Fraud Scams in the Past Year (2025)



Types of APP Fraud with Greatest Increase in Attacks



fraudsters will eventually cease contact with the victim, keeping the funds for themselves.

Our data reinforces industry concerns over APP fraud, showing tens of billions of dollars in estimated losses to BEC, confidence scams, and impersonation schemes. As criminals capitalize on faster payments and online channels, the industry faces mounting pressure to strengthen prevention capabilities.

Cyber & AI-Enabled Fraud Scams

In 2025, estimated losses from cyber-enabled scams — including BEC, phishing, and data breaches — reached $14.3 billion, representing 19.6% annualized growth over two years. This sharp rise highlights how increasing digitization of payment channels and the rapid adoption of AI among criminals are reshaping the global financial crime landscape and making fraud more lucrative and difficult to combat.[7]

In our survey, cyber-enabled crimes were identified as the top financial crime threat facing bank customers. At the same time, AI-enabled threats are proliferating across the industry, with 90% of survey respondents reporting an increase in AI-driven attacks over the past two years. In deep-dive interviews, industry experts pointed to two major examples of how the fraud landscape is shifting alongside technological change:

- **Scams-as-a-service,** where fraudsters sell successful infrastructures to operationalize the widespread use of scalable fraud scams and tactics, enabling high-volume fraud attacks and expanding and creating criminal networks, and
- **AI-enabled hyper scams,** where fraudsters use generative AI (GenAI) and deepfakes to create more convincing, personalized, and scalable scams.

Origination has moved beyond email inboxes scaling across social media platforms, with criminal tactics evolving from manual scripts to full-scale automated operations that pose a systemic risk. Meanwhile, criminal tactics are designed to reduce the detection lead time for banks, and funds are often moved via instant payment rails before a victim realizes they are being defrauded.

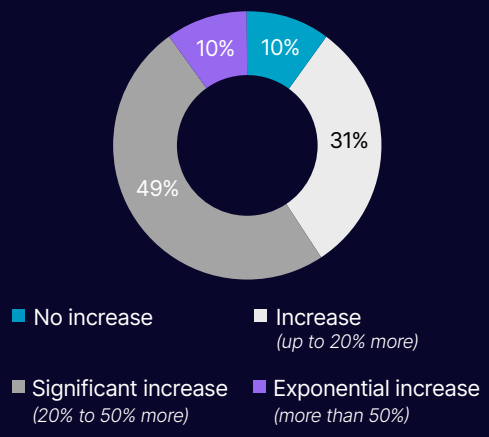
> “The ability to develop scams leveraging AI and other technology-based solutions has really created an epidemic for us.”
>
> - Industry Interviewee

Cyber-enabled scams reached

$14.3B ↑19.6%

2023–2025 CAGR

Change In Volume Of AI-Driven Fraud Attacks in Past Two Years



Elder Fraud

Elder financial exploitation is a multibillion-dollar challenge, with seniors losing an estimated $88.6 billion in 2025, representing approximately 15% of total fraud losses and annualized growth of 6.8% since 2023. Despite this increase, the rate of growth is lower than the overall 9.2% growth rate of total global fraud losses.

With a 2-year growth rate below other fraud types this trend may reflect positive progress towards elder fraud prevention. Industry initiatives — such as improved elder-focused education programs, stronger institutional safeguards, and wider availability of reporting channels — may be contributing to improved prevention and early detection. However, underreporting is a significant issue in capturing true losses to seniors, as elderly victims often do not come forward due to fear or shame.

The change in growth rate in elder financial exploitation may also signal a shift in criminal tactics and targets. The popularity and proliferation of social media, coupled with criminal exploitation of social media platforms, makes anyone a potential victim. Industry research[8] indicates that younger adults are more inclined to trust what they see on social media and are subsequently falling for scams at a higher rate than older adults.

> "A lot of the scams, especially around elderly fraud loss, involve scammers getting remote access to folks' devices and then taking over their accounts."
>
> - Chief BSA/AML and Sanctions Compliance Officer at North American Regional Bank

Seniors lost an estimated

$88.6B ↑**6.8%**

2023–2025 CAGR

Spotlight: Global Collaboration Against Scams

> "Scammers are using AI the same way legitimate businesses do — to work faster, cheaper, and at scale."
>
> - Jorij Abraham,
> *Managing Director of GASA*

Jorij Abraham
Managing Director of GASA

Emily Taylor
Co-founder and CEO of GSE

Lucien Taylor
Co-founder and CTO of GSE

Scams have become one of the most pervasive and damaging forms of financial crime worldwide. They move effortlessly across borders, exploit digital infrastructure at scale, and increasingly rely on sophisticated social engineering and AI. Unlike traditional fraud, scams do not confine themselves to a single sector or jurisdiction. They exploit gaps between institutions, platforms, and regulatory regimes — often long before financial transactions ever occur.

For the Global Anti-Scam Alliance (GASA), this reality made one conclusion unavoidable: no single organization, sector, or government alone can protect consumers from scams. Addressing the threat requires collaboration on a global scale, supported by real-time intelligence sharing that reflects how scams actually operate in the modern economy.

A global threat that demanded a different response

According to Jorij Abraham, Managing Director of GASA, the scale and reach of scams have grown far beyond what many institutions anticipated. Drawing on GASA's annual global consumer survey of approximately 50,000 respondents, Abraham estimates around 23% of the global population reports having been scammed in some form within the past 12 months.

"These are not edge cases anymore," Abraham noted. "Scams have grown significantly, and they impact far more people than I ever thought possible."

The threat itself has also evolved. What once appeared as isolated incidents in the form of undelivered goods, fake investment opportunities or impersonation scams, has become an industrialized ecosystem with organized crime adopting corporate-style operations and using AI as an accelerant. Abraham noted **"Scammers are using AI the same way legitimate businesses do — to work faster, cheaper, and at scale."**

Scam operations now rely on a complex supply chain that includes domains, hosting providers, advertising platforms, communication channels, and payment rails. That infrastructure is global by default, allowing bad actors to scale quickly and reemerge even after individual takedowns.

For GASA, this evolution exposed the limits of awareness campaigns or bilateral coordination alone. Protecting consumers at scale would require bringing all stakeholders to the same table around shared intelligence and concrete, operational solutions.

Collaboration as the foundation for consumer protection

GASA's mission is explicit — protect consumers worldwide from scams by fostering cross-sector collaboration and translating shared knowledge into action. Rather than positioning itself as an enforcement body, GASA operates as a catalyst, creating forums, research, and partnerships that allow stakeholders to coordinate more effectively against a common threat.

A recurring insight from GASA's work is that scams do not respect sector boundaries, but defenses often do. Financial institutions may only see scams at the point of transaction. Technology platforms may see malicious ads or content. Telecom providers may see suspicious traffic patterns. Law enforcement may see reports only after harm has occurred. Without a way to connect those perspectives in real time, response efforts remain fragmented.

That realization helped drive one of GASA's most significant initiatives: the creation of a shared, global mechanism for exchanging scam-related data across sectors and borders.

From collaboration principle to operational reality

The Global Signal Exchange (GSE) was launched in January 2025 as a not-for-profit, UK based initiative to operationalize the kind of collaboration GASA had been advocating for for years. Founded through a partnership between GASA, Google, and Oxford Information Labs Research, the GSE was designed to act as a neutral clearinghouse for scam and fraud signals.

Emily Taylor, Co-founder and CEO of the GSE, explains that the idea emerged from a recognition that many organizations were already sharing intelligence but mostly within their own verticals. "Organizations were sharing amongst themselves in silos — finance, tech, law enforcement," she said. "What was missing was a way to go cross-sector and cross-border."

The GSE was built to fill that gap. Rather than replacing existing systems, it functions as a superstructure, a shared layer that allows many organizations to exchange small but meaningful pieces of data through a single, trusted framework.

What a signal is and why it matters

At the heart of the GSE is the concept of a signal. A signal is a unit of intelligence: a URL, IP address, phone number, merchant identifier, or other indicator that may point to scam activity.

Crucially, the GSE is signal agnostic. It does not prescribe which data types are most valuable. Instead, it enables organizations to share what they already collect in the normal course of business and to decide how and with whom that information is shared.

"We don't vet signals; we vet organizations," Emily Taylor explained. "Participants are accredited, and they retain control over what they share and under what conditions."

That design reflects a deliberate trust model. Less sensitive signals, such as malicious URLs, can be shared openly. More sensitive data can be exchanged within restricted groups or with additional safeguards. This flexibility lowers the barrier to participation while maintaining high standards for privacy and governance.

From a technical perspective, Lucien Taylor, Co-founder and CTO of the GSE, likens signals to lightweight packets that are "very analogous to the TCP/IP protocol." Individually, a signal may appear insignificant. But when combined across sectors, those signals can expose shared infrastructure and coordinated scam networks that no single organization could identify alone. Taylor says GSE was designed as a practical mechanism that makes collaboration real, **"We needed to think like scammers — and then design a system that could move faster than they do. The power isn't in any single signal — it's what happens when signals connect across sectors and borders."**

Scale, speed, and early impact

Since launch, the GSE has grown rapidly. During its initial pilot phase, Google contributed over 100,000 URLs associated with fraudulent merchants, and the platform ingested approximately one million scam signals. As additional partners joined, the dataset expanded from a starting point of 40 million signals and, by January 2026, reached a 1 billion signals.

According to the GSE leadership team, the exchange now supports 45 full member organizations with more than 50 active data feeds. Engagement with over 160 organizations across onboarding and pilot stages within the system improves the collective ability to detect and counter fraudulent activities.

The value of that scale lies not just in volume, but in connectivity. In one example shared during the interview, a small number of URL-based signals enabled a partner organization to uncover a network of 17,000 connected accounts illustrating how limited intelligence can become a force multiplier when shared across the right ecosystem. Lucien Taylor pointed out that **"A small number of shared signals can unlock visibility that no single organization could achieve alone."**

Moving earlier in the scam lifecycle

Both GASA and GSE emphasize the importance of disrupting scams earlier — before victims are engaged and before funds move. This approach is described as moving "to the left" of the fraud attack chain.

Traditional takedown efforts frequently resemble a game of whack a mole: one site is removed, another appears. By contrast, the GSE aims to identify clusters of resources — the domains, hosting services, advertising infrastructure, and payment instruments that scammers reuse at scale.

This upstream focus is especially relevant as real-time payments and AI-driven scams compress response timelines. As Lucien Taylor noted, scammers can easily scale messaging, impersonate trusted entities, and operate from anywhere in the world. **"Signal sharing," he argued, "is one of the few ways to disrupt that at scale."**

What has worked and what needs to be done

Both organizations are candid about what it takes to make collaboration work. Trust, they argue, cannot be mandated. It must be built through strong governance, security, and respect for organizational constraints. The voluntary nature of the GSE has proven to be an advantage. "If people don't feel coerced to share, they tend to come more willingly," Emily Taylor observed.

At the same time, challenges remain. Legal complexity, uneven engagement across sectors, and the need for feedback loops — so contributors know whether shared intelligence was useful — are ongoing areas of focus. The GSE is actively working with members to improve multidirectional feedback, helping ensure that data sharing leads to visible outcomes rather than disappearing into a black hole.

Data as infrastructure for the future fight

For GASA, the GSE represents more than a technical platform. It is proof that real-time, cross- sector collaboration is possible and that data, when shared responsibly, can serve as infrastructure for consumer protection at global scale.

As scams continue to evolve, both organizations argue that success will depend less on isolated controls and more on shared situational awareness. By aligning stakeholders around common signals, shared trust, and early intervention, GASA and the GSE are laying the groundwork for a more coordinated global response to one of the fastest growing threats in financial crime.

Industry Insights: Key Priorities in the Fight Against Financial Crime

Meeting the AI Threat: Strengthening Financial Crime Prevention Through Advanced Technology

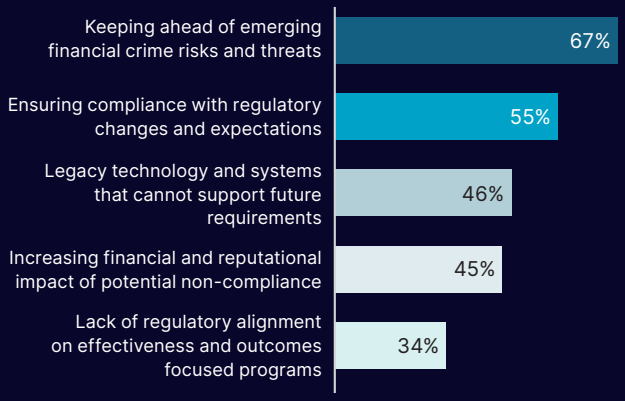
Looking ahead to the next five years, financial institutions are united in their concern about keeping pace with the evolving financial crime threat. 67% of banking professionals surveyed cite keeping ahead of emerging financial crime risks and threats as their greatest future challenge.

This concern reflects a threat environment shaped by increasingly sophisticated criminal networks, rapid technological change, and the accelerating misuse of AI. AI-driven fraud has emerged as a significant challenge to global bank fraud defenses: 90% of survey respondents report an increase in AI-driven attacks over the past two years at their institution. It appears that these are not isolated incidents, with more than half of respondents noting a signficant or exponential increase in attacks in recent years.

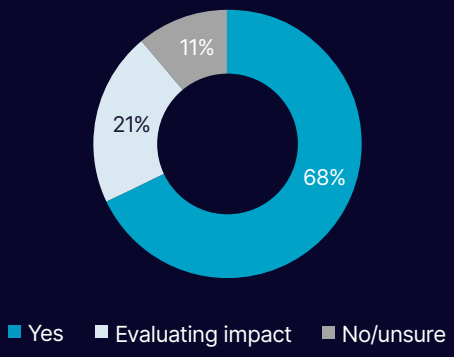
While the industry agrees that AI-enabled crime is among its biggest threats, it also strongly believes in the opportunity for AI to stop financial crime. Across the industry, there is a clear and growing recognition of the role AI can play in improving efficiency and reducing operating costs within anti-financial crime programs. Nearly nine in ten professionals report either using AI to augment their workforce and processes or are actively evaluating opportunities to do so. This shift is reflected in projected investment, the vast majority of respondents planning an increase in AI spending over the next two years. On average, survey respondents plan to increase spend on AI technologies for anti-financial crime by 13% over the next two years. For respondents at tier 1 financial institutions, that number rises to a planned 20% increase in spending on AI technologies.

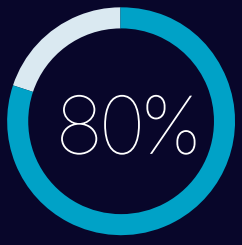
As AI-enabled fraud continues to accelerate, AI is increasingly viewed not as an emerging capability, but as a core requirement for effective financial crime management. Solutions incorporating advanced AI techniques — including machine learning analytics, GenAI and agentic AI — are delivering measurable gains in

Challenges of Greatest Concern in The Next 5 Years



Financial crime professionals using AI and automation to lower operational expense and enhance workforce effectiveness





of survey respondents plan to **increase spending on AI technologies** for anti-financial crime over the next two years

efficiency and detection quality, helping teams address persistent challenges such as false positives.

In parallel, organizational change is underway: nearly half of respondents reported that their institutions are currently transforming, or have recently completed the transformation of their anti-financial crime capabilities, reinforcing the link between technology investment, operational change, and improved outcomes.

Building Anti-Financial Crime Functions That Meet Tomorrow's Challenges

Resource pressure remains one of the most acute challenges facing anti-financial crime teams. These constraints are occurring against the backdrop of operationalized professional money laundering networks, growth in cyber-enabled crime, and the continued rise of APP fraud.

More than half of respondents note a lack of adequate resourcing — across people and technology — to manage financial crime risks. In response, institutions are deepening their investment in both talent and technology with most respondents noting an increase in headcount last year over the previous year. IT budgets for anti-financial crime have also expanded materially. 87% of respondents report increased spending on technology and operations since 2024.

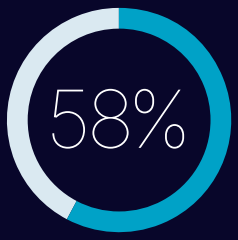
The volume of false positive alerts resulting from legacy monitoring are a pervasive, industry-wide problem that exacerbates operational challenges and resource constraints.

According to industry professionals, false positive alerts consume 27% of anti-financial crime team hours on average, exceeding 40% or more of analyst time at one in five teams surveyed.

Without material changes to detection models and AI-enabled workforces, additional investment will risk reinforcing inefficiency rather than improving outcomes.

Financial institutions increasingly view AI as a mechanism for strengthening their workforce and redeploying human expertise toward higher-value activities. Survey comments indicated a desire to shift investigator focus away from low-value, high-volume processes toward more complex investigations — an area where AI-driven efficiency gains can deliver meaningful returns.

> "With no regulatory demand to integrate AI technology or tools, our approach has been to ease our way into it on a risk-adjusted basis."
>
> - SVP Chief AML and Sanctions Officer at National Monoline in North America



Lack adequate resources, including personnel and technology, to combat financial crime

> "We need more guidance and clear guidance to help drive us into this new world of AI...I think the criminals are winning the arms race because of the lack of regulatory action."
>
> - Chief BSA/AML and Sanctions Compliance Officer at North American Regional Bank

Navigating Regulatory Change and Defining Effectiveness

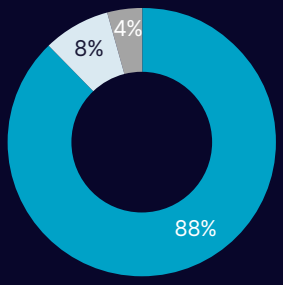
Ensuring compliance with regulatory change is the second highest concern for institutions, cited by more than half of respondents. Regulatory fragmentation across jurisdictions, evolving expectations, and limited clarity around effectiveness measures further strain teams already operating under significant operational constraints.

While banks face increasing expectations to reduce manual error, improve consistency and enhance monitoring, regulators have stopped short of providing clear guidance or standards for use of AI which is a critical enabler of efficiency in anti-financial crime programs. Such ambiguity compounds existing operational inefficiencies. In the absence of explicit regulatory guidance, institutions are taking a measured approach in their adoption of AI.

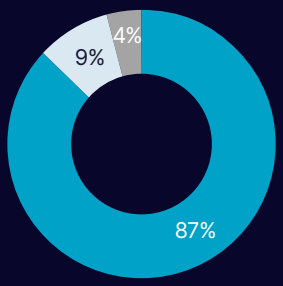
A critical barrier to progress remains the lack of standardized and transparent benchmarks for effectiveness, particularly those informed by regulator feedback. This gap sustains regulatory divergence, reinforces risk aversion, and limits the industry's ability to deploy AI and collaborative approaches at scale.

The industry's message is consistent: banks are asking for clearer, more harmonised guidance, practical definitions of effectiveness, and for regulators to act as more active partners in enabling innovation, collaboration, and meaningful improvements in financial crime prevention.

How does your 2025 financial crime headcount compare to 2024



2025 IT and AFC operations budget compared to 2024



On average, survey respondents report addressing false positives consumes

27%

of their team's day.

1/5

respondents report addressing false positives consumes

40%

or more of analyst time.

Spotlight: Australia Builds a Network to Fight Scams

> "If you detect something after it's happened, the criminality is already occurring."
>
> - Chris Sheehan, *Executive Lead for Investigations at National Australia Bank*

Chris Sheehan
Executive Lead for Investigations at National Australia Bank (NAB)

Ben Young
Head of Fraud Prevention at Westpac

David Pegley
Managing Director of AFCX

In Australia, the modern fight against financial crime did not begin with a single institution or a single law. It began with a shared realization that financial crime was no longer a banking problem alone. It had become a system wide threat — one that moved faster than traditional controls, exploited new technologies, and caused real harm to communities at scale.

The threat landscape is fast, scalable, and increasingly AI enabled

For Australian consumers and financial institutions alike, scams now represent the most visible and damaging form of financial crime. Chris Sheehan, Executive Lead for Investigations at National Australia Bank (NAB) describes scams **"as the single biggest threat"** customers perceive to their own financial safety, eclipsing more traditional forms of financial crime.

That assessment is shared across the Australian banking sector. At Westpac, the focus has similarly shifted from traditional fraud to also include scams as a dominant risk. As Ben Young, Head of Fraud Prevention at Westpac, said, **"all we talk about in Australia are scams — it's about customers being tricked into parting with their own money."**

What made this threat more dangerous is not just volume, but sophistication. Both NAB and Westpac point to the accelerating use of AI — deepfakes, synthetic documents, and automated social engineering — as a force multiplier for organized crime.

Why Australia had to act

For years, banks relied on post-event detection. Investigate the crime, report it, and try to recover funds after the fact. But as scams surged, that model no longer worked. Money was moving through mule accounts in hours, often disappearing offshore or into digital currencies before investigators could respond. "If you detect something after it's happened, the criminality is already occurring," Sheehan explained. "If you had prevented the crime from occurring in the first place, you could have avoided all of that."

The human cost was impossible to ignore. Customers were losing their life savings. Call queues at the banks stretched during peak scam waves. Media scrutiny intensified, and pressure from government escalated.

At the same time, it became clear that banks were only seeing the final step of a longer scam journey — one that often began with a text message, a fake website, or an online advertisement. "Banks can only see a very tiny portion of this," Sheehan noted. "The payment process is right at the end of the chain."

The Australian Financial Crimes Exchange (AFCX) saw the same issue from a different vantage point. Originally formed to address card fraud and identity compromise, the organization was forced to evolve as **"fraud morphed into scams, especially during COVID,"** as David Pegley, Managing Director of AFCX describes it. **"There was a dramatic surge in scam activity,"** said Pegley, compelling a broad range of institutions — telcos, digital platforms, and government agencies — to confront the issue collectively, whether they were ready or not.

The conclusion was unavoidable — no single institution, sector, or regulator could fix this alone.

Collaboration as infrastructure, not ideology

Australia's response was a reengineering of how institutions and industry would work together, anchored by real-time information sharing and a shared commitment to prevention.

At the center of this shift sits the AFCX, a not-for-profit intelligence sharing organization born out of collaboration between major banks. Today, AFCX supports 95 members across eight industries, including banks, telcos, digital currency exchanges, digital platforms, superannuation, insurers, and government agencies. It plays a critical role, acting as a trusted co-ordinator for actionable intelligence, shared at speed and at scale.

For NAB, AFCX transformed collaboration from informal relationships into operational infrastructure. "We do not compete with each other on crime — ever," Sheehan said. "The criminal hitting my customer today is hitting every other bank at the same time." That mindset enabled institutions to share vulnerabilities and learn from each other in near-real time.

From Westpac's perspective, the value of that structure is practical and immediate. When a customer transaction is identified as a scam, the intelligence can now be shared across participating banks within minutes through AFCX — ensuring that others do not have to "find out the hard way," said Young. That speed has proven critical for improving recovery outcomes and preventing repeat victimization across the system.

Outside of stopping scams at the source, one of the earliest and most impactful innovations was the Fraud Reporting Exchange (FRX). The FRX is a shared industry platform that allows Australian banks to report scam transactions directly to recipient institutions in real time, enabling faster account blocking and significantly improving the chances of recovering funds before they are moved. Before FRX, reporting a scam to a recipient bank could mean sitting in a public call queue for an hour. Now, banks submit scam reports through a dedicated platform, with defined service-level expectations for response. The result means faster blocking of recipient accounts and materially improved recovery outcomes.

Prevention moved even further upstream with the launch of the Anti-Scam Intelligence Loop (ASIL). This capability reflects the reality of today's scam landscape, that parties best positioned to stop a scam are often not banks. When a customer reports a scam, banks can now share verified indicators such as phone numbers, URLs and fraudulent ads through AFCX to telcos, digital platforms, and brands. Telcos block numbers. Platforms remove ads. Websites are taken down. **"It may not save my victim at that time," Sheehan explained, "but it will prevent potentially hundreds of other victims."**

AFCX emphasizes that this system only works because trust was built deliberately. "It's about demonstrating that you're going to deliver on something when you say you're going to," Pegley said. Over time, successful pilots created momentum and as Pegley describes it, "success bred success", bringing more industries and organisations into the loop.

At the institutional level, banks also rethought what effective prevention requires. At Westpac, intervention is not a side effect of fraud management — it is the job. As Ben Young put it, **"If I'm not intervening, I'm not really doing anything at all."** That philosophy aligns closely with NAB's shift towards real-time payment intervention, where suspicious transactions are paused and warnings inserted directly into the payment flow. Customers, NAB found, were willing to tolerate friction if it made them safer and it is this "positive friction" Sheehan notes, that prevents roughly a million dollars a day in potentially harmful payments from proceeding.

AI, trust, and the future of prevention

AI sits at the heart of both the threat and the defense. Criminals use AI to generate high-quality fake documents, impersonate executives, and groom victims. In response, Australian institutions are using AI to combine signals across banking behavior, device telemetry, and even telecommunications data, helping frontline staff have better, evidence-based conversations with customers who may be under psychological manipulation. "If you can put factual information in front of a customer," Sheehan noted, "you're more likely to have a successful outcome."

From Westpac's perspective, the challenge is only growing. Young described an "increasing circle of things you can't trust anymore" — from phone numbers and voices to social media content and online endorsements. As AI erodes traditional trust signals, the digital world becomes harder for customers to navigate safely, reinforcing the need to step in earlier and more decisively.

Why the collaboration worked

Ask leaders from NAB, Westpac and AFCX why Australia's model is working, and the answer is strikingly consistent: shared threat recognition, trust, and structure.

There was widespread acknowledgment that scams threaten the very fabric of the economy. The Australian government played a catalytic role by participating early, signaling comfort with voluntary intelligence sharing and later formalizing expectations through the Scams Prevention Framework. "You have to want to do it," Sheehan reflected. **"And you have to trust each other, and trust government to respect the collaborative process regarding sharing intelligence about criminality."**

Pegley emphasised that successful collaboration hinges on strong leadership and the courage of organizations to share information. By fostering a trusted operating model that others can depend on, these organizations set the foundation for effective partnerships. **"Trust is built through human interactions,"** he noted, adding that "it is further strengthened by consistently delivering tangible results."

Lessons for other jurisdictions

Australia's experience provides a powerful blueprint for jurisdictions facing similar threats. The key lessons are clear: start with strong leadership and foster voluntary collaboration across sectors. Establish a trusted intermediary to facilitate intelligence sharing and operationalize prevention efforts. Recognize that scams are an ecosystem-wide challenge, spanning banks, telcos, platforms, and government agencies. Prioritise real-time prevention over reactive measures, and proactively address emerging threats such as AI-enabled crime, which criminals are already exploiting.

As Pegley succinctly stated, **"This is a global problem. No jurisdiction should have to start from scratch."** The AFCX's scalable, adaptable, and proven model offers a ready-made framework for replication, providing a tested strategy for international co-operation in the fight against financial crime. By adopting AFCX's approach, other regions can build a robust defence against the evolving landscape of financial threats.

Industry Perspectives: Opportunities for Future-Proofing Anti-Financial Crime Programs in a Rapidly Evolving Threat Landscape

Enabling Progress Through Regulatory Clarity and Alignment

When asked what regulatory improvements would most improve anti-financial crime effectiveness, respondents consistently pointed to clearer regulatory support for innovation and collaboration.

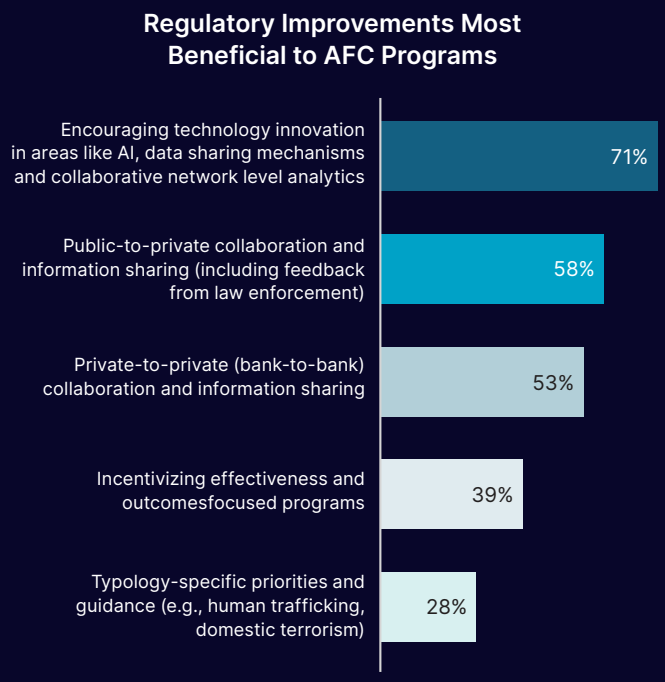
Encouraging technology innovation through AI, data sharing mechanisms, and collaborative network-level analytics was elevated as top area for improved regulation, underscoring how collaborative technologies benefit anti-financial crime programs. This was closely followed by improved public-private collaboration, and improved regulations in support of bank-to-bank information sharing.

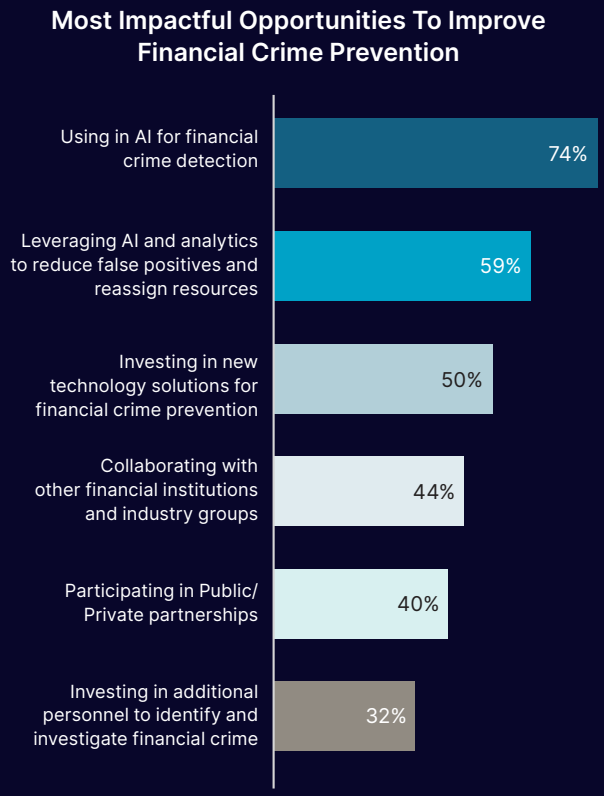
Banks are not calling for less regulation, but rather greater clarity, consistency, and modernization to support innovation. This includes harmonizing cross-border requirements, slowing the pace of new interventions, and providing clear, practical guidance on the use of data, AI, and consortium-based approaches. The opportunity for regulators to act as more effective enablers of collaboration and innovation — rather than solely supervisors — emerges as a defining theme for the years ahead.

Empowering Anti-Financial Crime Teams Through AI

AI technology has been applied in financial crime management for decades, but with the latest advances in generative and agentic AI there is greater potential for a step change in efficiency and effectiveness in the fight against financial crime.

Nearly three-quarters of respondents believe using AI for detection represents the most impactful opportunity to improve financial crime prevention.





Accordingly, financial institutions are continuing to explore AI's promise – 89% of respondents report either using or actively evaluating AI-based anti-financial crime solutions. While new AI capabilities are still evolving and adoption varies across the industry, financial institutions noted that returns on AI investment are most visible in AML transaction monitoring, followed by fraud detection and investigations.

GenAI adoption among banks is also accelerating. More than a third of respondents report GenAI or large language models (LLMs) in production, with an additional 35% in proof-of-concept stages. Use cases such as copilots, digital analysts, and automated SAR/STR generation are gaining traction, resulting in more efficient resource allocation and a stronger defense against financial crime — enabling teams to focus on genuine threats rather than spending time on resource intensive compliance workflows.

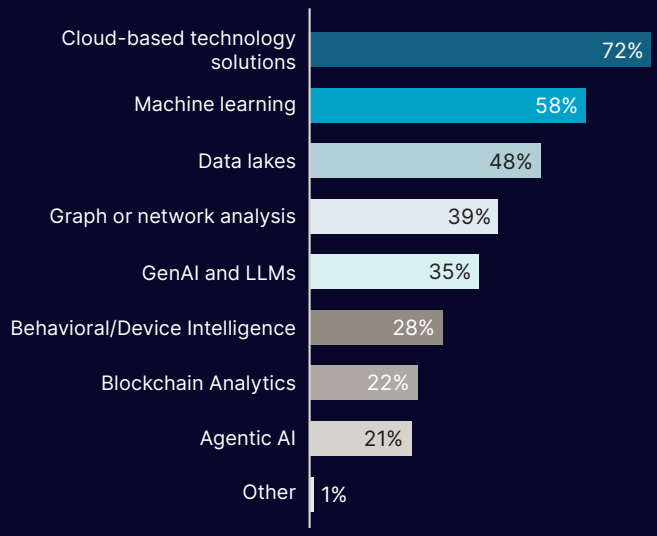
However, adoption is not without its challenges. 74% of institutions cite AI implementation as their biggest AML challenge, underscoring that integration and change management — not technology availability — are the primary bottlenecks to operationalizing this technology.

Closing the Gap in Collaboration

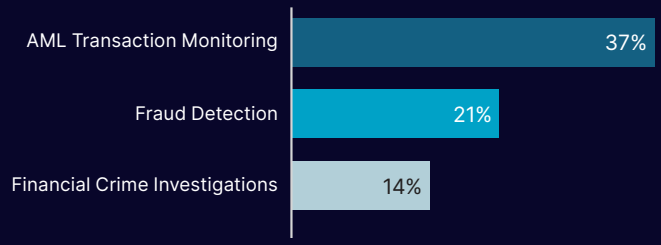
Collaboration across financial institutions and with public sector partners is vital to fight financial crime but remains challenging across the industry. Anti-financial crime professionals highlighted the challenges of both public sector collaboration, and private-to-private information sharing for their AML programs. Concerns over legal exposure and a lack of regulatory guidance remain the most cited barriers to sharing between banks, despite clear recognition of its value.

Our survey findings underscore a strong industry appetite for deeper public-private collaboration and more robust information sharing to strengthen anti-financial crime efforts. A majority of respondents indicated that collaboration between financial institutions and public sector stakeholders would materially benefit their anti-financial crime programs, noting in particular the need for regulators to play a more active role in enabling data sharing. These results highlight a clear opportunity for the public and private sectors to align around shared frameworks, defined measures of effectiveness, and coordinated action across regulators, law enforcement,

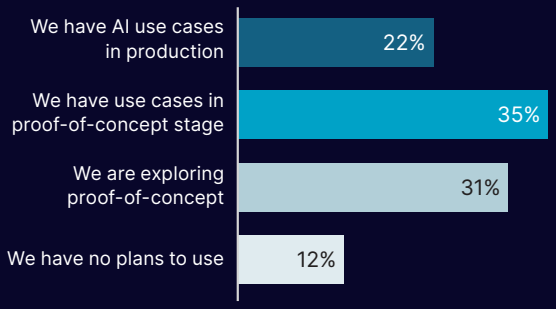
Technologies in Production for AFC
(inclusive of fraud detection and AML/CFT)



Top 3 Areas AI Technology is Having the Biggest Impact on Efficiency and Effectiveness



GenAI or Agentic AI in Use For AFC Processes



and financial institutions to better safeguard the integrity of the financial system.

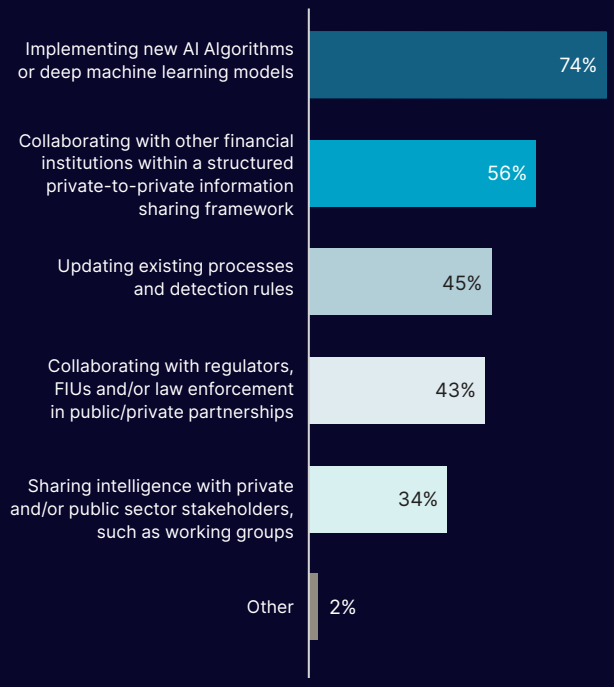
PPPs have emerged as a highly effective mechanism for translating collaboration into tangible outcomes. Interviewees named initiatives such as Project Protect in Canada and the UK's Joint Money Laundering Intelligence Taskforce (JMLIT) to demonstrate how banks can collaborate under government-led frameworks to more effectively track illicit financial flows linked to high impact predicate crimes, including human trafficking and fentanyl trafficking networks. By enabling the sharing of higher quality, actionable intelligence with authorities, these partnerships have supported increased law enforcement disruption of organized crime, with some PPPs further evolving to prioritize asset tracing and recovery.

Private-to-private information sharing platforms empower financial institutions to detect crime more effectively, respond quickly to threats, and prevent losses — while reducing redundant processes and costs. Along with a consortium data approach and its robust insights, banks gain comprehensive visibility into risks and suspicious activities, strengthening defenses and minimizing risk displacement.[9] Greater regulatory support and clarity in guidance is essential to enable broader industry adoption and maximize these collaborative benefits.

Law enforcement alerts and communication with other banks are the top tactics used by respondents to identify emerging threats, followed by leveraging internal data and analysis. This highlights an additional opportunity to strengthen collective intelligence within the walls of institutions, through shared insights and collaborative approaches.

By working together, institutions can share intelligence and expertise to broaden their visibility into financial crime risks. By removing the siloes created by working within their own dataset, with narrow views of customer behavior and transactions, collaborative frameworks enable financial institutions create a more complete and accurate picture of financial crime risk. Collaborative anti-financial crime frameworks increase the efficiency of fraud and money laundering investigations, offering investigators the full context needed to assess risk, provide actionable intelligence to law enforcement, and disrupt criminal activity.

Challenges Faced by Institutions Regarding AML Capabilities



Advancing Network-Level Detection with Collaboration and Innovation

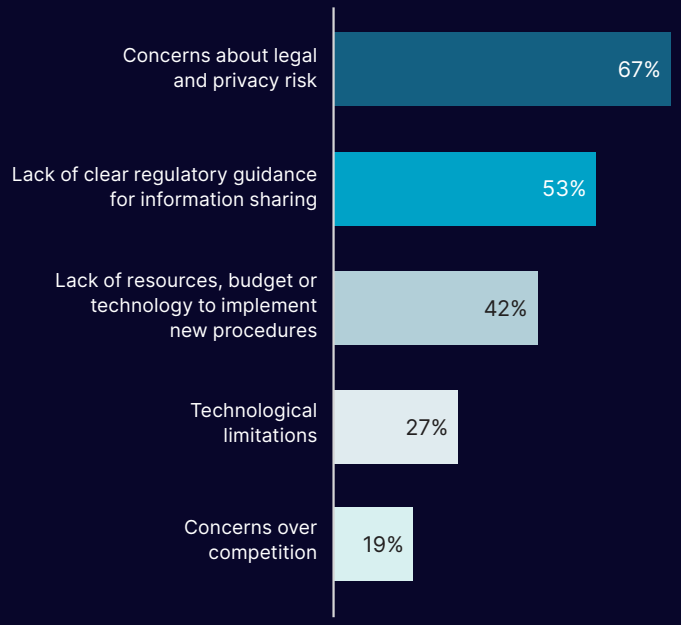
Today's financial crime threats are highly networked, adaptive, and distributed across institutions and channels, while most detection and prevention efforts remain institution-centric and fragmented. Criminal networks exploit this imbalance by operating below single institution visibility thresholds, moving funds rapidly across accounts, institutions, and jurisdictions in ways that are difficult to detect in isolation.

To close this gap, collective intelligence and consortium approaches can enable financial institutions to detect risk at the network level rather than the individual transaction or customer level. This collaborative model does not rely on direct sharing of Personally Identifiable Information (PII). Instead, it leverages privacy-protecting analytics applied across anonymized, aggregated signals contributed by many institutions, allowing patterns of coordinated or repeat criminal activity to emerge without exposing underlying customer data.

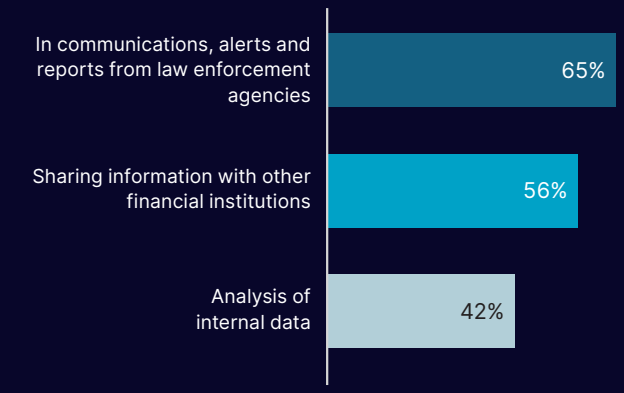
Anti-financial crime professionals emphasized the need for collective intelligence to identify emerging fraud typologies and coordinated scam activity earlier in the lifecycle, before losses are realized. The majority of respondents cited the improved use of innovative technology such as AI, advanced analytics, and the use of consortium data approaches as being one of the most beneficial ways to reduce consumer fraud losses from APP scams. By observing network-wide indicators, such as repeated account behaviors or mule-like transaction patterns, institutions can intervene earlier upstream, shifting fraud management from reimbursement and recovery toward proactive prevention.

Fraud, money laundering, mule activity, and predicate crimes are deeply interconnected, with criminal networks reusing the same accounts, intermediaries, and transaction pathways across institutions. Network-level analytics powered by consortium data allow these connections to be identified and signals shared, revealing coordinated risks that may otherwise be overlooked with a single bank-level view and without the complexities associated with structured information sharing partnerships.

Barriers In Bank-to-Bank Information Sharing



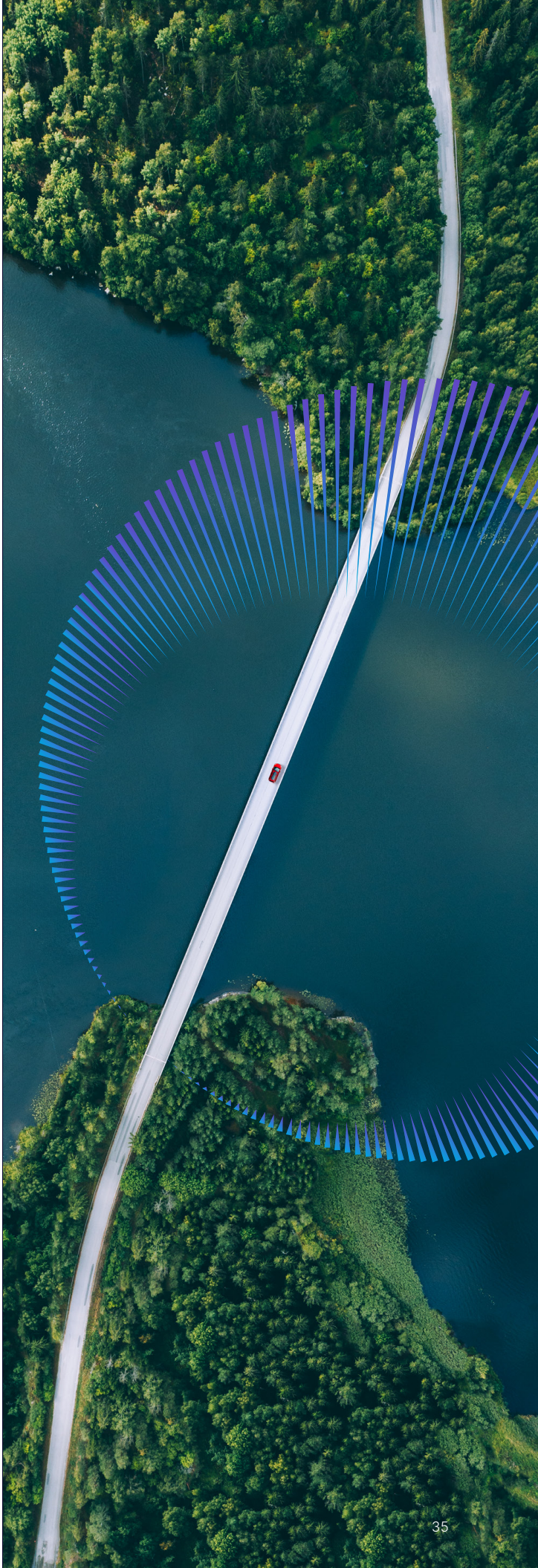
Top 3 Tactics to Identify New Threats & Trends



Collective intelligence and consortium analytics represent a powerful and practical mechanism for industry collaboration — one that complements existing regulatory frameworks while enabling institutions to act earlier, faster, and with greater confidence to disrupt connected criminal activity.

> The one thing we haven't touched on, which is still a bit of a dream, is cross-industry working and information sharing. This has been a topic for ten or more years, and while there are pockets of activity — in the US, Singapore, and the operational work of JMLIT in the UK — the resources and effort dedicated to it are minimal.

- Group Head of Compliance and Financial Crime Risk at G-SIB



Urgent Call to Collective Action

The scale, speed, and sophistication of today's financial crime perpetrators demand a response equal to the threat. Incremental improvements and siloed efforts are no longer enough. It's time for every sector impacted by the financial crime ecosystem to move decisively toward a solution together.

Set Strong Frameworks with Shared Responsibility

Governments and regulators are uniquely positioned to set the tone for a new age of crimefighting. Aligning on outcomes-focused priorities, creating clear guidance, and enabling innovation and collaboration across anti-financial crime frameworks can unlock more effective action across the private sector.

Responsibility must extend beyond financial institutions to cut off criminals at the source. Social media platforms and telecom providers have a critical role in helping to prevent exploitation through online channels. Likewise, AI platforms can provide vital insight into how criminals are leveraging tools and technology to their advantage — helping authorities stay ahead in an increasingly complex technology arms race.

Turn Collaboration into a Core Capability

No single institution, sector, or jurisdiction can combat financial crime alone. Today's criminal networks exploit fragmentation — between institutions and industries, as well as across borders and regulatory regimes. Closing these gaps requires collaboration that is not piecemeal or reactive, but systemic and sustained.

While successful partnerships for sharing intelligence exist around the world, there is an opportunity to expand those efforts and create a new global network model for collaboration. Every participant in the financial crime ecosystem has a role to play. Collaboration must become a core capability in the fight against financial crime, not a supplementary one.

Move at the Speed of Innovation

Bad actors are early adopters of new technology, leveraging AI to operate at speed and scale. To get ahead, the industry must lead anti-financial crime efforts with a technology-first mindset. Advances in AI are transforming the fight against financial crime by helping banks

overcome rising operational costs associated with check-box compliance processes, and delivering a step change in efficiency.

When combined with consortium data, collective intelligence, and network-level analytics, AI becomes more than a defensive tool — it becomes a strategic advantage. The industry clearly recognizes this potential. What is needed now is urgency: innovation must move at greater speed and scale than today's criminal threats.

The tools, technology, and insight to change the course of financial crime already exist.

What is required now is alignment — between the public and private sector, among industries, and across borders. By combining advanced AI with collective intelligence and shared accountability, we can disrupt criminal networks earlier, prevent harm before it occurs, and protect the integrity of the global financial system.

Glossary of Report Terms

Fraud Losses:
The estimate for total amount of losses from unauthorized bank fraud schemes and authorized fraud scams (where individuals or businesses incur a loss).

Unauthorized Fraud/Scams:
Fraudulent activity involving transactions or account actions executed without the legitimate customer's knowledge or consent, resulting from the compromise of credentials, payment instruments, or systems. As the customer did not authorize the activity, liability for the resulting financial loss typically rests with the financial institution in accordance with applicable consumer protection and payment regulations.

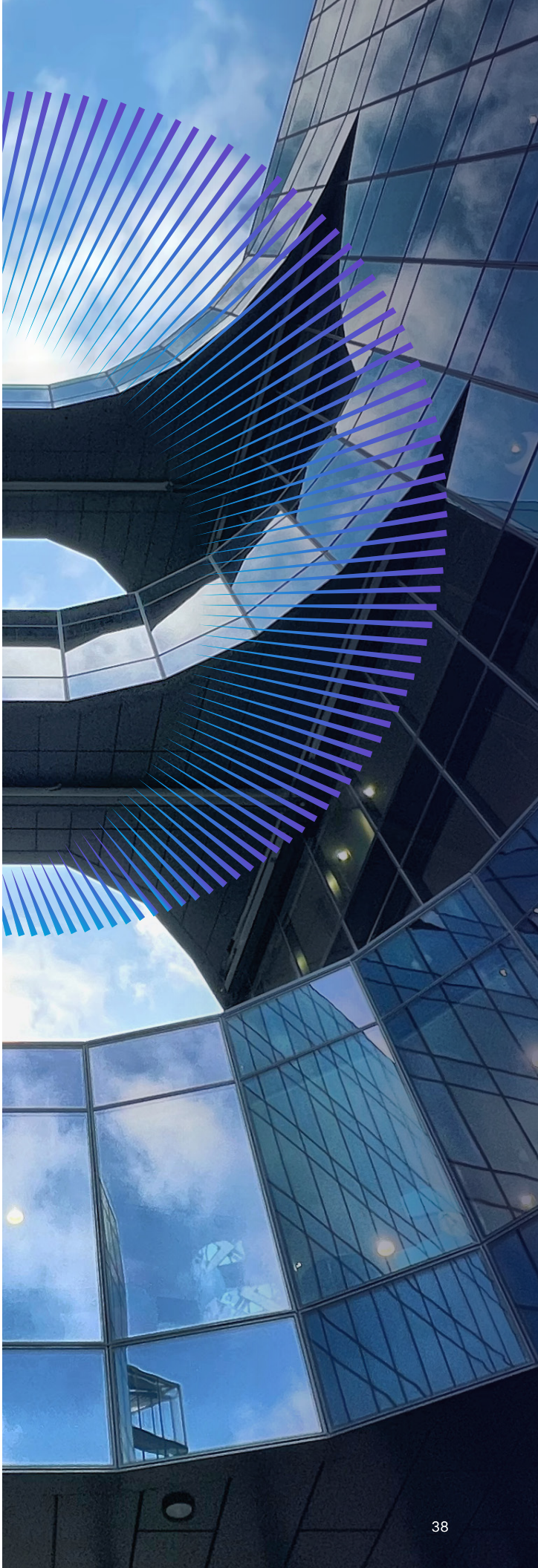
Authorized/Bank Fraud:
Fraudulent schemes in which an individual or business is deceived, manipulated, or coerced by a third-party fraudster into authorizing a transaction, payment, or disclosure of sensitive information under false pretenses. Although the transaction is technically authorized, it is induced through social engineering or misrepresentation, and the resulting financial loss is generally borne by the individual or business rather than the financial institution.

Cyber-Enabled Fraud:
Refers to fraud and losses connected specifically to Business Email Compromise (BEC), phishing attacks, and/or data breaches.

Elder Fraud:
A subset of total fraud where the loss was incurred by an individual senior. Within the context of this report, this data is distinct and is not additive with other reported loss statistics.

Cross-Border Illicit Funds Movement:
The flow of illicit funds from one country to another. This includes outgoing funds to an international destination or incoming funds originating from an international jurisdiction.

Domestic Illicit Funds Movement:
The flow of illegal funds strictly within a single country's borders.



References & Footnotes

[1] GDP was $106.9 trillion in 2023 and $114.8 trillion in 2025; presenting a 3.6% compound annual growth rate.

[2] Europe, Middle East, and Africa

[3] *Forced labour, modern slavery, and trafficking in persons,* International Labour Organization, 2025

[4] *World Drug Report,* United Nations Office on Drugs and Crime, 2025

[5] *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities,* Financial Crimes Enforcement Network, U.S. Department of the Treasury, 2021

[6] *Financial Crime Insights: Europe,* Nasdaq Verafin, 2025

[7] *How AI Is Revolutionizing Financial Crime Management,* Nasdaq Verafin, 2025

[8] *Report: 82.9% of Young Adults Have Been Tricked by Suspicious Links,* PYMNTS, 2025

[9] *A new era of private sector collaboration to fight economic crime,* The Future of Financial Intelligence Sharing Research Programme, 2025

Appendix A — Global, Regional, and Country-Level Estimates

Developed by Celent Research and Oliver Wyman as referenced in the Methodology section of this report.

Financial Crime: Global 2025

Subcategory		Global Total	2 YR CAGR	Total Americas	2 YR CAGR	Total EMEA	2 YR CAGR	Total Asia-Pacific	2 YR CAGR
Consumer & Business Fraud (Third-Party/Authorized)	**Aggregate Total**	**62,018**	**19.3%**	**20,851**	**22.8%**	**21,199**	**17.0%**	**19,969**	**18.2%**
	Cyber-enabled Fraud	14,271	19.6%	7,749	24.4%	4,091	15.6%	2,431	12.9%
	Business Email Compromise	9,599	19.9%	5,374	26.6%	2,671	14.1%	1,553	10.3%
	Phishing	528	19.7%	277	22.5%	147	13.9%	104	21.6%
	Data Breach	4,145	19.0%	2,098	19.5%	1,273	19.0%	773	17.6%
	Impersonation Scams	9,602	18.6%	2,334	21.0%	1,899	15.9%	5,369	18.6%
	Confidence/Romance Fraud	5,182	17.1%	1,392	22.2%	1,587	16.6%	2,203	14.6%
	Advance Fee/Lottery/Prize/Grant Fraud	27,323	19.5%	6,826	20.2%	11,457	18.4%	9,039	20.3%
	Employment Fraud	5,640	20.3%	2,549	27.1%	2,164	13.8%	927	19.8%
Bank Fraud (vFirst-Party/ Unauthorized)	**Aggregate Total**	**517,376**	**8.2%**	**190,686**	**17.9%**	**111,694**	**7.0%**	**214,996**	**1.9%**
	Account to Account Payments Fraud: Credit Transfers & Direct Debits	439,297	6.6%	132,721	13.7%	107,483	6.9%	199,093	2.3%
	Check Fraud	38,534	20.4%	34,192	27.5%	376	-9.7%	3,966	-11.8%
	Credit Card Fraud	39,546	17.7%	23,773	32.2%	3,835	11.6%	11,938	0.3%
Total Fraud		**579,395**	**9.2%**	**211,536**	**18.3%**	**132,893**	**8.4%**	**234,966**	**3.0%**
Fraud Against Elder Victims (Subset of Total Fraud)		**88,626**	**6.8%**	**28,283**	**7.8%**	**28,519**	**6.6%**	**31,824**	**6.1%**
Money Laundering	**Total Money Laundering**	**4,401,919**	**19.2%**	**1,623,208**	**24.0%**	**1,402,589**	**21.4%**	**1,376,123**	**12.2%**
	Terrorist Financing: Arms Trafficking, Foreign, Domestic, Domestic Violent Extremist (DVE)	16,203	18.8%	7,540	21.5%	5,278	19.4%	3,384	12.7%
	Human Trafficking: Sex Trafficking, Forced Labor (not Forced Marriage)	528,541	23.5%	181,388	29.0%	167,244	24.7%	179,910	17.6%
	Drug Trafficking & DTOs	1,073,523	17.1%	428,044	22.0%	321,979	19.2%	323,500	9.7%
	Other Crimes: Organized Crime, Fraud, Corruption, etc.	2,783,651	19.2%	1,006,236	24.1%	908,087	21.6%	869,329	12.2%
	Cross-border Illicit Funds Movement	**482,869**	**-**	**155,662**	**14.3%**	**221,870**	**-**	**105,337**	**-**
	Domestic Illicit Funds Movement	**3,919,050**	**-**	**1,467,546**	**25.2%**	**1,180,719**	**-**	**1,270,785**	**-**
	Money Mules Total	**284,020**	**-**	**63,929**	**31.1%**	**109,597**	**-**	**110,493**	**-**
	Money Mules (Cross-border)	57,295	-	13,719	41.5%	28,892	-	14,684	-
	Money Mules (Domestic)	226,724	-	50,210	28.7%	80,705	-	95,809	-

Financial Crime: Americas 2025

	Subcategory	Americas Total	2 YR CAGR	Total US	2 YR CAGR	Total Canada	2 YR CAGR	Total Latin America	2 YR CAGR
Consumer & Business Fraud (Third-Party/Authorized)	**Aggregate Total**	**20,851**	**22.8%**	**17,472**	**24%**	**1,411**	**23%**	**1,967**	**11%**
	Cyber-enabled Fraud	7,749	24.4%	6,782	25%	386	30%	581	13%
	Business Email Compromise	5,374	26.6%	4,755	28%	237	25%	381	12%
	Phishing	277	22.5%	209	14%	48	138%	21	11%
	Data Breach	2,098	19.5%	1,818	20%	101	23%	179	16%
	Impersonation Scams	2,334	21.0%	2,115	22%	87	22%	131	6%
	Confidence/Romance Fraud	1,392	22.2%	1,154	22%	65	9%	173	31%
	Advance Fee/Lottery/Prize/Grant Fraud	6,826	20.2%	5,700	23%	363	22%	763	4%
	Employment Fraud	2,549	27.1%	1,722	30%	510	22%	318	23%
Bank Fraud (First-Party/Unauthorized)	**Aggregate Total**	**190,686**	**17. 9%**	**178,833**	**19%**	**1,968**	**5%**	**9,885**	**8%**
	Account to Account Payments Fraud: Credit Transfers & Direct Debits	132,721	13.7%	122,257	14%	1,168	5%	9,296	7%
	Check Fraud	34,192	27.5%	33,628	28%	437	-3%	126	8%
	Credit Card Fraud	23,773	32.2%	22,948	33%	363	12%	462	29%
Total Fraud		**211,536**	**18.3%**	**196,306**	**19%**	**3,379**	**11%**	**11,852**	**9%**
Fraud Against Elder Victims (Subset of Total Fraud)		**28,283**	**7.8%**	**22,843**	**9%**	**1,344**	**5%**	**4,096**	**4%**
Money Laundering	**Total Money Laundering**	**1,623,208**	**24.0%**	**1,309,297**	**24%**	**65,207**	**18%**	**248,704**	**23%**
	Terrorist Financing: Arms Trafficking, Foreign, Domestic, Domestic Violent Extremist (DVE)	7,540	21.5%	6,069	21%	249	24%	1,222	24%
	Human Trafficking: Sex Trafficking, Forced Labor (not Forced Marriage)	181,388	29.0%	143,253	30%	6,770	19%	31,364	27%
	Drug Trafficking & DTOs	428,044	22.0%	336,591	22%	18,668	23%	72,785	20%
	Other Crimes: Organized Crime, Fraud, Corruption, etc.	1,006,236	24.1%	823,383	25%	39,520	15%	143,333	24%
	Cross-border Illicit Funds Movement	**155,662**	**14.3%**	**100,222**	**2%**	**4,991**	**-3%**	**50,449**	**65%**
	Domestic Illicit Funds Movement	**1,467,546**	**25.2%**	**1,209,075**	**27%**	**60,215**	**20%**	**198,255**	**17%**
	Money Mules Total	**63,929**	**31.1%**	**48,870**	**28%**	**2,372**	**20%**	**12,687**	**49%**
	Money Mules (Cross-border)	13,719	41.5%	8,370	23%	355	8%	4,994	117%
	Money Mules (Domestic)	50,210	28.7%	40,500	29%	2,017	22%	7,693	28%

Financial Crime: EMEA 2025

Subcategory		EMEA Total	2 YR CAGR	Total UK	2 YR CAGR	Total EU	2 YR CAGR	Total France	2 YR CAGR	Total Ger	2 YR CAGR	Total Other Europe	2 YR CAGR	Total Middle East	2 YR CAGR	Total Africa	2 YR CAGR
Consumer & Business Fraud (Third-Party/Authorized)	**Aggregate Total**	**21,199**	**17.0%**	**4,042**	**22%**	**8,875**	**17%**	**1,588**	**17%**	**2,972**	**28%**	**3,144**	**11%**	**2,787**	**17%**	**2,349**	**16%**
	Cyber-enabled Fraud	4,091	15.6%	399	10%	2,091	17%	344	8%	510	8%	978	19%	443	12%	180	11%
	Business Email Compromise	2,671	14.1%	257	8%	1,372	15%	223	6%	329	6%	645	18%	291	11%	106	4%
	Phishing	147	13.9%	21	31%	74	14%	16	20%	27	29%	29	7%	15	7%	8	19%
	Data Breach	1,273	19.0%	121	12%	645	20%	105	10%	155	10%	304	22%	137	15%	67	24%
	Impersonation Scams	1,899	15.9%	255	30%	983	18%	162	9%	240	9%	383	9%	208	13%	71	2%
	Confidence/ Romance Fraud	1,587	16.6%	305	30%	501	18%	22	24%	431	28%	179	7%	342	15%	261	11%
	Advance Fee/ Lottery/Prize/Grant Fraud	11,457	18.4%	2,955	22%	4,986	18%	884	22%	1,377	23%	1,429	7%	1,437	23%	651	28%
	Employment Fraud	2,164	13.8%	128	30%	315	18%	176	22%	413	-	175	7%	359	9%	1,187	14%
Bank Fraud (First-Party/ Unauthorized)	**Aggregate Total**	**111,694**	**7.0%**	**39,219**	**13%**	**55,218**	**0.18%**	**24,399**	**-1%**	**12,640**	**5%**	**8,728**	**17%**	**4,204**	**1%**	**4,325**	**65%**
	Account to Account Payments Fraud: Credit Transfers & Direct Debits	107,483	6.9%	38,324	14%	53,248	0.05%	23,345	-1%	12,510	5%	7,911	18%	4,039	0.17%	3,961	61%
	Check Fraud	376	-9.7%	28	-25%	293	-10%	204	-12%	3	-28%	40	16%	15	-10%	-	-100%
	Credit Card Fraud	3,835	11.6%	867	5%	1,677	7%	851	4%	127	12%	777	10%	149	15%	364	126%
Total Fraud		**132,893**	**8.4%**	**43,262**	**14%**	**64,093**	**2%**	**25,987**	**0.3%**	**15,612**	**9%**	**11,873**	**16%**	**6,991**	**6%**	**6,674**	**42%**
Fraud Against Elder Victims (Subset of Total Fraud)		**28,519**	**6.6%**	**3,084**	**9%**	**13,241**	**7%**	**2,306**	**6%**	**3,922**	**6%**	**6,292**	**4%**	**4,094**	**8%**	**1,808**	**4%**
Money Laundering	**Total Money Laundering**	**1,402,589**	**21.4%**	**151,087**	**24%**	**672,412**	**24%**	**118,903**	**22%**	**189,764**	**21%**	**306,686**	**20%**	**179,441**	**15%**	**92,962**	**19%**
	Terrorist Financing: Arms Trafficking, Foreign, Domestic, Domestic Violent Extremist (DVE)	5,278	19.4%	404	16%	2,373	23%	570	25%	710	16%	1,229	19%	856	15%	416	16%
	Human Trafficking: Sex Trafficking, Forced Labor (not Forced Marriage)	167,244	24.7%	19,265	27%	77,127	27%	15,513	29%	21,103	25%	34,328	24%	24,291	19%	12,233	24%
	Drug Trafficking & DTOs	321,979	19.2%	35,026	25%	158,025	21%	30,375	22%	44,763	23%	66,508	17%	40,891	13%	21,530	15%
	Other Crimes: Organized Crime, Fraud, Corruption, etc.	908,087	21.6%	96,393	23%	434,887	24%	72,446	20%	123,188	20%	204,621	20%	113,403	15%	58,783	20%
	Cross-border Illicit Funds Movement	**221,870**	**-**	**23,130**	**2%**	**154,412**	**2%**	**27,305**	**0.2%**	**43,577**	**0%**	**23,476**	**-**	**13,736**	**-**	**7,116**	**-**
	Domestic Illicit Funds Movement	**1,180,719**	**-**	**127,957**	**29%**	**518,000**	**34%**	**91,598**	**31%**	**146,186**	**31%**	**283,211**	**-**	**165,705**	**-**	**85,846**	**-**
	Money Mules Total	**109,597**	**-**	**10,653**	**24%**	**59,952**	**27%**	**9,470**	**21%**	**16,419**	**21%**	**20,240**	**-**	**11,692**	**-**	**7,060**	**-**
	Money Mules (Cross-border)	28,892	-	2,148	0%	21,865	21%	2,980	6%	5,168	7%	2,687	-	1,552	-	639	-
	Money Mules (Domestic)	80,705	-	8,505	33%	38,087	31%	6,489	30%	11,252	30%	17,553	-	10,140	-	6,421	-

Financial Crime: APAC 2025

Subcategory		APAC Total	2 YR CAGR	Total Australia	2 YR CAGR	Total Japan	2 YR CAGR	Total Singapore	2 YR CAGR	Total China	2 YR CAGR	Total Hong Kong	2 YR CAGR	Total Other Asia & Pacific	2 YR CAGR
Consumer & Business Fraud (Third-Party/Authorized)	**Aggregate Total**	**19,969**	**18.2%**	**2,780**	**29%**	**2,592**	**21%**	**423**	**24%**	**6,747**	**14%**	**870**	**4%**	**6,558**	**20%**
	Cyber-enabled Fraud	2,431	12.9%	288	18%	351	10%	73	27%	605	10%	37	9%	1,076	13%
	Business Email Compromise	1,553	10.3%	187	16%	206	3%	44	20%	397	9%	22	1%	698	12%
	Phishing	104	21.6%	13	29%	16	23%	2	19%	21	8%	2	41%	49	26%
	Data Breach	773	17.6%	88	20%	129	24%	27	43%	187	13%	14	21%	329	16%
	Impersonation Scams	5,369	18.6%	676	31%	238	7%	113	5%	1,196	3%	77	4%	3,069	27%
	Confidence/ Romance Fraud	2,203	14.6%	353	31%	263	56%	63	30%	623	3%	42	7%	858	11%
	Advance Fee/ Lottery/Prize/ Grant Fraud	9,039	20.3%	1,333	31%	1,682	23%	56	2%	4,127	20%	631	4%	1,211	19%
	Employment Fraud	927	19.8%	130	31%	57	23%	117	76%	196	14%	81	4%	345	14%
Bank Fraud (First-Party/Unauthorized)	**Aggregate Total**	**214,996**	**1.9%**	**7,050**	**-1%**	**7,879**	**-1%**	**311**	**9%**	**188,270**	**2%**	**93**	**5%**	**11,393**	**3%**
	Account to Account Payments Fraud: Credit Transfers & Direct Debits	199,093	2.3%	6,080	0%	7,337	-1%	207	15%	175,414	2%	-	-	10,053	5%
	Check Fraud	3,966	-11.8%	74	-21%	140	-22%	61	-5%	2,893	-10%	-	-	798	-15%
	Credit Card Fraud	11,938	0.3%	895	-3%	402	-1%	42	7%	9,963	0%	93	5%	542	3%
Total Fraud		**234,966**	**3.0%**	**9,830**	**6%**	**10,471**	**3%**	**734**	**17%**	**195,017**	**2%**	**962**	**4%**	**17,951**	**8%**
Fraud Against Elder Victims (Subset of Total Fraud)		**31,824**	**6.1%**	**1,584**	**9%**	**4,156**	**10%**	**324**	**6%**	**16,399**	**4%**	**261**	**5%**	**9,101**	**8%**
Money Laundering	**Money Laundering Total**	**1,376,123**	**12.2%**	**64,247**	**15%**	**133,753**	**4%**	**17,754**	**28%**	**795,633**	**16%**	**17,281**	**35%**	**347,455**	**6%**
	Terrorist Financing: Arms Trafficking, Foreign, Domestic, Domestic Violent Extremist (DVE)	3,384	12.7%	171	16%	462	30%	38	28%	1,559	16%	34	15%	1,120	3%
	Human Trafficking: Sex Trafficking, Forced Labor (not Forced Marriage)	179,910	17.6%	4,665	20%	15,202	4%	2,274	32%	106,158	24%	2,306	30%	49,305	10%
	Drug Trafficking & DTOs	323,500	9.7%	15,834	14%	25,797	0%	3,858	26%	192,154	14%	4,173	34%	81,683	3%
	Other Crimes: Organized Crime, Fraud, Corruption, etc.	869,329	12.2%	43,576	16%	92,292	5%	11,584	28%	495,761	16%	10,768	37%	215,348	6%
	Cross-border Illicit Funds Movement	**105,337**	**-**	**4,918**	**-**	**10,238**	**-**	**1,359**	**-**	**60,903**	**-**	**1,323**	**-**	**26,596**	**-**
	Domestic Illicit Funds Movement	**1,270,785**	**-**	**59,329**	**-**	**123,515**	**-**	**16,395**	**-**	**734,730**	**-**	**15,958**	**-**	**320,859**	**-**
	Money Mules Total	**110,493**	**-**	**4,125**	**-**	**9,277**	**-**	**1,239**	**-**	**69,234**	**-**	**1,504**	**-**	**25,115**	**-**
	Money Mules (Cross-border)	14,684	-	548	-	1,232	-	179	-	9,192	-	200	-	3,334	-
	Money Mules (Domestic)	95,809	-	3,577	-	8,045	-	1,060	-	60,042	-	1,304	-	21,780	-

Cautionary Note Regarding Forward-Looking Statements:
Information set forth in this report contains forward-looking statements that involve a number of risks and uncertainties. Nasdaq cautions readers that any forward-looking information is not a guarantee of future performance and that actual results could differ materially from those contained in the forward-looking information. Forward-looking statements can be identified by words such as "can" and "will," and other words and terms of similar meaning. Such forward-looking statements include, but are not limited to, statements related to anticipated efficiencies, cost savings, and loss reductions. Forward-looking statements involve a number of risks, uncertainties or other factors beyond Nasdaq's control. These risks and uncertainties are detailed in Nasdaq's filings with the U.S. Securities and Exchange Commission, including its annual reports on Form 10-K and quarterly reports on Form 10-Q which are available on Nasdaq's investor relations website at http://ir.nasdaq.com and the SEC's website at www.sec.gov. Nasdaq undertakes no obligation to publicly update any forward-looking statement, whether as a result of new information, future events or otherwise.

Nasdaq, a leading global technology company, is committed to advancing anti-financial crime efforts by delivering world-leading solutions that safeguard the financial system and strengthen the integrity of the world's economy.

Nasdaq Verafin provides cloud-based Financial Crime Management Technology solutions for Fraud Detection, AML/CFT Compliance, High-Risk Customer Management, Sanctions Screening, and Information Sharing. More than 2750 financial institutions globally, representing more than $11 trillion in collective assets, use Nasdaq Verafin to prevent fraud and strengthen AML/CFT efforts. Leveraging our unique consortium data approach and targeted typology analytics with artificial intelligence, Nasdaq Verafin significantly reduces false positive alerts and delivers context-rich insights to fight financial crime more efficiently and effectively.

To learn how Nasdaq Verafin can help your institution fight fraud and money laundering, visit www.verafin.com or call 1-877-368-9986.

Nasdaq
Verafin