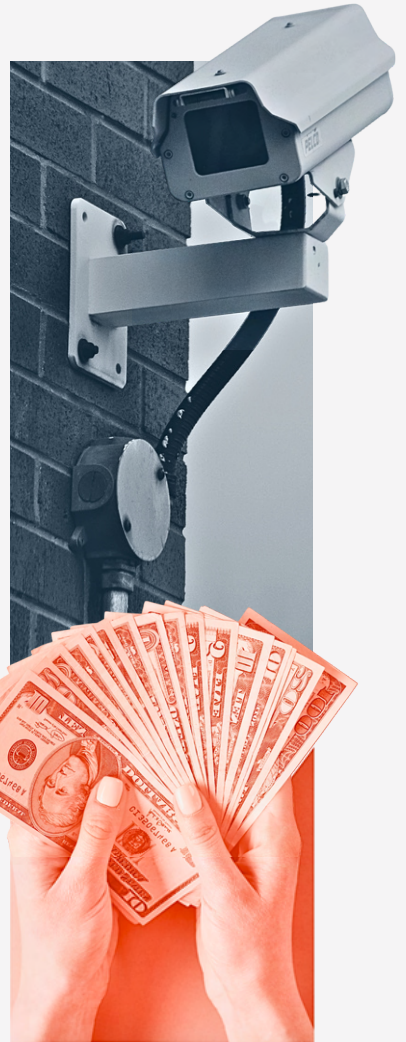


**2023-2024**

# **Financial Crime & Compliance Report**





# CONTENTS

<b>01.</b> About Us	02	<b>06.</b>	
		<b>The Shifting Landscape of Financial Fraud</b>	27
<b>02.</b> Foreword	03	Trends and Vulnerabilities in 2023	29
		Technology's Impact on Fraud	30
<b>03.</b> Executive Summary	04	Sector-Specific Vulnerabilities	32
		Future Strategies and Technologies in Combating Financial Fraud	34
<b>04.</b>		Survey Results	36
<b>AML Regulation &amp; Compliance</b>	08	<b>07.</b>	
EU AML Regulation Changes for 2023	09	<b>Cryptocurrencies</b>	39
US AML Regulations in 2023	12	Connection Between Cryptocurrencies and Money Laundering	41
Asian AML Regulation in 2023	15	Cryptocurrency Risks	43
Survey Results	17	AML & KYC Regulations in the Crypto Industry	45
		The Future of Cryptocurrency in 2024	50
<b>05.</b>		Survey Results	53
<b>Technology and AML Tools</b>	19	<b>08.</b>	
Effectiveness of Existing AML Tools	21	<b>Regional Trends on FinCrime, AML &amp; Fraud</b>	55
How to Leverage Technology: AI and Automation in AML	22	Asia-Pacific	56
Positive Impacts of AML Tools	23	Europe and United Kingdom	58
Survey Results	25	America	62
		Middle East and North Africa (MENA)	64
		Survey Results	66

# 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.



# Foreword

*Paul D. Volcker*  
Secretary of the Treasury  
*Lisa Sumastatao Rio*  
Treasurer of the United States.

# Foreword

In an era marked by ever-evolving complexities in the financial landscape, the imperative to combat money laundering, financial crime, risk, and fraud has taken on unparalleled significance. The dynamic interplay of global economic transactions and technological advancements necessitates a vigilant and collaborative approach among financial institutions worldwide. Within this context, we present a comprehensive report that illuminates the multifaceted dimensions of anti-money laundering (AML) and related concerns and charts a course for a more secure and resilient financial future.



## Navigating the Uncharted Waters of Financial Integrity

The financial world has recently been confronted with an intricate web of challenges from illicit financial activities. Financial crimes, like money laundering and fraud, have emerged as insidious threats that undermine the foundation of economic stability. Our report emerges as a beacon of knowledge, assembled through meticulous research and an analysis of global perspectives.

## Methodology: Shaping Insights Through Collaborative Endeavors

Central to the authenticity and depth of this report are the insights drawn from a series of comprehensive surveys conducted across more than **50** countries. We have forged an international partnership by engaging with our customers and tapping into firsthand experiences and expertise. This report is a compilation of data and a testament to the synergy achieved through global collaboration.

## Anticipating Insights: What to Expect in This Report

### Unveiling the Landscape: AML Regulations and Compliance

The journey commences with a close examination of AML regulations and compliance mechanisms that form the bedrock of financial integrity. This section delves into the nuanced tapestry of global regulatory frameworks, spotlighting successes, and acknowledging the areas that demand further harmonization. By juxtaposing diverse perspectives, we shed light on the evolving nature of these safeguards and their pivotal role in protecting financial systems.

### AML Tools and Technology

The symbiotic relationship between technology and AML strategies is the focal point of this section. Here, we delve into the transformative potential of technological innovations, from machine learning algorithms to blockchain solutions. Through insightful case studies, we showcase the cutting-edge tools that empower institutions to identify patterns of illicit activity and redefine the landscape of AML compliance.

### Cryptocurrencies

As cryptocurrencies continue to disrupt traditional financial paradigms, the report turns its lens toward the intersection of AML and this burgeoning field. By facilitating the complexities of crypto transactions and their implications, we endeavor to equip stakeholders with the knowledge necessary to navigate this uncharted territory without compromising integrity.

### Fraud

Fraud, a pervasive threat that transcends borders, takes center stage in the next segment. Through rigorous analysis, we illuminate the anatomy of fraud, dissecting the tactics employed by malevolent actors and underscoring the pivotal role of preventive strategies. This section serves as a vanguard for businesses seeking to fortify their defenses in an era where innovation and deceit often intertwine.

### Regional Trends: The Global Patchwork of Vulnerabilities

Global financial dynamics are anything but uniform, with regional features playing a pivotal role in shaping vulnerabilities. Our exploration of regional trends serves as an eye-opener, bringing to the forefront the divergent challenges and triumphs encountered by different regions. In recognizing the nuances that distinguish one jurisdiction from another, we emphasize the significance of tailor-made approaches to risk management.





# Executive Summary

Sanction Scanner designed this report by targeting to increase awareness and shed light on the fight against financial crime globally. The report includes both a comprehensive research of experts and existing literature, and news, sectoral improvements; in addition to the survey conducted over **400** respondents across **50** countries and various industries. It aimed at assessing the state of knowledge and practices related to AML and financial crime prevention in 2023-2024. The key findings from this comprehensive survey are outlined below:

Survey with  
**400+ people**  
from  
**50 countries**

## Key Findings

One prominent finding is the presence of a knowledge gap within organizations regarding AML and financial crime regulations. Many industry professionals expressed only a "somewhat familiar" level of understanding, emphasizing the need for deeper knowledge and heightened awareness to ensure compliance with evolving regulations.

Another noteworthy discovery is the uncertainty among respondents regarding whether their respective industries have unique AML and financial crime requirements. This uncertainty underscores the importance of providing clear guidance and ensuring compliance in industries with specific regulatory demands.

The survey also revealed reporting challenges faced by organizations, with the complexity of data management and reporting processes being a common obstacle. Limited resources for compliance reporting and difficulties in interpreting regulatory guidelines further compounded these challenges. Addressing these issues will require investment in resources and comprehensive training.

**Reporting**  
is a common  
obstacle

A concerning trend identified is the lack of confidence among a significant portion of respondents in their understanding of current AML regulations. This confidence gap underscores the need for enhanced training and educational initiatives to ensure better compliance within organizations.





Respondents reported that recent legal changes had caused confusion and necessitated adjustments in their industry's approach to AML and financial crime prevention. To remain compliant, organizations must maintain agility and adaptability in response to evolving regulations.

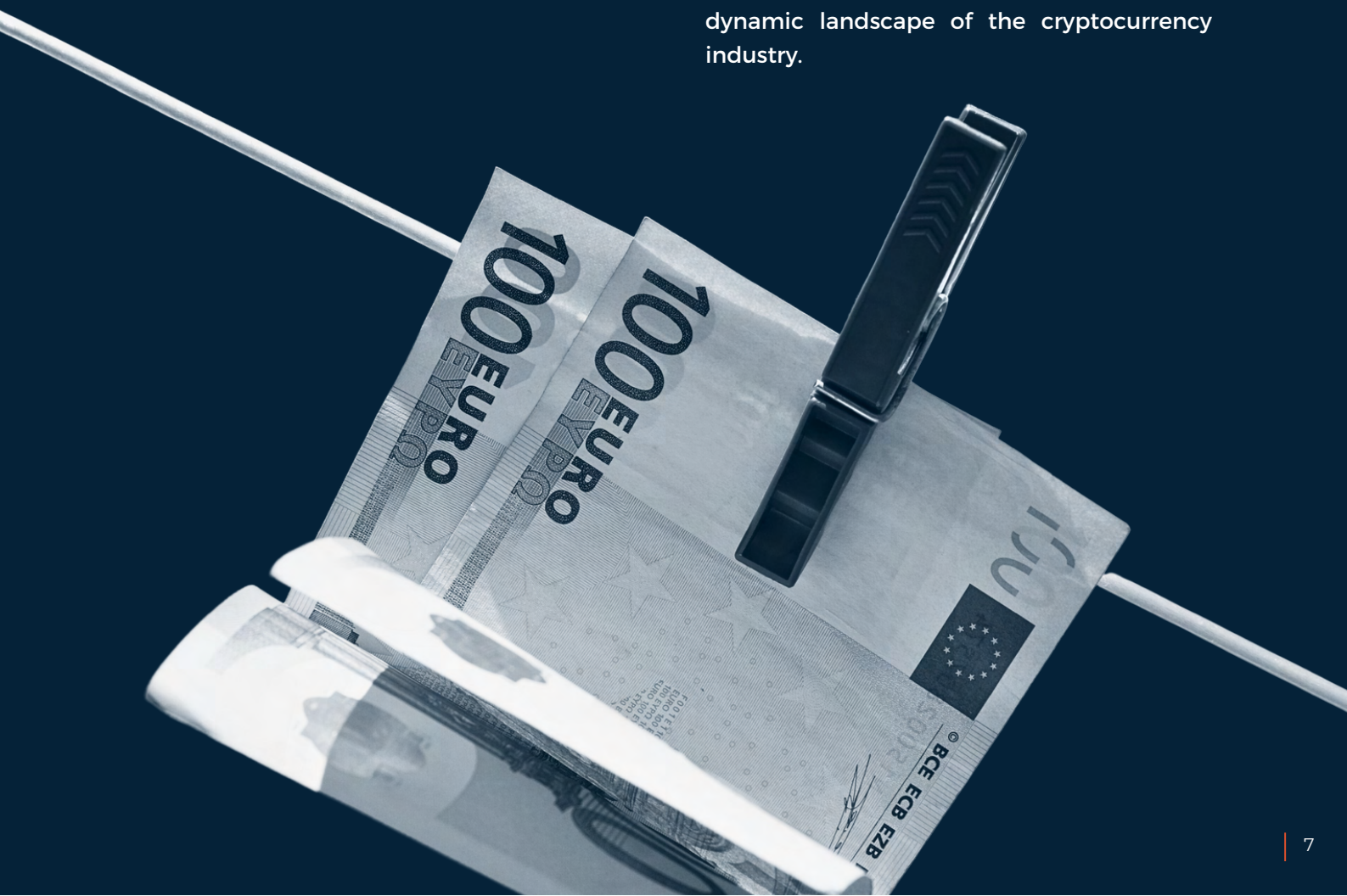
Furthermore, it revealed differing threat perceptions across industries, with the e-commerce sector seen as having a higher level of threats related to fraud and financial crime. Understanding these perceptions can help industries tailor preventive measures effectively.

In the context of cryptocurrency, there is a notable level of awareness among respondents regarding the connection between cryptocurrencies and money laundering. However, further education is needed to ensure a comprehensive understanding of associated risks.

Respondents emphasized the critical role of robust AML and transaction monitoring systems in cryptocurrency exchanges and wallet providers for ensuring security within the crypto space. Instances of non-compliance with AML regulations within the cryptocurrency industry were reported, highlighting the need for improved compliance measures in this rapidly evolving sector.

Individuals working in cryptocurrency-related roles reported experiencing crypto scams or fraud attempts, underscoring the vulnerability of those within the industry to fraudulent activities. Respondents expressed a need for further education and training in recognizing signs of suspicious activities within cryptocurrency transactions.

Collectively, these key findings emphasize the need for organizations to enhance their AML compliance efforts, improve regulatory awareness, address reporting challenges, and foster greater knowledge, both in traditional financial sectors and within the dynamic landscape of the cryptocurrency industry.





Section 1

# **AML Regulation & Compliance**



# AML Regulation & Compliance

## EU AML Regulation in 2023

The growing landscape of global finance necessitates continuous adaptation to AML regulations. The European Union's approach to AML reflects its commitment to combating emerging criminal threats, geopolitical shifts, and technological advancements. In the wake of recent events such as the COVID-19 pandemic and Russia's incursion into Ukraine, the EU's AML requirements have become even more intricate, underscoring the significance of regulatory compliance for organizations across the bloc.

Non-compliance with the EU AML regulations carries severe financial and criminal consequences. Notably, in 2022, Crédit Agricole faced a **€1.5 million** fine from France's financial regulator due to transaction monitoring and customer due diligence shortcomings. Similarly, Robeco was fined **€2 million** by the Netherlands' financial regulator for similar due diligence failings. Given the potential penalties, EU compliance officers must diligently account for a range of criminal and regulatory risks, while also comprehending the impact of forthcoming changes on their organization's products and services.

The EU's 2023 AML package introduces a host of new compliance challenges for companies of all sizes, spanning areas from data protection and cryptocurrency to reporting rules and economic sanctions. To facilitate preparedness for these challenges, this article aims to provide insights into key developments in the EU's AML landscape.



## Revamping the Sixth Anti-Money Laundering Directive (6AMLD)

Among the notable updates in the EU's AML package is a revised version of the Sixth Anti-Money Laundering Directive, known as the 'new' 6AMLD. The modifications encompass various legislative mechanisms and measures, including:

- Periodic national risk assessments every four years.
- Frameworks for financial intelligence units (FIUs) to analyze and submit suspicious activity reports (SARs).
- Clarifications regarding beneficial ownership information requirements.
- Introduction of cross-border asset registers.
- Establishment of public supervisory bodies to oversee the EU self-regulatory entities.
- Refinement of rules pertaining to collecting personal data within the context of AML/CFT.
- Enhanced protection for whistleblowers who expose financial crimes.

## Navigating Crypto Asset Transfer Regulations

The EU's Markets in Crypto Assets (MiCA) framework, set to become legally effective in 2024, represents a landmark initiative in regulating the cryptocurrency sphere. Designed to address unbacked crypto assets and stablecoins, MiCA introduces compliance requirements for cryptocurrency service providers, such as:

- Mandate for stablecoin issuers to maintain adequate liquid reserves for potential mass withdrawals.
- Obligation for crypto asset service providers to obtain authorization from national authorities to operate in the EU.
- Introduction of a public register of non-compliant crypto asset service providers overseen by the European Banking Authority (EBA).

Simultaneously, the Transfer of Funds Regulation (TFR) will be enacted alongside MiCA to address anonymity risks associated with cryptocurrency transactions. TFR mandates measures including:

- Collection of personal details for all parties involved in transactions exceeding **€1,000**.
- Screening of transaction beneficiaries against sanctions lists.
- Provision of customer personal data to authorities upon request.





## The Emergence of the EU AML Authority

A pivotal component of the EU's comprehensive AML package is the creation of an Anti-Money Laundering Authority (AMLA), proposed by the European Commission in 2021. This dedicated authority safeguards the EU's financial system against money laundering and terrorism financing threats. Expected to be operational in 2024, AMLA will work with existing national AML and countering the financing of terrorism authorities to establish a harmonized supervision system across the bloc. AMLA seeks to be a transformative force in the EU AML efforts by supervising high-risk cross-border financial entities and collaborating with national supervisors.

## Harmonizing Conduct Rules for Financial Institutions

Concurrently with the creation of AMLA, the EU plans to introduce a 'single rulebook' for AML/CFT across the union. Based on harmonized practices outlined in the AML Directives, this rulebook will lay out common conduct rules for financial institutions (FIs) operating within the EU. Noteworthy inclusions are:

- Detailed customer due diligence (CDD) rules tailored to different levels of risk.
- Clear guidelines for determining ultimate beneficial ownership (UBO), fostering consistency across the EU.
- Requirement for linking bank accounts to national registers, expediting information sharing processes.



## The UK's Economic Crime Bill

Despite the UK's departure from the EU in 2020, its AML/CFT regulations remain aligned with the bloc's standards. The second Economic Crime (Transparency and Enforcement) Bill, set to take effect in 2023, prioritizes curbing foreign money laundering and positioning the UK as a secure business hub. Notable provisions include:

- Enhanced investigative and enforcement powers for Companies House.
- Reforms to limited partnership regulations to prevent misuse by foreign entities.
- New regulatory authority to seize and recover crypto assets linked to financial crimes.
- Strengthened anti-money laundering regulations, including streamlined information sharing rules and a simplified SAR submission process.

This bill builds on the foundation laid by its predecessor, which introduced measures like an overseas entities register, a simplified unexplained wealth order process, and stringent liability for economic sanctions breaches. These legislative moves reflect the UK's commitment to addressing issues such as Russian manipulation of financial systems and the risks posed by cryptocurrencies.

# US AML Regulations in 2023

The year 2022 presented US compliance teams with numerous challenges, including the ongoing COVID-19 pandemic measures and the aftermath of Russia's invasion of Ukraine. These circumstances prompted swift regulatory responses from the US government, necessitating adaptability to an evolving AML/CFT risk environment to avoid detrimental penalties.

Given the ongoing Ukraine conflict and economic turbulence, the US AML regulations are expected to continue evolving in 2023 to address new financial crime risks. To help organizations navigate this complex compliance landscape and fulfill their obligations, it's crucial to understand the key upcoming changes in the US AML regulations.

## The FinCEN Final Rule

The Anti-Money Laundering Act of 2020, enacted on January 1, 2021, introduced novel rules for reporting beneficial ownership information (BOI) aimed at combating money laundering through shell companies and legal structures. To bolster this initiative, the Financial Crimes Enforcement Network (FinCEN) issued its final rule on BOI provisions in September 2022. This rule, slated for implementation on January 1, 2024, aligns closely with the initial proposals and introduces the following regulatory aspects:

- Definition of "reporting companies" obligated to comply with BOI rules.
- Definition of "beneficial owners," encompassing individuals exercising "substantial control" over a company or holding at least 25% control.
- Requirement for companies to report "company applicants" and individuals directing filing processes.
- Specification of ownership information to be reported, including names, addresses, and birthdates of owners, along with relevant identification documents.
- Stipulation for firms to report within 30 days of registration.
- Clarity on criminal and financial penalties for reporting violations, focusing primarily on individuals rather than reporting companies.





## National Illicit Finance Strategy

The US Department of the Treasury introduced the National Strategy for Combating Terrorist and Other Illicit Financing in May 2022, responding to threats identified in the 2022 National Risk Assessments. This strategy aims to strengthen the US AML/CFT framework by:

- Closing vulnerabilities to exploitation by shell companies and cash real estate purchases.
- Enhancing the AML/CFT framework by providing compliance guidance, promoting information sharing, and funding supervision and enforcement.
- Strengthening law enforcement against illicit finance.
- Addressing risks and threats posed by virtual assets and fintech innovations while leveraging their benefits.



## Responsible Financial Innovation Act

The Responsible Financial Innovation Act (RFIA), introduced in June 2022, seeks to establish a regulatory framework for digital assets in the US. The act designates the Commodity Futures Trading Commission (CFTC) as the primary regulator of digital assets and introduces reporting requirements for digital asset service providers. Key features of the RFIA include:

- Oversight by the CFTC.
- Reporting obligations for issuers of digital assets to the Securities and Exchange Commission (SEC).
- New prudential regulations for stablecoin issuers.
- Classification of Decentralized Autonomous Organizations (DAO) as business entities.

## Responsible Development of Digital Assets

In September 2022, President Biden unveiled the Comprehensive Framework for the Responsible Development of Digital Assets. This framework suggests forthcoming regulatory controls on digital assets, emphasizing:

- Issuance of guidance and rules by the Treasury to address emerging risks in the digital asset ecosystem.
- Collaboration between federal agencies and the US firms to provide regulatory guidance.
- Efforts led by the US Financial Literacy Education Commission (FLEC) to increase public awareness of digital asset risks.

## Global Sanctions and Ukraine

The ongoing Ukraine conflict will likely prompt the US and its allies to expand its sanctions against Russia. New economic restrictions may include export controls on Russia's defense and energy sectors and sanctions against Russian cybercriminals. The US is also expected to apply sanctions against other global targets, including China, in response to espionage activities.







# Asian AML Regulation in 2023

The Asia-Pacific region has witnessed a surge in financial crime investigations due to sweeping legislative reforms. While geopolitical events like the COVID-19 pandemic and global supply chain disruptions temporarily affected AML/ CFT efforts in 2021 and 2022, The Asian AML regulations are set to evolve in 2023. Organizations should prepare to navigate these changes, especially in the context of emerging risks from cryptocurrencies and digital assets and new global economic sanctions.

## Singapore's Vigilant Approach

The Monetary Authority of Singapore (MAS) plays a leadership role in financial crime enforcement. In October 2022, the MAS introduced the National Strategy for Countering the Financing of Terrorism, emphasizing cooperation among government agencies. The strategy's key priorities include coordinated risk identification, strong legal and sanctions enforcement frameworks, risk-based supervision, inter-agency law enforcement collaboration, and implementation of international standards.

The MAS is launching the Collaborative Sharing of ML/TF Information & Cases (COSMIC) platform to enhance inter-agency cooperation in 2023. Developed with input from major international banks, COSMIC will facilitate information sharing among organizations, focusing on issues like shell company abuse and illicit trade finance.

## Hong Kong's Emphasis on Technology

The Hong Kong Monetary Authority (HKMA) has identified tackling fraud and money laundering through mule accounts as priorities for 2023. The 2022 Risk Assessment report categorizes money laundering risk to the banking sector as "High," primarily due to fraud.

To address these concerns, HKMA is promoting the adoption of the AML technology through its Fintech 2025 strategy. This includes initiatives like the Commercial Data Interchange (CDI), aimed at fostering information sharing among financial institutions.





## China's Strengthened Scrutiny

China's focus on money laundering intensified in 2022, with the launch of a three-year action plan to combat money laundering. Coordinated by the People's Bank of China (PBOC) and the Ministry of Public Security, the plan emphasizes coordination and consultation between government departments, introducing new risk prevention mechanisms, AML training programs, and solutions for analyzing money laundering typologies.

China's efforts align with its fourth-round Mutual Evaluation Report by the FATF, which led to clarifying and extending CDD rules to various types of financial service providers beyond banks.

## Japan's Risk Mitigation

Following the FATF's Mutual Evaluation Report of Japan in 2021, the Japanese government initiated an action plan to address compliance gaps. Improving risk assessment, risk mitigation, and ongoing CDD measures emerged as key areas for enhancement.

Japan's Financial Services Agency (FSA) recognizes fintech advances as potential AML/CFT risks and encourages leveraging digital tools for more effective countermeasures. Japan is also focusing on cryptocurrency regulations, including extending the FATF's Travel Rule reporting requirement to cryptocurrency and stablecoin transactions.

## Australia's Inclusive Approach

In 2021, the Australian government launched an inquiry into the effectiveness of its AML/CFT regime, identifying risks from Designated Non-Financial Businesses & Professions (DNFBPs) that had not been included in certain AML/CFT reforms. The inquiry led to recommendations for extending AML/CFT reporting rules to DNFBPs, encouraging technology integration, and aligning regulations with international standards.

Australia plans to introduce a beneficial ownership registry to enhance law enforcement's ability to track foreign money launderers exploiting the country's financial system.





# Survey Results

Sanction Scanner has gathered valuable insights from a diverse pool of respondents, comprising over **400 individuals** from more than **50 countries** and various industries. In this section, we present key findings from the survey, shedding light on the current state of AML knowledge and practices.

## Familiarity with AML and Financial Crime Regulations

The survey results reveal that a significant portion of respondents described themselves as "somewhat familiar" with the latest AML and financial crime regulations for 2023 in their respective industries. This suggests that while many individuals possess a basic understanding of these regulations, there may be room for deeper knowledge and awareness.

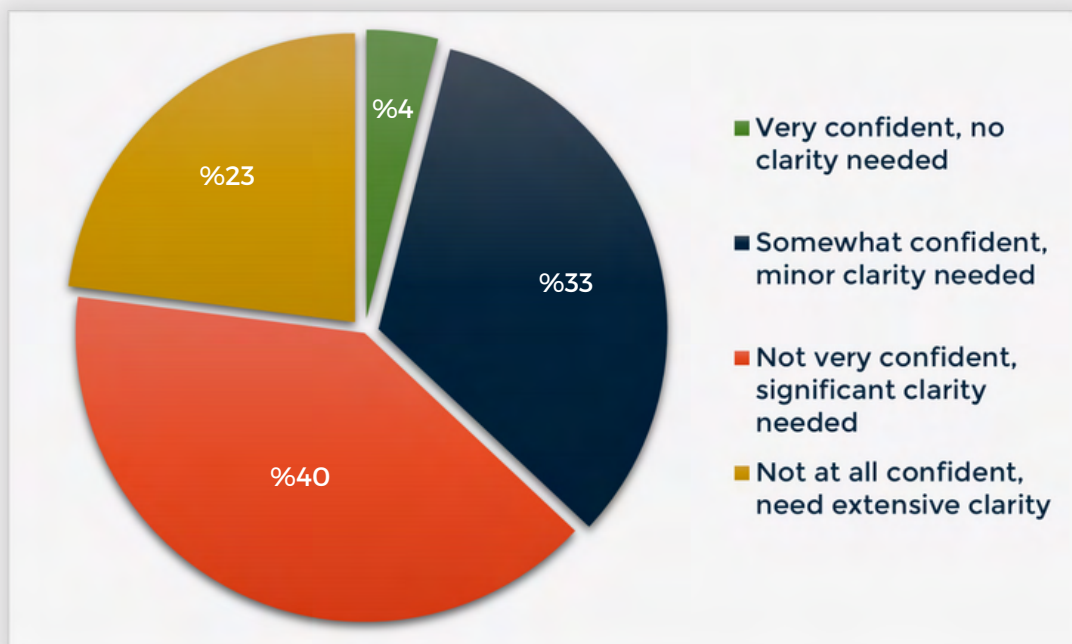
## Impact of Recent Legal Changes

Many respondents reported that recent legal changes had caused confusion and necessitated adjustments in their industry's approach to AML and financial crime prevention. It suggests that regulatory changes can have a significant impact on compliance efforts. Organizations should remain agile and adaptable in response to evolving regulations.

## Confidence in Understanding AML Regulations

A concerning trend is the significant portion of respondents who expressed "not very confident" in their understanding of current AML regulations. The lack of confidence may indicate a need for enhanced training and educational initiatives within organizations to ensure better compliance and adherence to regulations.

How confident are participants in their understanding of current AML regulations and compliance measures that apply to their industry?



## Reporting Challenges

The most commonly cited challenge faced by organizations is the complexity of data management and reporting processes. This underscores the need for streamlined and efficient reporting systems. Additionally, limited resources for compliance reporting and difficulties in interpreting regulatory guidelines were mentioned as significant challenges. These findings emphasize the importance of investing in resources and training to improve compliance capabilities.

## Unique AML Requirements

A notable finding is that a substantial number of respondents were uncertain about whether their industries had unique AML and financial crime requirements. It is important to highlight that there is a potential knowledge gap in understanding industry-specific compliance needs. Organizations should consider providing more clarity and guidance in this area.

It is important to make AML requirements specific to the institution, just like a suit prepared specifically for a person's measurements by a tailor, by taking into account issues such as the sector in which the institution operates, the country, and risk points

## Perception of Threats

According to respondent opinions, the e-commerce industry is perceived as having a higher level of threats related to fraud and financial crime, while the banking and finance sector is viewed as more vulnerable to these threats. Understanding these perceptions can help industries tailor their preventive measures accordingly.



The survey results highlight several key areas where organizations can enhance their AML compliance efforts. These include improving awareness and understanding of AML regulations, addressing reporting challenges, and staying agile in response to legal changes. By focusing on these areas, organizations can better protect themselves against financial crime and fraud while maintaining compliance with evolving regulations in 2023 and beyond.

The background of the entire page is a light orange color with a subtle, repeating pattern of circuit board traces and nodes. The traces are thin, light-colored lines that form a complex, interconnected network across the page. The nodes are small, solid orange circles of varying sizes, scattered throughout the circuit pattern.

Section 2

# Technology & AML Tools



# Technology and AML Tools

The world has witnessed rapid technological advancements over the past few decades, revolutionizing how we live, work, and conduct business. Concurrently, the outbreak of the COVID-19 pandemic in 2019 brought unprecedented changes to society and the global economy. These twin forces of technological progress and the pandemic have profoundly impacted financial crime, shaping both its nature and prevalence.

One of the most significant developments in recent years has been the digital transformation of financial services. The proliferation of online banking, digital payment platforms, and fintech innovations has made financial transactions more convenient than ever before. However, this digital revolution has also created new opportunities for financial criminals. Cybercriminals have exploited vulnerabilities in digital systems, leading to a surge in cyberattacks, data breaches, and identity theft. The ease of online financial transactions has enabled money laundering and fraudulent activities to occur more covertly.

## Economic Uncertainty and Financial Desperation

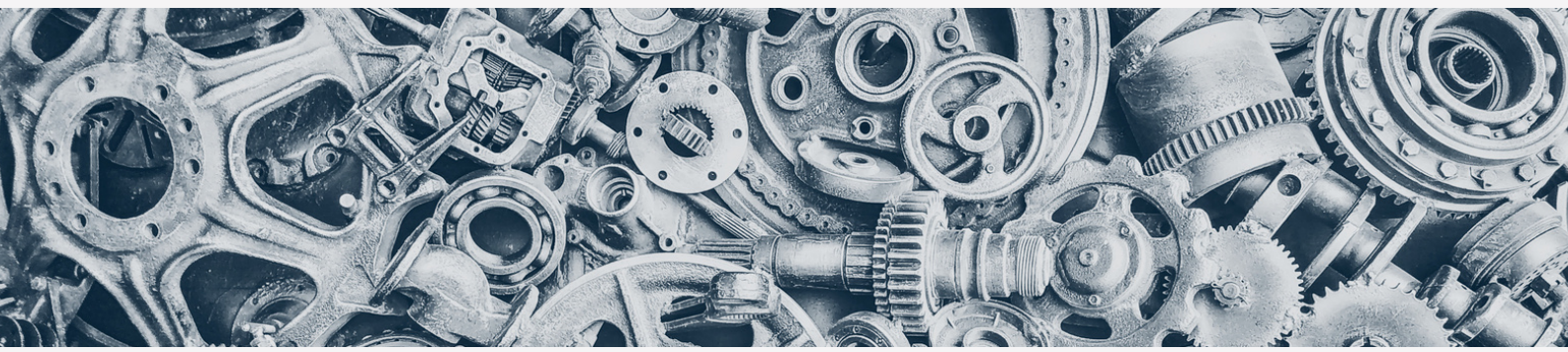
The economic fallout of the pandemic, marked by job losses and financial insecurity, created an environment ripe for financial crime. Individuals and businesses faced unprecedented challenges, making them more susceptible to fraudulent schemes promising financial relief. Scammers exploited fears and uncertainties, from fake COVID-19 treatments to fraudulent government assistance programs.

## Regulatory Responses

To combat the evolving landscape of financial crime in the digital age and during the pandemic, governments and regulatory bodies worldwide have introduced new measures and regulations. These include enhanced know your customer procedures, stricter AML controls, and cybersecurity guidelines. Financial institutions are under increased pressure to comply with these regulations while adapting to the changing financial crime landscape.

Technological improvements and the COVID-19 pandemic have fundamentally altered the financial crime landscape. While technology has provided tools to combat financial crime, it has also given rise to new and more sophisticated forms of illicit activity. The pandemic exacerbated vulnerabilities and desperation, making individuals and businesses more susceptible to fraudulent schemes. As we move forward, the battle against financial crime will require a dynamic response that combines innovative technological solutions with robust regulatory and security measures to protect individuals, businesses, and the global economy.





## Effectiveness of Existing AML Tools

The effectiveness of existing AML tools is paramount in the financial industry, with insights drawn from academic research and customer feedback shedding light on this critical issue.

Academic research has delved into the efficacy of AML tools, particularly emphasizing the role of machine learning (ML) algorithms. Studies have revealed that ML-based AML solutions can significantly enhance the detection of suspicious activities. For instance, one study highlighted that ML algorithms outperform traditional rule-based systems, thanks to their capacity to identify intricate patterns and anomalies in transaction data.

**28%**  
increase  
compared to  
non ML-Based  
solutions

False positives, a long-standing challenge in AML, have also garnered academic attention. Research has proposed strategies to mitigate this issue, including improved algorithm design and parameter tuning, which can help reduce the overwhelming burden of false positives on AML compliance teams.

Academic findings stress the importance of comprehensive data integration and advanced analytics in AML effectiveness.

By uniting data from various sources, such as adverse media and Politically Exposed Person databases, AML systems can bolster their capabilities.

On the other hand, customer reviews provide real-world insights into the practical effectiveness of AML tools. Users often praise the enhanced detection accuracy achieved through these solutions. They highlight the tools' ability to pinpoint suspicious transactions and entities that might have evaded manual scrutiny. User experience is another pivotal aspect. Customers appreciate AML solutions with user-friendly interfaces and efficient workflows, emphasizing that ease of use contributes significantly to overall effectiveness.

The problematic topic of false positive management shows up regularly in customer reviews. Solutions that effectively reduce false positives receive high praise, as they alleviate the burden on compliance teams and streamline processes.

Seamless integration with existing systems is a common theme. Customers find value in AML providers that offer straightforward integration, enabling organizations to harmonize AML efforts with their existing infrastructure. Additionally, the quality of customer support and responsiveness of AML providers play a crucial role in determining effectiveness. Prompt and helpful support can make a substantial difference in resolving issues and optimizing AML processes.



Customers assess AML tools' ability to stay informed of evolving regulatory requirements. Providers that offer regular updates and compliance features are viewed favorably, as they assist organizations in maintaining compliance with changing regulations.

The effectiveness of existing AML tools is a multifaceted issue, with academic research illuminating the potential of ML, data integration, and false positive reduction, while customer feedback provides practical insights into the tangible benefits and challenges of these tools. The convergence of these perspectives aids organizations in making informed decisions when selecting and optimizing their AML solutions.

## How to Leverage Technology: AI and Automation in AML

The fight against financial crime is undergoing a profound transformation with the integration of advanced technologies, particularly ML, artificial intelligence (AI), and automation systems. As the financial industry embraces these innovations to enhance AML efforts, we find ourselves at a critical juncture where technology-driven solutions collide with regulatory frameworks. This title of the report delves into the complex dynamics of ML, AI, automation, and their role in AML, while considering the questions they bring. Drawing on recent research and industry insights, we aim to shed light on the challenges and opportunities ahead.

## Regulators as Innovation Blockers

Regulators and governmental bodies often act as "blocking" forces, safeguarding the financial sector from potential risks associated with AI, ML, and automation adoption. While their motives are noble, protecting society from financial crime, their actions can sometimes hinder innovation. The plethora of Suspicious Activity Reports (SARs) and the impact on regulated entities demonstrate the regulatory challenges faced by the industry.

## The Role of Automation

Creative destruction, a term coined by economist Joseph Schumpeter, describes a process where innovations within an industry disrupt the existing paradigm. In the context of AML, this entails a shift towards automation systems powered by AI and ML algorithms. These systems have the potential to revolutionize how AML professionals detect and prevent financial crime. However, the ethical dimension of this transformation cannot be ignored, as the necessity to combat financial crime sometimes clashes with the moral implications of automation.







# Positive Impacts of AML Tools

## The Power of Technological Innovation in AML

Customers assess AML tools' ability to stay informed of evolving regulatory requirements. Providers that offer regular updates and compliance features are viewed favorably, as they assist organizations in maintaining compliance with changing regulations.

The effectiveness of existing AML tools is a multifaceted issue, with academic research illuminating the potential of ML, data integration, and false positive reduction, while customer feedback provides practical insights into the tangible benefits and challenges of these tools. The convergence of these perspectives aids organizations in making informed decisions when selecting and optimizing their AML solutions.

## Enhanced Detection and Accuracy

One of the standout advantages of these technological tools is their ability to enhance detection and accuracy. ML and AI algorithms are adept at sifting through massive volumes of financial data, identifying intricate patterns, and swiftly flagging potentially suspicious activities. This level of precision is an asset that AML professionals can rely on with confidence.

## Efficiency and Productivity

Automation systems powered by AI and ML algorithms have brought about a significant boost in efficiency. Manual tasks that once consumed valuable time and resources can now be streamlined, allowing AML professionals to focus on higher-value tasks, such as complex investigations and strategic decision-making. This efficiency translates into increased productivity and more effective utilization of resources.

**67%**  
reduction in  
manual work  
by AI&ML



## False Positive Reduction

For years, false positives have been a pain point in AML efforts, overwhelming compliance teams and diverting attention away from genuine risks. Technological solutions have made significant strides in addressing this issue. By fine-tuning algorithms and incorporating advanced data analytics, the number of false positives can be substantially reduced. This not only lightens the workload but also ensures that genuine threats receive the attention they deserve.



## Adaptability and Regulatory Compliance

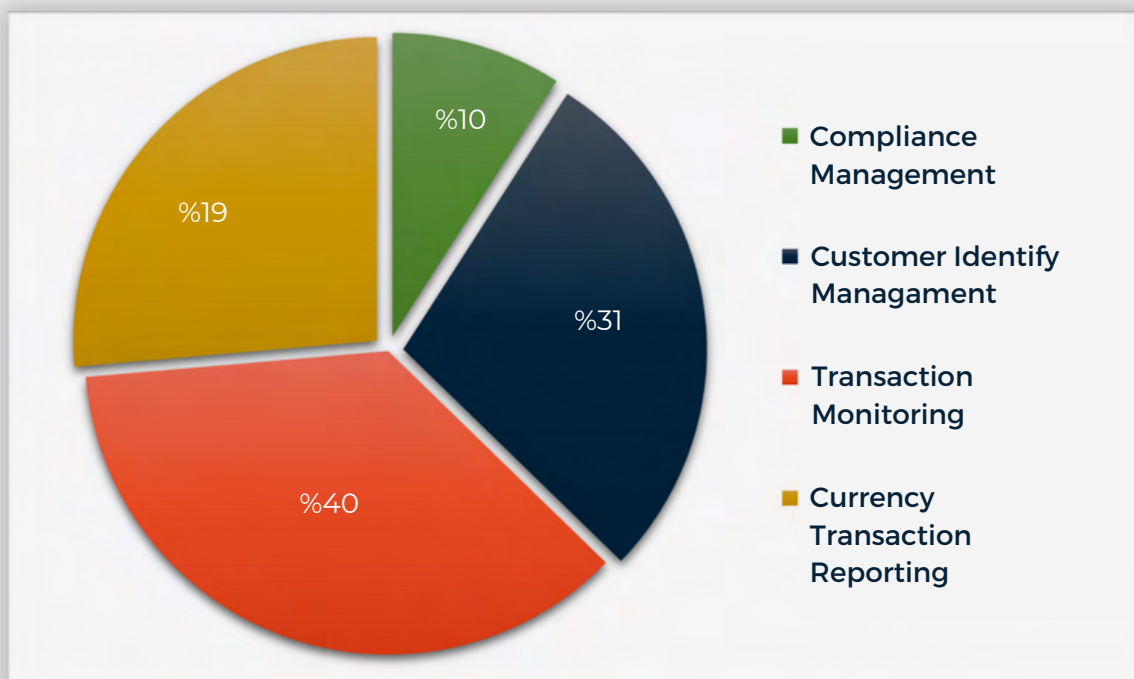
Technology-driven AML tools offer a unique advantage in keeping up with evolving regulatory requirements. They can be swiftly updated to align with new rules and guidelines, ensuring that organizations remain compliant. This adaptability is crucial in an environment where regulatory frameworks are constantly evolving.

## Empowering AML Professionals

Rather than replacing human expertise, these technological tools empower AML professionals to make more informed decisions. They provide valuable insights, streamline processes, and offer a level of precision that augments the capabilities of compliance teams. In essence, they become indispensable partners in the fight against financial crime.

## A Bright Future for Fight against Financial Crime

The integration of AI and automation into AML efforts is ushering in a new era of effectiveness and efficiency. These technological tools are not adversaries to regulatory frameworks; they are allies in the battle against financial crime. With their assistance, AML professionals are better equipped than ever to safeguard the integrity of financial systems and protect against illicit activities. For the future of AML, technology lights the way toward a more secure and compliant financial landscape.





# Survey Results

The survey, Sanction Scanner conducted, included different parts that serve the whole report. In terms of the dynamic world of digitalization and its impact on AML solutions, it demonstrated these insights:

## Satisfaction with Current AML Tools and Technologies

The majority of respondents reported being "somewhat satisfied" with the current AML tools and technologies available in the market. It implies that while these tools meet certain requirements, there may be opportunities for improvements to enhance overall satisfaction.

**41%**  
of users are  
"somewhat  
satisfied" with  
AML tools

## Control in In-House vs. Outsourced AML Systems

A significant number of respondents believe that both in-house and outsourced solutions have their advantages, indicating a balanced perspective. Organizations recognize the benefits of flexibility in choosing the most suitable approach for their specific needs.

**70%**  
believe both  
systems have  
their advantages

## Integration of AI and Automation

Respondents generally expressed support for the integration of AI and automation in AML processes, albeit with some reservations. This indicates an awareness of the potential benefits of these technologies while recognizing the importance of addressing any associated concerns, such as ethical and regulatory considerations.

**76%**  
supports the  
integration of AI  
& automation in  
AML processes

## Use of In-House vs. Outsourced AML Systems

The majority of respondents indicated that their organizations use a combination of in-house and outsourced AML systems. This approach likely reflects the need for a balance between internal control and leveraging the expertise of third-party providers.

**64%**  
both in-house  
and external  
systems are used



## Willingness to Adopt New Technologies

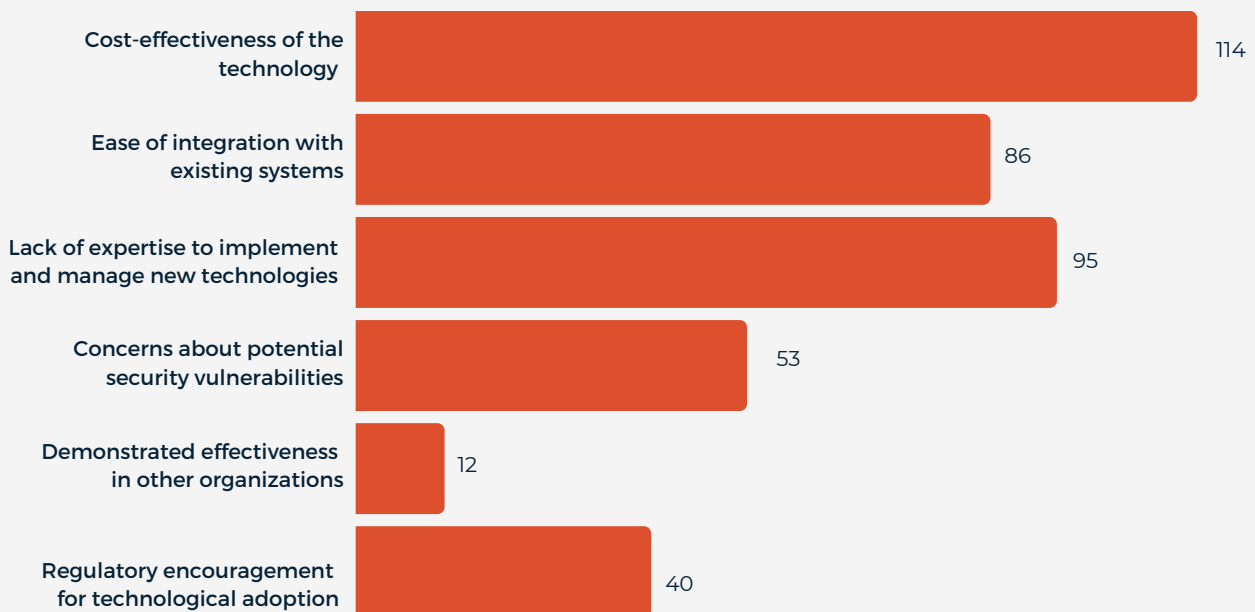
The most prevalent response suggests that organizations are generally unwilling to adopt new technologies for fraud prevention and AML, as they prefer existing methods and tools. The reluctance here could be due to concerns about the learning curve, potential disruption, or uncertainty about the benefits of adopting new technologies.

## Effectiveness of Existing AML Tools and Technologies


The most popular response indicates that respondents perceive their existing AML tools and technologies as "moderately effective." While these tools are providing some level of support, there might be room for improvement in enhancing their effectiveness to combat financial crime and money laundering more efficiently.

## Factors Influencing Technology Adoption for Fraud Prevention

Several factors were identified as influential in the decision to adopt new technologies for fraud prevention. These include ease of integration with existing systems, cost-effectiveness, and the lack of expertise to implement and manage new technologies. These findings underline the importance of not only the technology's capabilities but also practical considerations such as implementation ease and cost-effectiveness.



The survey results suggest that organizations are generally open to the idea of leveraging technology for AML and fraud prevention but are cautious about implementation and the effectiveness of existing tools. There's a need for further exploration of how to enhance the effectiveness of AML tools, address concerns related to technology adoption, and ensure that new technologies align with organizational goals and regulatory requirements.



Section 3

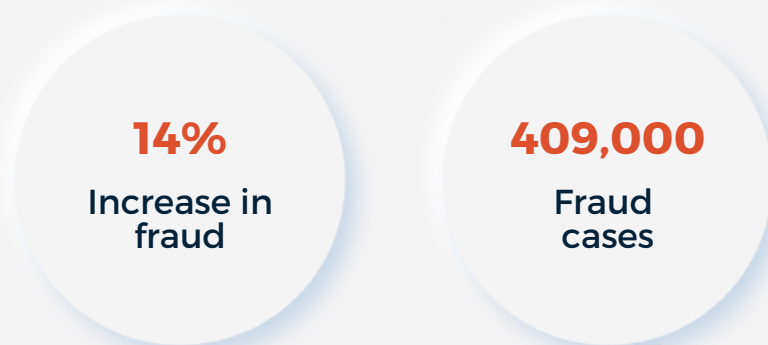
# The Shifting Landscape of Financial Fraud



# Navigating the Shifting Landscape of Financial Fraud

In an age characterized by digital transformation and interconnected financial systems, the battle against fraud remains a formidable challenge for the AML industry. As we navigate the intricate landscape of 2023, a comprehensive understanding of the evolving dynamics of fraud is paramount. This section of the AML Industry Annual Report explores the current landscape of fraud, revealing the tactics, trends, and vulnerabilities that define the present state of affairs.

In the complex world of financial crime, an in-depth understanding of the contemporary fraud landscape is essential for formulating effective strategies to combat it. As we delve into the AML Industry Annual Report, our focus is squarely on the state of fraud as it stands today. To gain comprehensive insight into this multifaceted issue, we turn to the data and insights garnered from 2022.



The year 2022 bore witness to an alarming surge in fraudulent activities, with the National Fraud Database (NFD) recording an unprecedented **409,000 cases**. This figure represents a disconcerting **14%** increase compared to the previous year, equating to a rise of **48,840 cases**. Even more concerning is the fact that this surge extends beyond the pandemic's influence, signifying a **12%** increase when compared to the pre-pandemic era. This resilience and adaptability of fraudsters highlight the ongoing challenge posed by this ever-evolving threat.

A particularly concerning revelation is that 68% of misuse of facility cases tied to bank accounts exhibited intelligence indicative of money mule activity. Individuals aged 21 to 25 continue to be prominently involved in these activities, with social media platforms serving as key facilitators for recruiting unwitting participants.





# Trends and Vulnerabilities in 2023

Cybercriminals continually evolve their tactics, posing ongoing challenges for defenders. Key trends and vulnerabilities this year include:

- **Rapid Attacks:** Cyberattacks occur **every 39 seconds**, demanding constant vigilance from organizations and cybersecurity professionals.
- **Ransomware Surge:** Ransomware attacks persist, especially targeting healthcare, highlighting the need for robust security and response strategies.
- **Email Risks:** A concerning **92%** of malware infections originate from email-based attacks, underscoring the urgency of enhancing email security.
- **Website Infections:** **4.1 million** websites harbor malware, necessitating regular security audits and hygiene practices.
- **Detection Delays:** Organizations take an average of **49 days** to identify ransomware attacks, emphasizing the need for improved detection and response capabilities.
- **Financial Consequences:** Cyberattacks result in substantial financial losses, exemplified by a hacker stealing **\$29 million** from a fintech company.
- **Plugin Vulnerabilities:** WordPress plugins are a common point of exploitation, contributing to **97%** of security breaches demanding better plugin management and security practices.
- **Cryptocurrency Risk:** Cryptocurrency theft remains persistent, with **\$3 billion** worth stolen in hacks this year, urging enhanced security measures.

These trends underline the ever-growing need for organizations to adapt and enhance their cybersecurity measures to stay ahead of cyber threats.

**\$3  
Billion**  
Worth of  
Cryptocurrency  
stolen

**4.1  
Million**  
Websites  
harbor  
malware



# Technology's Impact on Fraud

In an era where information travels fast and transactions occur in the blink of an eye, financial institutions and regulatory bodies find themselves facing a relentless tide of threats. These threats manifest in a variety of forms, from sophisticated cyberattacks that target digital infrastructures to subtle identity theft schemes that prey on individuals' personal information. The landscape is dynamic, marked by a constant arms race between those seeking illicit gains and those striving to safeguard the integrity of financial systems.

Staying ahead of fraudsters requires a combination of advanced technologies, collaboration, and adaptive strategies in the rapidly evolving landscape of financial fraud in 2023. Financial institutions and regulators must remain vigilant, continuously updating their anti-fraud measures to protect the integrity of the global financial system.

## The Importance of Preventing Identity Theft

In the ever-evolving landscape of crime, identity theft stands as a pervasive and formidable adversary, posing devastating consequences for individuals and organizations alike. As we navigate the complexities of the digital age, where personal information is incessantly exchanged through both online and offline channels, safeguarding one's identity has never been more critical.

Identity theft reached unprecedented levels, painting a picture of the current security landscape in 2023. According to the Federal Trade Commission (FTC), a staggering 5.7 million total fraud and identity theft reports were filed, with 1.4 million cases specifically related to identity theft. These numbers reflect a 23% increase in identity theft cases compared to the previous year, highlighting the escalation of this crime.

Government documents or benefits fraud emerged as the leading identity theft category in 2023, with 395,948 reported cases. Impersonation, particularly in the form of current address fraud, accounted for 74% of filing reasons, totaling 206,534 cases and marking a 16% increase from the previous year. A notable trend was the surge in false identities, with organizations reporting an 84% rise, driven by the increased use of synthetic identities.

**5.7  
Million**

Fraud and  
identity theft  
reports

**23%**

Increase in  
identity theft

**84%**

Rise in  
synthetic  
identities





## Online Channels: A Breeding Ground for Fraud

A staggering **86%** of identity fraud cases in 2023 occurred through online channels. However, the report also reveals a significant uptick in identity theft cases linked to retailers (a 132% increase) and dealers (a staggering 246% increase). These statistics suggest that threat actors are exploring new avenues to circumvent online identity verification controls, posing a unique challenge to security measures.

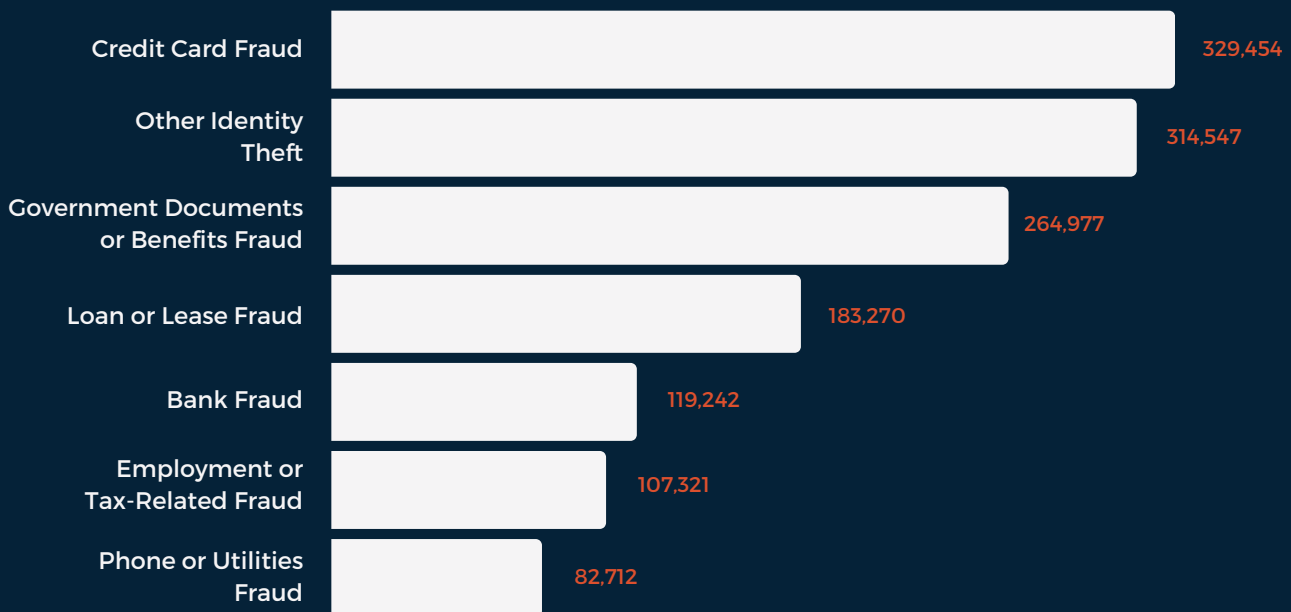
## Targets and Motivations

Identity thieves continued to target plastic cards, using stolen information to purchase goods that could be resold, contributing to the perpetuation of this crime. Additionally, identity fraud against telecom products witnessed a rise, where victim identities were exploited to purchase mobile phones for resale.

## Demographic Trends

The demographics of identity theft victims in 2023 paint a concerning picture. While individuals over the age of **31** were most commonly targeted, there were significant increases in cases involving those aged 61 and above. This suggests that identity thieves are indiscriminate in their choice of victims, targeting individuals across a wide age spectrum.

The surge in cases, the diversification of methods employed by threat actors, and the targeting of individuals across age groups call for urgent attention and enhanced security measures. As we continue to navigate the complex web of personal information exchange, it is imperative that individuals, organizations, and policymakers work collaboratively to mitigate the devastating consequences of identity theft and protect the identities of citizens in an increasingly interconnected world.



Source: Federal Trade Commission



# Evolving Threat Landscape of Cyber Attacks and Data Breaches

The battle between cyber criminals and defenders of data security rages on. The year 2023 has proven to be no exception, with an alarming number of data breaches and cyberattacks impacting organizations of all sizes and sectors.

Data breaches have become a common occurrence, and 2023 is no different. These incidents involve unauthorized access to an organization's data, often resulting in the theft or exposure of sensitive information. In the first three quarters of 2023 alone, a staggering **767 data** breaches have been reported. These breaches have compromised a total of 692,097,913 records, highlighting the magnitude of the issue.

One of the most notable breaches of the year targeted Twitter, where cybercriminals managed to breach the defenses of this tech giant, compromising 220 million user records. Such high-profile breaches serve as stark reminders that even industry leaders are not immune to the relentless persistence of cyber attackers.

## Sector-Specific Vulnerabilities

The cybersecurity landscape remains dynamic, with industries facing unique vulnerabilities.

### Healthcare: Ransomware Reigns

The healthcare sector is a prime target, with **125** reported breaches in the first quarter of 2022. Ransomware attacks are rampant, exemplified by incidents at New York-Presbyterian (NYP) Hospital and Aveanna Healthcare. India's healthcare industry also suffered, reporting **1.9 million** attacks by November 2022. Third-party breaches add to the concerns. The urgency for robust healthcare cybersecurity is evident.

**1.9  
Million**  
Cyber attacks  
in India

### Education: Battling Ransomware & Phishing

Education institutions faced nearly **2,000** attacks per week in 2022, primarily from ransomware groups. Latin America experiencing a **62%** surge in attacks. U.S. schools suffered data breaches affecting over **1 million** students, emphasizing the need for enhanced security.

**2000  
Attacks**  
Per week on  
educational  
institutions

**1,300%**

Increase in  
ransomware  
attacks

**95%**

Increase in Cyber  
attacks against  
governments

**43%**

of cyber  
attacks target  
SMBs

## Financial Services: Proliferation of Ransomware and Phishing

The financial sector saw a **1,300%** increase in ransomware attacks, coupled with a surge in phishing. Banking, insurance, payment, and e-money services are some of the sectors in this arena.

Weak authentication practices and threats like banking malware pose significant challenges. High-profile breaches, like the **\$29 million** Transit Finance incident, illustrate the gravity of the issue.

## Government: Escalating Cyber Threats

Governments faced a **95%** increase in cyberattacks in late 2022. Attacks on Vanuatu and a Colorado county highlighted vulnerabilities. Governments globally have incurred substantial losses to ransomware attacks. Proactive measures, such as cybersecurity training in Victoria, Australia, are crucial to prevent these attacks.

## Small Businesses: Neglecting Cybersecurity

Small and mid-sized businesses (SMBs) are not immune, with **43%** of all cyberattacks targeting them. However, only **26%** of SMBs prioritize cybersecurity surprisingly. Human error contributes to **52%** of SMB attacks, primarily through phishing. Financial implications are significant, with the average cost of an SMB cyberattack claim reaching **\$139,000**. Industries grapple with evolving cyber threats. Robust cybersecurity measures, employee training, and adaptability are imperative to combat these challenges effectively. Neglecting cybersecurity could result in severe consequences for organizations and individuals.





# Future Strategies and Technologies in Combating Financial Fraud

In this dynamic age of digital transformation and interconnected financial systems, the battle against financial fraud has intensified. As outlined in this report section, we have witnessed an alarming increase in fraudulent activity and identity theft. To effectively address these challenges, we must look ahead and embrace innovative strategies and technologies that can fortify our defenses against financial fraud in the years to come.

## Quantum-Resistant Encryption

Blockchain and DLT offer immutable and transparent transaction records, which can be a game-changer in fraud prevention. These technologies enhance the traceability of financial activities, making it more difficult for criminals to launder money or manipulate records. Smart contracts, powered by blockchain, can automate compliance checks and reduce the risk of fraudulent transactions. Moreover, the decentralized nature of blockchain reduces the vulnerability to single points of failure.

## Enhanced Email Security

The report highlights that a significant portion of cyberattacks originate from email-based phishing attempts. Therefore, enhancing email security is paramount. Advanced email filtering technologies, AI-powered threat detection, and robust user education programs can help organizations thwart phishing attacks and protect their networks and sensitive information.

## Blockchain and Distributed Ledger Technology (DLT)

Blockchain and DLT offer immutable and transparent transaction records, which can be a game-changer in fraud prevention. These technologies enhance the traceability of financial activities, making it more difficult for criminals to launder money or manipulate records. Smart contracts, powered by blockchain, can automate compliance checks and reduce the risk of fraudulent transactions. Moreover, the decentralized nature of blockchain reduces the vulnerability to single points of failure.

## Remote Work and Cybersecurity Challenges

The shift to remote work has raised concerns in the cybersecurity landscape, with 74% of IT experts considering it an extreme threat to cybersecurity. Secure remote work solutions and comprehensive employee training are imperative to mitigate these risks effectively.



## Real-Time Cyber Threat Intelligence Sharing

In response to the escalating sophistication of fraudsters, financial institutions are turning to advanced machine learning and artificial intelligence (AI) solutions. These technologies can analyze vast datasets and detect subtle patterns indicative of fraudulent behavior. Moreover, AI-driven behavioral analytics continuously monitor user interactions and can flag anomalies, helping to identify potentially fraudulent activities in real-time. By investing in and refining these technologies, organizations can stay one step ahead of evolving fraud tactics.

## Advanced Machine Learning and AI-Based Behavioral Analytics

In response to the escalating sophistication of fraudsters, financial institutions are turning to advanced machine learning and AI solutions. These technologies can analyze vast datasets and detect subtle patterns indicative of fraudulent behavior. Moreover, AI-driven behavioral analytics continuously monitor user interactions and can flag anomalies, helping to identify potentially fraudulent activities in real time. By investing in and refining these technologies, organizations can stay one step ahead of evolving fraud tactics.

## Biometric Authentication and Verification

Identity theft continues to be a significant concern, especially in 2023, in which there has been a notable increase in cases, especially related to government documents and benefits fraud. According to research conducted by Sanction Scanner, the primary concern among people is identity theft when it comes to fraud threats. To combat this, financial institutions are increasingly adopting biometric authentication methods, such as facial recognition, fingerprint scanning, and voice recognition. These technologies enhance identity verification processes, making it significantly more challenging for fraudsters to impersonate individuals.

## Investment in Cybersecurity

In response to the growing threat landscape, it is encouraging to note that 66% of Chief Information Officers (CIOs) are planning to increase investment in cybersecurity. This reflects the recognition of the need for proactive security measures to combat the ever-evolving nature of financial fraud.

As we navigate the intricacies of financial fraud in 2023, it is imperative that the AML industry remains proactive and forward-thinking. Embracing these tailored strategies and technologies, along with heightened investment in cybersecurity and a focus on remote work security, will empower us to address the specific challenges outlined. Vigilance, investment in security measures, and employee education are key elements in the ongoing battle to protect sensitive data and critical systems from cyber threats.



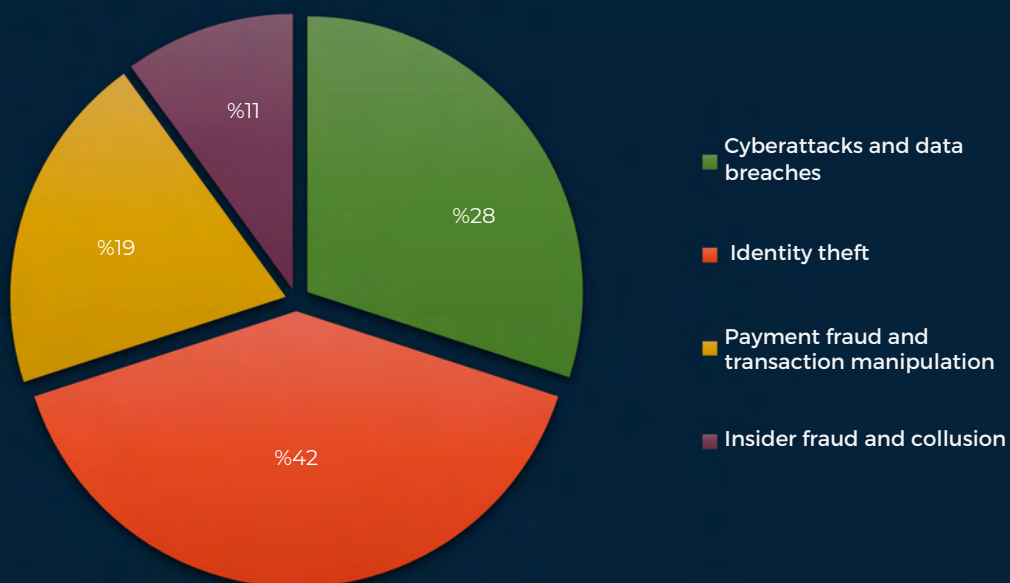
# Survey Results

With over 400 participants contributing their perspectives, our survey provides a comprehensive view of the current state of fraud and financial crime threats and the strategies employed by organizations to combat them.

## Pressing Fraud and Financial Crime Threats

Respondents were asked to identify the most pressing fraud and financial crime threats in 2023. The standout concern that emerged from our survey results was "identity theft", reflecting the paramount importance of addressing this specific threat in the current landscape. Additionally, respondents also highlighted other significant threats, including cyberattacks and data breaches, payment fraud and transaction manipulation, as well as insider fraud and collusion.

**Identity theft**  
is the biggest concern



## Influence of Technology on Fraud

In this question, respondents were queried about how advancements in technology have influenced the sophistication and frequency of fraudulent activities. The majority of respondents indicated that technology has led to increased sophistication and frequency of fraudulent activities. This underscores the need for organizations to continually adapt their defenses to combat technologically savvy adversaries.



**Rapidly  
evolving fraud  
techniques  
are the biggest  
challenge**

## Challenges in Detecting and Mitigating Fraud

Respondents were asked about the primary challenges organizations face in detecting and mitigating fraud. The most commonly selected challenges included rapidly evolving fraud techniques, insufficient fraud detection tools, and employee collusion or insider threats. These findings emphasize the need for continuous improvement in fraud detection capabilities.

## Effectiveness of Reporting and Investigation

Respondents expressed varying levels of confidence in the effectiveness of fraud incident reporting, investigation, and resolution within their industries. The majority of respondents suggested that there is room for improvement in this regard.

## Emerging Trends in Fraud

A significant number of respondents reported observing new or emerging trends in fraudulent activities. While some indicated only minor variations from previous trends, these observations highlight the dynamic nature of fraud and the importance of staying informed about evolving threats.

## Employee Training and Awareness

Regarding the awareness and training provided by organizations to their employees on fraud prevention and reporting, the survey showed that many respondents believe there is a need for greater emphasis on training and awareness programs.

**There's room  
to improve  
fraud reporting**

**The dynamic  
nature  
should be  
observed**

**More training  
Less fraud**



## Promising Strategies and Technologies

Survey participants identified several promising strategies and technologies for enhancing fraud detection and prevention in the future. These included enhanced data analytics and profiling, real-time transaction monitoring systems, and strengthened industry collaboration and information sharing. These insights can guide organizations in their efforts to bolster their anti-fraud measures.

## Industry-Specific Vulnerabilities


When it comes to industry-specific vulnerabilities contributing to higher fraud rates, the survey revealed that a significant number of respondents believe vulnerabilities are high, but organizations are inadequately prepared. This highlights the importance of tailoring fraud prevention measures to address specific industry challenges.

## Awareness of Regulatory Measures

The survey showed a range of awareness levels regarding current regulatory measures to deter and prevent fraud within the financial sector. Many respondents expressed some awareness but were unsure about their effectiveness, indicating a need for greater clarity and education regarding regulatory compliance.

The survey results show that organizations must remain adaptable, prioritize employee training and awareness, and explore innovative strategies and technologies to stay ahead of increasingly sophisticated fraudulent activities. Additionally, regulatory clarity and industry collaboration are essential components of a robust defense against fraud and financial crime.





# Section 4

## Cryptocurrencies



# Cryptocurrencies

The year 2023 unfolds as a pivotal moment in the global financial arena, with cryptocurrencies assuming a central role in the ongoing battle against financial impropriety and the pursuit of robust regulatory adherence. The rapid rise of cryptocurrencies, starting with Bitcoin and followed by many other digital coins, has not only caused significant changes in traditional financial systems but has also brought about new challenges and opportunities in the realm of combating financial misconduct and ensuring regulatory compliance.

These digital assets have attracted attention not only for their potential to transform the financial landscape but also for their vulnerability to exploitation by individuals with illegal intentions. They leverage the inherent anonymity and decentralized nature of cryptocurrencies to nefarious ends.

In an era where technological leaps often outpace the establishment of regulatory frameworks, businesses navigate a labyrinth of compliance requirements to foster trust and credibility both among investors and regulatory authorities.



Simultaneously, the cryptocurrency sphere experienced a surge in active addresses, doubling over the past two years to reach an astounding 15 million. This remarkable growth owes itself to a diverse array of applications and services, including on-chain games, which provide users with innovative avenues for engagement.

Decentralized Finance (DeFi) and Non-Fungible Tokens (NFTs) activities have embarked on a resurgent journey, with an increasing number of individuals engaging in NFT purchases and monthly trading volumes exceeding \$100 billion on decentralized exchanges. This marks the third consecutive month of positive growth in trading volume.

In this dynamic and transformative landscape, the cryptocurrency revolution is redefining the financial world, prompting a call to action for vigilance, adaptability, and proactive compliance efforts from all stakeholders.

**15 Million**  
active  
addresses

## Connection Between Cryptocurrencies and Money Laundering

Cryptocurrencies have emerged as a transformative force in the financial world, offering numerous legitimate advantages, including fast, cost-effective, and globally accessible payment systems. They also hold the promise of providing financial services to the unbanked populations around the world. However, this innovative financial landscape is not without its challenges, as cryptocurrencies can also be misused by individuals with illicit intentions.

Cryptocurrencies have gained notoriety as a preferred tool for money launderers due to several key factors that facilitate illicit financial activities. Understanding this connection is essential for regulatory authorities, financial institutions, and law enforcement agencies. These are some of the critical factors that contribute to this association:

- **Pseudonymity and Anonymity:** Cryptocurrencies offer a degree of pseudonymity, allowing users to transact without revealing their real-world identities. While this enhances privacy and security, it also creates an ideal environment for money launderers to hide their illicit gains through multiple addresses and mixers.
- **Global and Borderless Nature:** The decentralized nature of cryptocurrencies enables cross-border transactions without intermediaries like banks. Criminals exploit this feature to move funds rapidly across jurisdictions, making it challenging for law enforcement to track them.





- **Lack of Central Oversight:** Cryptocurrencies operate independently of central authorities, avoiding traditional regulatory controls. This absence of centralized oversight can attract individuals seeking to evade detection and regulation while engaging in money laundering activities.
- **Crypto Exchanges and Mixing Services:** Cryptocurrency exchanges and mixing services can unintentionally or intentionally aid in money laundering. Weak AML/KYC procedures on some exchanges enable criminals to convert illegal gains into cryptocurrencies. Mixing services further obscure the source of funds by blending them with those of other users.
- **Regulatory Gaps:** The rapidly evolving nature of cryptocurrencies has created regulatory gaps in some jurisdictions, leaving room for exploitation by money launderers due to inconsistent or inadequate regulations.
- **Complex Transaction Structures:** Money launderers often employ intricate transaction structures that involve multiple wallets, cryptocurrencies, and exchanges to obscure the origins of illicit funds, making it challenging for investigators to follow the money trail.
- **Use of Privacy Coins:** Privacy-focused cryptocurrencies like Monero and Zcash provide enhanced anonymity features, making tracing transactions and wallet balances nearly impossible. Criminals may prefer these privacy coins to further shield their financial activities.
- **Cybercrime and Ransomware:** Cryptocurrencies are often used in cybercrime activities, such as ransomware attacks. Criminals demand ransoms in cryptocurrencies, making it challenging for victims to track payments and law enforcement to recover stolen funds.



To combat the connection between cryptocurrencies and money laundering effectively, regulatory bodies and law enforcement agencies worldwide are working to establish robust AML/KYC regulations, enhance transaction monitoring, and foster cooperation between cryptocurrency businesses and traditional financial institutions. This evolving landscape demands vigilance and adaptability, as staying ahead of money laundering threats remains a top priority for the financial industry and regulators alike.



# Cryptocurrency Risks

While digital assets have gained significant popularity, they are not without their risks. The risks associated with cryptocurrencies are multifaceted and encompass a range of factors that individuals, investors, and regulatory authorities should consider. These are some of the key risks associated with cryptocurrencies:

According to the Global Finance Execs which of the following will be the biggest issue to crypto currency adaption.



## – Security and Custody Risks

Security breaches, hacks, and vulnerabilities in crypto wallets and exchanges pose significant risks. Users are responsible for safeguarding their private keys, with varying degrees of custody options.

## – Evolving Regulatory Landscape

Government regulations around cryptocurrencies vary significantly across jurisdictions and continue to evolve. The legal landscape can change rapidly, impacting the use, taxation, and legality of cryptocurrencies.



## – Market Volatility and Its Implications

Cryptocurrencies, as a whole, are a young and emerging market, resulting in unusually high price volatility. Factors contributing to dynamic price movements include the 24/7 nature of crypto trading and the influence of global news and social media. The rapid price swings can attract both legitimate investors and speculators while also creating opportunities for market manipulation and fraud.

## – Privacy, Transparency, and Transaction Risks

Cryptocurrency transactions are recorded on public ledgers, offering transparency but also challenging user privacy. Users' wallet addresses and transaction details may be visible, potentially compromising anonymity. Transaction privacy concerns can affect compliance with AML and KYC regulations.

## – Scams, Fraud, and Phishing Risks

The cryptocurrency space is rife with scams, fraudulent projects, and phishing attempts. Users must exercise caution, conduct due diligence, and stay vigilant against potential fraud.

## – Smart Contracts and Code Vulnerabilities

Smart contracts on blockchain platforms introduce potential coding errors or malicious code. Flawed smart contracts can lead to financial losses and disputes.

## – Taxation, Reporting, and Compliance Obligations

Taxation of cryptocurrencies is a complex and evolving area, with compliance challenges. Individuals and businesses must navigate tax obligations related to crypto transactions. Adherence to tax laws and reporting requirements is crucial for regulatory compliance.





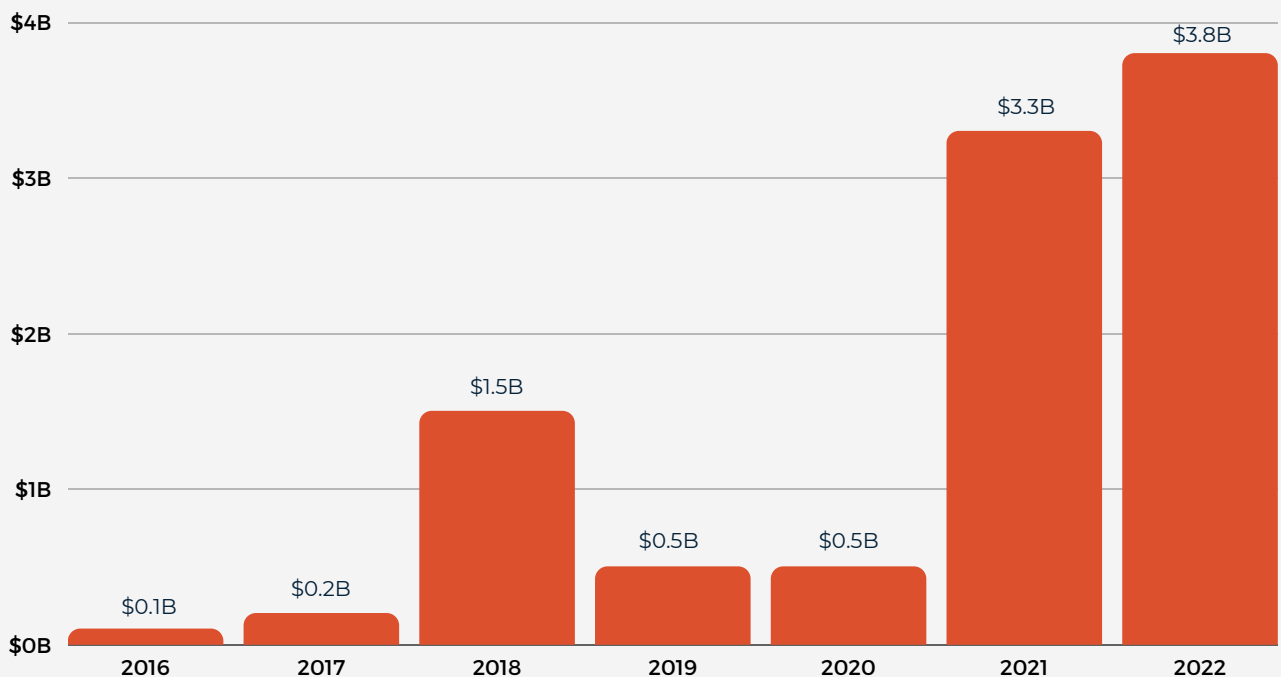
# AML & KYC Regulations in the Crypto Industry

The cryptocurrency landscape, characterized by its rapid growth and decentralized nature, has captured the attention of both legitimate users and malicious actors looking to exploit its anonymity for illicit purposes. To combat these threats, governments and regulatory bodies worldwide are intensifying their efforts to enhance AML and KYC regulations, bolstering the safety and integrity of the crypto industry.

## The Crucial Role of AML and KYC Compliance in Crypto

While the crypto industry has undoubtedly brought innovation and opportunities, it has also witnessed a surge in fraudulent activities and financial crimes. In 2022 alone, approximately **\$3.8 billion** was stolen through crypto-related scams, with billions more being funneled into various criminal enterprises. On the other hand, effective AML and KYC procedures serve as a powerful deterrent, making it significantly more challenging for bad actors to exploit cryptocurrencies for illegal purposes.

Total Value Stolen in Crypto Hacks , 2016-2022



Source: Chainalysis

In the United States, the OFAC considers AML non-compliance a grave risk to national security. This failure opens the door to money laundering, which not only has adverse effects on economies but also bolsters criminal activities. Consequently, the sanctions for non-compliance are substantial, encompassing million-dollar criminal fines and prison sentences per violation.

Within the European Union, under the 5AMLD, fiat-to-crypto exchanges and custodian wallets that do not adhere to AML regulations may face fines of up to **€200,000** per violation.



## Why Do Crypto Companies Need KYC and AML Compliance?

The implementation of AML and KYC regulations in the crypto industry serves several critical functions:

- 1. Preventing Illicit Activities:** The surge in cryptocurrency-related scams and money laundering cases underscores the urgency of robust AML and KYC procedures. These regulations act as a formidable barrier, dissuading criminals from using cryptocurrencies for illegal activities.
- 2. Building Trust:** KYC procedures establish a foundation of trust between users and crypto service providers. Customers can be confident that their data and funds are secure, while potential malevolent users are discouraged from engaging with KYC-compliant platforms.
- 3. Reducing Identity Theft:** AML regulations, enforced by identity verification providers, are instrumental in detecting and thwarting fraudsters who attempt to employ fake or stolen identities to infiltrate crypto platforms and launder ill-gotten funds.
- 4. Ensuring Regulatory Compliance:** Failure to adhere to AML and KYC regulations can result in substantial fines and legal repercussions. Compliance safeguards crypto businesses from governmental risks and ensures their long-term viability.

## Recent AML Regulatory Changes in Key Regions

### AML Regulatory Changes in the EU

The EU has taken significant strides in AML regulation with its AML Package, consisting of four key legislative pieces. As of March 28, 2023, the EU Parliament committees voted on crucial components, including the Anti-Money Laundering Regulation (AMLR), the 6th AML Directive (6AMLD), and the AML Authority Regulation (AMLAR). These new laws place a strong emphasis on the cryptocurrency sector, mandating that Virtual Asset Service Providers (VASPs) implement AML/KYC procedures, prohibit anonymous accounts, set thresholds for crypto transfers, and introduce the Travel Rule for VASPs. Notably, AML requirements also extend to Decentralized Autonomous Organizations (DAOs) and DeFi arrangements if they offer crypto-asset services.





### AML Regulatory Changes in the US

In the United States, the Anti-Money Laundering Act, 2020 (AMLA) has introduced significant changes to AML frameworks. This legislation addresses asset classes like cryptocurrency, requiring VASPs to identify the UBOs of client companies and assess their risk profiles, particularly when dealing with shell companies. VASPs must also periodically update client information to monitor evolving risks during ongoing client relationships. Robust CDD and KYC procedures are now mandatory.

### AML Regulatory Changes in the UK

The UK's AML regulations closely align with the EU's 6th AML Directive. FCA enforces regulations such as the Travel Rule, which mandates the relay of information for transactions exceeding **€1,000**. Transactions with incomplete information must be delayed until all requirements are met. The FCA's strict oversight has positioned the UK as one of the safest jurisdictions for cryptocurrency users. Upcoming regulations will necessitate licensing for firms involved in various crypto-related activities, with specific registration required for cryptocurrency exchange, custody, and intermediation.

Threshold is  
**1,000 Euros**

## Impact of Strengthened AML and KYC Regulations

The implications of these regulatory changes are far-reaching, benefiting both users and crypto businesses:

- **Enhanced User Confidence:** Users can engage with cryptocurrencies confidently, knowing that the origins of their digital assets are secure and that stringent CDD and KYC procedures are in place to filter out wallets linked to illegal activities.
- **Reduced Risks for Crypto Businesses:** Compliance with enhanced AML procedures and controls minimizes the risk of illicit activities occurring on crypto platforms. Increased transaction transparency facilitates the detection and prevention of criminal activities, safeguarding the reputation of crypto businesses and engendering trust among users.





## Strategies for Effective AML and KYC Compliance

To navigate these evolving regulatory landscapes effectively, crypto businesses should:

- 1. Comprehensive Understanding:** Thoroughly comprehend the AML and KYC regulations applicable in their jurisdiction.
- 2. Professional Guidance:** Seek professional assistance to interpret and establish AML policies and procedures that encompass CDD and KYC architecture, risk assessments, and continuous transaction monitoring.
- 3. Resource Allocation:** Allocate resources for technology, personnel, and automation to ensure seamless compliance.
- 4. Monitoring and Reporting:** Implement robust systems for monitoring and reporting suspicious transactions, guaranteeing transparency and cooperation with relevant authorities.
- 5. Employee Education:** Train employees to prevent compliance breaches due to negligence, ensuring that they are well-versed in compliance protocols.



## Lessons Learned from Recent Non-Compliance Cases

### The Tornado Cash Case

In 2022, the US government penalized Tornado Cash for its involvement in money laundering, accusing the crypto mixer of laundering \$7 billion worth of virtual currencies. This resulted in the founder's imprisonment. Some of the laundered money had been stolen by a group of hackers supported by the North Korean government, further highlighting the crypto business's use in cleaning money from hacking attacks.

**\$7 billion**  
worth of virtual  
currency  
laundering

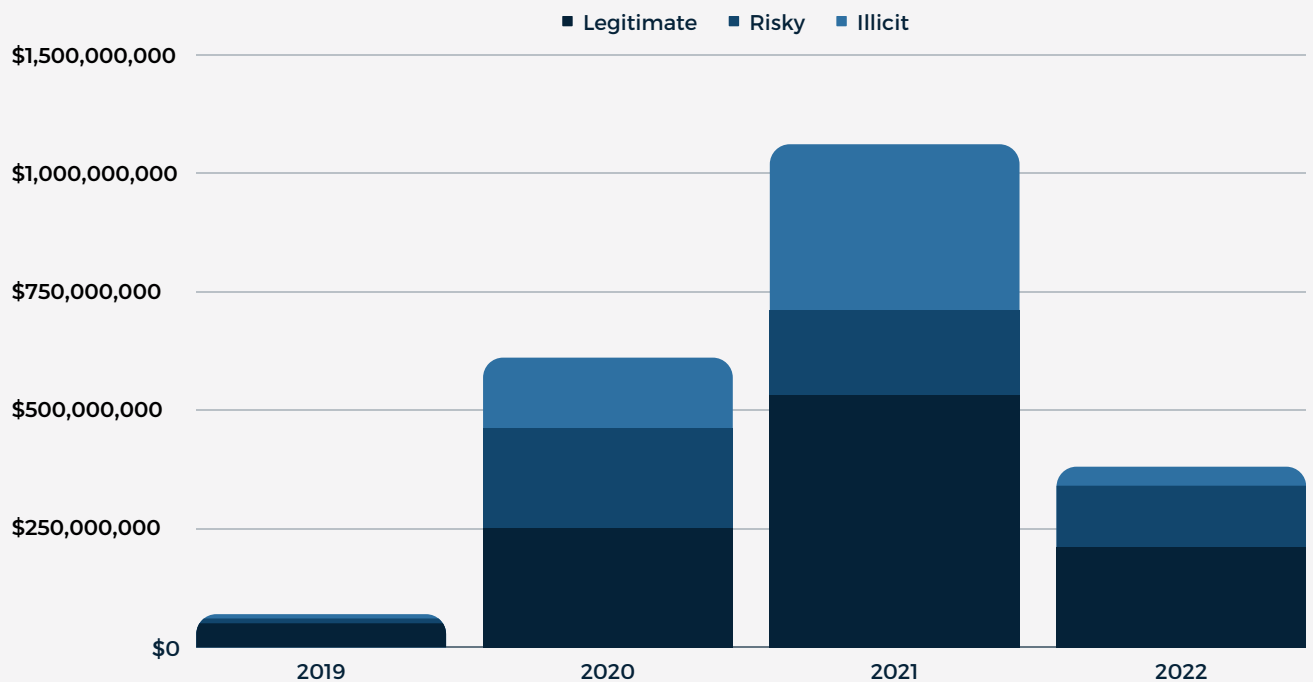


## The Bitzlato Case

In a recent case, Bitzlato, a cryptocurrency firm, faced severe legal consequences when its owner and key shareholders were charged with processing **\$700 million** in illicit funds. The main contributing factor was deficient KYC procedures, which allowed criminals to launder money from drugs and ransomware with ease.

**\$700 M**  
in illicit funds

Yearly cryptocurrency value received by Bitzlato by source: Legitimate, Risky, and Illicit by Year 2019-2022.



Source: Chainalysis

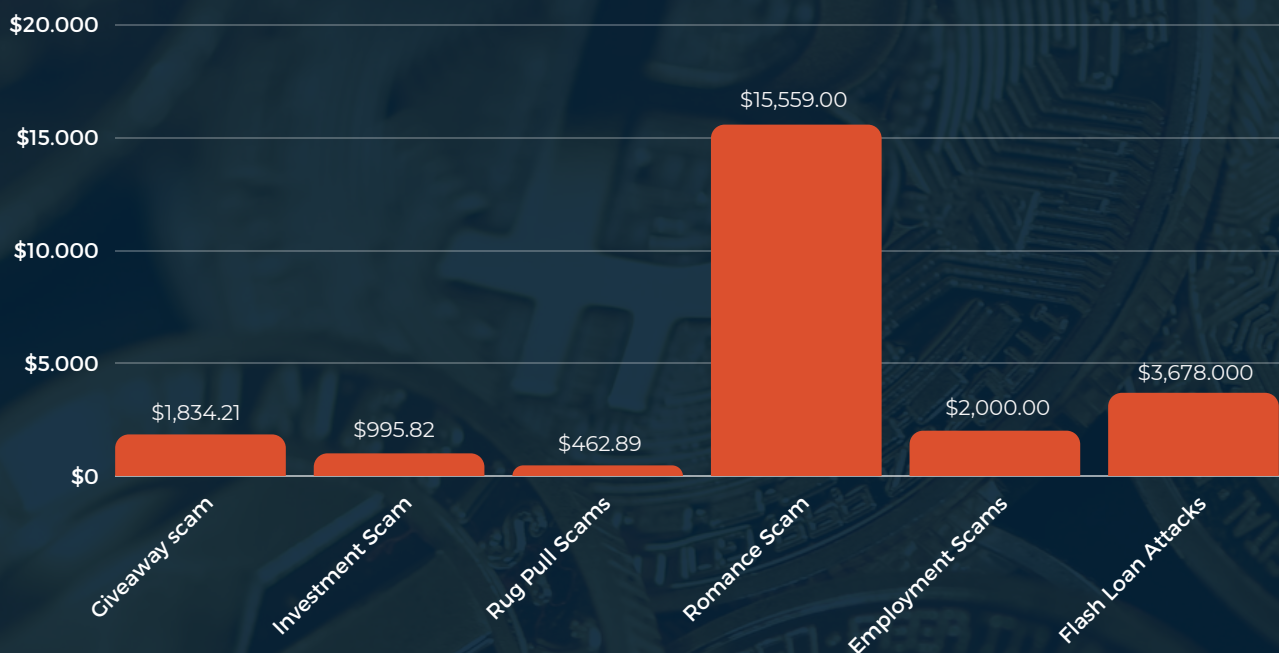
These real-life examples underscore the imperative role of robust AML and KYC procedures in preventing illicit financial activities and protecting the integrity of the cryptocurrency industry. As regulatory bodies continue to refine and strengthen these regulations, crypto businesses must adapt and prioritize compliance to ensure a secure and successful future for the digital asset ecosystem.



# The Future of Cryptocurrency in 2024

The cryptocurrency landscape is poised for another year of significant change and evolution in 2024, as governments and regulatory bodies worldwide continue to grapple with the challenges and opportunities presented by digital assets. As the crypto market matures and gains wider adoption, the need for effective regulatory oversight becomes increasingly apparent.

Average victim deposit size by scam type, 2022



## Rug Pull Scams

Fraudsters manipulate the value of new projects, NFTs, or coins to attract investments, only to disappear once they have secured funds. These scams can leave investors with valueless assets.

## Romance Scams

Dating apps have become breeding grounds for online romance scams, where perpetrators build trust with victims before convincing them to invest in cryptocurrency. Once the funds are transferred, the scammer vanishes.

## Bitcoin Investment Schemes

Scammers posing as experienced investment managers entice investors with the promise of substantial returns. They often request an upfront fee and personal identification information, ultimately stealing both funds and sensitive data.

## Phishing Scams

Despite being a longstanding threat, phishing scams remain prevalent. Scammers send deceptive emails with malicious links, aiming to steal cryptocurrency wallet keys and personal information.



### Man-in-the-Middle Attacks

Public Wi-Fi networks can be vulnerable to man-in-the-middle attacks, where sensitive information, including cryptocurrency wallet keys, can be intercepted. Using virtual private networks (VPNs) is crucial to thwarting these attacks.

### Social Media Cryptocurrency Giveaway Scams

Fraudulent posts on social media platforms promise Bitcoin giveaways, often featuring fake celebrity endorsements. Victims are lured into verifying their accounts through payments, leading to financial losses and data theft.

### Fake Cryptocurrency Exchanges

Deceptive exchanges promise lucrative deals but disappear once they receive deposits. Sticking to reputable exchanges is key to avoiding these traps.

### Employment Scams

Scammers impersonate recruiters or job seekers, enticing victims with job opportunities that require cryptocurrency payments. This approach can lead to both financial losses and data breaches.

### Flash Loan Attacks

Flash loans, a popular feature in DeFi, are vulnerable to attackers manipulating prices for profit. Such attacks can result in substantial losses, as seen in the Platypus Finance case.

### Ponzi Schemes

Scammers lure investors with promises of high profits, relying on funds from new investors to pay older ones. These schemes are inherently risky and unsustainable.

## Enhanced Taxation & Reporting Requirements

Taxation in the cryptocurrency world is an area that has been evolving rapidly. In 2024, we can anticipate more comprehensive tax regulations aimed at ensuring that cryptocurrency transactions are properly reported and taxed. Governments are keen to capture revenue from the crypto sector, and as a result, tax authorities are becoming increasingly determined in their tracking of crypto-related income and gains.

Cryptocurrency users should expect stricter reporting requirements, and tax agencies are likely to collaborate more closely with exchanges to obtain transaction data. This shift underscores the need for crypto enthusiasts to maintain accurate records and adhere to tax obligations diligently.

More  
comprehensive  
**tax**  
regulations



## Stricter KYC Regulations on the Horizon

One of the prominent trends in the future of cryptocurrency regulations is the strengthening of KYC procedures. KYC requirements are not new in the financial sector, but they are gaining more prominence in the crypto world due to the surge in money laundering activities on both centralized and decentralized platforms.

| 52

Regulatory authorities recognize that cryptocurrencies, which can serve as financial instruments and stores of value, have become a breeding ground for malicious activities. To combat these threats and protect customer funds, regulators are extending KYC obligations to encompass blockchain services and Virtual Asset Service Providers (VASPs). This expansion means that not only will users need to verify their identities, but transaction details and the parties involved may also come under scrutiny.



## Balancing Privacy and Compliance

The delicate balance between user privacy and regulatory compliance will remain a central theme in 2024. While regulators seek transparency and accountability, many cryptocurrency users value the anonymity and decentralization inherent in digital assets. Innovations like Zero-Knowledge Proofs (ZK proofs) and privacy-focused cryptocurrencies aim to address this challenge by allowing users to maintain privacy while still complying with regulatory requirements.

The success of these solutions in striking this balance will be closely monitored and could influence the direction of future regulations. It's expected that regulators will increasingly engage with blockchain developers and experts to find practical ways to reconcile privacy and compliance.

# Survey Results

The survey has yielded valuable insights into the awareness and perceptions surrounding cryptocurrencies and their potential involvement in money laundering activities. It reached a diverse audience, including individuals with varying degrees of familiarity with cryptocurrency and financial regulations. Here are the key findings:

## Awareness of Cryptocurrency-Money Laundering Connection

A significant portion of respondents indicated that they were "somewhat aware" of the connection between cryptocurrencies and potential money laundering activities. This suggests that there is a notable level of recognition of this connection, but further information and education are still needed for many.

## Familiarity with AML and KYC Regulations

A prevalent response was that respondents were "moderately familiar" with the AML and KYC regulations applicable to cryptocurrency transactions in their respective regions. While many have some knowledge in this area, there remains uncertainty resulting from the need for new regulations and explanatory guidance.

## Encounters with Non-Compliance

A notable number of respondents reported having encountered a few cases where cryptocurrency platforms failed to comply with AML regulations. It indicates that there is room for improvement in compliance within the cryptocurrency industry.

## Perceived Risk of Cryptocurrency for Money Laundering

The majority of respondents believed that cryptocurrencies pose a moderate risk for money laundering and other illicit financial activities. This view reflects a common perception that while there are risks associated with cryptocurrencies, they may not be as high as some other financial channels.





## Encounters with Non-Compliance

A notable number of respondents reported having encountered a few cases where cryptocurrency platforms failed to comply with AML regulations. It indicates that there is room for improvement in compliance within the cryptocurrency industry.

## Importance of AML and Transaction Monitoring Systems

A notable number of respondents reported having encountered a few cases where cryptocurrency platforms failed to comply with AML regulations. It indicates that there is room for improvement in compliance within the cryptocurrency industry.

## Experience with Crypto Scams or Frauds

A significant number of respondents who work in cryptocurrency-related roles reported having experienced crypto scams or fraud attempts. This highlights the vulnerability of individuals within the industry to fraudulent activities.

## Awareness of Suspicious Activity Signs

The most common response to awareness of signs of suspicious activities in cryptocurrency transactions was "somewhat aware but could use more guidance." In this case, there is a need for further education and training in recognizing suspicious activities.

The results underscore the evolving landscape of cryptocurrency and its connection to money laundering concerns. While there is a general awareness of the risks associated with cryptocurrencies, there is also a need for greater education and clarity regarding regulations and suspicious activity recognition. It is evident that robust AML measures are considered crucial in the cryptocurrency industry, and addressing compliance challenges remains a priority for stakeholders. As cryptocurrencies continue to gain prominence in the financial world, efforts to enhance security and compliance should also evolve to mitigate potential risks effectively.







Section 5  
Regional Trends  
on FinCrime,  
AML & Fraud



# Regional Trends on FinCrime, AML & Fraud

## Asia-Pacific



### Beneficial Ownership Transparency

The "Financial Crime Compliance (FFC) Asia 2023" event emphasized challenges in advancing beneficial ownership transparency in Asia. This indicates a growing awareness of the need for transparency in financial transactions to combat money laundering. Beneficial ownership transparency involves identifying the individuals who ultimately control or benefit from a company. In the context of this event, discussions revolved around the importance of accurate reporting and how it contributes to anti-money laundering efforts.

### Leveraging AML Measures for Tax Improvement

The International Monetary Fund (IMF) explores the potential of using AML measures to enhance tax collection. This approach suggests a multifaceted strategy to address financial issues. By leveraging AML measures, countries can improve their ability to track financial transactions, identify tax evasion, and reduce illicit financial flows. This initiative aims to strengthen fiscal governance and enhance revenue collection.

## Fraud & Financial Crime Focus

Financial crime and AML in Asia present pressing challenges, reflecting global trends. The surge of scams and fraud in the region has evolved into a sophisticated and industrialized threat that demands immediate attention. Asian financial institutions are responding by merging fraud and AML departments into "FRAML" units and exploring technological solutions, like analytics-driven payment data overlays, for fraud detection. Collaboration with technology companies and international cooperation are vital components of combating financial crime in Asia. Additionally, challenges related to asset recovery mechanisms, the alignment of sanctions with AML efforts, and the increasing concern about environmental crime underscore the complexity of the financial crime landscape in the region. A comprehensive approach and international collaboration are essential to address these issues effectively.

## Financial Crime Market Outlook

### — Rising Authoritarianism and Declining Democracy

Authoritarian governments in various Asia-Pacific countries prioritize economic recovery over anti-corruption efforts. Additionally, countries like the Philippines, Bangladesh, and India have seen declining democracy with restrictions on free speech. This rise in authoritarianism and decline in democracy exacerbate human rights violations and financial crime, requiring governments to ensure citizen voices are heard, and organizations to conduct robust risk assessments.

### — Corruption Perceptions Index (CPI) and Anti-Money Laundering Measures

Transparency International's 2022 CPI revealed high corruption levels in countries like Afghanistan, Cambodia, Myanmar, and North Korea. The Philippines faces increased monitoring by the Financial Action Task Force (FATF) due to deficiencies in countering money laundering and terrorist financing. The implications include increased financial crime and risks for organizations operating in these regions.

### — Wildlife Trafficking

Illegal wildlife trafficking is a major international crime. It is widely emphasized in the industry that the need for increased cooperation and enforcement measures to combat this issue has become more crucial recently.

### — Forced Labor

The Asia-Pacific region has the highest number of people in forced labor globally. Authorities suggest recognizing high-risk areas and conducting extensive risk analysis audits to avoid exploitative practices within supply chains.

### — Hong Kong's AML/CTF Legislation Amendments

Hong Kong has made amendments to its AML/CFT legislation to align with the FATF standards, enhancing the region's status as an international financial center.





## Europe and the United Kingdom



The year 2023 was a pivotal moment in the fight against financial crime in Europe and the UK. With a renewed focus on AML compliance, and a concerted effort to regulate the rapidly evolving world of cryptocurrency, this year saw significant progress in the ongoing battle against fraud and corruption. Throughout the year, policymakers and industry leaders alike worked to address new trends in financial crime, while navigating the complex and ever-changing landscape of digital assets. From enhanced AML regulations to innovative new approaches to fraud detection, the developments of 2023 have laid the groundwork for a more secure and transparent financial future. In this section of the report, we will explore the key highlights of these groundbreaking initiatives and examine how they have reshaped the financial landscape in Europe and the UK for years to come.

In 2023, the Financial Conduct Authority (FCA) placed a paramount emphasis on combating financial crime, aligning with its core priorities. It recognized the dynamic nature of financial crime and adopted a proactive stance across various aspects of the financial landscape. The FCA's expectations were clear: firms were required to establish robust governance, effective procedures, and internal mechanisms to manage financial crime risks. These mechanisms were not to remain static but evolve in tandem with the evolving threats in the financial crime landscape.

One prominent catalyst for change in 2023 was the escalating cost of living crisis, which brought about a surge in various scams, including loan fee fraud and ghost broking. As these financial crime threats evolved, so too did the imperative for updated systems and controls within financial institutions.

## Key Developments in Anti-Money Laundering (AML)

### — MLR Update

The Money Laundering, Terrorist Financing, and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) underwent significant amendments in response to HM Treasury's Call for Evidence and consultation. These changes aimed to align the UK with international AML and CFT standards, strengthening and clarifying the UK's AML regime. Notable updates included the exclusion of Account Information Service Providers (AISPs) from the MLR scope and provisions for Suspicious Activity Reports (SARs) accessibility by AML/CFT supervisors.

### — Proliferation Financing Risk Assessment

In line with international standards, the MLRs required financial institutions and designated non-financial businesses to conduct a risk assessment related to proliferation financing (PF) risks. This involved establishing policies, controls, and procedures to mitigate and manage PF risks effectively.

### — Transfers of Crypto-Assets

The MLRs extended to include the FAFT Recommendation 16, also known as the "travel rule," necessitating the sharing and recording of information on the originator and beneficiary of wire transfers exceeding **GBP £1,000**. This rule also applied to cryptocurrency exchange providers and custodian wallet providers, with a grace period granted for compliance.

### — Unhosted Wallets:

Virtual asset businesses were required to collect beneficiary and originator information for unhosted wallet transfers on a risk-sensitive basis, evaluating the potential for illicit finance in each transaction.

### — Acquirers of Cryptocurrency Firms

Proposed acquirers of crypto-Asset firms were mandated to notify the FCA ahead of acquisitions, enabling fit and proper assessments and potential objections.

### — The Economic Crime and Corporate Transparency Bill

This bill introduced provisions for inter-firm information sharing, expanded powers for law enforcement, and enhanced the Companies House framework.





### — Significant Amendments to the Proceeds of Crime Act 2002

From January 5, 2023, the threshold for bank transactions without committing money laundering offenses under the Proceeds of Crime Act 2002 increased **from £250 to £1,000**. This adjustment aimed to enhance the SAR regime and free up resources for law enforcement.

### — Continuing Enforcement Focus on AML Systems and Controls

AML investigations by regulators remained complex and intrusive, requiring firms to maintain proper records, provide adequate training, and rigorously challenge explanations in the face of warning signs.

### — The Register of Overseas Entities

Amendment regulations in 2022 addressed practical difficulties in verifying information, including exemptions for certain entities and revised verification processes.

### — Sanctions Compliance

The FCA emphasized sanctions compliance, especially regarding the UK sanctions on Russia and Belarus. Firms were expected to establish robust systems and controls to counter the risk of being used for financial crime.

### — Second Economic Crime Plan

Expected in spring 2023, this plan aimed to enhance policing responses to economic crime in light of rising levels of fraud and money laundering.

These developments underscored the FCA's unwavering commitment to combatting financial crime and ensuring robust AML compliance in a rapidly evolving financial landscape in 2023.

On the other hand, the [EU](#) finds itself in the midst of a dynamic and rapidly changing landscape concerning AML, compliance, fraud, and financial crime. It continues to be at the forefront of global efforts to combat money laundering and terrorist financing. In early 2023, the MiCA officially came into force, marking a significant milestone in the regulation of crypto-assets within the EU. The MiCA aims to create a harmonized set of rules for crypto-assets and related activities, making it harder for digital assets to be used for money laundering.

The EU's commitment to AML is demonstrated by its rigorous enforcement of existing regulations. Albania and Gibraltar, both subject to increased monitoring by the FATF due to strategic deficiencies, serve as examples. Albania faces challenges linked to corruption and weak institutions, while Gibraltar's gambling sector has attracted regulatory scrutiny. In 2023, both jurisdictions are expected to make progress in addressing these concerns under the watchful eye of FATF.

## Compliance in a Changing Landscape

With the implementation of the MiCA and other evolving regulations, businesses operating in the EU's financial sector are under increased pressure to ensure compliance. The focus is shifting from legislators to regulators, demanding proactive engagement from service providers and businesses.

Germany's Supply Chain Diligence Act, effective from January 1, 2023, mandates large companies to observe social and environmental standards in their supply chain. This highlights the EU's commitment to sustainable and responsible corporate behavior, as well as its determination to reduce cross-border money laundering risks.



## Fraud and Financial Crime

2023 is expected to witness an ongoing rise in synthetic identity fraud (SIF), a fast-growing financial crime in the EU. Criminals are increasingly using advanced technologies like artificial intelligence and deep learning to create sophisticated fraudulent identities. This poses a challenge to financial investigators who must adapt to new methods of detection.

To combat SIF, organizations are incorporating AI software into their compliance programs to identify subtle patterns of suspicious behavior and build detailed risk profiles. The emphasis is on gathering more information beyond basic documentation to verify the authenticity of individuals, mitigating the risk of synthetic fraud.



## America

Efforts to combat financial crimes, including money laundering and terrorist financing, continue to be a top priority for regulators and businesses in North and Latin America. The year 2023 witnessed significant progress in AML enforcement and fraud prevention in these regions, with major trends emerging in this regard. The latest developments and emerging challenges are delved into, and insights are provided into their impact on businesses and policymakers. Moreover, recommendations are presented for enhancing the financial system in the region to better guard against financial crimes.

One of the major trends seen in AML enforcement and fraud prevention is the increased use of technology and data analytics on the continent. Regulators and businesses are leveraging advanced technologies to identify suspicious activities and patterns, and this has resulted in improved detection and prevention of financial crimes. The use of blockchain technology and cryptocurrencies has also gained momentum in the region, with regulators and businesses exploring their potential for combating financial crimes.





# North America

## AML Enforcement Trends

AML enforcement remained a top priority in North America throughout 2023. Regulatory bodies in the United States and Canada intensified their efforts to combat money laundering. This included a notable increase in scrutiny directed at financial institutions, leading to stricter compliance requirements.

The countries continued to prioritize AML enforcement with a particular focus on regulatory enhancements and intensified scrutiny of financial institutions. Here is a deeper insight into AML enforcement trends:

### — Regulatory Vigilance

Regulatory bodies in North America, including those in the United States and Canada, maintained a vigilant stance against money laundering. They introduced and updated regulations to stay ahead of evolving financial crime tactics. Regulatory adjustments were designed to close potential loopholes and address emerging threats.

### — Enhanced Scrutiny

A notable development in 2023 was the increased scrutiny directed at financial institutions. Regulators raised the bar for compliance, necessitating more comprehensive AML programs and due diligence procedures. Financial institutions were required to strengthen their internal controls and risk assessment processes to align with these stricter compliance requirements.

### — Global Cooperation

Recognizing that money laundering is a global issue, North American countries actively collaborated with international organizations, including FATF. This cooperation aimed to harmonize AML efforts and improve information sharing to combat cross-border financial crimes more effectively.



## Fraud and AML Trends

The year also witnessed evolving trends in fraud and AML. Financial institutions in North American countries such as the USA and Canada embraced advanced technologies such as AI and machine learning to enhance their ability to detect suspicious activities effectively. These technologies played a crucial role in staying ahead of increasingly sophisticated financial criminals.



## Latin America

### Preventing Crypto-related Crime

In Latin America, efforts to prevent crypto-related crime gained momentum in 2023. Authorities and businesses collaborated to establish robust regulations and oversight in the cryptocurrency space. These measures aimed to combat illicit activities associated with digital currencies, enhancing the region's financial security.

### AML and FinCrime Compliance

Latin American countries also made significant strides in enhancing AML and Financial Crime (FinCrime) compliance. Initiatives focused on strengthening due diligence processes and fostering collaboration with international organizations. These efforts were aimed at bolstering the region's ability to combat financial crimes effectively.

## Middle East and North Africa (MENA)

The Middle Eastern financial services industry (FSI) has witnessed rapid growth in the post-pandemic era, driven by the need for digital accessibility due to lockdowns. However, this digital transformation has introduced new risks, exploited by financial criminals. In response, Gulf Cooperation Council (GCC) FSI regulators are taking measures to combat financial crime, encouraging the integration of technology into financial crime control frameworks. Notable directives include the Central Bank of the United Arab Emirates (CBUAE) promoting 'Digital ID' for customer due diligence, the Saudi Central Bank (SAMA) mandating a 'Counter-Fraud Framework,' and the Qatar Central Bank (QCB) emphasizing resources, including technology, for financial crime risk mitigation.



These are crucial steps in how financial institutions can adopt anti-financial crime technologies, focusing on identity verification and transaction monitoring:

### — Identity Verification

FIs face the risk of impersonation fraud during digital customer onboarding. While multi-factor authentication has been used, criminals find ways to bypass it. Advances in AI offer solutions, such as identification document verification (checking documents' authenticity) and biometric validation (using facial recognition, liveness detection, and more). These AI-driven solutions enhance security, reduce manipulation risk, and optimize compliance resources.

### — Transaction Monitoring (TM)

FIs face the risk of impersonation fraud during digital customer onboarding. While multi-factor authentication has been used, criminals find ways to bypass it. Advances in AI offer solutions, such as identification document verification (checking documents' authenticity) and biometric validation (using facial recognition, liveness detection, and more). These AI-driven solutions enhance security, reduce manipulation risk, and optimize compliance resources.

The MENA region have experienced remarkable growth in the realms of Fintech and blockchain technology. These advancements offer substantial benefits; however, they also pose significant challenges, particularly concerning ML/TF.

MENA countries face the ongoing task of effectively managing these risks. This entails the continuous enhancement of their regulatory frameworks to align with the evolving landscape of money laundering and terrorist financing. Failure to do so not only exposes these nations to internal vulnerabilities but also subjects them to international scrutiny, primarily from organizations like the FATF.





# Survey Results

Customers, compliance officers, and experts from different regions answered the survey questions according to their conditions where they are located. The results show that they have diversified situations but similar challenges.

## Confidence in Financial Institutions

The most common response indicates that respondents are "very confident" in the ability of financial institutions in their region to detect and prevent money laundering activities. It demonstrates a high level of trust in the effectiveness of these institutions in combating financial crimes.



High  
confidence in  
**regional  
institutions**

## Effectiveness of AML Measures

The most common perception is that AML measures in the region are "moderately effective" in deterring financial crimes. While there is a level of effectiveness, there is room for improvement to further strengthen AML efforts.

## Factors Contributing to Financial Crimes

Lack of public awareness is the factor most commonly believed to contribute to the prevalence of financial crimes in the region. This shows that there is a need for public education and awareness campaigns to help combat financial crimes effectively.



**More  
stringent  
regulatory  
frameworks**

## Stringency of Regulatory Landscape

The prevailing view is that the regulatory landscape for AML and fraud prevention has become "somewhat more stringent" in recent years. There is a perception that regulators are increasing their focus on combating financial crimes, which can impact how organizations approach compliance.



## Familiarity with AML Violations

A majority of respondents reported being aware of cases of AML violations or fines imposed on financial institutions in their region, even if they might not have detailed knowledge of these cases. This awareness underscores the importance of monitoring AML compliance within the financial sector.

High  
**AML Breach  
Awareness**

More  
**Robust  
Monitoring  
Systems  
needed**

## Areas for Improvement in AML Efforts

Respondents identified transaction monitoring as an area where AML efforts in the region could be improved. It reminds the need for more robust monitoring systems to detect suspicious activities effectively.

## Collaboration for AML and Fraud Prevention

The most popular response indicates a "neutral" stance regarding increased collaboration between businesses, regulatory bodies, and technology providers to enhance AML and fraud prevention efforts. While there is openness to collaboration, there may be reservations or uncertainties about how it should be implemented.

## Awareness of Industry Initiatives or Partnerships

A significant portion of respondents reported being aware of industry initiatives or partnerships aimed at improving AML and compliance practices, even if they did not have detailed information about them. This awareness suggests that efforts are already underway to enhance AML practices through collaborative initiatives.

The results indicate a generally positive perception of the effectiveness of financial institutions in combating money laundering activities. However, there is room for improvement in AML measures, particularly in transaction monitoring and public awareness. Respondents also see potential for increased collaboration and are somewhat aware of existing initiatives to enhance AML and regional compliance practices. These findings can inform regional strategies for strengthening AML and fraud prevention efforts.

# Key Takeaways from The Year 2023

- AML regulations in 2023 are characterized by a global push to strengthen frameworks, enhance technology adoption, and address emerging financial crime risks. These changes aim to create a more robust and coordinated response to money laundering and terrorist financing threats across regions. Organizations should stay informed and adapt to these evolving regulations to ensure compliance and mitigate financial crime risks effectively.
- Technology is both a double-edged sword and a powerful ally in the fight against financial crime. While it has created new challenges, it also offers solutions to enhance the effectiveness of AML efforts, making them more efficient and precise. Regulatory bodies and industry professionals must navigate these changes to maintain compliance while leveraging technology to protect the integrity of financial systems.
- The financial fraud landscape is evolving, requiring proactive measures, technological innovations, and collaboration to combat the growing threats effectively. Enhanced cybersecurity, investment in security measures, and a focus on remote work security are crucial elements in safeguarding sensitive data and critical systems from cyber threats in the digital age.
- In 2024, global regulatory frameworks for cryptocurrencies are expected to evolve. Taxation and reporting requirements are becoming stricter, and KYC procedures are strengthening. The balance between privacy and compliance remains a central issue. The cryptocurrency landscape is dynamic, offering both promise and risk, and it is essential for stakeholders to stay vigilant and adaptable to navigate this evolving financial world.
- Global efforts to combat financial crime, money laundering, and fraud are marked by distinct regional trends. In the Asia-Pacific, there is a growing emphasis on beneficial ownership transparency to counter money laundering, with discussions highlighting the importance of accurate reporting and technological solutions to tackle the surge in fraud. Europe and the UK saw significant strides in AML compliance, cryptocurrency regulation, and enforcement, with the FCA taking a proactive stance. In North and Latin America, AML enforcement was a top priority, driven by technology adoption and collaboration with international organizations, while Latin America also focused on crypto-related crime prevention. The MENA region embraced digital transformation, integrating technology into financial crime control frameworks, and emphasizing identity verification and transaction monitoring. These global developments signify a concerted effort to adapt and innovate in the fight against financial crime.



# Our Customers



More than 500+ customers from 50+ different countries trust us!

## Get in Touch



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



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



+44 20 4577 0427



+90 (212) 963 01 84



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



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



Join us, and let's  
fight financial  
crimes together.  
Request a demo  
today.

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/resource-library](https://sanctionscanner.com/resource-library).

