The Future of Financial Crime — Challenges and Trends

Authors: **Paweł Karp** — AML Practice Lead, Accenture Sp. z o.o.

Bartosz Segit — AML Practice Lead, Accenture Sp. z o.o.

accenture

Technology as a Tool in the Hands of Criminals — Cryptocurrencies and Dark Web Markets

Criminals are increasingly exploiting cryptocurrencies to conceal illicit proceeds, using advanced techniques designed to break transactional trails. Among the most commonly employed tools are **decentralized exchanges (DEXs) and cross-chain bridges**, which enable the transfer of assets between different blockchains, thereby complicating the tracking of financial flows.

One of the most striking examples of such techniques was the largest theft in the history of cryptocurrency exchanges, which occurred on 21 February 2025 at Bybit. The attack, which involved **malware used to authorize unauthorized transactions**, resulted in the theft of assets worth approximately **USD 1.46 billion**. According to analyses by Elliptic and confirmed by the FBI, the hack was carried out by the North Korean group Lazarus. Immediately after the theft, the assets were converted into more liquid tokens such as Ether, using decentralized exchanges to avoid freezing by token issuers. The funds were then dispersed across dozens of wallets, with subsequent laundering stages involving transfers through cross-chain bridges, swaps into other cryptocurrencies, and the use of mixing services such as Cryptomixer and Wasabi Wallet to further obscure transaction trails.

The Lazarus Group has been using similar schemes for years, systematically moving **stolen funds through various blockchains and decentralized platforms**. In recent years, as regulatory pressure has mounted on traditional mixers, criminals have increasingly turned to **decentralized finance (DeFi) tools, including DEXs and cross-chain bridges**, which facilitate the anonymous and rapid transfer of large sums.

Dark web markets constitute another critical element of this ecosystem. Through **anonymization technologies** such as Tor or I2P, criminals can operate in ways that are virtually untraceable. The dark web enables the trade of illicit goods and services—including drugs, weapons, and personal data—using cryptocurrencies as the primary means of payment. The use of cryptocurrency mixing services further **complicates the identification of fund origins**, making the detection and prosecution of financial crime an even greater challenge for law enforcement authorities.

The development of **blockchain technologies and DeFi tools** has dramatically expanded the possibilities for money laundering in the digital environment. The Bybit case illustrates just how advanced and organized cybercriminal operations in the cryptocurrency market have become.

Deepfake Technologies

The development of deepfake technology, which uses **generative artificial intelligence to create realistic falsified images, voices, and videos, poses a growing threat to identity verification systems in AML processes**. Criminals employ this technology to produce convincing counterfeit identity documents, social media profile photos, and even biometric simulations, enabling them to bypass KYC safeguards.

According to a report by Europol, deepfakes are used for **identity fraud, document manipulation, and financial scams**. Particularly dangerous are cases where deepfakes allow the takeover of bank accounts or impersonation of **public figures to extort funds**. In Poland, a high-profile case involved Rafał Brzoska, owner of InPost, who won a lawsuit against Meta for the unauthorized use of his image in deepfakes published on Facebook.

In Southeast Asia, criminal groups **leveraging deepfakes and generative AI stole as much as USD 37 billion in 2023**, using unregulated gambling platforms and cryptocurrencies for money laundering.

In **Europe**, the problem is especially visible in the **financial sector**. A report by Signicat found that:

6.5%

of attempted financial fraud in 2024 involved the use of deepfakes

more than 2000%

increase over the previous three years

Countries such as **Latvia**, **Ukraine**, and **Estonia** recorded the **highest number of identity fraud cases using this technology**.

Particularly dangerous is the use of deepfakes to penetrate biometric security systems. These technologies can generate real-time video simulations of a user's face or clone their voice, undermining the effectiveness of advanced verification methods. One such example occurred in 2024, when North Korean hackers from the Lazarus Group used a deepfake video to secure employment in the AI department of KnowBe4, gaining access to sensitive data.

To counter these threats, financial institutions are deploying solutions based on **multi-layer authentication and systems capable of detecting anomalies in facial muscle movements or voice patterns**.

Privacy-Enhancing Technologies (PETs) in the AML Context

An effective fight against money laundering requires moving beyond the traditional silo-based approach to **data analysis and adopting sector-wide solutions** that enable cooperation between financial institutions and supervisory authorities. At the same time, expanded collaboration cannot come at the expense of client data security or transaction confidentiality. In this context, **Privacy-Enhancing Technologies (PETs)** play a crucial role, allowing for the analysis and exchange of data in compliance with regulatory requirements while minimizing the risk of confidentiality breaches.

Definition and Importance of PETs

Privacy-Enhancing Technologies are advanced tools and methods that enable the processing of data in line with privacy regulations, such as the **General Data Protection Regulation (GDPR)**, while preserving its analytical utility. PETs allow financial institutions to analyze client data without revealing sensitive details, which is vital in the context of **anti-money laundering (AML)**. They address the fundamental dilemma between the need to collect data for analytical purposes and the obligation to safeguard privacy, by enabling compliant data sharing through methods such as **homomorphic encryption, differential privacy, and zero-knowledge proofs**.

PETs in Practice – Lessons from the Aurora Project

The Aurora Project, conducted by the **BIS Innovation Hub,** demonstrated that the combination of **PETs, network analytics, and machine learning** can identify complex money laundering schemes more effectively than traditional, silo-based approaches. The project analyzed **synthetic transactional data** at both **national** and **cross-border levels**, testing different models of cooperation (centralized, decentralized, and hybrid) while applying PETs to protect sensitive information.

Key findings from the Aurora Project show that **shared analysis of transactional data using PETs** enabled the detection of **up to three times more** money laundering cases than traditional rule-based systems, while simultaneously **reducing false positives by 80 percent**. The best results were achieved in scenarios where data was **protected yet consolidated in a central system**, and where network analysis focused on the behavior of **entire transactional networks rather than individual entities**. **PETs** also enabled effective cross-border cooperation without breaching data protection regulations—an aspect of particular importance in the context of global financial flows. The project also emphasized that technology alone is insufficient: **new frameworks for public-private cooperation, along with adjustments to regulations and data standards, are essential.**

PETs represent a breakthrough in the effectiveness of **AML systems**. They allow for more efficient use of data while safeguarding client privacy, reduce the risk of data breaches through advanced encryption and anonymization methods, and facilitate international cooperation and information sharing between financial institutions and supervisory authorities. The Aurora Project illustrates that a **sector-wide, collaborative approach to money laundering prevention using PETs** can significantly enhance the effectiveness of AML efforts, while simultaneously minimizing risks related to data protection.

Balancing Technological Progress and Regulatory Oversight

Regulators' Adaptation to New Technologies

Modern regulatory authorities face the challenge of adapting to the rapid pace of technological innovation in the financial sector. Traditional regulatory models, based on rigid rules, have proven **inadequate** in the face of innovations such as **blockchain, artificial intelligence (AI), and big data**. In response, regulators around the world are adopting more flexible, outcomes- and risk-based approaches, which allow for more effective oversight of emerging technologies.

These technologies demand not only that regulators understand their technical aspects but also that they **anticipate their potential impact** on financial system stability and data security. Consequently, an increasing number of regulatory institutions are investing in **technological expertise and establishing specialized teams** dedicated to fintech and regtech. In many advanced economies, such as the United Kingdom and the United States, regulatory sandboxes enable the testing of new solutions under controlled conditions. Such initiatives are essential to building a balance between fostering innovation and ensuring compliance with legal requirements.

The Importance and Development of RegTech

RegTech—**technologies that support the implementation of regulatory requirements**—plays an increasingly important role in the effective deployment of AML/CFT solutions. According to a report by the Financial Action Task Force (FATF), as many as **52 percent of respondents** indicated that **the greatest benefits from adopting new technologies can be achieved in the area of RegTech**. The most significant impacts relate to the processing and analysis of large datasets essential for risk assessment, due diligence, and transaction monitoring.

New technologies not only enable faster and more accurate data processing but also automate procedures, relieving employees from repetitive tasks and allowing them to focus on high-priority cases. RegTech also enhances **auditability, transparency, and data quality**, which translates into more effective supervision and reporting. At the same time, despite the growing number of RegTech solutions on the market, the report points to a significant gap in their adoption by supervisory authorities and regulators, which remains a challenge for the further development of this segment.

Public-Private Partnerships

Public-private partnerships are playing an increasingly important role in the effective implementation of technologies supporting the **fight against money laundering (AML)**. Cooperation between regulators, financial institutions, and technology firms enables more efficient use of resources and expertise, leading to the development of more advanced AML systems.

International Initiatives

UN PET Lab

A United Nations program supporting the development of Privacy-Enhancing Technologies (PETs), which **facilitate the secure sharing of data between organizations**. PETs are critical to cross-border financial information exchange in compliance with regulatory requirements.

UK-US Joint Challenges

A partnership between the United Kingdom and the United States focusing on the development of technologies such as **federated learning**, which allows data analysis without compromising privacy. This initiative is of major significance for the global fight against money laundering.

Ethical Issues and Privacy in the Context of AML Technologies

Balancing Privacy and Oversight

One of the **key challenges** in implementing advanced technologies—particularly artificial intelligence (AI)—within anti-money laundering (AML) systems is reconciling effective financial oversight with the **protection of fundamental rights**, including **privacy and the security of personal data**. The use of AI tools enables the analysis of massive volumes of information and the detection of complex money laundering schemes, but it also raises significant risks related to large-scale processing of client data and the potential violation of individual rights.

The report *"Deploying Artificial Intelligence for Anti-Money Laundering and Asset Recovery: The Dawn of a New Era"* stresses that integrating AI into AML/CFT frameworks opens new opportunities but also requires particular attention to **ethics and data protection**. The authors note that AI can significantly enhance AML effectiveness, but only if **implemented transparently**, with appropriate safeguards for personal data, and with respect for individual rights.

Both the **OECD Guidelines on AI** and the **EU Artificial Intelligence Act (AI Act)** highlight the necessity of ensuring that AI systems comply with the law, safeguard human rights, and provide transparency and auditability of algorithms. In the AML/CFT context, these technologies must be deployed in ways that allow for human oversight, explainability of decisions, and robust protection against unauthorized access to data. It is equally critical that AI systems do not result in **mass surveillance or discrimination**, and that solutions are proportionate to the risks while adhering to the principle of privacy by design.

The Risks of Overreliance on Technology

Automating AML processes with the use of AI offers tangible benefits, such as reducing the number of false positives and easing the workload of compliance teams. However, it also introduces serious ethical and legal risks. These systems may replicate biases present in their training data, leading to **discrimination** against certain groups of clients or to **erroneous decisions** whose underlying mechanisms are difficult to explain (the so-called "black box" problem).

A high degree of automation may also result in the **loss of control over decision-making processes** and limit the ability of humans to effectively supervise and verify system outputs. For this reason, both the OECD guidelines and the draft AI Act require that AI systems used in AML remain subject to human oversight, ensure full auditability, and undergo regular testing for effectiveness and potential biases.

To manage these risks, financial institutions should implement **hybrid systems** that combine advanced technologies with human supervision. This approach allows institutions to benefit from the efficiencies of automation while ensuring ethical oversight and the capacity to interpret complex situations that extend beyond the capabilities of algorithms.

Conclusion

Technological progress is fundamentally transforming the landscape of countering financial crime, providing financial institutions with highly effective new tools in the fight against money laundering and terrorist financing. Artificial intelligence (AI), machine learning, and advanced data analytics enable the detection of subtle patterns and anomalies across massive volumes of transactions, significantly **improving the effectiveness of AML systems.** Case studies such as those of HSBC and CitiBank demonstrate that automation and network analytics can uncover complex money laundering schemes, reduce false positives by as much as **60 percent**, and support more efficient risk management.

A major breakthrough lies in sector-wide solutions, such as Poland's SCU AML or the United Kingdom's Vocalink, which facilitate the **sharing and analysis of data across the entire financial sector**. This allows for the more effective identification of links between entities and enables rapid responses to emerging threats. International cooperation and public-private partnerships are becoming essential to strengthening the resilience of AML systems against increasingly complex and cross-border criminal schemes.

Blockchain technology and cryptocurrency analytics tools introduce a new level of **transparency**, making it possible to track fund movements even across decentralized platforms. The implementation of biometric identity verification and Privacy-Enhancing Technologies (PETs) enhances the security and efficiency of AML processes while safeguarding client privacy.

At the same time, these very innovations are exploited by **criminals**. Cryptocurrencies, decentralized exchanges, anonymization technologies, as well as deepfakes and generative AI tools, allow for the concealment of identities and sources of funds. Cases such as the Bybit exchange attack and the large-scale use of deepfakes in identity fraud show that cybercrime is becoming increasingly sophisticated, with the arms race between cybersecurity teams and criminals accelerating rapidly.

The deployment of **advanced AML** technologies requires balancing effective financial oversight with the protection of fundamental rights, including privacy and the security of personal data. It is essential that solutions remain **auditable**, subject to **human oversight**, and **compliant** with regulations such as the **EU AI Act** and the **OECD guidelines**. A modern approach to AML must therefore encompass not only technology but also flexible regulation, the development of expertise, and the cultivation of trust and cooperation between the private and public sectors.

Technology is both a tool and a challenge in the fight against financial crime – the effectiveness of AML systems depends on the pace of innovation adoption and the capacity for sector-wide and international cooperation.

Criminals exploit new technologies (cryptocurrencies, DeFi, deepfakes), which compels the continuous enhancement of AML systems and the implementation of multilayered safeguards as well as hybrid oversight models that combine automation with human control.

Sector-wide solutions and PETs enable more effective detection of complex money laundering schemes, while minimizing privacy risks and enhancing the efficiency of data analysis. Only through cooperation can the security of the entire financial sector be ensured. Current silo-based approaches to AML are exploited by criminals to obscure the origins of illicit funds.

Balancing innovation with regulation and ethics is essential – AML systems must be transparent, auditable, and designed in line with the principle of privacy by design, with decision-making processes remaining under human oversight.

The future of effectively combating financial crime rests on synergy – the integration of technology, sectoral cooperation, flexible regulation, and the continuous development of expertise to address emerging threats and tools.

In summary, only a **comprehensive** and **integrated** approach—combining **advanced technology**, **cooperation**, and **responsible risk management**—will allow for an effective response to increasingly sophisticated financial crime in the digital era. This goal can be achieved only through the strengthening of cooperation across the entire financial sector, in the interest of safeguarding its clients.

Paweł Karp

AML Practice Lead,
Accenture Sp. z o.o.

Bartosz Segit

AML Practice Lead,
Accenture Sp. z o.o.