

2024 - 2025

# Financial Crime & Compliance Report



## About the Report

The third edition of the 2024-2025 Financial Crime and Compliance Report aims to provide a comprehensive analysis and industry insights to combat global financial crime. This report consolidates critical information on emerging threats, regulations, and compliance processes worldwide, backed by up-to-date data from industry leaders.

At Sanction Scanner, our mission is to secure financial systems and assist industry stakeholders in establishing an effective line of defense against financial crime. This report is designed to help organizations keep pace with the rapidly changing dynamics of the financial world by serving as a valuable resource for developing compliance strategies for both today and the future.

# TABLE OF CONTENTS

---

03

**About Us**

04

**The Year in Review**

07

**Financial Crime Through a Geopolitical Lens**

United States of America  
United Kingdom  
European Union  
Middle East and Africa  
Asia Pacific

37

**Geopolitical Turbulence: How Global Tensions Shape Financial Crime**

Sanctions and Their Ripple Effects  
Cross-Border Crime: New Challenges, New Solutions  
The Role of Global Tensions in Compliance

46

**Disruptive Fraud Schemes in 2024**

Fraud Trends  
Sector-Specific Fraud Tactics

61

**The Technological Vanguard in Financial Crime Prevention**

67

**Cryptocurrency and Beyond: The New Frontier of Financial Crime**

Crypto Crimes  
The Role of Blockchain Analytics  
Regulatory Responses to Digital Assets

75

**Spotlight on Industry-Specific Financial Crime**

83

**Strategic Roadmap for 2025**

# About Us

**Sanction Scanner** is an Anti-Money Laundering and Risk solutions provider established in 2019. It screens customers and transactions in a comprehensive data of 220+ countries. It also provides a transaction monitoring solution, and with this, every transaction can be monitored in real-time and be identified which one is suspicious. Besides, it offers an all-in-one compliance approach with 360° risk assessment by analyzing these data instantly and presenting it as a report to its users.

Sanction Scanner aims to minimize financial risks in accordance with the changing regulations of each country. It serves customers from various industries, such as banking, investment, finance, insurance, payment and fintech, crypto, money transfer, leasing, and factoring.

A woman with blonde hair tied back, wearing a white button-down shirt, is sitting at a desk in a library. She is smiling and looking at a silver laptop. Her hands are on the keyboard. In the background, there are bookshelves filled with books. The entire image has a blue color overlay.

# The Year in Review

# The Year in Review

As 2024 draws to a close, it is evident that this year has been anything but typical for the world of financial crime and compliance. The landscape has been reshaped by staggering financial crime statistics, evolving regulations, and mounting geopolitical tensions. The impact of these changes has been felt across the globe, influencing both immediate responses and long-term strategies.

To put things in perspective, **\$3.1 trillion** worth of illicit funds moved through the global financial system last year. This colossal figure includes approximately \$782.9 billion from drug trafficking, \$346.7 billion from human trafficking, and \$11.5 billion from terrorist financing. These numbers not only highlight the enormity of the problem but also underscore the urgent need for innovative solutions from financial institutions worldwide.

**In 2023, around 3.1 trillion dollars in illicit funds circulated through the global financial system.**



**\$782.9 billion**  
obtained from  
drug trafficking

---



**\$346.7 billion**  
obtained  
through fraud

---



**\$346.7 billion**  
obtained from  
human  
trafficking

---



**\$11.5 billion**  
used to finance  
terrorism

---

Geopolitical events have further complicated the picture. The ongoing situation in the West Bank and Gaza has led to increased scrutiny of financial transactions linked to terrorism and the misuse of humanitarian aid. Unlike the Russia-Ukraine conflict, where sanctions are easier to implement and enforce, the situation in the Middle East presents a more complex and uncertain challenge. Identifying and targeting situational abusers in this context is much more difficult and requires a nuanced approach. It calls for a thorough assessment of institutions' regional involvement and their readiness for potential sanctions.

Economic difficulties have further complicated matters. During times of financial hardship, societies struggle with increased instability and unpredictability while the hidden threat of money laundering intensifies behind the scenes. Financial institutions are under intense pressure as the global economy slows down and budgets tighten, grappling with the rising impact of economic strains on criminal activities. This has led to a greater demand for more efficient solutions and smarter resource management.

In response, technology has rapidly evolved to address these challenges. Artificial intelligence (AI), for instance, has emerged as a crucial ally in detecting and preventing financial crime, offering advanced tools for analysis and monitoring. On the other hand, technological progress also brings new risks. Criminals are exploiting AI to craft sophisticated deepfakes and synthetic identities, further complicating organizations' efforts to keep pace with evolving threats.



**38%**  
of compliance officers view the complexity of enforcement as the biggest challenge in 2024.

This year has been fast-paced and challenging, with the emergence of cross-border financial crime, new fraud trends, and changes in high-risk countries. A survey by Sanction Scanner revealed that 38% of compliance officers, like most of us, identified 'the complexity' of sanctions as the biggest challenge in '24.



# Financial Crime Through a Geopolitical Lens



# Financial Crime Through a Geopolitical Lens

## United States

The United States remains a focal point in the global fight against financial crime, facing a multifaceted threat landscape that continues to grow in complexity. With an estimated **\$300 billion** laundered annually—constituting 15% to 38% of global money laundering activities—the stakes have never been higher. The challenges posed by illicit finance are surged by rapid advancements in technology, the evolving regulatory environment, and geopolitical tensions.

This section focuses on key developments in the U.S. that have shaped the financial crime landscape in 2024, examining the impacts of legislation, regulatory scrutiny, and emerging threats.

With the large volumes of regulatory requirements inherent with the U.S. compliance landscape, often the simplest approach is the best. The Risk Based Approach is an important first step in gaining insight into your institution, program, customer base and products. A well thought out assessment is critical to any sustainable AML Program.



**Mario M. Duron**  
Chief Compliance Officer



## The U.S. National Strategy for Combatting Terrorist and Other Illicit Financing

The U.S. Department of the Treasury's [2024 National Strategy for Combatting Terrorist and Other Illicit Financing](#) outlines a comprehensive framework to tackle critical financial crime threats. This strategy, informed by the 2024 National Risk Assessments, zeroes in on significant risks such as large-scale fraud, ransomware attacks, and the financing of terrorism. Conflicts in the Middle East and Ukraine underscore the urgency of addressing these vulnerabilities as adversaries increasingly exploit gaps in the financial system.

To counter these threats, the strategy focuses on four key priorities:

First, closing legal and regulatory gaps by operationalizing the beneficial ownership registry and finalizing rules for high-risk sectors such as real estate and investment advisement.

Second, improving the U.S. AML/CFT regulatory framework to enhance efficiency and effectiveness through clearer guidance and better resource allocation.

Third, strengthening the operational capabilities of law enforcement and related agencies to prevent illicit actors from finding safe havens.

Finally, embracing technological innovation to advance payment technologies and compliance mechanisms, thus staying ahead of evolving threats.

The strategy is designed to align public and private sector efforts, ensuring a unified approach to mitigating the most pressing illicit finance risks. By enhancing transparency, regulatory efficiency, and technological capabilities, the 2024 Strategy aims to strengthen the U.S. financial system's resilience against sophisticated financial crimes.



## Enhancing Beneficial Ownership Transparency

The enactment of the [Corporate Transparency Act \(CTA\)](#) on January 1, 2024, marks a significant milestone in the United States' efforts to combat financial crime. The CTA's implementation is the culmination of years of legislative effort, following its initial passage in 2021 and critical amendments in 2023. The act targets the pervasive issue of anonymous shell companies, which have long been used to launder money, finance terrorism, and evade taxes. According to the Financial Crimes Enforcement Network (FinCEN), anonymous shell companies were implicated in **85%** of the money laundering cases investigated between 2016 and 2023, highlighting the critical need for this legislation.

Under the CTA, over 32 million domestic and foreign entities operating in the U.S. are now required to disclose their beneficial ownership information (BOI) to FinCEN. This requirement aims to eliminate the veil of secrecy that has historically allowed situational abusers to exploit legal entities for illicit purposes. The CTA mandates that companies provide detailed information on their beneficial owners, including full names, dates of birth, current addresses, and unique identification numbers, such as passports or driver's licenses. Non-compliance carries hefty penalties, with fines reaching up to \$500 per day (up to \$10,000) of violation and potential imprisonment for up to two years. These stringent measures reflect the U.S. government's commitment to ensuring transparency and accountability in corporate ownership.



FinCEN's new reporting system, developed in 2023, is designed to handle the massive influx of data expected from these disclosures. The system's effectiveness is critical in enabling law enforcement agencies to trace illicit funds, identify criminal networks, and hold offenders accountable. However, the success of the CTA will depend on FinCEN's ability to manage and analyze the BOI data effectively, as well as the compliance of businesses with the new regulations.

## Crypto Regulations

The explosive growth of cryptocurrencies has created new challenges for regulators, with 2024 witnessing a significant surge in both the adoption of digital assets and the associated risks of financial crime.

In 2023 alone, the global cryptocurrency market cap reached approximately **\$2.6 trillion**, with the U.S. accounting for nearly **40%** of global trading volume.

However, this rapid growth has also made cryptocurrencies a prime target for money laundering, fraud, and terrorist financing, leading to a sharp increase in regulatory scrutiny.

The [Financial Industry Regulatory Authority \(FINRA\)](#) played a pivotal role in this intensified scrutiny, conducting reviews of crypto asset communications. FINRA found that nearly 70% of the crypto communications it examined contained potential violations, most commonly related to misleading or deceptive statements. These findings have set the stage for aggressive enforcement actions in 2024, targeting companies that fail to comply with regulatory standards.

A landmark case that has influenced the regulatory landscape is the trial of [Sam Bankman-Fried \(SBF\)](#), the former CEO of FTX, once one of the world's largest cryptocurrency exchanges. The collapse of FTX in late 2022 led to losses exceeding \$10 billion for investors and became a symbol of the risks inherent in the largely unregulated crypto industry. SBF's trial, which concluded in early 2024, resulted in a guilty verdict on charges of fraud, money laundering, and conspiracy to commit numerous kinds of fraud. This high-profile case, combined with the increasing use of cryptocurrencies by terrorist organizations, has significantly shaped the U.S. government's approach to crypto regulation.



In response to these developments, the Biden administration took decisive action in 2024, starting with releasing the world's first Decentralized Finance (DeFi) Illicit Finance Risk Assessment. This assessment, which was in development throughout 2023, highlights the risks posed by DeFi platforms, including their use in laundering over \$1 billion by North Korean situational abusers and their role in facilitating ransomware attacks that cost U.S. businesses nearly **\$600 million** in 2023 alone. The report has sparked discussions in the U.S. Congress about the need for stricter regulations on DeFi platforms, including enhanced Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements.

Another significant legislative development is the passage of the [Financial Innovation and Technology for the 21st Century Act \(FIT21\)](#) in the House of Representatives. Introduced in 2023 and passed in 2024, the FIT21 Act seeks to establish a comprehensive regulatory framework for digital assets, providing much-needed clarity in the crypto market. The act proposes new consumer protection measures and updates to registration regimes, with the aim of reducing the risks associated with crypto investments and ensuring that digital assets are integrated into the financial system in a safe and transparent manner.



## Investment Advisers and the Push for Compliance

Investment advisers, managing an **estimated \$110 trillion** in assets globally, have come under increasing scrutiny in the United States, particularly regarding their exposure to money laundering risks. A comprehensive risk assessment conducted by the U.S. Treasury in 2023 revealed that **nearly 20%** of investment advisers had inadequate AML programs, making them vulnerable to criminal exploitation.

Recognizing these risks, FinCEN proposed new regulations at the end of 2023, which have taken effect in 2024, bringing investment advisers under the same AML and CFT obligations as other financial institutions.

The new regulations require investment advisers to implement robust AML and CFT programs, conduct regular risk assessments, and report suspicious activities to FinCEN. These requirements are expected to affect approximately 14,000 registered investment advisers in the U.S., who collectively manage over \$100 trillion in assets. Non-compliance with these regulations could result in substantial fines and other penalties as FinCEN and the SEC ramp up their enforcement efforts in 2024.

In 2023 alone, the SEC levied fines totaling over [\\$1.5 billion](#) on financial institutions for AML violations, a figure expected to rise as the new regulations come into full effect. These developments reflect a broader trend toward tightening financial crime controls across the U.S. financial services sector, ensuring that all players, from large banks to smaller investment firms, adhere to the highest compliance standards.

The United States' approach to combating financial crime in 2024 reflects a broader strategy of increasing transparency, tightening regulations, and addressing emerging threats. As the country continues to adapt to the evolving landscape, the effectiveness of these measures will be critical in safeguarding the integrity of the financial system. The intersection of technology, regulation, and geopolitics will play a decisive role in shaping the future of financial crime prevention in the U.S., making it imperative for policymakers, regulators, and industry stakeholders to stay vigilant and proactive in their efforts.



## United Kingdom

As 2024 draws to a close, the United Kingdom has continued to advance its strategies and frameworks for combating economic crime, reflecting both persistent challenges and significant progress. The Economic Crime Plan 2 (ECP2), [launched in 2023](#), represents a strategic investment of £400 million aimed at enhancing the UK's capabilities in tackling economic crime.

ECP2 is centered on several core objectives:

- Reinforcing AML regulations.
- Improving cross-border information sharing.
- Fostering greater collaboration among regulatory bodies and law enforcement agencies

A major focus is to strengthen the National Crime Agency's (NCA) capacity to investigate and prosecute complex financial crimes with expanded resources and improved technological tools to detect and disrupt illicit activities.

Another focus of the plan is also emphasizing better coordination between domestic and international partners to more effectively address global financial crime networks.

To enhance corporate transparency and accountability, the UK implemented The [Economic Crime and Corporate Transparency Act \(ECCTA\) 2023](#), marking a significant shift in the its legislative approach to economic crime.





This act introduces several key reforms designed to enhance corporate transparency and accountability.

Among its provisions is the creation of a new offense for firms that fail to prevent fraud, targeting organizations that meet specific financial thresholds and employee counts. ECCTA also grants Companies House expanded authority to request additional information, enforce corrective measures, and share data more proactively. This change aims to improve the accuracy and integrity of corporate records and reduce misuse opportunities.

Additionally, the act requires all company directors and 'People with Significant Control' to undergo identity verification either directly with Companies House or through approved providers, improving the reliability of beneficial ownership information.

One of ECCTA's notable updates is the regulation of crypto assets. The act introduces new powers to seize and recover crypto assets linked to criminal activities, reflecting the increasing recognition of risks associated with digital currencies. This provision is part of a broader effort to address the misuse of crypto assets for illicit purposes and ensure that the regulatory framework evolves with technological advancements.



The UK's regulatory landscape continued to evolve in 2024, with HM Treasury's publication of its [AML/CTF supervision report for 2022-2023](#) in May 2024. The report outlines the progress and challenges in the sector. It points out that roughly 10% of regulated businesses were considered high-risk. While the total fines imposed in this period amounted to **£197 million**—a drop from **£504 million** in the previous year—the FCA remained the most active, issuing the highest average fines of **£19.4 million**.

The report identifies sectors particularly vulnerable to economic crime, such as retail and wholesale banking, wealth management, and crypto-asset firms. It emphasizes recurring issues in AML policies, such as inadequate risk assessments, insufficient staff training, and poor record-keeping, underscoring the ongoing need for vigilance and improvements in AML controls.

In terms of enforcement, 2024 has seen significant action. Notably, Gamesy Operations Limited was [fined £6 million](#) by the Gambling Commission in January '24 for failing to conduct adequate AML checks. The FCA has also been active, rejecting over 88% of crypto registration applications due to inadequate AML controls. This shows the regulator's firm stance on ensuring financial institutions adhere to strict AML requirements.

The FCA,  
remained the most active,  
issuing the highest average fines  
**of £19.4 million**



The UK Gambling Commission has provided an update on financial risk checks as part of the broader regulatory landscape. On 22nd February, the commission outlined the next steps to address financial vulnerability in the gambling sector, with a focus on identifying risks such as bankruptcy orders and unpaid customer debts. This follows the Government's Whitepaper on Gambling, which introduced several reforms. Additionally, the UK government [has imposed](#) a £5 stake limit for adults aged 25 and over and a £2 limit for those aged 18 to 24 on online slot games. These limits are part of a broader effort to reduce the risk of compulsive gambling and ensure responsible gaming practices.

In January 2024, the UK introduced amendments to its Money Laundering Regulations (MLRs), redefining the treatment of [PEPs](#). Under the updated regulations, domestic PEPs will still be subject to enhanced due diligence (EDD) but will generally be treated as lower risk than overseas PEPs. Additionally, the

definition of “high-risk third countries” [was updated](#) to align with those identified by the FATF, signaling a shift toward more globally coordinated AML/CFT efforts. The government's ongoing consultation on the reform of the MLRs is also expected to bring further improvements to the UK's AML framework, with a focus on making customer due diligence more proportionate and effective.

In parallel, the UK Law Commission's current consultation on recognizing digital assets as personal property is a significant development. This proposal, launched in early 2024, suggests the need for a new category of personal property to encompass digital assets that may not fit traditional definitions of property. The consultation explores how this classification could be applied to digital assets and the potential legal rights and responsibilities that could arise, particularly concerning ownership, tort, and related remedies. This evolving legal framework demonstrates the UK's wider efforts to regulate new technologies while protecting against potential abuses.



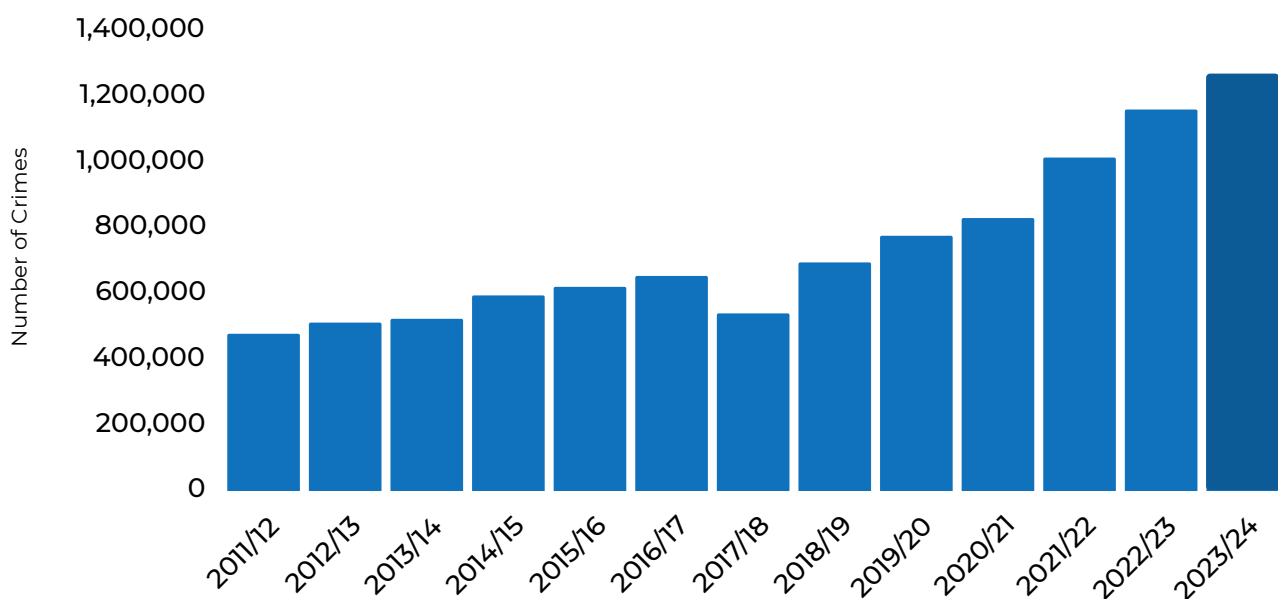
A notable development is the establishment of the Environment Agency's [Economic Crime Unit](#), which focuses on tackling money laundering within the waste sector, an area increasingly linked to illicit financial flows. The unit aims to conduct targeted investigations, pursue asset denial measures, and collaborate with other enforcement agencies to address financial crime within the industry.

Fraud remains one of the most pressing challenges in the UK, with the [2023 Half Year Fraud Report](#) revealing that **77%** of all Authorized Push Payment (APP) fraud originated from online platforms, while **45%** of fraud losses involved telecommunications scams. In response, the government introduced a new strategy in May 2023, with over 50 measures aimed at reducing fraud and cybercrime by 10% by 2025.

The launch of the Online Fraud Charter at the end of 2023 also marked a significant step toward curbing online scams, with 12 major tech companies committing to more stringent fraud prevention measures.

Despite the challenging situation, the UK is making steady progress day by day. [UK Finance reported](#) that consumers lost **£1.168 billion** to fraud and scams in 2023, a **4% reduction** compared to the previous year. Authorized fraud, particularly APP scams, saw a **5% decline** in losses, demonstrating that banks' investments in education, technology, and fraud detection systems are yielding results. However, given the complexity of modern financial crimes, further vigilance and continued investment in technology-driven solutions are essential for maintaining momentum in the fight against fraud.

Fraud Offenses in UK



Kaynak: statista.com

## European Union (EU)

The EU has taken significant strides in enhancing its regulatory framework to combat money laundering, terrorist financing, and other financial crimes. These efforts have become increasingly critical as the financial landscape evolves, particularly with the rise of digital assets, AI, and the ever-changing geopolitical environment. By the end of 2024, the EU will have implemented or will be finalizing several key regulatory measures, reflecting its commitment to maintaining the integrity of the EU financial system.

### Strengthening Anti-Money Laundering Arrangements: The Role of 6AMLD

The EU's approach to AML and CFT has undergone significant refinement with the adoption of the Sixth Anti-Money Laundering Directive (6AMLD) and the establishment of a single rulebook for AML. These updates introduce stricter measures for verifying customer identities and conducting due diligence, which apply to all AML-obliged entities, including banks, asset managers, and crypto asset service providers (CASPs). One of the notable new requirements is the extension of AML obligations to top-tier professional football clubs, as they must verify the identities of customers involved in significant financial transactions, including player transfers and sponsorship deals, as of 2024. The directive also places heightened vigilance on ultra-high-net-worth individuals, aiming to close the loopholes often exploited in high-value transactions.



These regulations are part of a broader package that includes the formation of the Anti-Money Laundering Authority (AMLA), which is set to oversee the enforcement of these rules across member states. While the exact deadlines for the full implementation of these regulations are not yet clear, it is expected that the AMLA will be fully operational by 2029, ensuring consistent application of AML standards across the EU.



## Key Provisions of 6AMLD

- **Expanded Definition of Money Laundering:** 6AMLD broadens the definition of money laundering to encompass a wider range of activities and methods. This includes not only the classic methods of disguising illicit funds but also new techniques that have emerged with digital and financial innovations. The directive explicitly criminalizes the act of participating in money laundering schemes, regardless of the individual's level of involvement.
- **Harmonization of Penalties:** One of the most significant aspects of 6AMLD is the harmonization of penalties across member states. The directive mandates that member states establish effective, proportionate, and dissuasive penalties for individuals and entities involved in money laundering. This aims to prevent jurisdictional discrepancies that could be exploited by criminals seeking more lenient legal environments.
- **Enhanced Focus on Beneficial Ownership:** 6AMLD places a stronger emphasis on the identification and verification of beneficial owners. It requires financial institutions to conduct thorough due diligence to uncover the individuals who ultimately own or control entities involved in transactions. This measure is designed to combat the use of shell companies and other complex structures to conceal the true owners of illicit funds.
- **Mandatory AML Training:** The directive mandates that financial institutions and designated non-financial businesses implement regular AML training for their employees. This ensures that staff are well-equipped to recognize and report suspicious activities, enhancing the overall effectiveness of AML measures.

- **Strengthened Cooperation and Information Sharing:** 6AMLD promotes enhanced cooperation and information sharing among member states, regulatory authorities, and financial institutions. This includes the exchange of information related to beneficial ownership and suspicious activities, facilitating a more coordinated response to cross-border money laundering threats.
- **Increased Focus on High-Risk Areas:** The directive specifically targets high-risk areas, such as virtual currencies and pre-paid cards, which have been increasingly exploited for money laundering. Financial institutions are required to apply enhanced due diligence measures in these sectors to mitigate associated risks.

## Implementation and Impact

The implementation of 6AMLD requires member states to amend their national legislation to align with the directive's provisions. This includes updating AML frameworks, enhancing compliance procedures, and ensuring that penalties for non-compliance are effective and deterrent.

The impact of 6AMLD is expected to be profound. By standardizing AML practices and penalties across the EU, the directive aims to reduce the chances of exploiting inconsistencies in national regulations. The enhanced focus on beneficial ownership and high-risk areas ensures that financial institutions are better equipped to detect and prevent money laundering activities.

Furthermore, the emphasis on training and information sharing fosters a more informed and collaborative approach to AML. Financial institutions will benefit from clearer guidelines and a more unified regulatory environment, leading to improved compliance and a stronger defense against financial crime.

Despite its strengths, the implementation of 6AMLD poses challenges. Financial institutions may face difficulties adapting to new requirements, particularly in areas such as EDD and staff training. Additionally, the effectiveness of the directive relies on the consistent and rigorous enforcement of its provisions across member states.





## Regulation of Crypto-Assets

The EU has also been proactive in addressing the risks associated with the growing crypto-asset market. The European Banking Authority (EBA) has issued comprehensive guidelines to help CASPs identify and mitigate risks related to money laundering and terrorist financing. These guidelines emphasize the need for CASPs to consider various risk factors, such as customer profiles, product offerings, and geographical operations, to tailor their AML efforts effectively.

Additionally, the EBA has initiated consultations on the implementation of the "Travel Rule" which mandates that CASPs and payment service providers exchange information about the originators and beneficiaries of crypto-asset transfers to enhance transparency and traceability.

In parallel, the European Securities and Markets Authority (ESMA) has published detailed technical standards under the Markets in Crypto-Assets Regulation (MiCA), providing clarity on the authorization process for CASPs, the requirements for financial entities intending to offer crypto-asset services, and the procedures for addressing customer complaints. These measures are expected to be fully implemented by the end of 2024, marking a significant step towards a more regulated and secure crypto-asset market in the EU.

## Transparency in Financial Markets: MiFIR and MiFID II

To further bolster the integrity of its financial markets, the EU has introduced amendments to the Markets in Financial Instruments Regulation (MiFIR) and the Markets in Financial Instruments Directive (MiFID II). These changes aim to enhance market data transparency, ensuring that investors have access to consolidated market data that is essential for informed decision-making.

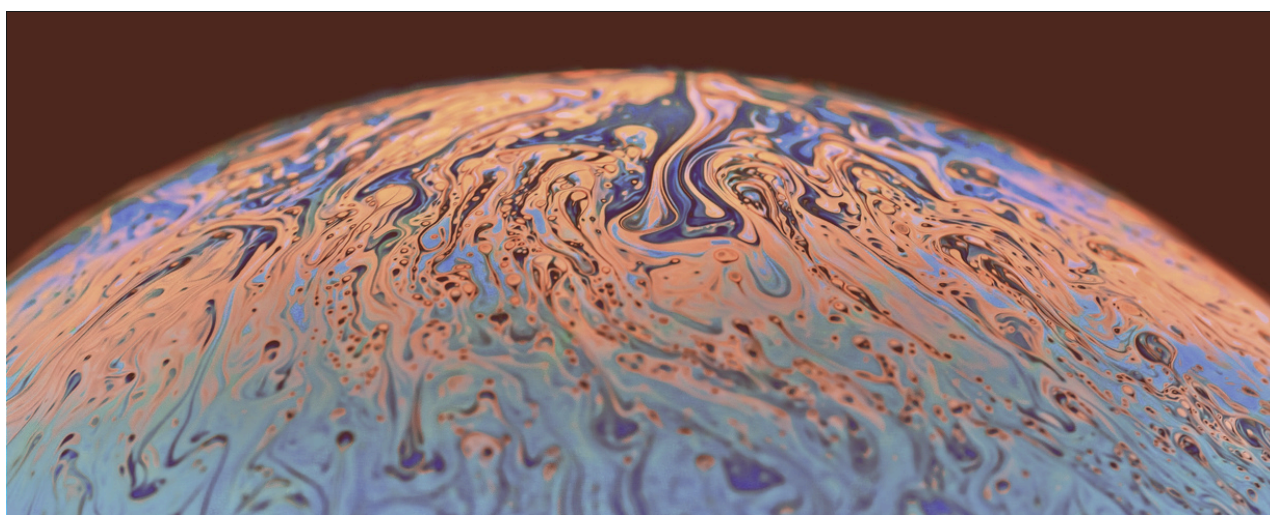
By strengthening these regulations, the EU seeks to promote a level playing field for all market participants and improve the global competitiveness of its capital markets.

The revisions to MiFIR and MiFID II are particularly important in light of the rapid digitalization of financial markets, which has increased the complexity and volume of transactions. Enhanced transparency measures are designed to address these challenges by providing investors with a clearer view of market dynamics and reducing the risk of market abuse.

## European Digital Identity and the EU AI Act

In addition to its efforts in financial regulation, the EU has made significant progress in the digital realm with the adoption of the European Digital Identity (eID) framework and the EU Artificial Intelligence (AI) Act. The eID framework, which mandates that all member states provide a digital identity wallet to their citizens by 2026, represents a major step towards a unified digital identity system across Europe. These wallets will enable EU residents to access public and private services online and offline, with enhanced security features such as free e-signatures and transaction dashboards.

The EU AI Act, now a law, categorizes AI systems based on their risk levels and imposes varying compliance obligations accordingly. For instance, AI systems deemed “high-risk” are subject to stringent regulatory requirements, including robust data governance, transparency, and accountability measures. This regulation is part of the EU’s broader strategy to lead in the global governance of AI, ensuring that AI technologies are developed and used in ways that are ethical and aligned with European values.





## Challenges and Future Directions

Despite these advancements, the EU faces ongoing challenges in fully implementing and enforcing its AML and financial crime regulations. For instance, the European Commission has called out several member states, including Ireland, France, and Latvia, for failing to correctly transpose the 4AMLD and 5AMLD into national law.

Moreover, Europol's threat assessment of financial and economic crimes in Europe underscores the growing sophistication of criminal networks and the increasing convergence between organized crime and sanctions evasion. The report revealed that approximately **70%** of criminal networks employ basic money laundering techniques, making it clear that traditional methods remain prevalent despite technological advances. Furthermore, **80%** of crimes involve the misuse of legal business structures, such as shell companies, complex structures, and cash-intensive businesses, which are often used to obscure the true origin of illicit funds. The report also highlighted that **60%** of these crimes include some form of corruption, emphasizing the pervasive influence of corrupt practices in facilitating financial crimes.

To address these issues, the EU will likely need to continue refining its regulatory framework, with a particular focus on emerging threats such as cybercrime and the misuse of new technologies. Additionally, greater coordination between member states and EU institutions will be crucial to ensuring that regulatory measures are consistently applied and effectively enforced across the Union.

As the EU approaches 2025, it leads global efforts to combat financial crime and regulate emerging technologies. Recent regulatory measures reflect its commitment to safeguarding the financial system and protecting citizens from money laundering and terrorist financing. Success will depend on overcoming enforcement challenges and ensuring all member states comply with high standards. The next few years will be critical for the EU to maintain its leadership and address evolving threats to its financial and digital ecosystems.

**Approximately 70%**  
of criminal networks employ  
basic money laundering  
techniques.



## Middle East & Africa



The Middle East and Africa, two regions rich in cultural diversity and geopolitical significance, grapple with an intricate web of sanctions that reflect their complex international relationships and security challenges. In the Middle East, the clash of political interests and ongoing conflicts have shaped a landscape where sanctions serve as both a tool for diplomatic leverage and a mechanism to curb illicit activities. Meanwhile, Africa's diverse economies and political climates necessitate a nuanced approach to sanctions, targeting specific threats while fostering stability. This dual focus on geopolitical tensions and regional stability underscores the impact of sanctions on shaping the economic and political contours of these vibrant regions.

The GDP of the Middle East is expected to reach **\$4.55 trillion** by 2029.

The Middle East, a region known for its economic diversity and complex regulatory landscape, has demonstrated notable economic progress in recent years. The region's GDP has grown from **\$2.460 billion** in 2015 to **\$3,570 billion** by 2024. According to the [International Monetary Fund](#), this upward trend is expected to continue, with projections indicating a GDP of **\$4.550 billion** by 2029. This economic expansion is accompanied by significant regulatory developments aimed at addressing financial crime and enhancing transparency.

## United Arab Emirates (UAE)

The UAE's financial sector has been under intense scrutiny by global regulatory bodies, especially after the FATF placed the country on its "grey list" in 2022 due to strategic deficiencies in UAE's AML and CTF measures. However, the UAE responded swiftly and effectively to these concerns. By February 2024, the UAE was officially removed from the FATF grey list following extensive reforms aimed at strengthening its regulatory environment. This move followed a series of regulatory enhancements to bolster financial transparency and combating illicit financial activities.

The country's progress in this area is evident through reforms such as the Federal Decree-Law No. 41/2023 on Accounting and Auditing. This new legislation imposes stricter accounting standards and introduces tougher

penalties for financial misreporting, aiming to bolster corporate governance and transparency

The Financial Services Regulatory Authority (FSRA) has updated its guidelines for virtual asset providers to align with the FATF's Travel Rule. These updates mandate rigorous AML protocols, including enhanced customer due diligence and transaction monitoring. Additionally, the Central Bank of the UAE (CBUAE) has established a new regulatory framework for stablecoins, requiring them to be fully backed by UAE Dirhams. This initiative seeks to stabilize digital currencies and mitigate financial risks. The formation of the General Commercial Gaming Regulatory Authority (GCCGRA) further reflects the UAE's commitment to regulatory oversight, now overseeing the country's first authorized lottery operation.



## Türkiye

Türkiye's regulatory environment underwent a major overhaul in 2024, particularly within the cryptocurrency sector. On July 2, the Grand National Assembly passed comprehensive legislation mandating licensing for crypto-asset service providers. Given Türkiye's high level of cryptocurrency usage, this law is a crucial step in structuring the rapidly growing market and aligning with global financial regulations.

This regulatory reform is a key factor behind Turkey's removal from the FATF Grey List in June, a move that is expected to enhance investor confidence and support the country's integration into the international financial system.



## Iran

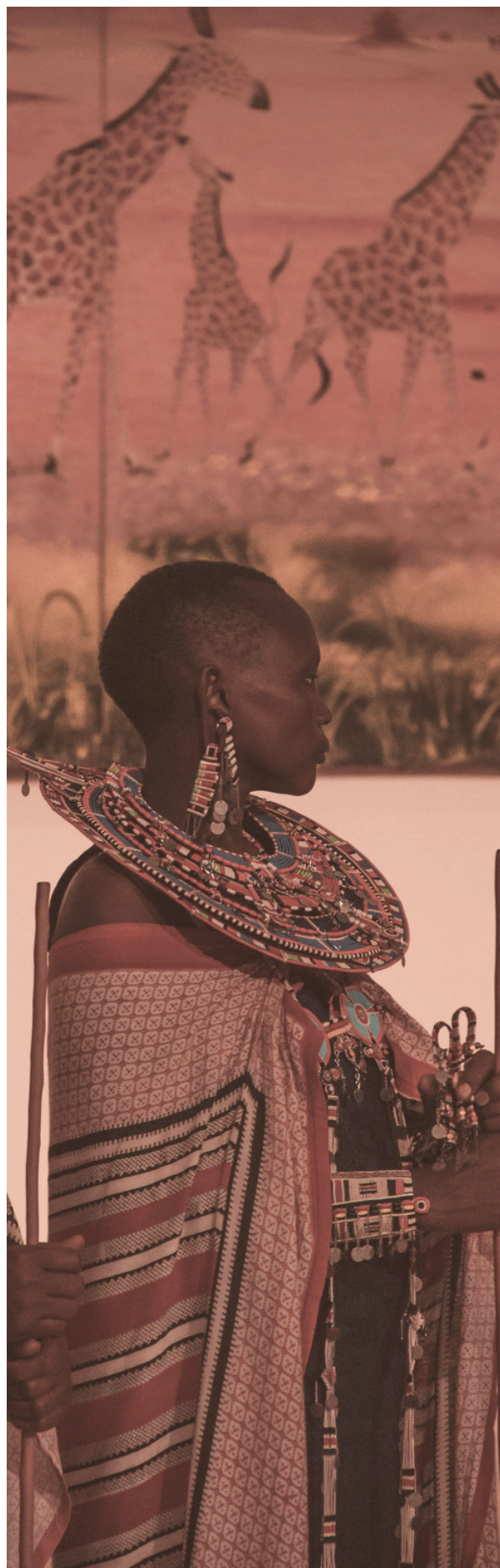
Iran continues to be a focal point of international sanctions due to its controversial policies and activities. As of 2024, the country has faced a broad sanctions regime involving [227 individuals and 42 entities](#). These sanctions encompass asset freezes, travel bans, and restrictions on trade and financial transactions. Recent EU sanctions, imposed on March 15, target individuals and entities involved in human rights abuses and regional destabilization, aiming to pressure the Iranian government to address these critical issues. Meanwhile, the United States has introduced new measures specifically targeting Iran's oil and gas sector, aiming to limit its financial capacity to support nuclear and militant activities.

## Africa

Africa's economic landscape in 2024 reflects a mix of growth and persistent challenges. Despite notable progress, including economic expansion and regional developments, the continent continues to face significant issues related to financial crime and illicit activities. Human trafficking remains a severe problem, particularly in countries such as Eritrea, South Sudan, and Somalia. These regions grapple with ongoing conflict and instability, underscoring the need for stronger regional cooperation and legal frameworks to protect vulnerable populations.

Illegal mining and wildlife trafficking are also prominent issues across the continent. The Democratic Republic of the Congo (DRC) faces considerable challenges with gold smuggling and unregulated mining, which not only undermine economic stability but also contribute to environmental degradation. The use of explosive precursor chemicals in illegal activities, such as blast fishing in Central Africa, exacerbates environmental damage and complicates efforts to address financial crime.

The broader landscape for AML and CTF efforts in Africa is marked by significant regional instability, weak governance, and socio-economic disparities. These factors create a fertile ground for various forms of financial crime, including money laundering, terrorist financing, and human trafficking. Africa loses an estimated **\$60 billion** annually to illicit financial flows driven by activities such as human trafficking, arms trafficking, wildlife trafficking, and gold smuggling. The continent's vast natural resources and weak regulatory environments make it a hotspot for criminal networks.





West Africa and the Sahel are particularly troubled by deteriorating security conditions exacerbated by terrorist groups like Boko Haram and the Islamic State. These groups engage in various illicit activities, including the trafficking of explosives and arms, further destabilizing the region. In Central Africa, countries such as the DRC and the Central African Republic (CAR) grapple with illegal mining operations and the smuggling of precious metals, particularly gold. These activities are often linked to armed conflicts, with proceeds used to finance rebel groups and terrorist organizations.

Amid these challenges, efforts to enhance regulatory frameworks and enforcement capabilities are ongoing. South Africa has taken significant steps to address financial crimes, focusing on wildlife trafficking and gold smuggling. In 2023, South Africa formed a task force in collaboration with the United States to combat wildlife trafficking, a major source of illicit finance. The country is also intensifying its crackdown on gold smuggling operations used by criminal gangs to launder money and evade sanctions.

Nigeria is witnessing a rise in digital fraud, including mobile, computer, and point-of-sale fraud. The government is responding by bolstering regulatory and technological measures to combat the growing threat of cyber-enabled financial crimes.

International cooperation remains crucial in Africa's fight against financial crime. The European Union and other global powers continue to impose and enforce sanctions on entities and individuals involved in destabilizing activities, particularly those linked to terrorist financing and organized crime

# Asia Pacific

## China

China's regulatory landscape in 2024 saw significant advancements aimed at strengthening AML measures and combating financial crime. One of the key developments was the ongoing crackdown on money laundering networks with international ties. In June 2024, U.S. authorities charged 24 Chinese individuals involved in laundering over **\$50 million** for Mexican drug cartels. These operations exploit China's capital controls, leading to limits on citizens sending more than **\$50,000** abroad per calendar year, creating demand for underground financial networks that cartels have tapped into.

China introduced an amendment to its local Anti-Money Laundering Law (AMLL), which expands the scope of AML regulations. The updated law, expected to take full effect by the end of 2024, places new compliance requirements on financial institutions and non-financial entities, including real estate and precious metals sectors. Key provisions include stricter customer due diligence (CDD), enhanced risk management systems, and mandatory reporting of beneficial ownership to regulatory authorities.

Further reinforcing transparency, the Administrative Measures for Beneficial Ownership Information will come into force in November 2024. Issued by the People's Bank of China (PBOC) and the State Administration for Market Regulation (SAMR), these regulations require companies, partnerships, and foreign branches to report ownership details. The new rules target the concealment of ultimate ownership, particularly by foreign entities, and are designed to curb money laundering through complex corporate structures.



In addition to these developments, China also focuses on online gaming and digital assets. On December 22, 2023, the “Measures for the Management of Online Games” were introduced for public consultation. These measures aim to ensure and promote the “prosperity and healthy development” of the online gaming industry. Key provisions include technical equipment requirements and restrictions, with a strong emphasis on protecting minors and vulnerable players. Online game providers in China will be directly impacted by these regulations. On February 20, 2024, the Hong Kong Monetary Authority (HKMA) published Guidance on Expected Standards on Provision of Custodial Services for Digital Assets by Authorized Institutions.

This guidance includes provisions on risk assessment, AML/CFT compliance, disclosure, record keeping, and safeguarding client assets. Authorized institutions engaged in virtual asset-related activities such as intermediaries, distributing tokenized products, or providing standalone custodial services are affected.

Starting June 1, 2024, all virtual asset trading platforms operating in Hong Kong must be either licensed by the Securities and Futures Commission (SFC) or “deemed-to-be-licensed” VATP applicants under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO). This regulation impacts all VATPs operating in Hong Kong.

Additionally, despite a ban on cryptocurrency trading since 2021, illegal crypto activities persist in China. In May 2024, Chinese nationals traded approximately \$90 billion in cryptocurrencies, prompting renewed enforcement efforts. The crackdown on illegal virtual currency transactions remains a key priority for regulators, especially given the rising use of crypto in cross-border financial crime.

Looking forward, China's regulatory tightening in 2024 reflects its intent to align with international AML standards and strengthen financial oversight. These reforms, driven by the PBOC and other regulatory bodies, demonstrate China's commitment to combating financial crime both domestically and through international cooperation.





## Singapore

In June 2024, Singapore unveiled its [updated](#) Money Laundering National Risk Assessment (ML NRA), a pivotal update aimed at fortifying the AML framework in light of evolving financial crime threats. This updated assessment integrates data from the Suspicious Transaction Reporting Office (STRO) and feedback from both local and international stakeholders. It highlights the challenges posed by Singapore's role as a leading international financial center and trading hub, where its economic openness and advanced financial infrastructure are leveraged by criminals to launder illicit funds.



The updated ML NRA underscores that Singapore's primary money laundering threats include cyber-enabled fraud, foreign predicate crimes, organized crime, corruption, tax crimes, and trade-based money laundering. The assessment reveals that foreign and domestic cyber-enabled fraud remains a significant risk, driven by sophisticated criminal syndicates. Furthermore, it identifies key money laundering typologies such as the flow of illicit funds into or through Singapore's banking system, misuse of legal persons like shell companies, and the placement of illicit funds into high-value assets, including real estate and precious metals

In response to these identified threats, Singapore's regulatory landscape has been notably revised. On April 1, 2024, the Monetary Authority of Singapore (MAS) launched the COSMIC platform, a centralized digital tool designed to enhance the secure sharing of customer information among financial institutions. This platform, developed in collaboration with six major banks, allows institutions to exchange data on suspicious activities, significantly improving the timeliness and accuracy of risk assessments. This initiative is part of MAS's broader effort to strengthen AML and CFT measures.

Additionally, on April 2, 2024, MAS announced amendments to the Payment Services Act (PSA), which will take effect in stages from April 4, 2024. These amendments expand the regulatory scope to include digital payment token (DPT) service providers, aligning with the latest FATF standards. The revised PSA now covers activities such as custodial services for DPTs, facilitation of DPT transmissions, and cross-border money transfers.

In addition to these regulatory updates, Singapore's enforcement efforts have been significant. From [January 2022 to June 2023](#), MAS imposed **\$12.96 million** in civil penalties, including **\$7.88 million** in financial fines and compositions, the highest since the initiation of MAS Enforcement Reports in 2019. Of these fines, **\$7.10 million** were specifically related to violations of AML and CFT requirements





# Geopolitical Turbulence

# Geopolitical Turbulence: How Global Tensions Shape Financial Crime

## Sanctions and Their Ripple Effects

Sanctions have become one of the most prominent tools in the modern geopolitical landscape, used by countries to exert economic pressure on others in pursuit of foreign policy objectives. The scope, scale, and consequences of sanctions have grown dramatically over recent decades, especially with the advent of complex financial systems that allow for more targeted and far-reaching measures. This trend has only accelerated with the onset of major global conflicts, including Russia's invasion of Ukraine in February 2022. Sanctions, while designed to cripple the economic capabilities of targeted nations, often produce far-reaching effects that extend well beyond their intended scope, creating a range of economic, political, and humanitarian consequences.

The global response to the Russia-Ukraine conflict represents one of the largest and most comprehensive uses of sanctions in modern history. Since February 2022, [more than 16,500 sanctions](#) have been imposed on Russia by a coalition of Western countries, including the United States, the European Union, the United Kingdom, and Canada among others. These sanctions have primarily targeted key sectors of the Russian economy, such as energy, finance, and defense. They have also focused on oligarchs and other influential figures close to the Kremlin, aiming to dismantle the financial networks that support President Vladimir Putin's regime and its war efforts.



A key part of this sanctioning effort has been the freezing of Russia's foreign currency reserves, amounting to approximately [\\$350 billion](#). This has significantly curtailed Russia's ability to stabilize its economy and fund its war machine. Moreover, Western countries have frozen about 70% of the assets of Russian banks, cut many of them off from the international SWIFT system, and imposed strict export controls on technology crucial for weapon production. In addition to financial sanctions, the G7 imposed a price cap on Russian oil at [\\$60 per barrel](#), aiming to restrict the revenue Moscow could generate from its energy exports

Despite these extensive measures, the effectiveness of the sanctions has been a topic of much debate. In 2022, the Russian economy contracted by [2.1%](#), according to the International Monetary Fund (IMF). However, rather than collapsing as some predicted, Russia's economy proved more resilient, managing to grow by [2.2%](#) in 2023, with further growth of [1.1%](#) forecasted for 2024. This resilience is partly due to Russia's ability to reorient its trade relations, particularly with China and India, which have dramatically increased their imports of Russian oil and gas. India, in particular, has emerged as a key buyer of Russian crude, and China has helped fill the void left by Western suppliers by providing alternative technology and goods.

One of the reasons for the mixed impact of sanctions is that nations under sanctions often find ways to circumvent restrictions. For example, Russia has utilized a ["shadow fleet"](#) of tankers to export oil above the price cap, and countries like Kazakhstan, Kyrgyzstan, and Belarus have acted as intermediaries, smuggling sanctioned goods into Russia. These workarounds illustrate a broader challenge in enforcing sanctions: while sanctions can disrupt direct trade, the globalized nature of supply chains allows for alternative routes and smuggling networks to form. Sanctioned goods and services can thus continue to flow into the target country, albeit more expensively and less efficiently.





Sanctions on neighboring countries reduce trade in the region by **9% on average**

While sanctions are primarily intended to pressure the leadership of the target country, they often have unintended effects on neighboring nations. [Research](#) into sanctions imposed between 1989 and 2015 found that, on average, neighboring countries saw their trade decline by about 9% following the imposition of sanctions on a nearby state. This is due to the disruption of trade routes, increased transportation costs, and the loss of key trading partners.

For instance, sanctions imposed on Iraq following its invasion of Kuwait in 1990 led to economic hardship for [21 neighboring countries](#), including Jordan and Turkey, both of which had strong trading ties with Iraq.

However, [in some cases](#), neighboring countries have benefited economically from sanctions. For example, when sanctions were imposed on Haiti in 1987, the Dominican Republic saw an increase in import trade, likely due to cross-border smuggling and the redirection of trade flows.

Similarly, Kenya's trade expanded after sanctions were imposed on Somalia in 1992. These examples highlight the complexity of sanctions and the potential for unintended economic opportunities in neighboring nations. In the case of Russia, neighboring Kazakhstan has experienced an increase in trade as Russian companies relocate production facilities there to avoid sanctions.

Sanctions also pose significant humanitarian risks, especially when they are comprehensive or involve broad trade embargoes. The economic isolation of a nation can lead to shortages of essential goods, including food, medicine, and energy. In extreme cases, this can result in deteriorating health outcomes, increased mortality rates, and the destabilization of governance structures. Sanctions on Iran, Venezuela, and Cuba have been cited as [examples](#) where broad-based sanctions have severely impacted civilian populations, leading to worsening living conditions and inadvertently shoring up support for the very regimes they were designed to weaken. In these cases, governments often rally domestic support by framing sanctions as foreign-imposed suffering, thus reinforcing their grip on power.

One of the most significant developments in the use of sanctions is their role in technological and strategic competition. For instance, the United States has imposed sweeping sanctions on China to limit its access to advanced semiconductor technology, a crucial sector for both military and economic development. These measures aim to curtail China's ability to produce cutting-edge technology and maintain strategic superiority in the tech space. However, over time, such sanctions can also backfire by incentivizing the sanctioned country to develop its domestic production capabilities or seek alternative

sources. This has been the case with both Russia and China, which have increased their efforts to become self-sufficient in critical industries.

The ripple effects of sanctions are not confined to the direct economic consequences. Sanctions can also trigger shifts in global alliances and trade patterns. For example, Russia's invasion of Ukraine and the subsequent sanctions have accelerated Europe's transition away from Russian energy. Before the war, Europe was heavily dependent on Russian oil and gas, which accounted for about 40% of its natural gas supply. The conflict and the sanctions have forced European countries to diversify their energy sources, turning to renewables, liquefied natural gas (LNG), and other suppliers. This diversification is likely to have long-term effects on global energy markets, reducing Russia's share and increasing investment in alternative energy sources.

Furthermore, sanctions often become entrenched and difficult to remove, even when after achieving their initial objectives. Domestic interest groups in sanctioning countries may develop a vested interest in maintaining sanctions, as seen with the long-standing U.S. embargo on Cuba. In this case, U.S. sugar producers benefitted from the embargo by avoiding competition from Cuban sugar, leading to continued political support for the sanctions despite shifting geopolitical objectives.



Looking forward, the use of sanctions is likely to remain a central tool of foreign policy, especially in addressing global crises such as territorial aggression, human rights abuses, and nuclear proliferation. The sanctions imposed on Russia have demonstrated both the potential and the limitations of this approach. On one hand, they have inflicted significant economic damage and limited Russia's access to critical resources. On the other, they have failed to bring about the desired political change and have generated unintended consequences for neighboring countries and global markets.

The continued use of sanctions will require policymakers to carefully consider not only their immediate impact but also their long-term effects on global trade, economic stability, and humanitarian conditions. As sanctions become an increasingly preferred method of geopolitical coercion, it is crucial to develop more sophisticated enforcement mechanisms to prevent circumvention and mitigate unintended consequences. Additionally, recognizing the broader economic and humanitarian impacts of sanctions can help create more effective and targeted policies that minimize collateral damage while still achieving strategic goals.

## Cross-Border Crime

In the current geopolitical landscape marked by significant global tensions, cross-border crime has evolved into a formidable challenge, shaped by the shifting dynamics of international relations and economic disruptions. As nations grapple with the effects of geopolitical turbulence, the intricate nature of cross-border crime demands an equally sophisticated response.

In 2024, geopolitical tensions such as the Russia-Ukraine and conflicts in the Middle East have influenced financial crime trends. Sanctions have pushed criminals to develop new methods for money laundering using cryptocurrencies, DeFi, and shell companies. Trade-based money laundering has become more sophisticated, involving complex cross-border transactions to evade sanctions. The financing of terrorism has also increased, with global financial systems being used to support activities in conflict zones. In response to these trends, financial institutions are strengthening controls over PEPs, cross-border payments, and correspondent banking relationships.



**Vivek Mishra**

AML/KYC Professional

Geopolitical tensions and conflicts often create fertile ground for the proliferation of cross-border crime. Political instability, economic sanctions, and strained diplomatic relations can disrupt law enforcement and regulatory frameworks, allowing criminal networks to exploit gaps and weaknesses. Geopolitical upheavals have contributed to a **35% increase** in cross-border criminal activities over the past year. Conflict-ridden regions, such as Eastern Europe and the Middle East, have become hotspots for illicit operations. The ongoing conflict in Ukraine has significantly impacted human trafficking, with reported cases rising in these areas as criminal groups exploit the chaos to expand their reach.



Economic sanctions, such as those imposed on Russia, have inadvertently facilitated the growth of illicit activities by disrupting traditional financial channels. The emergence of alternative financial systems, often unregulated, has been exploited by criminal organizations. Illicit financial flows involving sanctioned countries have increased by 25%, highlighting the challenges posed by geopolitical tensions to global financial systems.

## New Challenges in Combating Cross-Border Crime

The confluence of geopolitical upheaval and cross-border crime presents several key challenges:

### Jurisdictional and Legal Complexities:

Differing legal frameworks and enforcement practices across countries create opportunities for criminals to evade detection. Variations in data privacy laws and investigative techniques have been exploited by cybercriminals, making cross-border attacks harder to combat.

**Technological Advancements:** Criminal organizations increasingly use advanced technologies, such as encryption and blockchain, to facilitate cross-border crimes. Despite the 2021 cryptocurrency collapse, crypto-related crime remained stable in 2022. [Data](#) shows **\$7.8 billion** in Ponzi schemes, **\$1.5 billion** spent on darknet markets, and **\$3.7 billion** stolen through hacks. A shift from Bitcoin dominance to a multi-chain reality has allowed criminals to exploit cross-chain bridges and chain-hopping to obscure illicit funds.

**International Cooperation and Resource Constraints:** Geopolitical tensions can strain international collaboration, hindering joint investigations and information sharing. Conflicting national interests and diplomatic disputes often delay responses and undermine coordinated anti-crime efforts



## Innovative Solutions and Responses

In response to these challenges, several innovative solutions and international initiatives are emerging:

### Technological Advancements in Law Enforcement:

Law enforcement agencies are adopting advanced technologies like AI and machine learning to track and disrupt cross-border crime. The use of AI-driven tools by Europol has led to an increase in successful interceptions of illicit activities.

**Regulatory Innovations:** To address the rise of digital currencies, regulatory bodies are implementing updated frameworks. The FATF has introduced new guidelines for cryptocurrency transactions, emphasizing enhanced AML measures and stricter KYC requirements.

**Enhanced International Collaboration:** New international coalitions, such as the Global Alliance Against Cross-Border Crime, are improving coordination and information sharing. This coalition has facilitated several joint operations, including the dismantling of major smuggling rings and the arrest of prominent criminals.

**Humanitarian and Support Initiatives:** Organizations like the International Organization for Migration (IOM) are focusing on the humanitarian impact of cross-border crime. In 2023, IOM expanded its victim assistance programs, providing support to over 18,000 survivors globally.



As we move into 2024 and beyond, the landscape of cross-border crime will continue to evolve parallel to unexpected global events, mainly politics. Dealing with these challenges requires a comprehensive approach that combines new technology, enhanced international collaboration, and robust regulations.

## The Role of Global Tensions in Compliance

How human beings communicate with each other has changed a lot over the last 20 years. This applies to international relations as well. They have to deal with more complicated situations, like more crime between countries and stricter rules about money.

One big change is that more and more countries are being told they cannot trade with other countries. This is causing problems for businesses that work internationally. For example, Russia and some other countries are facing these trade restrictions because of ongoing conflicts. This makes it harder for companies to trade, move money around, manage their assets, etc.



These trade restrictions don't just affect the countries involved. They also have an impact on the whole world's financial markets. Financial institutions, in particular, are under a lot of pressure to make sure they do not act against these restrictions. Consequently, regulators are intensifying their focus, with penalties for non-compliant parties growing more severe. Eventually, organizations are focusing more and more on compliance, conducting more checks and reinforcing their internal audits.

In the wake of escalating global tensions, regulators have ramped up efforts to combat financial crimes, particularly those related to money laundering and terrorism financing. Cross-border financial flows, especially those involving regions under sanctions, have come under intense scrutiny.

The emergence of alternative financial systems and digital currencies has further complicated the compliance landscape. Criminal organizations have exploited these unregulated channels, leading to an increase in illicit financial activities. Consequently, companies and financial institutions face growing pressure to monitor cryptocurrency transactions more rigorously. Regulators have issued updated guidelines mandating stronger safeguards against the misuse of digital assets, including more comprehensive reporting obligations for cross-border transactions.

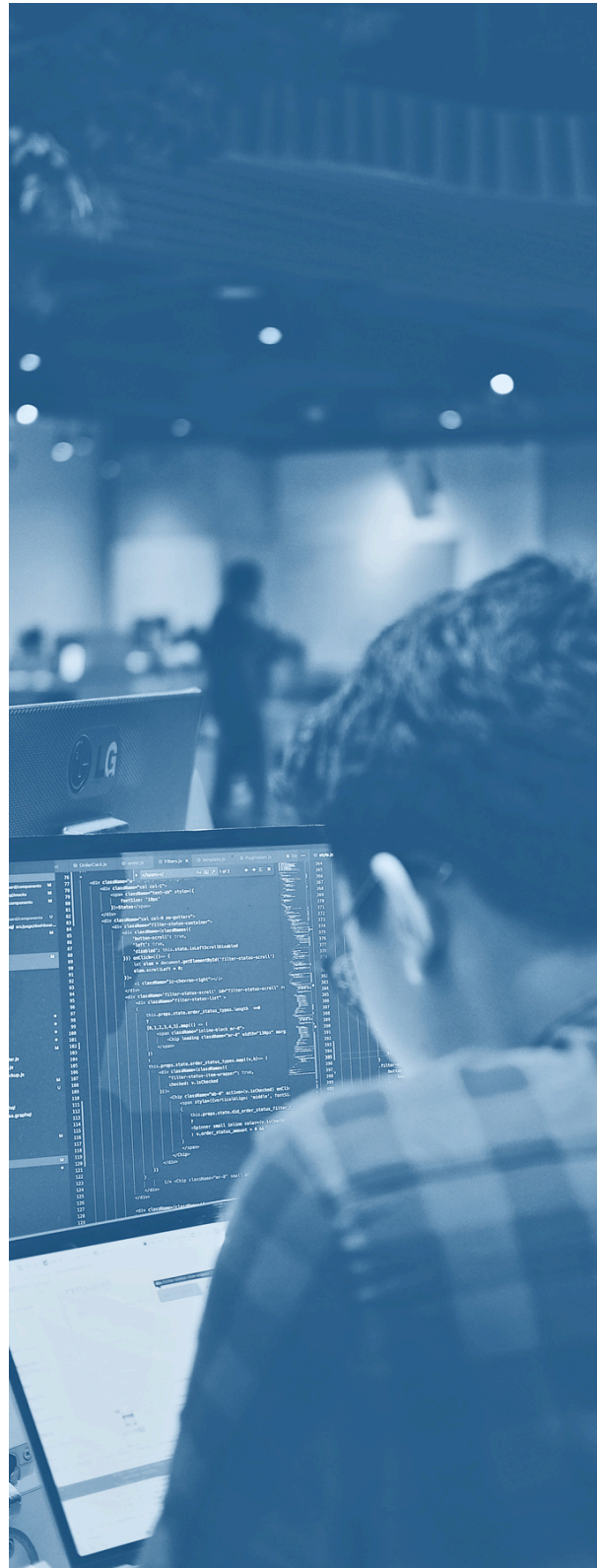
Keep in mind that geopolitical conflicts can result in sudden changes to regulations. Compliance teams must be able to adapt quickly to new export controls, financial embargoes, and trade restrictions. Failing to stay updated on these changes can lead to significant fines, harm to reputation, and disruptions to business operations.

As international tensions escalate, regulators are placing greater emphasis on transparency and accountability. Companies need to demonstrate a strong understanding of their global supply chains to ensure they do not inadvertently violate sanction rules. Implementing thorough due diligence processes is crucial for identifying and mitigating risks associated with cross-border operations.

In response to the heightened compliance demands brought on by geopolitical turbulence, many organizations are turning to technology to streamline their efforts. The use of artificial intelligence (AI) and machine learning (ML) has enabled compliance teams to automate complex tasks, such as transaction monitoring and risk assessments.

These technologies help identify patterns of suspicious behavior more efficiently, allowing organizations to detect and respond to potential violations in real-time.

Blockchain technology, too, has emerged as a potential solution in maintaining transparency and traceability in cross-border transactions. By providing immutable records of financial flows, blockchain can enhance the integrity of compliance systems, ensuring that transactions adhere to evolving regulatory frameworks.



# Disruptive Fraud Schemes



```
export default function Dashboard() {
  const classes = useStyles();
  return (
    <div>
      <GridContainer>
        <GridItem xs={12} sm={6} md={3}>
          <Card>
            <CardHeader color="warning" stats icon>
              <CardIcon color="warning">
                <Icon>content_copy</Icon>
              </CardIcon>
              <p className={classes.cardCategory}>Used Space</p>
              <h3 className={classes.cardTitle}>
                49/50 <small>GB</small>
              </h3>
            </CardHeader>
            <div className={classes.stats}>
              <Danger>
                <Warning />
              </Danger>
            </div>
          </Card>
        </GridItem>
      </GridContainer>
    </div>
  );
}
```

# Disruptive Fraud Schemes

As we wrap up 2024, the fight against fraud has reached a critical juncture. The total global cost of fraud, spanning from direct financial losses to the resource burdens of prevention efforts, has continued to escalate, reaching unprecedented levels. In 2023 alone, global fraud losses amounted to **\$485.6 billion**, reflecting a sharp increase in fraudulent schemes across all sectors and regions.

Financial institutions, consumers, and regulatory bodies have struggled to keep pace with increasingly sophisticated fraud tactics that continue to evolve in response to technological advancements.

Fraud is now one of the most pervasive and damaging economic crimes worldwide, with its impact felt in almost every corner of society. In the UK, fraud accounted for **over 40%** of offenses, making it the most common crime, and in the U.S., **60%** of credit card holders have been victims of fraud.

With the advent of Artificial Intelligence (AI) and Fraud-as-a-Service (FaaS) models, fraudsters have been able to scale their operations, creating more devastating financial disruptions than ever before.

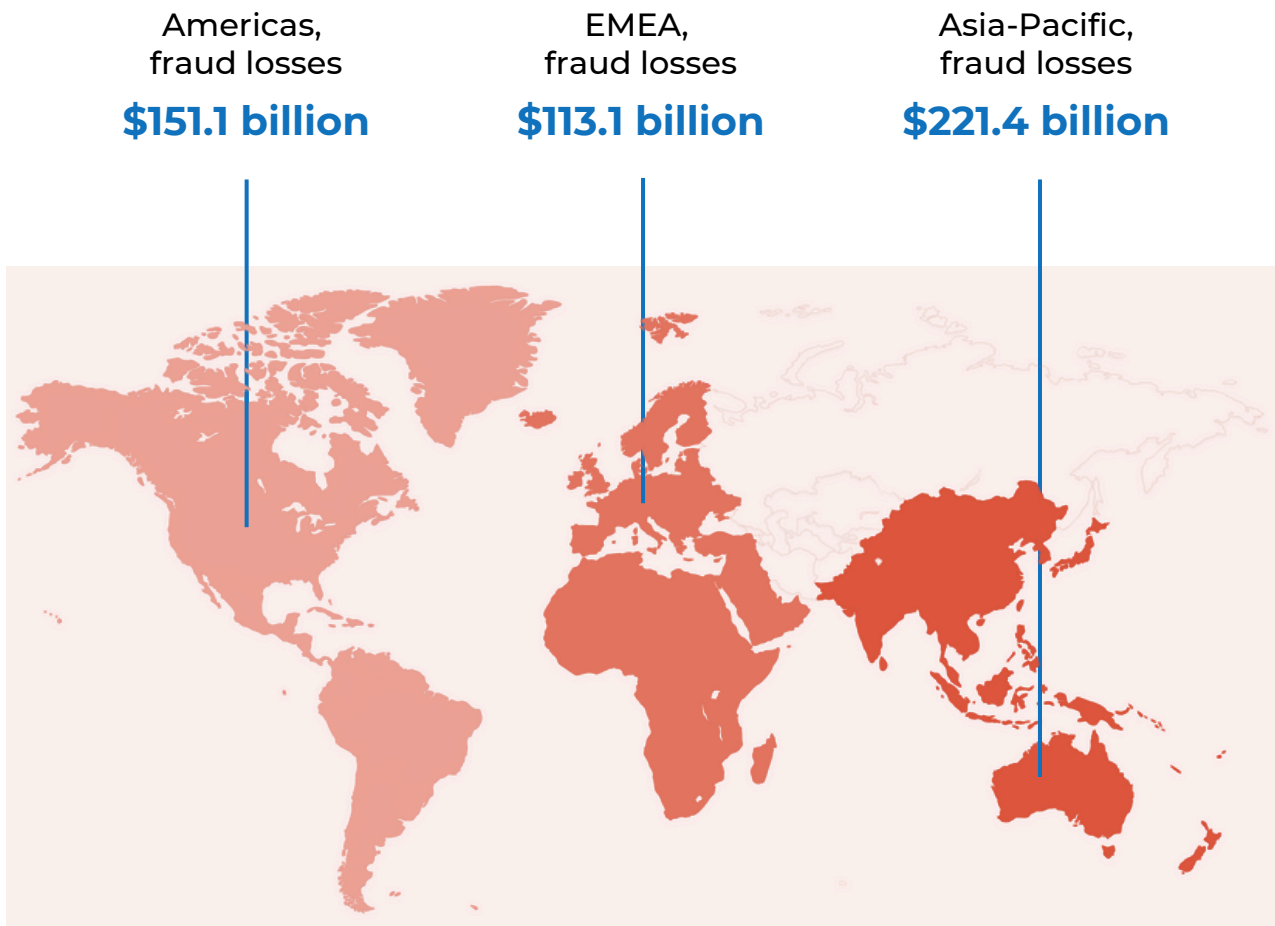


2023 global fraud losses amounted to **\$485.6 billion**

## Fraud Trends

Fraud continues to have an overwhelming impact across global financial systems, with losses in key regions reaching alarming levels. In 2023, a staggering **\$485.6 billion** succumbed to different fraudulent activities, and this pattern persisted in 2024. The Asia-Pacific region emerged as the most affected by fraud, with **\$190.2 billion** in payments fraud alone, making up nearly half of global fraud losses in this category.

In the Americas, fraud losses reached **\$151.1 billion**, driven largely by \$102.6 billion in payments fraud, \$21 billion in check fraud, and \$13.6 billion in credit card fraud. Europe, the Middle East, and Africa (EMEA) also reported significant fraud losses, with the total hitting **\$113.1 billion**, led by \$94 billion in payments fraud and \$8.2 billion in advance fee scams.



This surge in fraudulent activities was fueled by evolving fraud tactics, including cyber-enabled fraud schemes, deepfake technology, and the exploitation of identity verification loopholes. Fraud schemes targeting businesses, consumers, and governments now operate at a scale that challenges even the most advanced fraud detection systems.

## Identity Theft and Synthetic Fraud

Identity theft has become one of the most pervasive fraud types worldwide, with criminals utilizing stolen personal information to carry out a range of fraudulent activities. In the U.S. alone, **52 million** Americans experienced fraudulent charges on their credit or debit cards in 2023, with total unauthorized purchases exceeding **\$5 billion**. The median fraudulent charge rose to **\$100**, a 26% increase from 2021.

However, identity theft is increasingly taking a more insidious form—synthetic identity fraud. This type of fraud, in which criminals create fake identities by combining real and fabricated data, now represents **10-15%** of charge-offs in unsecured lending portfolios, according to The Aite Group. Synthetic identity fraud has been particularly difficult to detect and prevent, as the criminals behind these schemes exploit the weaknesses in identity verification systems across various sectors.

Synthetic identity fraud is estimated to reach **\$23 billion** by 2030

The U.S. has seen a substantial rise in fraud losses due to synthetic identity fraud, which reached **\$8.8 billion** in 2022. As a growing concern, estimates place potential losses at **\$23 billion** by 2030. Financial institutions, fintechs, and other industries reliant on customer verification have had to invest heavily in AI-driven tools and dynamic fraud detection systems to combat these evolving threats.






## Imposter Scams and APP Fraud

Imposter scams have become one of the most devastating and widespread fraud trends, accounting for **\$2.7 billion** in losses in the U.S. alone in 2023. These scams involve fraudsters impersonating well-known businesses, government agencies, or even colleagues to trick individuals into transferring money or divulging sensitive information. Business imposters led to **\$752 million** in reported losses, while government imposters added significantly to the total. These types of fraud have become increasingly common in an interconnected digital world, where criminals leverage social engineering techniques to manipulate victims.

Authorized Push Payment (APP) fraud has become a particularly destructive form of fraud, especially in the UK, where losses reached **£459.7 million** in 2023. APP fraud occurs when victims are tricked into sending money directly to criminals, typically through convincing schemes such as impersonating bank staff or police officers. A significant portion of these losses were due to purchase scams, which accounted for 67% of APP fraud cases. The rise of social media and messaging platforms, particularly Facebook, WhatsApp, and Instagram, has fueled APP scams, with 60% of scams in 2023 originating from these platforms.

While **£287.3 million** of APP losses were returned to victims in 2023, marking 62% of total losses, the persistence of APP scams highlights the ongoing challenge in safeguarding consumers and businesses from these schemes. Efforts by regulators and banks to enhance real-time fraud detection and improve customer awareness have shown some success, but fraudsters continue to adapt their techniques to exploit new vulnerabilities.



In the UK, losses from APP fraud amounted to **£459.7 million**

## Procurement Fraud and Elder Financial Exploitation

Ranked among the top three economic crimes globally, it remains a serious concern for both small enterprises and large corporations. Despite advances in fraud detection, criminals are using technology to manipulate procurement processes, inflating costs, and siphoning funds through fraudulent schemes such as falsified invoices, kickbacks, and collusion between vendors and internal staff.

[A PwC survey](#) revealed that **59%** of companies conducted fraud risk assessments in the past year, yet **nearly 20%** do not use data analytics to detect procurement fraud. This gap leaves many organizations vulnerable to sophisticated fraud schemes, particularly as fraudsters exploit weaknesses in enterprise resource planning (ERP) systems and procure-to-pay processes. SMEs are especially exposed, as they often lack the advanced fraud detection systems of larger companies, making them prime targets for procurement fraud, which costs them millions each year.

In 2024, the use of shell companies and fake third-party suppliers increased, allowing fraudsters to create fraudulent suppliers that bill businesses for non-existent services or goods. Internal employees have also been complicit in some cases, establishing these shell companies to divert funds.

To combat procurement fraud, more companies are turning to machine learning and data analytics, allowing for real-time monitoring and the detection of suspicious transactions. Whistleblower programs and internal audits have also proven crucial in uncovering fraudulent activities.

## Contactless and Instant Payments Fraud

As the adoption of contactless and instant payments surged in 2024, fraudsters took full advantage of these rapidly growing payment methods. By the end of 2024, **over 1 billion** people were using contactless mobile payments, up from **782 million** in 2022. This widespread adoption of near-field communication (NFC) technology in smartphones, digital wallets, and wearable devices like ApplePay and GooglePay facilitated seamless transactions but also created lucrative opportunities for fraud





Losses from  
contactless fraud  
reached  
**£100.2 million**

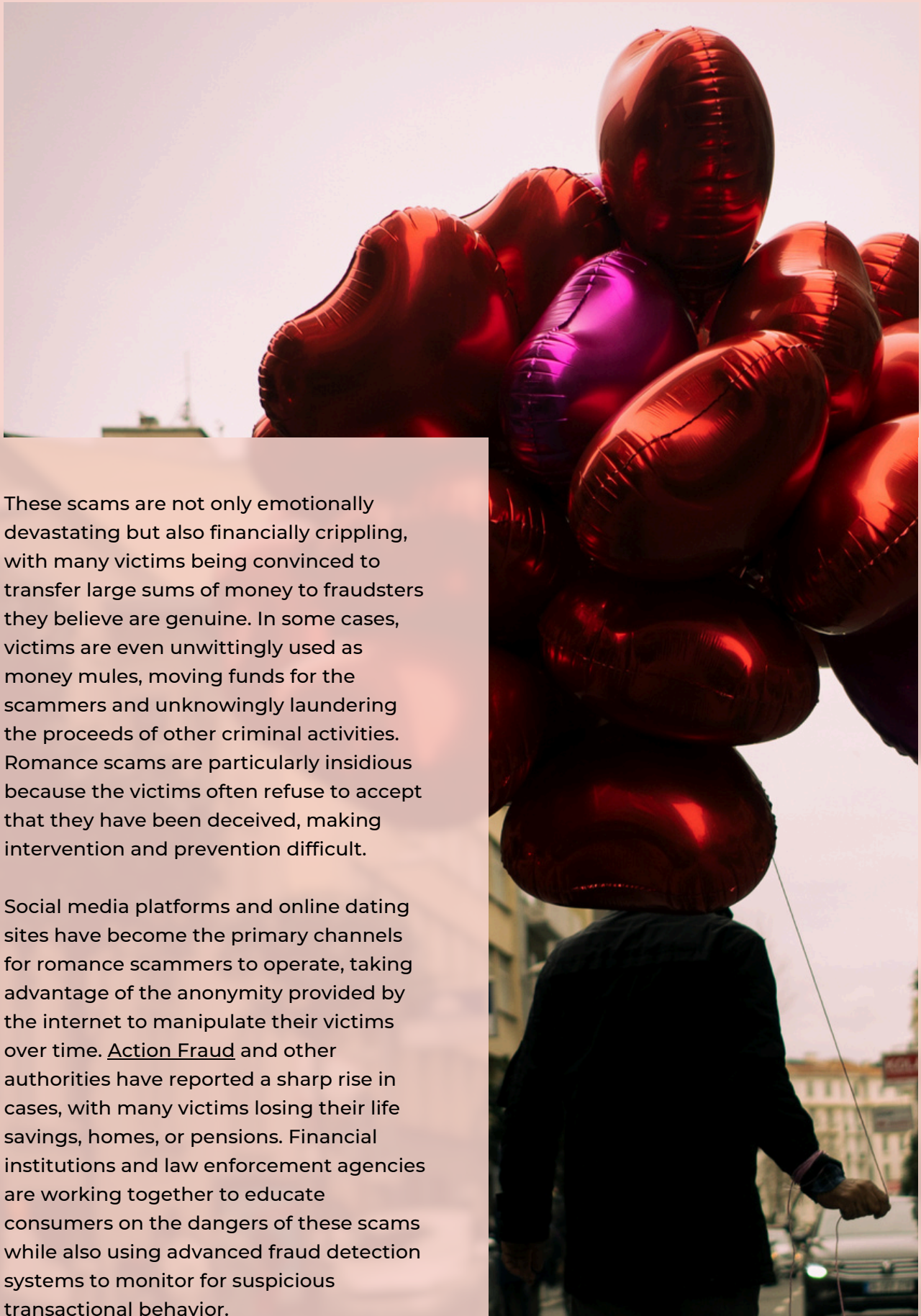
In the UK, contactless fraud surged by **82% in 2023**, and losses related to stolen or lost cards reached **£100.2 million**. With instant payments, such as ACH transfers, crypto payments, and digital wallets becoming increasingly common, the risk of fraud rises. Instant payments accounted for a **45%** share of the total credit transfer volume in the SEPA region, reflecting their growing role in the financial ecosystem. However, the speed of these transactions leaves little time for banks and financial institutions to block or reverse fraudulent transfers, making them particularly attractive to scammers.

Criminals exploit these systems through various tactics, including APP fraud, where victims are tricked into sending money to accounts controlled by fraudsters. As real-time payments become more prevalent, banks are investing in enhanced fraud detection systems that can analyze transactional patterns and flag anomalies in real-time. However, the rapid rise of these payment methods continues to pose significant challenges.

## Romance Scams and Confidence Schemes

Romance scams and other confidence schemes have shown significant growth over the past year, with victims worldwide being manipulated by fraudsters posing as romantic partners, friends, or trusted individuals. In 2023, **\$3.8 billion** was lost globally to romance scams, representing one of the fastest-growing types of fraud. Confidence schemes, which include a wide range of scams based on trust, prey on vulnerable individuals, particularly those isolated or seeking companionship.

In 2023  
**\$3.8 billion**  
was lost globally to  
romance scams



These scams are not only emotionally devastating but also financially crippling, with many victims being convinced to transfer large sums of money to fraudsters they believe are genuine. In some cases, victims are even unwittingly used as money mules, moving funds for the scammers and unknowingly laundering the proceeds of other criminal activities. Romance scams are particularly insidious because the victims often refuse to accept that they have been deceived, making intervention and prevention difficult.

Social media platforms and online dating sites have become the primary channels for romance scammers to operate, taking advantage of the anonymity provided by the internet to manipulate their victims over time. [Action Fraud](#) and other authorities have reported a sharp rise in cases, with many victims losing their life savings, homes, or pensions. Financial institutions and law enforcement agencies are working together to educate consumers on the dangers of these scams while also using advanced fraud detection systems to monitor for suspicious transactional behavior.

## Elder Financial Exploitation and Vulnerable Victim Fraud

Fraudsters are increasingly targeting elderly and vulnerable individuals, exploiting their limited familiarity with modern technology and financial systems. [Elder financial exploitation \(EFE\)](#) saw a dramatic rise in 2023, with total losses reaching **\$77.7 billion**. Seniors are frequently targeted with scams involving impersonation, fear tactics, and social engineering, such as the grandparent scheme, in which a fraudster impersonates a victim's grandchild and requests urgent financial assistance for a fake crisis.

The National Crime Agency reported that 1 in 10 elderly people in the UK were victims of financial exploitation in 2023, yet for every known case of elder abuse, 23 cases go unreported. Elderly victims often avoid reporting these crimes due to embarrassment, fear of losing their independence, or a desire to simply forget the traumatic experience. This underreporting makes it challenging for authorities to fully grasp the extent of the problem.

Elder financial exploitation is not limited to one type of fraud. Scammers employ various schemes, including impersonation fraud, identity theft, and romance scams, to convince elderly victims to part with their money. Financial institutions play a critical role in protecting seniors from these types of fraud by monitoring for suspicious activities, providing educational resources, and working closely with law enforcement to detect and prevent exploitation before significant financial harm occurs.

**1 in 10  
elderly  
people  
were victims  
of financial  
exploitation**





## High-Tech Scams: From AI to Deepfakes

In 2024, the use of deepfakes in financial fraud has evolved into a serious and widespread issue, no longer a futuristic concept but a growing reality that poses immense risks to institutions and individuals. One of the most striking examples comes from Hong Kong, where a finance worker transferred [\\$39 million](#), believing they were on a legitimate video call with their CFO and colleagues. In reality, the entire meeting was orchestrated by fraudsters using deepfake technology to impersonate trusted executives. This incident showcases how deepfake scams have moved beyond theoretical discussions into real-world operations, wreaking havoc in the financial sector.

The implications of deepfake technology extend beyond financial loss. These AI-generated manipulations are also being used to spread false information, damage reputations, and erode trust in digital

communication. With the increasing sophistication of AI tools, scammers can now convincingly mimic voices, craft highly realistic fake videos, and send fraudulent emails that seem entirely legitimate, making it incredibly difficult for recipients to identify malicious activities.

One of the most vulnerable sectors to this new wave of fraud is cryptocurrency, which accounted for a staggering **88%** of all deepfake-related fraud cases detected in 2023. The digital and decentralized nature of the crypto industry makes it an attractive target for advanced fraud techniques, with criminals exploiting the high financial stakes and digital anonymity to perpetrate large-scale scams. Deepfake attacks on crypto transactions are often highly sophisticated, using AI to create convincing fake identities or impersonate trusted figures within the organization.

The financial technology (FinTech) industry is also grappling with the rise of deepfake scams. Incidents involving deepfakes in fintech surged by **700%** in 2023, reflecting the rapid adoption of generative AI by cybercriminals to facilitate fraudulent activities. These AI-powered scams are particularly dangerous because they often bypass traditional security measures. In a trend that mirrors the broader financial sector, deepfake face swap attacks on identity verification systems increased by **704%** last year, as fraudsters used virtual cameras and AI-generated "face swaps" to circumvent remote verification processes.

Despite the rapid escalation of these fraud techniques, a significant portion of business leaders remain unprepared for this threat. In fact, nearly one in four executives had little to no familiarity with deepfake technology by the end of 2024, leaving their organizations exposed to potential risks. As these AI-driven scams grow in complexity and frequency, experts predict that fraud losses facilitated by generative AI technologies will escalate to **\$40 billion** in the United States alone by 2027, up from **\$12.3 billion** in 2023.

The rise of deepfake scams signals an urgent need for financial institutions to bolster their defenses. In this landscape, it is crucial for finance leaders to stay ahead by regularly reviewing security protocols, training staff to recognize suspicious requests, and investing in advanced anti-deepfake technologies that can detect and neutralize fraudulent activities before significant damage occurs.

Deepfake cases  
in the FinTech  
sector increased  
by **700%**



Institutions must recalibrate their fraud detection systems by incorporating AI-powered anomaly detection and behavioral biometrics to tackle AI-based scams. Real-time transaction monitoring, combined with advanced machine learning models, can flag suspicious patterns that deviate from normal user behavior. Human oversight remains critical to validate flagged cases, especially in high-stakes situations, ensuring a layered defense against the evolving threat of deepfakes.



**Baptiste Forestier**  
Head of Compliance

## Sector-Specific Fraud Tactics

In 2024, various industries faced tailored fraud tactics, each exploiting unique vulnerabilities to perpetrate financial crimes. From finance and banking to retail and real estate, fraudsters have honed sector-specific techniques that exploit industry-specific processes and weaknesses.

### Financial Services

The financial services sector remains a top target for fraud due to the significant sums of money processed daily. One prominent threat is synthetic identity fraud, which accounted for **10-15%** of charge-offs in unsecured lending portfolios. This type of fraud, where criminals combine real and fake information to create new identities, continues to plague banks and lenders. Identity theft losses in the U.S. totaled nearly **\$8.8 billion** in 2022, and this number is expected to rise significantly in the coming years as synthetic identity fraud becomes even more prevalent. Account takeover (ATO) fraud is another major issue, with a **61%** increase in fraud attempts from consumer accounts being reported across the fintech and banking industries in 2023.

The increasing popularity of instant payments has added complexity to the financial landscape. While faster transaction methods like ACH, digital wallets, and real-time payments offer convenience, they also open up new opportunities for fraud. Real-time payments make it extremely difficult to reverse fraudulent transactions once they are initiated, putting financial institutions in a tough spot as they try to prevent or recover lost funds. One example of this is APP fraud, which saw a 12% increase in cases and resulted in losses of **£459.7 million** in 2023. This type of fraud often involves scammers deceiving victims into sending money directly to them by pretending to be legitimate contacts or companies, and it disproportionately impacts individuals and small businesses.





## Retail and E-Commerce

In the retail sector, particularly e-commerce, fraud has exploded as online shopping continues to grow. With over a quarter of UK retail sales taking place online in March 2023, fraudsters have ramped up their efforts to exploit weaknesses in online transactions. Card-not-present (CNP) fraud remains one of the most common schemes, where criminals use stolen credit card details to make purchases online.

The high volume of digital transactions during events like Black Friday or holiday shopping seasons exacerbates this issue, allowing fraudsters to hide their activities among the millions of legitimate transactions.

Another growing concern is parcel delivery scams, where fraudsters pose as delivery companies and ask customers to pay additional fees or reschedule deliveries. This tactic preyed on nearly **40 million UK adults** in the first quarter of 2023 alone, and the problem is expected to worsen as online shopping continues to rise. Ticket scams are also rampant, particularly surrounding high-demand events such as concerts and sporting matches. In the past year, fraudulent Premier League ticket sales alone cost UK victims **£40,000**, with criminals using social media platforms like Facebook Marketplace to target unsuspecting fans.

In conclusion, the increase in e-commerce fraud demands vigilance from both consumers and retailers. Consumers should watch for signs of fraud, use strong passwords, and shop only on trusted sites. Retailers must proactively protect customer information, detect fraud, and promote secure payment methods.

On the financial institution's side, we often see incidents that take advantage of consumers' low financial and technological literacy, ranking high among the types of fraud frequently encountered. Fraud cases carried out with social engineering due to underdeveloped financial literacy and lack of technological awareness parallel to the frequency of social media use are also at the top of the most striking fraud cases in 2024.

Especially due to the development of e-commerce and the increase in people's shopping culture through applications, IBAN fraud based on intimidation through the names of the prosecutor's office, police, or public institutions developed both on social media and the internet, is quite common with stolen accounts and stolen cards.

Another common issue is the unconscious real or legal persons who want to make money easily but cannot calculate exactly how they will be dragged into a legal case and who allow qualified fraudsters to use their accounts. These people either use their cards in POS fraud, POS fraud, etc. or become tools for the transactions of qualified fraudsters or money launderers and money launderers in irregular transactions made through their POS by gambling and betting intermediaries as a member business.



**Tuba Erdem**  
Director of Compliance  
& Internal Control

In 2023,  
**1 in 8 rental applications**  
were found to contain some form of fraud, which poses a higher risk of eviction and claims for property managers.



## Real Estate and Property Management

In the real estate sector, rental application fraud has seen a sharp increase. Fraudsters are exploiting digital systems to forge documents, with altered bank statements and pay stubs becoming more sophisticated. In 2023, 1 in 8 rental applications contained some form of fraud, leading to higher risks of eviction and bad debt for property managers. Rental fraud is also particularly prevalent in the luxury property market, where fake documents can pass undetected, causing significant financial loss for property owners.

In the broader property market, title fraud is an emerging threat. Criminals use stolen identities to change property ownership records and secure loans or sell properties they do not own. The increase in remote transactions during the pandemic has amplified this issue, and recovery from title fraud can be costly and time-consuming for victims.

## Healthcare and Insurance

The healthcare industry continues to grapple with insurance fraud, a problem exacerbated by rising medical costs and complex billing processes. In 2022, fraudulent insurance claims totaled **£1.1 billion**, with motor insurance fraud being the most prevalent. Fraudsters often exaggerate claims or submit entirely fictitious incidents to defraud insurance companies, driving up premiums for consumers.

Medical identity theft is also becoming a pressing issue in healthcare, where fraudsters use stolen identities to access medical services or obtain prescription drugs. The impact of this type of fraud is not just financial; it can lead to inaccurate medical records and compromised patient care. As healthcare providers continue to digitalize their services, the need for robust fraud prevention systems becomes more urgent.

**£1.1 billion**  
of fraudulent  
insurance claims  
recorded



## Technology and Telecommunications

The telecommunications industry faces a surge in toll fraud as the adoption of cloud communications increases. Fraudsters exploit vulnerabilities in phone systems, making unauthorized international calls to premium-rate numbers, generating billions in illicit gains. Toll fraud is particularly rampant in businesses that rely heavily on Voice over Internet Protocol (VoIP) systems, as these technologies often lack the security needed to prevent such attacks. In fact, toll fraud is one of the leading types of fraud in the telecommunications sector, with losses expected to grow as VoIP adoption increases globally.

The tech industry also struggles with Artificial Inflation of Traffic (AIT) fraud in Application-to-Person (A2P) messaging. Fraudsters generate large volumes of fake traffic to inflate enterprise costs, causing significant financial strain on businesses relying on A2P for customer communications, including two-factor authentication (2FA). As SMS-based 2FA remains a popular security measure, AIT fraud presents a growing concern for businesses across multiple sectors.



# **The Technological Vanguard in Financial Crime Prevention**



# The Technological Vanguard in Financial Crime Prevention

In 2024, the financial world found itself during a technological transformation, with cutting-edge advancements playing a critical role in preventing fraud, money laundering, terrorist financing, and other financial crimes. As criminal organizations grow more sophisticated in exploiting new technologies for illicit purposes, financial institutions have continuously evolved to safeguard their operations. The integration of AI, blockchain, robotic process automation (RPA), and other technologies has fundamentally reshaped how financial institutions detect, prevent, and respond to financial crime.

**Artificial intelligence (AI) and machine learning (ML)** have become the cornerstones of modern financial crime prevention. No longer confined to experimental stages, these technologies have taken center stage in fighting fraud, money laundering, and terrorist financing. AI's capacity to analyze vast amounts of data in real-time allows institutions to flag suspicious activities almost instantaneously. In 2024, AI-driven monitoring systems now offer enhanced precision in identifying unusual transactions by learning from historical data and detecting patterns that humans might miss.

Through the analysis of extensive transaction data, AI can detect shifts in customer behavior that could signal potential money laundering. This encompasses the identification of unanticipated substantial transfers as well as the recognition of irregularities in international payments.

Moreover, machine learning algorithms can be trained to improve continuously, adapting to new criminal tactics and ensuring financial institutions remain a step ahead of criminals.

AI's role is not limited to AML—CTF is another area where its potential is being harnessed. AI models, integrated with geopolitical data and social intelligence, are proving vital in identifying small yet suspicious financial transactions linked to terrorist networks.



Blockchain analytics tools, AI-driven KYC/AML systems, and quantum computing hold the most promise for combating financial crime. Blockchain allows for enhanced transparency and traceability of transactions, while AI can process vast amounts of data to detect fraudulent patterns. Quantum computing, though still emerging, could revolutionize encryption and decryption methods, strengthening security frameworks across the financial sector. Embracing these technologies will be key to staying ahead in the fight against financial crime.

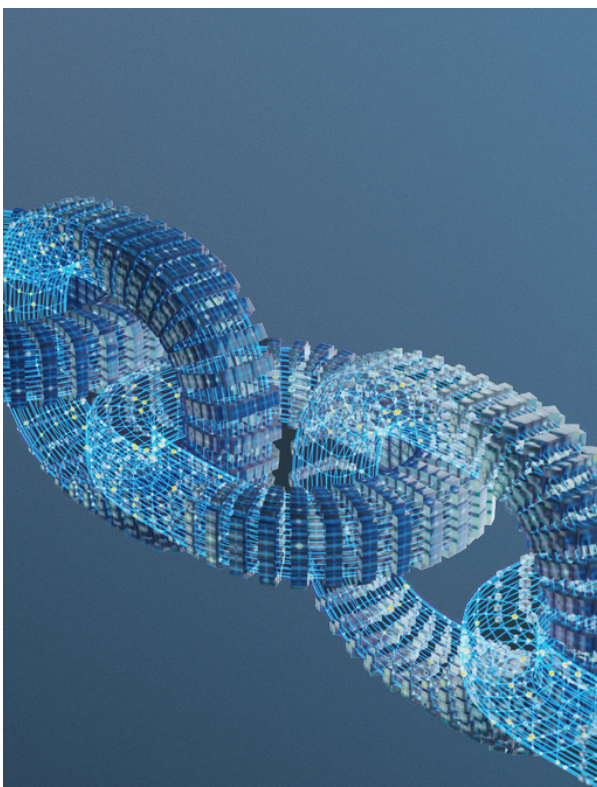


**Baptiste Forestier**  
Head of Compliance

Beyond just detection, AI is being used to optimize compliance processes, reducing operational burdens on institutions. AI-driven automation is employed in performing KYC procedures, using biometric verification and AI-powered identity checks to screen customers in real-time, ensuring that onboarding processes remain compliant while reducing friction for legitimate users.

**Blockchain**, initially known for its role in cryptocurrencies, has evolved into a powerful tool in financial crime prevention. In 2024, blockchain's decentralized and immutable nature is being leveraged to enhance transparency across financial systems, particularly ensuring compliance with KYC and AML regulations. Financial institutions are using blockchain to share verified KYC data across borders securely, which not only streamlines compliance but also ensures that criminals can no longer exploit fragmented regulatory frameworks in different jurisdictions.

Furthermore, blockchain technology allows for real-time tracking of transactions, making it significantly harder for criminals to launder money or hide their financial activities. Smart contracts are being deployed in international trade, automatically executing AML checks when certain financial thresholds are reached, reducing human intervention and the possibility of error. The potential of blockchain extends beyond AML and KYC, as it is now being applied in cross-border payment systems to increase transparency and reduce the risk of fraud.





**Open-source intelligence (OSINT)** is also playing an expanding role in financial crime prevention. By leveraging publicly available information, OSINT enables financial institutions to enhance their due diligence processes and enrich their understanding of global crime networks. More institutions are turning to OSINT to monitor the dark web and social media for illicit activity, providing critical intelligence on potential threats such as fraudulent schemes, terrorist financing, and money laundering efforts. OSINT's ability to detect early warning signs from external sources has enabled institutions to act quickly, preventing losses before they materialize.

**Robotic process automation (RPA)**, while not as headline-grabbing as AI or blockchain, plays a critical role in streamlining compliance tasks. RPA's ability to automate repetitive tasks such as transaction monitoring, risk assessments, and customer due diligence allows

financial institutions to manage the growing complexity of compliance requirements more efficiently. Globally, financial institutions have adopted RPA to speed up processes and reduce the cost of compliance, ensuring that suspicious activity reports are filed promptly and accurately. The automation of these tasks not only cuts down on human error but also allows compliance teams to focus on more strategic, high-priority investigations.

Meanwhile, **intelligent automation (IA)**—a blend of RPA and AI—continues to streamline compliance processes. In 2024, IA is being used to automate routine tasks like transaction monitoring, KYC procedures, and customer due diligence. As fraud attempts become more complex, IA helps to manage the growing volumes of compliance data, reducing the operational burden on institutions and freeing up human resources for more strategic, high-priority investigations.

## Quantum computing is emerging as a potential game changer in the prevention of financial crime.

While **cloud computing** has long been a driver of digital transformation, its role in financial crime prevention is growing. In 2024, financial institutions are increasingly using cloud-based platforms to enable real-time collaboration and data sharing between global entities. This level of interconnectedness allows institutions to respond quickly to emerging threats and share intelligence more efficiently. Cloud platforms are also providing enhanced security features like end-to-end encryption and advanced threat detection, ensuring that sensitive financial data is protected from cyberattacks, which have become increasingly common as financial crimes move into the digital realm. Cloud computing enables real-time data sharing, giving institutions the power to collaborate seamlessly on financial crime prevention while maintaining data privacy through privacy-enhancing technologies (PETs).

Looking toward the future, **quantum computing** is emerging as a potential game-changer in financial crime prevention. Although still in its infancy, pilot programs in 2024 are exploring the use of quantum algorithms to process and analyze vast datasets at unprecedented speeds. In theory, quantum computing could revolutionize transaction monitoring by enabling institutions to detect suspicious activities in real-time across even the most complex global financial networks. Additionally, quantum-resistant cryptography is beginning to emerge as a necessary defense against future cyber threats, ensuring that financial institutions remain secure even as quantum computing matures.






Moreover, **biometric authentication technologies**, such as facial recognition and fingerprint scanning, are becoming widely adopted in 2024 to prevent unauthorized access to sensitive financial systems. These technologies are particularly valuable in preventing identity theft and account takeovers, two prevalent forms of financial crime that have surged in recent years. By integrating biometric data into customer verification processes, financial institutions can ensure that the person initiating a transaction is, in fact, the rightful account holder.

As we look ahead to 2025, it is clear that the financial crime prevention landscape will continue to be shaped by technology. However, with the increasing reliance on digital platforms comes the heightened risk of cybercrime, requiring institutions to adopt even more advanced security measures. The evolution of these technologies, from AI-driven fraud detection to blockchain-enabled transparency, will be instrumental in shaping the future of compliance. Financial institutions that leverage these innovations will be better equipped to meet the growing complexity of financial crimes and ensure the integrity of the global financial system.

In conclusion, technology is no longer an optional tool but necessary in the ongoing battle against financial crime. The innovations of 2024 have shown that AI, blockchain, RPA, and other emerging technologies are not only effective in preventing fraud, money laundering, and terrorist financing but also in transforming the entire compliance framework.





**Cryptocurrency and Beyond:  
The New Frontier of  
Financial Crime**

# Cryptocurrency and Beyond: The New Frontier of Financial Crime

The intersection of cryptocurrency and financial crime continues to evolve rapidly. The digital asset realm is still a dynamic frontier where both innovation and exploitation are present. While cryptocurrencies promise significant advancements in decentralized finance (DeFi), NFTs, and cross-border transactions, they also present substantial regulatory and compliance challenges.

As of April 2024, there are **13,656** available cryptocurrencies, with Bitcoin alone commanding a market cap of over **\$1.3 trillion** and a 24-hour trading volume of **\$116.61 billion**. While the benefits of digital currencies are substantial, the scope of illicit activity within this ecosystem is equally vast. High-profile scandals, evolving regulatory frameworks, and the ever-growing sophistication of fraud tactics demonstrate that combating financial crime in the digital asset ecosystem requires forward-thinking, multi-faceted solutions.

## Crypto Crime

In 2024, crypto crime continues to grow in sophistication, with criminals leveraging the decentralized and pseudonymous nature of blockchain to evade detection. While digital assets like Bitcoin, Ethereum, and other cryptocurrencies offer transparency through public ledgers, they are also exploited by criminals to commit various financial crimes, from money laundering and fraud to ransomware attacks and illicit trading.

As of 2024,  
there are  
**13,656** available  
cryptocurrencies



## Rising Crypto Crime Trends

The latest [Crypto Crime Report](#) underscores the escalating scale of criminal activity within the crypto space, revealing that **\$20 billion** in illicit transactions occurred in 2023, marking a 40% increase from the previous year. Criminals have become adept at exploiting vulnerabilities in decentralized finance (DeFi) platforms and other blockchain-based systems. In particular, DeFi hacks and exploits have been a primary driver of these rising numbers, with over **\$9 billion** laundered through decentralized exchanges in 2023 alone. These platforms offer anonymity and operate without intermediaries, making them fertile ground for money laundering and other illicit activities.

One of the fastest-growing areas of crypto crime in 2024 is the use of ransomware. Criminal groups increasingly demand ransom payments in Bitcoin and other cryptocurrencies to avoid detection and prosecution. According to recent reports, ransomware payments in crypto surged to **\$1.4 billion** globally, with hackers targeting critical sectors like healthcare, finance, and government infrastructure. Moreover, criminals are leveraging privacy coins such as Monero and Zcash, which obscure transaction histories and make it even more difficult for regulators to trace illicit funds.

In addition, crypto ATMs have emerged as a significant weak spot in AML frameworks. Criminals are using these ATMs to convert fiat currencies into cryptocurrencies without proper identification checks. By 2024, there are **over 40,000** crypto ATMs operating worldwide, many of which have been flagged for suspicious activities. Law enforcement agencies have reported that **up to 70%** of transactions at these ATMs are linked to criminal activities, including drug trafficking and money laundering.



In the crypto sector, **\$20 billion** worth of illegal transactions occurred in 2023.

## Fraud and Scams in the Crypto Space

Fraud in the cryptocurrency market has also reached alarming levels in 2024. While [57%](#) of crypto investors have made money, 14% report losses and only 7% feel they made significant profits. This disparity has led to a proliferation of scams aimed at both new and seasoned investors.

Ponzi schemes, phishing attacks, and rug pulls (where developers disappear after raising funds) are common tactics used by fraudsters. In 2023, victims of these scams lost approximately **\$3.6 billion**, a number expected to rise in 2024 as new scams emerge, including sophisticated deepfake attacks targeting investors through fake video and audio impersonations.

APP fraud is another growing threat in the crypto ecosystem. In this scam, fraudsters deceive victims into transferring large sums of cryptocurrency to accounts under their control, often through BEC attacks. The deception is simple yet effective: the scammer impersonates a legitimate business or payee, convincing the victim to make payments that are difficult to reverse due to the immutable nature of blockchain transactions. Losses from APP fraud reached \$6.7 billion globally in 2023, a figure that could rise as criminals become more adept at exploiting these techniques.

In 2023, victims of these scams lost approximately **\$3.6 billion**





## Terrorism Financing and Dark Web Markets

Terrorist organizations are increasingly turning to cryptocurrencies to finance their operations, taking advantage of the borderless nature of digital currencies. In 2024, **over \$100 million** in crypto transactions were linked to terrorist financing, according to intelligence reports. These transactions often involve smaller, incremental payments designed to avoid detection by blockchain analytics tools.

Moreover, the rise of dark web markets has facilitated the sale of weapons, drugs, and illicit services in exchange for cryptocurrency, further complicating efforts to curb these activities. In 2023 alone, dark web transactions accounted for **over \$1.2 billion** in illicit crypto transactions.

## The Role of Blockchain Analytics

Despite the growing complexity of crypto crime, law enforcement agencies and financial institutions have made significant strides in using blockchain analytics and OSINT to trace and recover stolen funds. These tools allow investigators to follow the flow of cryptocurrency across multiple wallets and platforms, identifying key players in criminal operations. In 2024, the use of these technologies helped recover **over \$1.2 billion** in stolen assets, a critical win for the industry. Companies like Sanction Scanner are at the forefront of these efforts, developing sophisticated tools that provide real-time tracking of illicit transactions.

However, while blockchain analytics can identify suspicious activity, regulatory gaps remain a significant challenge. The global adoption rate of cryptocurrency is at **4.2%**, with over 420 million users worldwide. As adoption continues to grow, so does the need for comprehensive regulatory frameworks to address the unique risks posed by digital assets. Many countries have yet to implement robust KYC and AML regulations for decentralized platforms, creating opportunities for criminals to operate with relative impunity.

## Regulatory Responses to Digital Assets

As the cryptocurrency market continues its rapid expansion, with a global adoption rate of **4.2%** as of 2024, regulators around the world are scrambling to keep pace with the new challenges posed by digital assets. In 2024, Bitcoin remains the dominant player in the market, with a staggering market cap of **\$1.3 trillion**, while DeFi and NFTs also maintain significant growth. Yet, the rise of these digital innovations has also exposed vulnerabilities that threaten the integrity of global financial systems, spurring a wave of regulatory responses.



### The U.S. and Global Frameworks

The U.S. government, under the Biden administration, has taken a leading role in responding to the rise of cryptocurrency. In early 2024, the U.S. Securities and Exchange Commission (SEC) introduced updated guidelines aimed at enhancing transparency and reducing fraud in digital asset markets. The SEC has classified several cryptocurrencies, particularly tokens used in initial coin offerings (ICOs), as securities, subjecting them to the same regulations as traditional financial instruments. This move aims to curb the growing instances of Ponzi schemes and fraudulent investment projects within the crypto sector.

In tandem, the Commodity Futures Trading Commission (CFTC) has ramped up

its oversight of crypto derivatives trading platforms, ensuring that exchanges comply with existing financial regulations.

Meanwhile, the FinCEN has placed stricter AML requirements on crypto exchanges and wallet providers, mandating more rigorous KYC procedures. As of 2024, FinCEN's rules require exchanges to report any transactions over \$10,000 and impose heavy fines for non-compliance.

Globally, the FATF has continued to shape its "Travel Rule" mandate, which requires virtual asset service providers (VASPs) to collect and share information about the identities of participants in crypto transactions above a certain threshold. In 2024, over 50 countries have either fully implemented or are in the process of adopting this rule to strengthen global cooperation in tracking illicit cryptocurrency flows.

A stack of gold Bitcoin coins is placed on top of Euro banknotes. The top coin is clearly visible, showing the Bitcoin symbol and the words 'BITCOIN DIGITAL DECENTRALIZED PEER TO PEER'. The banknotes below are Euro notes, with the number '50' and the word 'EURO' visible. The background is a soft-focus image of more Euro banknotes.

In the EU in 2023,  
stablecoin  
transactions totaled  
**500 billion  
dollars**

## The EU's MiCA and Other Global Initiatives

In Europe, the Markets in Crypto-Assets (MiCA) regulation stands as one of the most comprehensive regulatory frameworks for digital assets. Approved in 2023 and set for full implementation by mid-2024, MiCA aims to create a unified legal framework for crypto assets across the European Union. Its provisions include transparency requirements for crypto issuers, capital requirements for stablecoins, and consumer protection measures. MiCA also provides clear definitions of different types of crypto assets, thereby reducing regulatory uncertainty for businesses operating in the sector.

One of the significant impacts of MiCA will be its focus on stablecoins, given their increasing use for cross-border payments and remittances. The regulation will ensure that stablecoin issuers maintain sufficient reserves and adhere to stringent operational and transparency standards. This is a timely measure, considering that \$500 billion in stablecoin transactions occurred in the EU alone in 2023, a number projected to rise sharply in 2024.

Elsewhere, Singapore has become a leading example of how to create a forward-looking regulatory environment for digital assets. The Monetary Authority of Singapore (MAS) introduced new rules in 2024 that not only enhance AML/CFT measures but also encourage innovation within the blockchain and crypto industries. This delicate balance has attracted numerous crypto startups to Singapore, further cementing its role as a global hub for blockchain technology.



## Regulation in the DeFi Space

Decentralized Finance (DeFi), a burgeoning sector with a projected Total Value Locked (TVL) of \$26.1 billion in 2024, presents unique regulatory challenges. By design, DeFi platforms operate without intermediaries, relying instead on automated smart contracts to facilitate transactions. This raises questions about how regulatory authorities can enforce compliance when there is no central authority to hold them accountable.

To address these concerns, several regulatory bodies, including the European Banking Authority (EBA), are exploring ways to incorporate DeFi into existing frameworks. Proposals include requiring DeFi platforms to implement programmable compliance, whereby smart contracts automatically enforce KYC and AML rules before processing transactions. While still in the early stages, such measures could help mitigate the risk of DeFi platforms being used for illicit activities such as money laundering and terrorist financing.



DeFi, a burgeoning sector with a projected TVL of **\$26.1 billion**

## Global Coordination and Crypto Regulation

The global nature of cryptocurrencies demands coordinated efforts from regulators across different jurisdictions. In 2024, the International Monetary Fund (IMF) and the World Bank launched a joint initiative to create a standardized regulatory framework for digital assets, particularly focused on emerging markets. These regions have seen a surge in crypto adoption, with countries like Nigeria and El Salvador embracing Bitcoin as a legal tender or a major part of their financial systems. However, the lack of cohesive regulation in these regions has also made them more susceptible to crypto crime.

To promote transparency, both the IMF and World Bank are advocating for the implementation of real-time transaction monitoring systems that can track and trace large crypto transactions across borders. These efforts aim to prevent large-scale money laundering schemes and curb the flow of illicit funds through cryptocurrencies.



# **Spotlight on Industry-Specific Financial Crime**

# Spotlight on Industry-Specific Financial Crime

Industry-specific financial crimes continue to challenge global markets, with each sector facing its own vulnerabilities and evolving threats. While some industries have adapted to the growing sophistication of financial criminals, others are still lagging in implementing the robust measures necessary to protect their financial ecosystems.

## Financial Services

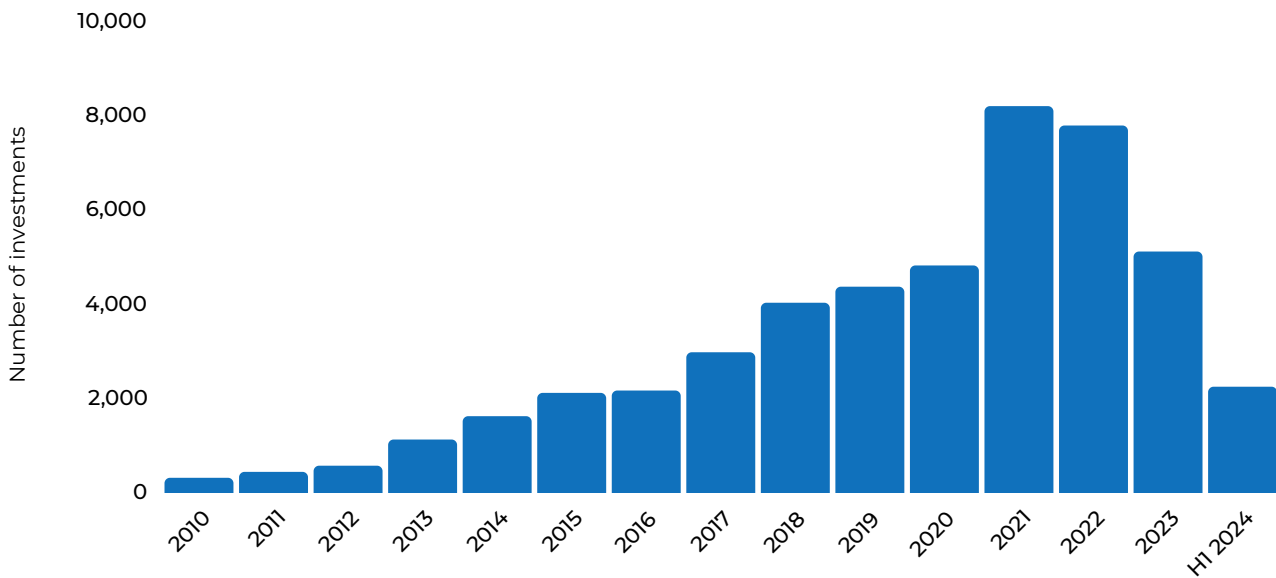
The financial services sector, with over **30,000 fintechs** globally in 2024, faces rising challenges from both traditional fraud and emerging threats in the digital banking space. Online banks are gaining popularity, especially in Europe, where the highest number of challenger banks operate, while regions like Africa lag behind. This shift to digital banking, combined with increasing customer reliance on mobile banking and digital wallets, has introduced new fraud risks.

One of the most concerning trends is the rise of synthetic identity fraud, where fraudsters create fake identities using a mix of stolen and false information. In 2024, this type of fraud represented 10-15% of charge-offs in U.S. unsecured lending portfolios. Likewise, account takeover fraud, fueled by phishing attacks and data breaches, has surged, with global losses expected to surpass **\$25 billion** this year.

Another key threat is contactless payment fraud, particularly in regions like the UK, where it rose by **82%**. As digital payments increase, fraudsters exploit vulnerabilities in NFC technology to carry out unauthorized transactions.



Number of investments in fintech



Source: statista.com

While these technologies have significantly improved fraud detection, regulators have also stepped up efforts to combat financial crime. The European Union’s AMLD6 has placed greater scrutiny on banks’ CDD practices, requiring stricter KYC protocols and greater transparency in financial transactions. In the U.S., the FinCEN Beneficial Ownership Rule, which went into effect in 2024, mandates that financial institutions collect and verify information about the true owners of companies to prevent criminals from using shell companies to hide illicit funds.

The evolving landscape of financial services, bolstered by technological advancements and stringent regulations, is reshaping the industry’s approach to combating fraud. With the rise of fintechs and online banks, financial institutions must stay vigilant and continue to innovate to stay ahead of the increasingly sophisticated fraud schemes threatening their operations.

Financial institutions are adopting AI-powered monitoring systems to better detect suspicious activities, reducing false positives. EDD for high-risk clients and agile compliance frameworks are being implemented to keep up with regulatory changes. These measures aim to improve the accuracy of transaction monitoring, risk-based client onboarding, and faster adaptation to new global sanctions.



**Vivek Mishra**  
AML/KYC Professional

## Insurance

The insurance industry is facing a multitude of financial crime risks, from fraud to money laundering, driven by the growing complexity of global operations and digital transformations. While insurance fraud remains a top concern, with global losses exceeding **\$80 billion** annually, other crimes like money laundering are increasingly infiltrating this sector, exploiting weaknesses in compliance frameworks and digitalization.

Insurance fraud has long been a persistent issue in its various forms—such as false claims, staged accidents, and premium diversion. In 2023, motor insurance fraud alone accounted for 59% of fraudulent claims globally, with the average fraudulent claim valued at \$15,000. The sector is also contending with policyholder misrepresentation and provider fraud, where healthcare and service providers submit false bills or inflate the costs of services. Fraud detection in insurance is evolving, but fraudsters continue to adapt, taking advantage of digital platforms and the relative anonymity of online applications.



Insurance fraud results  
in losses that exceed  
**80 billion dollars**  
each year.

Money laundering has become a significant issue for insurance firms, particularly through life insurance policies and reinsurance arrangements, which are seen as less scrutinized avenues for illicit financial activity. Criminals can buy high-value insurance products, surrender them prematurely, and then receive refunds that appear to be legitimate funds. The insurance sector has become an attractive target for these schemes due to the size of transactions and the ability to hide the origins of illicit funds.

## Healthcare

In 2024, the healthcare industry continues to be a primary target for fraud and cyberattacks, largely driven by the massive amounts of sensitive data that medical organizations manage. The global rise in healthcare fraud has been particularly evident in the U.S., where fraud losses in Medicare and Medicaid systems are expected to surpass **\$100 billion** by the end of the year. Fraud schemes such as phantom billing, kickbacks, and upcoding remain prevalent, and as telemedicine services grow, fraudsters are finding new ways to exploit these digital platforms.

The shift toward digital health solutions, accelerated by the COVID-19 pandemic, has led to a surge in cybercrime against healthcare institutions. In 2024, ransomware attacks on healthcare organizations increased by 32%, with hackers exploiting outdated security systems. These attacks often result in data breaches, exposing sensitive patient information and leading to costly compliance failures, especially under data protection laws like GDPR and the U.S. Health Insurance Portability and Accountability Act (HIPAA). As a result, regulatory bodies have increased pressure on healthcare providers to bolster their cybersecurity defenses, including mandatory encryption, multi-factor authentication, and continuous monitoring of digital infrastructures.



## Real Estate

The real estate sector remains one of the most attractive avenues for money laundering activities. Criminals continue to exploit real estate purchases as a means to launder illicit funds, particularly in regions where real estate markets are opaque and regulatory oversight is limited. In 2024, FinCEN reported a notable increase in suspicious real estate transactions, with a 15% rise in money laundering activities related to luxury property investments in the U.S. alone. The problem is particularly acute in markets such as Miami, Los Angeles, and New York, where high-value real estate transactions are often conducted through anonymous shell companies.

Globally, the FATF has tightened its recommendations for transparency in real estate transactions, pushing governments

to require more rigorous reporting from real estate agents and title companies. The European Union, under the AMLD6, has introduced stricter KYC requirements for real estate transactions over €10,000, ensuring that parties involved in high-value property transfers are subject to more stringent scrutiny.

In addition to money laundering, real estate investment fraud surged in 2024, particularly in markets experiencing rapid growth. Fraudsters have exploited the housing boom by creating fake investment opportunities or manipulating property valuations, leading to significant financial losses for investors. This year, an estimated \$6.4 billion was lost globally to fraudulent real estate investment schemes, underscoring the need for stronger oversight in the industry.



## Energy Sector

The energy industry, particularly oil and gas, has long been a hotspot for financial crime, with corruption, bribery, and money laundering at the forefront of the risks. In 2024, the rise of green energy investments has introduced new financial crime risks as the sector transitions to more sustainable energy solutions. Criminals are capitalizing on the influx of investment into renewable energy projects by creating fraudulent green bonds and manipulating carbon credit markets.

Moreover, regulatory bodies, such as the DOJ and SFO, have been increasingly focused on addressing corruption and bribery in the energy sector. A prominent case in 2024 involved a multinational energy corporation fined \$1.2 billion for

bribery charges related to securing contracts in West Africa. Such high-profile cases highlight the ongoing risks within the sector and the increasing role of international cooperation in prosecuting financial crimes.

The transition to renewable energy has also seen an increase in investment fraud tied to green energy projects. Scammers have created fictitious green energy ventures to attract investors, exploiting the growing demand for sustainable investments. As governments continue to push for carbon neutrality, regulatory bodies are likely to introduce new compliance requirements for green energy projects to prevent fraud and financial mismanagement.





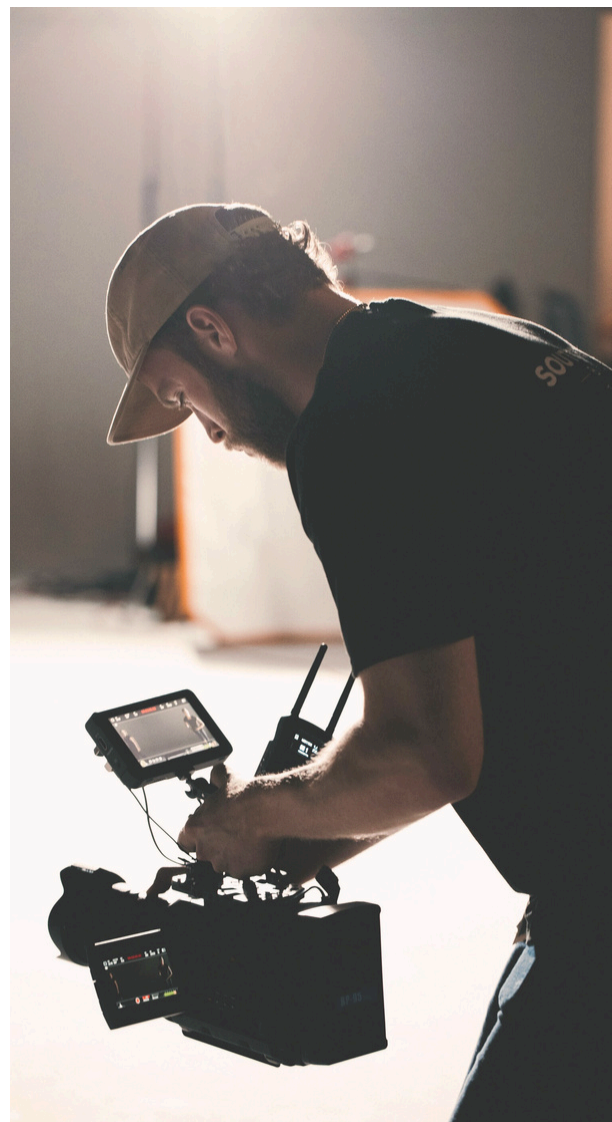
## Entertainment Industry

The entertainment industry has not been immune to the wave of financial crimes impacting various sectors. In 2024, the sector has seen a surge in intellectual property (IP) theft, particularly in film, music, and gaming. Fraudsters are using sophisticated methods to pirate content, costing the industry an estimated **\$20 billion** in lost revenue this year alone. Digital platforms, especially those offering streaming services, remain vulnerable to hacking, resulting in unauthorized access to premium content and subscription fraud.

Additionally, celebrity endorsement scams have grown in 2024, with fraudsters impersonating well-known personalities to promote fake investment schemes, particularly in the cryptocurrency space. These scams have resulted in significant financial losses for unsuspecting fans and investors who fall prey to fraudulent schemes advertised through social media.

As a response, the Motion Picture Association (MPA) and other entertainment bodies have been working closely with technology firms to develop better anti-piracy measures and prevent fraud in subscription-based services. The focus on strengthening Digital Rights Management (DRM) systems and using blockchain technology to track content ownership has become a priority in protecting intellectual property rights.

Content piracy cost  
the industry  
**\$20 billion**  
this year.



A photograph of a rocket launch against a clear blue sky. The rocket is positioned in the upper right quadrant, angled upwards and to the right. It is surrounded by a bright, white, and somewhat turbulent plume of smoke and fire, which extends downwards and to the left, forming a long, curved trail that fills the lower half of the frame. The overall composition is dynamic and suggests forward motion and progress.

# **Strategic Roadmap for 2025**

# Strategic Roadmap for 2025

As financial crime grows more intricate, institutions are urged to adopt strategies that address both current risks and anticipate future threats. In 2025, the rapid advancement of technologies, evolving regulatory landscapes, and sophisticated criminal tactics will redefine how financial crime prevention is approached. Leveraging AI, blockchain, and machine learning, institutions can detect, prevent, and respond to crime with greater precision, essential as new challenges like DeFi and cryptocurrencies introduce unique complexities that require adaptive risk management.

With digital financial networks crossing traditional borders, there's an increasing demand for cross-border collaboration and regulatory alignment. Coordinated global efforts and partnerships between public and private sectors will play a critical role in combating both established and emerging threats, promoting resilience across the financial ecosystem.

Sanction Scanner's third annual report highlights key strategies shaping the future of financial crime prevention, providing institutions with actionable insights to modernize compliance, enhance technological capabilities, and proactively counter new risks. By adapting to this evolving landscape, organizations can better protect their assets, ensuring a more secure and transparent financial system for all.



## Tailoring AI for Real-Time Financial Crime Detection

By 2025, the successful implementation of AI and machine learning in combating financial crime will hinge on the ability of financial institutions to deploy these technologies with greater specificity. While AI has become commonplace for fraud detection, its role in identifying patterns in money laundering and terrorist financing will become more refined. The shift from reactive to predictive models will be essential, with AI systems not just flagging suspicious activities but providing real-time risk assessments that predict which transactions are most likely to lead to financial crime.

One of the key challenges financial institutions will face in 2025 is the integration of AI into legacy systems. Many institutions continue to rely on outdated infrastructure that cannot accommodate real-time AI processing. The forecast for 2025 sees leading institutions investing in hybrid AI architectures that can work alongside older systems while ensuring seamless real-time compliance monitoring. Experts anticipate that intelligent automation will play a crucial role in bridging this gap, using AI-driven workflows to automate routine compliance tasks while enhancing investigative capabilities.

Furthermore, by 2025, we predict that AI-based open-source intelligence (OSINT) will be widely adopted as a critical tool in identifying emerging criminal networks and illicit activity in decentralized environments, such as crypto trading platforms and peer-to-peer financial networks. OSINT tools will be specifically tailored to monitor social media platforms, dark web forums, and encrypted communication channels, providing financial institutions with proactive threat intelligence that is scalable and adaptable.

AI and machine learning are becoming essential for detecting financial crime by analysing data patterns and improving fraud detection. Blockchain analytics offer traceability, making it easier to track illicit funds. Quantum computing, though still in development, could potentially crack encrypted criminal networks. Biometric authentication technologies, like iris and facial recognition, are enhancing security to prevent fraud. These technologies will play a key role in future financial crime prevention strategies.



**Vivek Mishra**

AML/KYC Professional

## Blockchain's Role in Corporate Transparency and AML Compliance

In 2025, blockchain technology is set to play a much larger role in AML compliance beyond simply offering immutable transaction records. The real innovation will come in the form of cross-border blockchain networks, which allow multiple financial institutions to share transaction data securely and in real-time. This shift toward decentralized, transparent compliance systems will empower institutions to respond faster to red flags and streamline the KYC process using self-sovereign identity verification mechanisms.

DeFi will continue to present unique sets of challenges, particularly as criminals attempt to exploit these platforms for money laundering and terrorist financing. In 2025, regulatory frameworks governing DeFi will require institutions to adopt advanced analytics tools that can track the Total Value Locked (TVL) within DeFi ecosystems in real-time. This capability will enable a more granular level of scrutiny into suspicious transactions and will become particularly crucial as peer-to-peer exchanges and non-custodial wallets proliferate, further complicating efforts to trace illicit funds.

The implementation of smart contracts for AML compliance is expected to see significant growth in 2025, allowing institutions to embed compliance rules directly into the transaction flow. This will ensure that any transaction not meeting compliance standards is automatically flagged or halted, reducing the need for post-transaction investigations.

An AML Program which follows regulatory guidance on the Risk Based Approach should take care and be ready to act swiftly upon changes in the crypto industry. Do you have an assigned SME team member or engaged third party provider to conduct horizon scanning? This is the act of purposefully looking for regulatory changes on a regular basis. Take it a step further by speaking with your screening and monitoring service providers as they may be able to assist in getting the monitoring data you need to see incoming threats or evolving schemes. This is crucial as it will allow you to adapt your compliance posture in quick order. Involve your SMEs to assist in analyzing this data as they are your strongest line of defense against these threats.



**Mario M. Duron**

Chief Compliance Officer



## Regulatory Shifts and Global Coordination

Global regulatory frameworks for financial crime prevention will continue to evolve in 2025, focusing on greater collaboration between regulators and financial institutions, particularly in regions with high financial crime risks. Regulatory technology (RegTech) solutions will become more integrated into compliance departments, offering automated tools to ensure institutions remain compliant with varying regional regulations. In particular, we foresee the FATF and other international bodies pushing for standardized frameworks that accommodate both traditional banking systems and rapidly evolving digital asset ecosystems.

In the cryptocurrency space, 2025 will likely see greater enforcement of cross-border regulatory cooperation to tackle crypto-related financial crime. Governments will demand enhanced transparency from crypto exchanges, particularly those facilitating Decentralized Autonomous Organizations and decentralized financial applications, where illicit activities can be difficult to detect. Regulatory sandboxes will likely become common for testing innovative compliance technologies, especially in regions with emerging digital currencies.

Additionally, provisional credit regulations will be tightened, particularly as neobanks and fintechs continue to face challenges in preventing fraud during money transfers and ACH payments. These institutions will increasingly look to real-time fraud detection systems integrated with AI and blockchain to manage provisional credit risks before funds are fully settled.

## Combatting Financial Crime in the Cryptocurrency Ecosystem

As digital assets continue to evolve, financial crime within the cryptocurrency sector will require institutions to adopt specialized tools that monitor and trace decentralized networks. Cryptocurrency intelligence platforms will be instrumental in following money trails across complex chains, particularly as criminals increasingly shift illicit activities across multiple chains in an effort to obscure their movements.

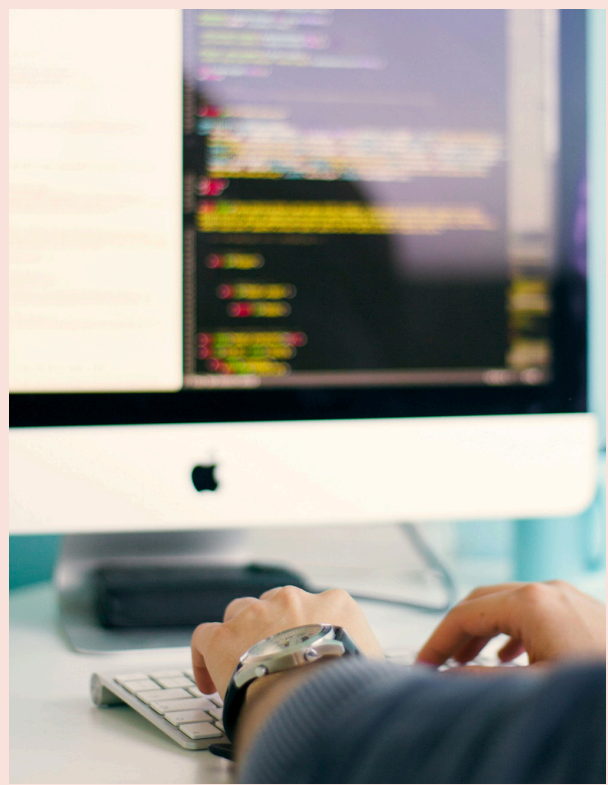
In 2025, it is expected that the rise of stablecoins will pose additional challenges for AML compliance. Stablecoins, often pegged to fiat currencies, provide liquidity in decentralized markets and are frequently used in cross-border transactions, creating vulnerabilities for smurfing and layering techniques in money laundering. To mitigate these risks, institutions will need to deploy AI systems capable of tracking not only individual stablecoin transactions but also the flow of funds across multiple asset classes, ensuring compliance with AML regulations even in the most blurred environments.

Financial institutions should implement zero-trust security models and multi-layer encryption for cyber resilience.

## Strengthening Cyber Resilience in 2025

With the growing digitization of the financial services sector, cybercrime will remain one of the most significant threats. In 2025, financial institutions will need to enhance their cyber resilience by implementing zero-trust security models and multi-layered encryption protocols across their networks. These advanced security frameworks must be paired with behavioral analytics that can detect anomalies in user behavior, further enhancing the institution's ability to preempt attacks.

The continued development of deepfakes and voice replication technology will present heightened risks for social engineering attacks. Financial institutions must invest in biometric security systems and voice recognition technologies to verify user identity across digital channels, reducing the likelihood of successful fraud. Generative AI systems capable of creating real-time defenses against these attacks will become essential in countering the growing sophistication of cybercriminal networks.



## Emerging Technologies and Their Impact on Financial Crime

Looking ahead, quantum computing could fundamentally reshape the landscape of financial crime prevention, offering unprecedented speed in transaction monitoring and cryptographic analysis. While still in its nascent stages, quantum computing could provide financial institutions with real-time capabilities that surpass the speed and scale of current AI and blockchain systems.

First, the Risk Based Approach is an important first step in gaining insight into your institution, program, customer base and products. A well thought out risk assessment is critical to any sustainable AML Program. Your assessment should be tailored to your industry, company, services and products as no two- companies are alike. Make a decision. This is a simple statement which can make or break a department, launch, or delay products/services. Analysis paralysis is very real, and it can be made worse in high-risk industries. Taking it slow can be beneficial, but it can also lead to loss of focus and attention which can lead to gaps being missed. Ownership of your decision can inspire confidence from your team and show regulators you are willing to take accountability.



**Mario M. Duron**  
Chief Compliance Officer

In parallel, the use of digital twin technology is expected to provide advanced simulation environments for compliance testing. By creating virtual models of financial systems, institutions can identify vulnerabilities before they are exploited by criminals, ensuring that their real-world counterparts are fortified against attacks.

Finally, OSINT, combined with AI-based threat intelligence platforms, will remain at the forefront of financial crime detection in 2025. By leveraging OSINT, institutions will be able to collect data from disparate sources, including social media, deep web forums, and other open platforms, providing them with the proactive intelligence necessary to identify emerging threats long before they materialize.

In conclusion, there is a critical need for financial institutions to adopt more specialized and proactive approaches to combat financial crime. From advanced AI and blockchain innovations to enhanced regulatory cooperation and the rise of cyber-resilience measures, the future of financial crime prevention will demand agility, technological investment, and global coordination to address the sophisticated methods employed by criminals. Institutions that embrace these emerging trends and technologies will be best positioned to navigate the complex and rapidly evolving landscape of financial crime.



## Our Customers



More than 500 customers from 60+ different countries trust us!



## Contact Us



27 Old Gloucester Street, London,  
United Kingdom, WC1N 3AX



+44 20 4577 0427



Yildiz Technical University Technopark  
C-1 Block No: 106-8 Istanbul, Turkey



+90 (212) 963 01 84



[info@sanctionscanner.com](mailto:info@sanctionscanner.com)



[sanctionscanner.com](http://sanctionscanner.com)



Join us and  
let's fight  
financial crime  
together.

Disclaimer: Please be advised that the contents of this document are intended for informational purposes only. The information presented herein should not be construed as legal advice. Sanction Scanner assumes no responsibility for the accuracy, completeness, or timeliness of the information provided and disclaims all liability for any actions taken based on this information.

For detailed information regarding the source materials utilized in this guide, kindly visit [sanctionscanner.com](https://sanctionscanner.com)

