Discai
Powered by KBC

Trusted AI in AML: a blueprint for success

Key challenges, market trends and proven approaches to help financial institutions outsmart technology-driven financial crime.

Discai nv
Professor Roger Van Overstraetenplein 2
3000 Leuven
Belgium
E-mail: info@discai.com

Executive summary

Money laundering is growing more complex as digital tools and global networks expand. Financial institutions face real challenges: **sophisticated fraud**, **heavy regulatory demands**, a **shortage of skilled professionals**, and **outdated systems**. This whitepaper helps industry leaders understand these threats and respond effectively with proven, AI-driven approaches.

It provides a blueprint for strengthening anti-money laundering (AML) strategies, with a focus on **how AI can improve detection**, **reduce false positives**, and **support compliance** now and in the future.

Readers will find recommendations on how to combine the right technology, skilled people, clear processes, robust control frameworks and strong governance to build lasting value.

By applying these insights, financial institutions can **proactively manage money laundering risks more effectively**, **stay ahead of regulatory changes**, and **protect their reputation**.

Use this guide to **measure your current AML efforts**, **spot weaknesses**, and **move toward solutions** that deliver sustainable results.

Table of contents

Challenges

1 Growing sophistication

The use of innovative tools like artificial intelligence, cryptocurrency, and high-speed transactions is transforming money laundering operations. Financial institutions need to keep up with these changes to counteract complex illicit activities while remaining fully compliant.

International financial crime networks

Criminals take advantage of **regulatory loopholes** and **fragmented oversight** across jurisdictions. The global flow of illicit money is estimated to be between 607 billion and 1.58 trillion Euro, demonstrating the importance of cross-country collaboration. [1]

Money launderers use **multi-layered structures** involving shell companies, offshore accounts, and digital assets to make illicit transactions harder to trace. These networks often use **trade-based money laundering (TBML)**, where fraudulent invoices, misrepresented goods, and complex supply chains hide illegal money flows. They also leverage legal financial institutions, moving money through **quick**, **high-volume transactions** designed to evade detection.

Money mule schemes are **a significant component of these networks**. Criminal organisations recruit individuals, sometimes unknowingly, to transfer illicit funds across borders, making tracking more difficult. These money mules are often students, vulnerable people, or those enticed by social media advertisements promising quick earnings. [2]

*The Financial Action Task Force (FATF) addresses the "money mule" concept in its work on **professional money laundering.** According to the FATF, **money mules** are individuals who, knowingly or unknowingly, transfer illegally acquired money on behalf of others. They are often recruited to move funds through their own bank accounts or via money transfer services, helping to obscure the origin and destination of illicit proceeds.*

Money mules are commonly used in layering stages of money laundering to break the audit trail and complicate investigations.

They may be:

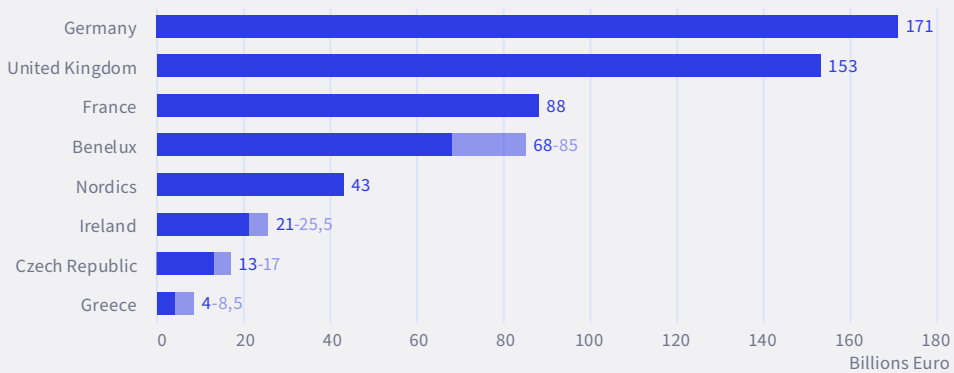
- ***Witting participants** (knowingly aiding criminals);*
- ***Unwitting participants** (duped via scams or fake job offers);*
- *Or **coerced individuals** (forced under threat or manipulation).*

*The FATF emphasises the **importance of transaction monitoring systems** in identifying mule activity, such as:*

- *Fast movement of funds through accounts;*
- *Use of multiple accounts with no clear business rationale;*
- *Transfers inconsistent with customer profile.*

2-5%
of **GDP**
is estimated to be laundered globally

ESTIMATED MONEY LAUNDERING AMOUNTS IN EUROPEAN COUNTRIES/REGIONS



Global Data estimates 2025. BOE, BIS, SNP, D&B all 2025. LNRS, Oxford Economics 2024, Chartis estimates.

1. United Nations Office and Drugs and Crime.
2. Europol (2025), European Union Serious and Organised Crime Threat Assessment - The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg.

CASE EXAMPLE

JuicyFields large scale Ponzi scheme

In the "JuicyFields" investment fraud case, suspects lured victims into **fraudulent crowdsourcing investments** in the cultivation and distribution of cannabis for medicinal purposes. Upon the purchase of a cannabis plant, with a minimum investment of €50, investors could collect high profits from the sale of marijuana to authorised buyers.

The platform was not only present in the digital world, but upheld the image of a trustworthy legal business structure with physical offices, staff and representation at cannabis events. Initially, the 500.000 "e-growers", or digital growers, were receiving their investment returns.

In July 2022, the criminals behind the scheme abruptly removed company profiles from social media and stopped users from logging in to their accounts, thus freezing cash withdrawals.

The scheme impacted a very high number of victims throughout the EU, with a total of reported damages of around €645 million, but they could be significantly higher. The criminal network had a strong cross-border dimension, led by Russian masterminds, with strawmen in Germany and money laundering activities in Cyprus.

The rise of cyber-enabled financial crime adds another layer of complexity. Ransomware attackers, dark web marketplaces, and fraud rings increasingly use **cryptocurrencies** to facilitate payments, taking advantage of their decentralised nature. While blockchain can make transactions easier to trace, privacy-based cryptocurrencies help criminals move and hide money more easily. **International differences in regulations make it harder to enforce anti-money laundering rules**. Countries with weak AML enforcement often attract illegal money, while financial institutions in stricter regions struggle to meet compliance expectations when handling transactions across borders. This results in growing pressure for better cooperation between Financial Intelligence Units (FIUs), international law enforcement agencies, and private sector stakeholders.

Geopolitical instability

Geopolitical instability is now **a key factor driving money laundering risks**. Events like **trade wars**, **economic sanctions**, and **political changes** affect how financial institutions manage these risks. Sanctions on countries like Russia and Iran have led to more illegal money flows, as entities try to get around the restrictions. Destabilising conflicts and economic crises in certain regions have also led to a rise in illicit activities such as terrorist financing.

People in positions of political power (PEPs) require ongoing monitoring because they carry a higher risk. Dealing with anti-money laundering rules in this turbulent geopolitical environment requires strong cooperation between governments, banks, and intelligence agencies.

The graph below shows that:

- The United States remains a leader in AI development, driving innovation and technological advancements;
- China stands out in deploying AI at scale across various industries;
- Europe, on the other hand, finds itself at a crossroads, striving to balance regulation and competitiveness.

The **current rollback of financial crime (FinCrime) regulations** under the Trump 2.0 administration adds more uncertainty and could potentially affect the global financial system and the use of AI in this area. Europe now faces the challenge of keeping up with these changes while maintaining its relevance in AI and FinCrime.

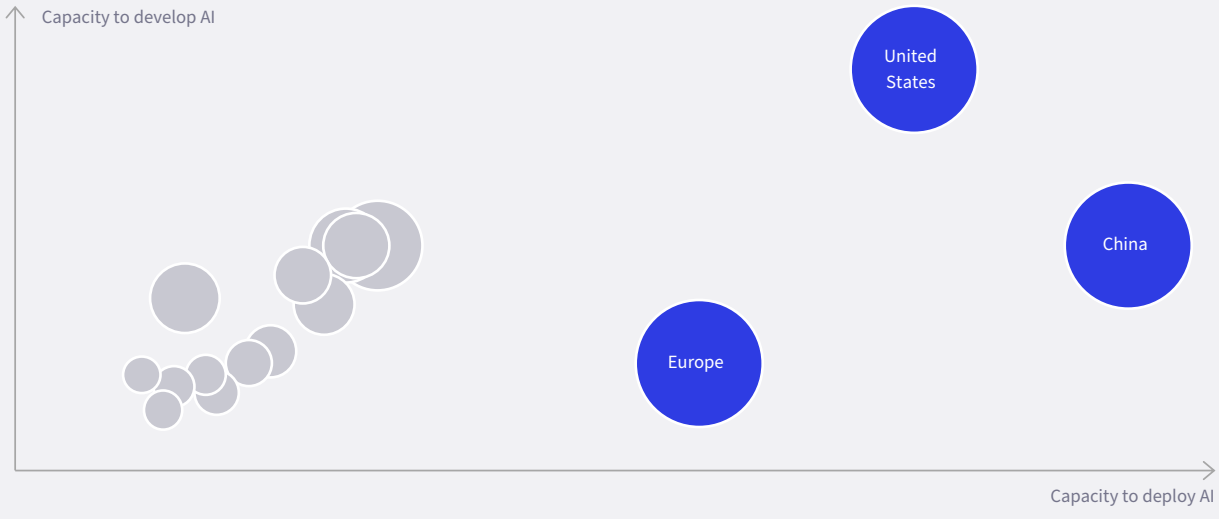
*According to the **Financial Action Task Force (FATF)**, a **Politically Exposed Person (PEP)** is an individual with a **prominent public function**. Due to their position and influence, many PEPs are in roles that can be abused for the purpose of laundering illicit funds or engaging in corruption or bribery.*

> It is interesting, though not surprising, to see how different geographies follow different paths when it comes to embracing technology.
>
> Over the past decade, most new technologies have emerged from the 'land of the free' (the **United States**) driven by libertarian capitalism and the innovation engine of Silicon Valley. **China**, as a state-driven economy, has excelled at rapidly copying and deploying technologies across entire sectors and regions. Although lately, it is increasingly becoming a hub for development. **Europe** is literally in the middle and tries to make a careful trade-off between technology, politics, and consumer interest.
>
> To me, it's clear that **these three levers need to point in the same direction**. Only then can we achieve sustainable change or development and move from a push-driven to a pull-driven market.

Stefan Delaet
General Manager Financial Crime at KBC Group

For more on Stefan's perspective on international AML regulations and cross-border cooperation, see the full interview in the annex.

AI DEVELOPMENT AND DEPLOYMENT WORLDWIDE



BCG Henderson Institute: Europa can catch up, but must act – today.
IMD World Competitiveness Centre, World Economic Forum; BCG Henderson Institute analysis.

*FATF Recommendations **12 and 22** require financial institutions and designated non-financial businesses and professions (DNFBPs) to apply **enhanced due diligence (EDD)** when dealing with:*

- ***Foreign PEPs**;*
- ***Domestic PEPs**;*
- ***PEPs from international organisations**;*
- *And their **family members and close associates**.*

*It should be noted that these measures are **preventive** and don't imply that all PEPs are involved in criminal activity. However, due to the higher risk associated with their positions, transaction monitoring systems must flag unusual activity involving PEPs for further checks.*

Remote onboarding

The **shift to digital banking** has enabled seamless remote onboarding processes. Unfortunately, these advancements also increased risks of identity fraud, synthetic identity creation, and money mule activities. The use of **AI-generated deepfake identities** has made it increasingly difficult for traditional verification methods to tell real people apart from fraudsters.[3]

Digital onboarding reduces customer acquisition costs and improves customer experience. However, it also requires stronger checks, called **enhanced due diligence (EDD)**, to maintain compliance.

Regulators stress that financial institutions must find a **balance between efficiency and strong fraud detection** mechanisms to stop criminals from taking advantage of digital onboarding.

Faster payment schemes

Instant payment systems like SEPA Instant Credit Transfers have revolutionised the speed and efficiency of financial transactions. However, these faster payment schemes also bring new challenges for fighting money laundering.

Illicit funds are moved quickly across jurisdictions before measures can be taken. Techniques like "**smurfing**" and **account takeovers** have become more common because of instant payment capabilities. Financial institutions need to integrate machine learning models to effectively stop emerging threats before they escalate.

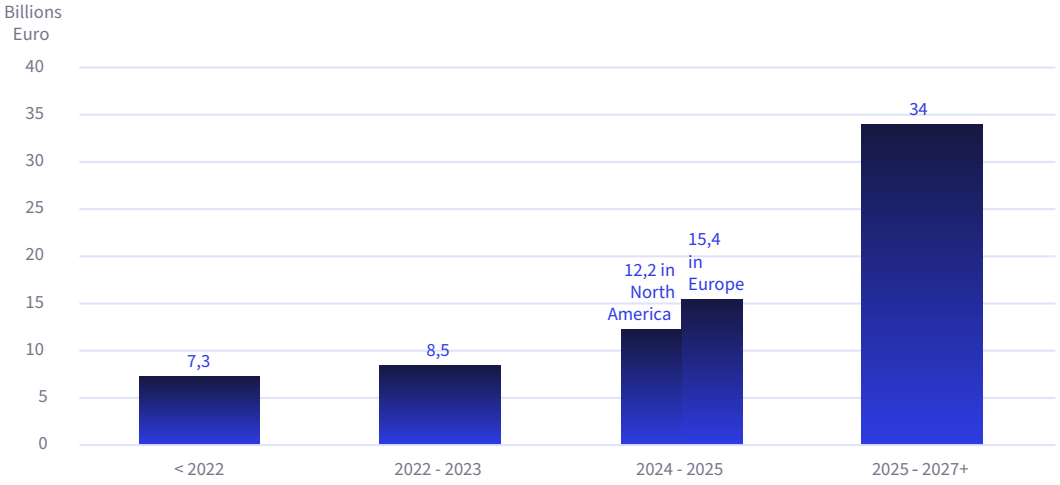
*The **Financial Action Task Force** (**FATF**) covers the term "smurfing" under the broader category of structuring, which is a recognised money laundering technique.*

***Smurfing** (**or structuring**) is the practice of breaking up large amounts of money into multiple smaller transactions that fall below the reporting threshold, to avoid detection by financial institutions and regulators. These transactions are often conducted by multiple individuals (called "smurfs") and are designed to evade **Suspicious Transaction Reports** (**STRs**).*

*This technique is often used during the **placement stage of money laundering**, where illicit funds are put into the financial system in a way that avoids triggering AML alerts.*

3. Finance worker pays out $25 million after video call with deepfake 'Chief Financial Officer' | CNN

EXPECTATIONS OF FRAUD AND IMPACT OF GENERATIVE AI



Chartis Research: Thomson Reuters (2025), Deloitte (2024), JRC (2025)

Criminal use of Generative AI

AI and other new technologies are fundamentally reshaping the serious and organised crime landscape in two main ways: as a **catalyst for crime**, and as a **driver for criminal efficiency**.[4]

Generative AI has opened new dimensions of financial crime, enabling money launderers to create realistic forged documents, deepfake videos, and automated phishing campaigns. Celent estimates that AI was behind roughly **20% of fraud cases** in 2024 and is expected to fuel even more fraud moving forward.[5]

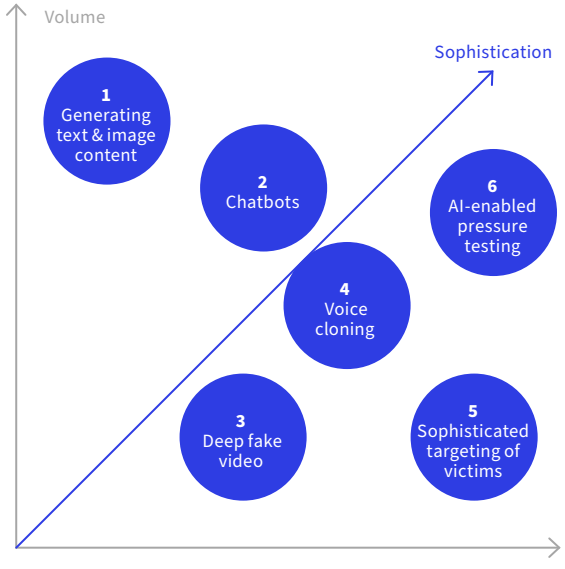
Some examples of the use of AI:

- **AI-driven chatbots** are used to impersonate customer service representatives, tricking victims into disclosing sensitive financial information.
- **AI-generated synthetic identities** are used to get past KYC checks and open fraudulent accounts.

Because Generative AI can automate cybercrime at scale, there is a **growing need for advanced detection systems**. Financial institutions must improve digital forensics capabilities, use AI to detect anomalies, and adopt strong identity verification frameworks to effectively fight AI-driven threats.

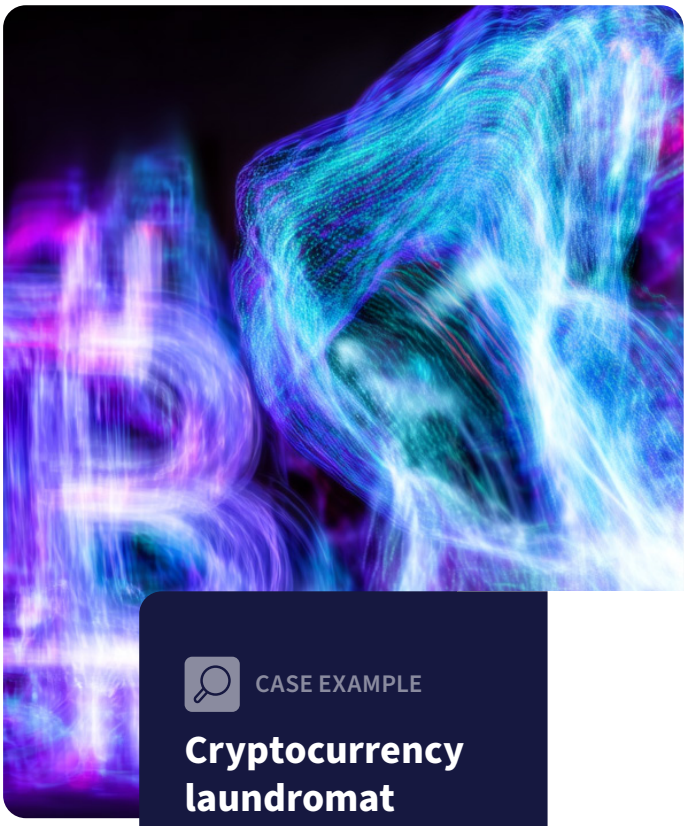
This visual from the UNODC (United Nations Office on Drugs and Crime) shows the **main ways AI tools are used to perpetrate cyber-enabled fraud and scams**.[6]

AI TOOLS IN CYBER-ENABLED FRAUD AND SCAMS



Elaboration based on research conducted by Price Waterhouse Cooper, 2024

4. Europol (2025), European Union Serious and Organised Crime Threat Assessment - The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg
5. Mitigating Fraud in the AI Age: Understanding the Challenge | Celent
6. Transnational Organised Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape October 2024, United Nations Office on Drugs and Crime



CASE EXAMPLE

Cryptocurrency laundromat washed out

In March 2023, law enforcement authorities took down ChipMixer, an unlicensed cryptocurrency mixer, for its alleged involvement in money laundering activities. The service allowed users to deposit Bitcoin, which was then broken down into standardised amounts called "chips." These chips were mixed together to obscure the origin of the funds, making it difficult to trace transactions.

Investigators believe that ChipMixer may have laundered approximately 152,000 Bitcoins, equivalent to around €2.73 billion, linked to various forms of criminal activity, including ransomware attacks, darknet markets, and stolen crypto assets.[8]

> "A key issue is that funds don't always come directly from a crypto exchange. They'll use **different intermediary payment providers** and switch between them over time. Even with sophisticated transaction monitoring, it's hard to tell what you're missing."
>
> KBC Group Compliance Staff

Crypto platforms

Cryptocurrencies and decentralised finance (DeFi) platforms have become **attractive tools for money laundering because of** their **anonymity and speed**. Criminal organisations use these platforms to move illicit funds across countries. Regulatory bodies worldwide are increasing their oversight of crypto exchanges, implementing stricter KYC and AML requirements.

However, the **decentralised nature** of many crypto transactions complicates rule enforcement. To fight crypto-enabled money laundering, financial institutions need to adopt blockchain analytics tools capable of tracing illicit transactions and work closely with regulatory authorities.[7]

7. Europol (2025), European Union Serious and Organised Crime Threat Assessment - The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg
8. Office of Public Affairs | Bitcoin Fog Operator Sentenced for Money Laundering Conspiracy | United States Department of Justice

2
Complex regulatory landscape

Regulatory requirements are increasingly detailed and demanding. Organisations need to manage multiple rules and oversight mechanisms, balancing compliance with operational needs while responding to ongoing scrutiny.

AML package and authority (AMLA)

The European Union has introduced a **new AML package** to **address the rising threats of money laundering and terrorist financing**. Its main goal is to enhance the integrity and security of the EU's financial system and make sure it stays resilient against money launderers. With the package, it wants to close existing loopholes, improve transparency, and foster more collaboration among member states.

The key components of the package are:

- **Regulation**: The new regulation sets uniform AML standards across the EU. It creates a more consistent approach in the application of AML measures and reduces regulatory fragmentation.
- **Directive 6**: This introduces stricter rules for customer due diligence, beneficial ownership transparency, and the use of cryptocurrencies. It also requires better cooperation and information sharing between countries.

"I expect the changes from setting up AMLA will happen step by step. However, over time, these changes will be fundamental. They will affect several areas:

• Unification of AML rules across the EU
The AMLA will support more consistent rules across the whole EU. This is especially helpful for institutions operating in several countries, as they currently have to adjust and customise their AML systems for each market due to local differences.

• Balanced rules for everyone
Today, some countries are stricter than others when it comes to AML checks. The authority will help create a level playing field so all players will face the same expectations, regardless of where they operate.

• Direct supervision for large financial groups
Some of the bigger financial firms will be directly supervised by the AMLA. These groups will likely need to invest heavily to meet AMLA's expectations and roll out a unified system in every country they do business in."

Jiří Feix
General Manager of the Financial Crime Unit at KBC Group

- **Anti-Money Laundering Authority (AMLA)**: This new centralised authority oversees and coordinates AML efforts across member states. The AMLA will directly supervise high-risk financial institutions and enforce compliance with AML regulations.
- **Transfer of funds**: New rules will improve the traceability of transfers of funds, including those involving cryptocurrencies. The goal is to prevent the misuse of financial systems for money laundering and terrorist financing.

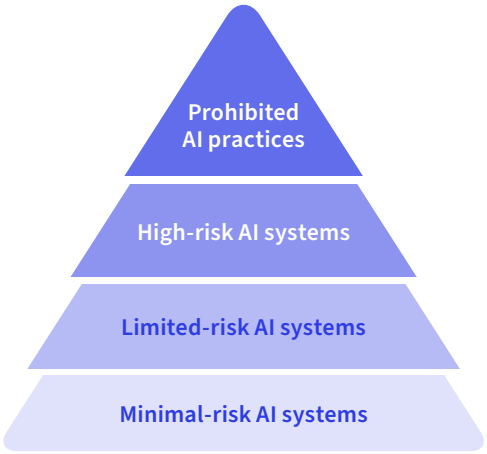
EU AI Act

The European Union (EU) introduced the Artificial Intelligence (AI) Act to **create a complete legal framework governing the development**, **deployment**, **and use of AI systems**.

Its **primary goal** is to make sure that **AI systems are safe**, **respect fundamental rights**, **and align with EU values**. This is needed because, although AI systems have huge potential, using them the wrong way can cause significant harm.

In the fight against money laundering, AI solutions that analyse financial transactions could unintentionally flag legitimate activities as suspicious. These errors could lead to inefficiencies and even reputational damage. The AI Act wants to mitigate these risks by setting out rules for transparency, accountability, and fairness.

The AI Act regulates AI systems with a risk-based approach, dividing them into four categories based on the potential harm they could cause:



Companies that build or use high-risk AI systems have to follow these principles:

- **Risk management**: Evaluate and mitigate potential risks.
- **Data governance**: Maintain datasets that are unbiased and high quality.
- **Transparency**: Provide clear documentation and logging for auditability.
- **Human oversight**: Set up mechanisms to allow human intervention and override.
- **Cybersecurity measures**: Prevent misuse or vulnerabilities.

THE AML DIRECTIVES

1st AML Directive

ADOPTED
June 1991

FOCUS
Criminalisation of money laundering related to drug trafficking

KEY FEATURE
Customer due diligence (CDD) and suspicious transaction reporting for financial institutions

2nd AML Directive

ADOPTED
December 2001

EXPANDED SCOPE
Included lawyers, accountants, real estate agents, and dealers in high-value goods

NEW PREDICATE OFFENCES
Extended beyond drug trafficking

3rd AML Directive

ADOPTED
October 2005

ALIGNED WITH FATF RECOMMENDATIONS

INTRODUCED
Risk-based approach, politically exposed persons (PEPs), and beneficial ownership requirements

4th AML Directive

ADOPTED
May 2015

FOCUS
Transparency of beneficial ownership, enhanced CDD, and risk assessments

INTRODUCED
Risk-based approach, politically exposed persons (PEPs), and beneficial ownership requirements

This is the timeline of the AI act:

- **2021**: The European Commission proposed the AI Act.
- **2023-2024**: The European Parliament and Council were expected to give final approval.
- **2024-2025**: The transition period for implementation begins.
- **2025-2026**: AI providers and deployers are required to fully comply.

Data privacy and protection

Data privacy regulations, including the **General Data Protection Regulation** (**GDPR**), **play a critical role in AML compliance strategies**. Financial institutions need to carefully balance customer data protection with their AML duties. They have to safeguard personal information while being transparent about transaction monitoring.

Cross-border data transfers are specifically challenging, especially after the **Schrems II ruling**. If they don't follow data privacy laws, they risk significant fines, legal actions, and reputational damage. This emphasises the need for a balanced approach to AML compliance and data protection.

*The **Schrems II ruling** refers to the **Court of Justice of the European Union (CJEU) judgment in Case C-311/18**, delivered on 16 July 2020. It is a crucial ruling in the field of **data protection and international data transfers**.*

- *The case was brought by Maximilian Schrems, an Austrian privacy advocate, against Facebook Ireland Ltd.*
- *Schrems challenged the legality of transferring personal data from the EU to the United States, arguing that U.S. surveillance laws didn't properly protect EU citizens' data.*
- *The case followed the earlier Schrems I ruling (2015), which invalidated the Safe Harbor agreement.*

Digital Operational Resilience Act (DORA)

The **Digital Operational Resilience Act** (**DORA**) is a **groundbreaking EU regulation** brought to life to **make the financial sector more resilient against cyber threats and operational disruptions**.

DORA mandates financial institutions to:

- Set up comprehensive ICT risk management frameworks;
- Carry out regular penetration testing;
- Make sure third-party service providers stick to strict cybersecurity standards.

5th AML Directive

ADOPTED
July 2018

RESPONSE TO
Panama Papers and terrorist attacks

KEY ADDITIONS
- Public access to beneficial ownership registers
- Regulation of virtual currencies and prepaid cards
- More scrutiny of high-risk third countries

6th AML Directive

ADOPTED
30 May 2024

FOCUS
Harmonisation of AML rules across the EU

KEY FEATURES
Stronger cooperation between FIUs and law enforcement

AML Regulation (Single Rulebook)

ADOPTED
30 May 2024

APPLIES FROM
10 July 2027 (2029 for football sector)

PURPOSE
Uniform AML rules across the EU

COVERS
Private sector obligations, beneficial ownership transparency, and anonymous instruments

Anti-Money Laundering Authority (AMLA)

SEAT CHOSEN
Frankfurt, February 2024

OPERATIONAL START
Mid-2025

ROLE
Direct and indirect supervision of high-risk entities, coordination of national supervisors, and enforcement of AML rules

The Act mandates companies to **report cyber incidents** and breaches quickly and **implement corrective measures**. Financial institutions are also required to establish operational continuity plans to mitigate the impact of cyberattacks.

Because of the growing use of cloud computing and digital payments, a **proactive approach to resilience** is more important than ever. That's why DORA is a key component of modern financial crime prevention strategies. Non-compliance with DORA can result in regulatory penalties and closer oversight from national and EU-level supervisors. As cyber threats keep changing, DORA helps financial institutions stay agile and well-prepared to handle emerging risks.

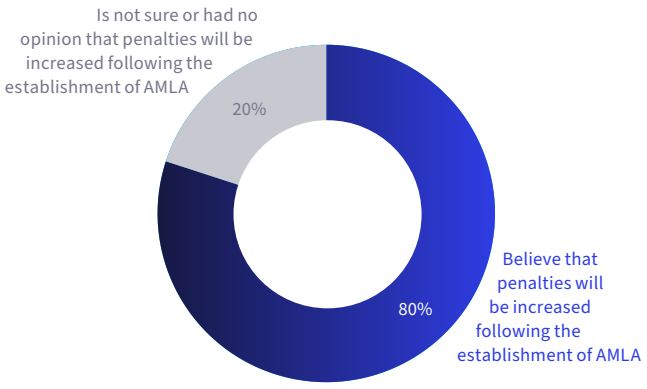
Regulatory scrutiny

Regulators worldwide are paying more attention to AML rules, imposing record-breaking fines and enforcement actions on institutions that are not compliant.

Some examples:

- In 2024, **Binance**, the world's largest cryptocurrency exchange, was fined $4.3 billion for AML violations.
- **TD Bank** also faced $3.1 billion in penalties for failing to prevent illicit transactions.

DO YOU BELIEVE THAT PENALTIES WILL BE INCREASED FOLLOWING THE ESTABLISHMENT OF AMLA?



AMLA: Transforming EU anti-money laundering efforts | EY - Global

These cases show that regulators are increasingly focusing on enforcing AML compliance and holding financial institutions accountable.

Beyond financial penalties, regulatory scrutiny affects business continuity, investor confidence, and customer trust. Institutions must adopt **proactive compliance measures** (like automated transaction monitoring, enhanced due diligence (EDD), and AI-driven detection) **to mitigate regulatory risks**.

Since regulatory expectations keep changing, financial institutions must stay alert, continuously updating their compliance programs to align with changing laws and industry best practices.

€23

billion levied **globally** in fines against financial institutions for AML/KYC sanctions violations since 2008.

€9,79

billion levied in 2015 alone, the most punitive year for fines.

€7,56

billion was the highest fine ever issued (levied by the US DoJ against a French Bank in 2015).

€76,55

million is the average global fine issued.

€1,45

billion levied AML fines in **Europe** in the last 10 years across 84 separate fines.

€765

million is the highest regional fine in 2018 against a Dutch bank.

€769

million levied in 2018: a record year for AML and sanctions fines – 3 times more than 2017.

€17,26

million regionally average AML fine issued in Europe.

Chartis Research: Fenergo (2024). Global Fines Infographic.

3
Resource and talent management

AI means more skilled AML professionals needed, not less!

FC tech expert Shlomit Wagman tells WiFC Summit[9]

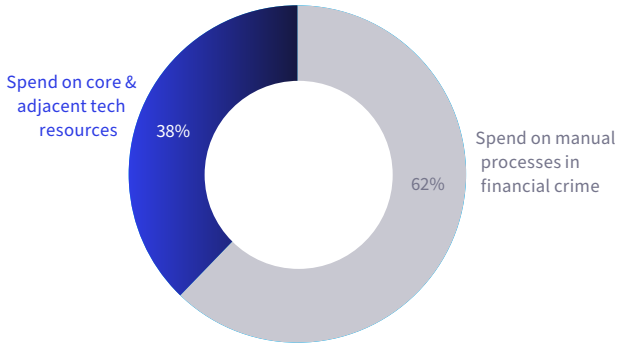
Effective AML depends on skilled professionals who can manage complex regulatory environments, analyse large volumes of transactional data, and use advanced technologies. Yet financial institutions worldwide face challenges in attracting, retaining, and developing AML talent.

Attracting talent

The growing demand for AML professionals has led to a **highly competitive job market**, making it difficult for financial institutions to attract top talent.

The sector needs experts who combine legal, compliance, and technological skills. However, **there is a clear shortage of candidates with this interdisciplinary expertise**. According to a recent PwC report, "finding skilled staff is the most

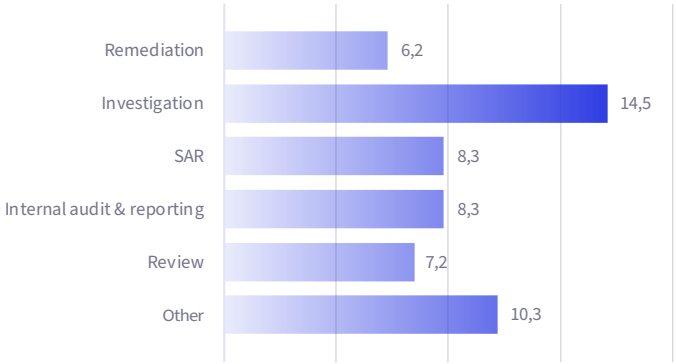
RATIO MANUAL VERSUS TECH & RELATED IN 2024



Chartis research: Data from LexisNexis Risk Solutions 2025, Oxford Economics, 2024 Dun & Bradstreet 2023, The Banker 2024

9. News: AI means more skilled AML professionals needed, not less AFC tech expert Shlomit Wagman tells WiFC Summit - AML Intelligence

SPENDING ON MANUAL PROCESSES IN FINANCIAL CRIME 2024 (EURO BN)



Chartis research: data from LexisNexis Risk Solutions 2025, Oxford Economics 2024, Dun & Bradstreet 2023, The Banker 2024

> The **composition of teams** will be gradually shifting. In the past, there was one person or a small number of people who set up the system for transaction monitoring or KYC – and armies of investigators who were processing the individual cases.
>
> With increasing efficiency, automation, and the use of AI, the **need for manual processing will decline**. At the same time, demand will rise for experts who deeply understand AML, KYC and KYT, and who can manage systems, drive automation, assess performance and deliver innovations and insights.

Jiří Feix
General Manager of the Financial Crime Unit at KBC Group

important factor for effective AML compliance" with **over 90% of respondents stating that they plan to grow their AML teams by at least 10%**.[10]

Moreover, strict regulatory requirements and evolving AML frameworks mean that institutions must constantly look for talent with **up-to-date knowledge**. Additionally, the **high-pressure** nature of AML roles (often involving the investigation of suspicious transactions and compliance with complex legal frameworks) can deter potential candidates from entering the field.

Retaining good professionals

Hiring AML talent isn't the only struggle. **Keeping them on board is challenging too, for a number of reasons:**

- Increasing workload from tighter regulatory oversight;
- Need for manual reviews (often focused on false positives);
- Limited feedback on relevance from investigation units;
- Lack of convictions and confiscations (Europol's 2025 report shows confiscations remains at around 2% of illicit proceeds).[11]

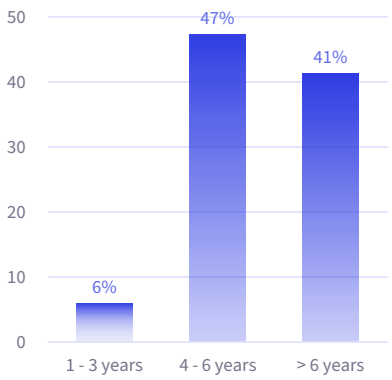
These factors can lead to job dissatisfaction and high turnover.

To retain AML staff, organisations should:

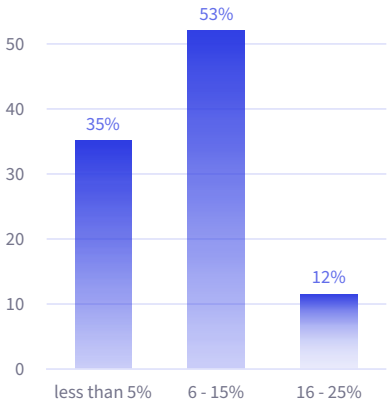
- Focus on employee engagement, career growth, and work-life balance;
- Use automation to reduce administrative burdens;
- Build a strong compliance culture.

10. EMEA AML Survey 2024: Spotlight on Effectiveness
11. Europol (2025), European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime, publications Office of the European Union, Luxemburg

AVERAGE EXPERIENCE LEVEL
AML STAFF IN YEARS



AVERAGE ANNUAL AML
EMPLOYEE TURNOVER RATE



Chartis research: 1LoD Financial Crime Leadership network

Training and upskilling teams

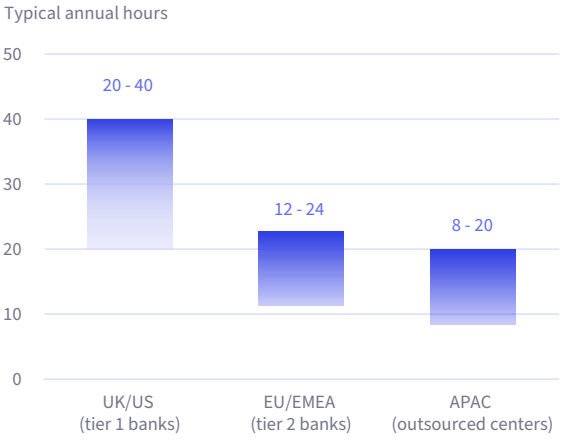
AML professionals must stay ahead of new money laundering techniques, regulatory changes, and technological advancements. To support this, **institutions should invest in ongoing education** such as AML certification programs (e.g., CAMS: Certified Anti-Money Laundering Specialist), in-house training, and AI-powered learning platforms.

Cross-functional training that **combines compliance and data analytics** equips professionals to better address money laundering challenges. Some institutions have also started using **simulation-based training**, where employees work through real-life AML scenarios to improve their investigative skills.

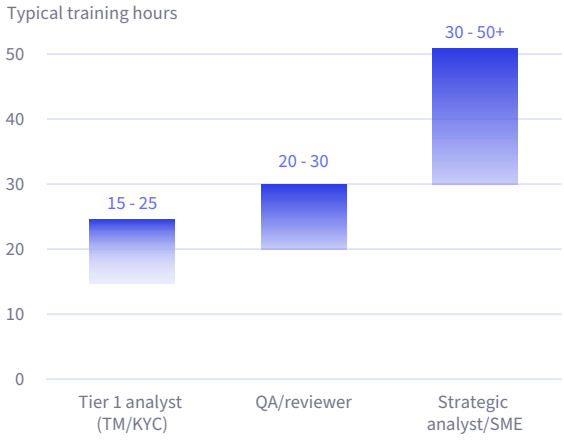
> “It takes **one to two years** to **fully train a KYC or KYT operations professional from scratch**. However, developing someone with enough experience to manage and improve these systems takes even longer and requires a mix of talent and skills, including analytical thinking, data knowledge, ICT, and creativity.”

Jiří Feix
General Manager of the Financial Crime Unit at KBC Group

CHALLENGES RESOURCE &
TALENT MANAGEMENT PER REGION



CHALLENGES RESOURCE &
TALENT MANAGEMENT PER ROLE TYPE



Chartis research: 1LoD Financial Crime Leadership network

Profiles and skillsets

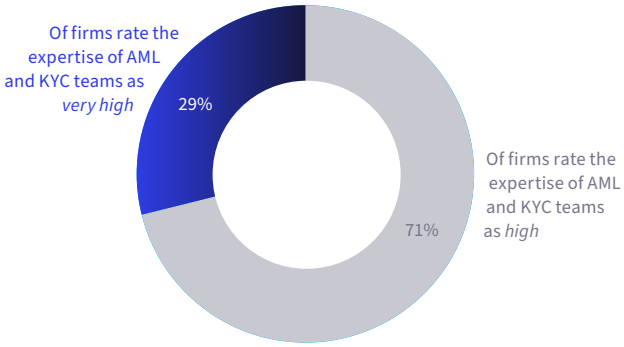
AML professionals need to evolve along with the landscape. While **regulatory and legal expertise** and **critical thinking and investigative skills** have long been foundational to effective AML work, today's challenges demand a broader and more integrated approach.

The modern AML workforce needs to combine traditional strengths with new capabilities:

- **Regulatory & legal knowledge**: A deep understanding of local and international AML laws remains essential, along with the agility to adapt to frequent regulatory changes.
- **Critical thinking & investigative skills**: The ability to analyse complex transactions, uncover illicit activities, and trace criminal networks continues to be a core requirement.
- **Process thinking, IT & data science integration**: What's new is the need to embed AML efforts within robust process frameworks, leverage IT systems effectively, and apply data science techniques, like machine learning and big data analytics, to improve detection and monitoring.
- **Strategic prioritisation**: With expanding tools and data, success increasingly depends on placing the right emphasis on the right activities, so technology and analytics serve the broader compliance and investigative goals.

As the industry continues to transform, firms that proactively invest in talent, technology, and continuous learning will be better positioned to counter financial crime effectively.

RESOURCE & TALENT MANAGEMENT CHALLENGES



Chartis research: 1LoD Financial Crime Leadership network

> "I want to stress that **common sense will remain crucial** for analysing behavioural patterns and intent. That's not surprising, as every digital profile reflects a human being. Digital profiles often mirror the physical world, but the interactions occur at a much faster pace."

For more on Stefan's perspective on international AML regulations and cross-border cooperation, see the full interview in the annex.

Stefan Delaet
General Manager Financial Crime at KBC Group

4
Data management

Strong data management underpins effective AML, yet many organisations continue to struggle. Robust data practices must address architecture and quality, maintain a balance between privacy and security, mitigate risks of bias and discrimination, and uphold trust and governance.

Vision, architecture and quality

Effective transaction monitoring in AML requires a strong data management framework, including clear strategy and vision, architecture, and data quality. **One common problem** organisations face is **scattered data from different sources**, often caused by mergers and acquisitions. These disparate systems often lack integration, making it difficult to access reliable, consistent information for monitoring and analysis.

In AML operations, **high-quality data is essential**. Financial institutions often need to pull information from many different sources, including legacy banking systems and third-party vendors. This makes data consolidation difficult. Poor data quality can lead to more false positives in transaction monitoring, escalating operational costs and prolonging investigation times.

Additionally, the **lack of entity resolution** makes it harder to identify individuals and organisations involved in suspicious activities. Without a unified view, accurate tracking and monitoring of transactions is difficult. Future developments, like insight sharing through partnerships (see 'Article 75' on page 36 in this paper) may increase the need for entity resolution. Legacy architecture adds to these challenges, as **outdated technology struggles to handle the complexities of modern AML requirements**. This leads to inefficiencies and a higher risk of undetected financial crimes.

*According to the "**Encyclopedia of Machine Learning**" by Indrajit Bhattacharya and Lise Getoor.*

***Entity resolution** is the process of identifying and linking references that refer to the same real-world entity across one or more datasets. It involves resolving uncertain or imprecise references by discovering the unique set of underlying entities and mapping each reference to its corresponding entity.*

This typically includes:

- *Identifying references with different attributes that refer to the same entity.*
- *Disambiguating references with similar attributes that refer to different entities.*

*Entity resolution is also known by other terms such as **record linkage**, **deduplication**, **co-reference resolution**, and **object consolidation**.*

45%

of EMEA firms identified **data quality** as the primary obstacle to adopting new AML technology.

20-30%

of TM alerts is estimated as invalid or false positives due to **flawed data**, resulting in wasted analyst effort and increased burden on AML teams.

45%

of financial crime professionals rank **poor and siloed data** among the top barriers to risk detection, as the primary obstacle to adopting new AML technologies.

Chartis research:
1LoD Financial Crime Leadership network

Data standardisation is key to keeping AML processes consistent, especially for multinational financial institutions working under different regulations. To meet these challenges, institutions should use robust data validation methods, thorough data cleansing and AI-driven anomaly detection to improve data accuracy.

Moreover, the **lack of a dedicated financial crime data platform** limits the ability to gather and analyse relevant data effectively. Such a platform is crucial for creating a central repository of financial crime information, which helps improve detection and prevention of illegal activities. Tackling these issues calls for a strategic approach to data management, including the adoption of advanced technologies and methods to ensure data integrity, consistency, and accessibility.

It is important to tailor **data quality governance** specifically to AML principles and requirements, rather than trying to cover all data in the bank. A focused approach makes the governance framework effective and manageable, by concentrating on the areas most critical to AML compliance.

A well-maintained data governance framework is essential in this context. It helps keep data accurate, complete, and up to date, which minimises compliance risks and makes overall AML efforts more effective. By **prioritising data quality for AML**, financial institutions can improve operational efficiency and strengthen their compliance an increasingly strict regulatory environment.

Privacy-security balance

Data privacy and security are **essential pillars of AML compliance**, but they must be understood within the **broader legal framework**. Financial institutions are required to protect customer data under laws like the General Data Protection Regulation (GDPR), yet AML obligations, such as those under the EU Anti-Money Laundering Directives, may take precedence when necessary to prevent financial crime.

> “If data management or quality were easy, development would move faster, implementation times would shorten, costs would decrease, and stakeholder confidence would increase. Beyond the data itself, **a crucial factor is stable staffing and strong (domain) understanding of the data used in modelling**. GDPR presents challenges, as tokenisation and data analysis often don’t mix well.”

Alpha Peeters
AML Program Manager
Financial Crime Unit,
KBC Group

This means that **AML programs need to strike a careful balance**:

- **Aligning with global and local data protection laws**, including GDPR.
- **Ensuring compliance with AML/CFT regulations**, which may require data sharing, retention, and processing beyond what GDPR typically allows.

To manage this tension, institutions use techniques such as:

- **Data encryption**: Securing sensitive information during storage and transmission.
- **Anonymisation and tokenisation**: Minimising exposure of personal data while maintaining analytical utility.
- **Purpose limitation and access controls**: Ensuring data is used strictly for AML-related activities.

The European Commission and regulators like the EBA have clarified that **AML measures** are **considered** a **legitimate legal basis for processing personal data**, even if this involves restrictions on data subject rights under GDPR .

This underscores the principle that **protecting the financial system from abuse is a public interest** that can override certain privacy constraints.

CASE EXAMPLE

Amazon's AI recruiting tool (2014–2018)

What happened?
Amazon developed an internal AI system to help automate the screening of job applicants. The tool was trained on **10 years of resumes** submitted to the company, most of which came from **male candidates**, reflecting the tech industry's gender imbalance.

Problem
- The AI system learned to prefer male candidates and penalised resumes that included terms like "women's chess club captain" or degrees from women-only colleges.
- It also downgraded resumes with certain keywords linked to women.
- The bias was not intentionally programmed but emerged from the training data, which reflected past hiring trends.

Outcome
- Amazon scrapped the tool in 2018 after internal audits uncovered the bias.
- The case became a cautionary example of the risks involved in using historical data without addressing embedded societal biases.

Discrimination, bias and accountability

All AML solutions (whether AI-driven or not) must be **rigorously tested to prevent unintentional discrimination and bias**, especially in areas like transaction monitoring and customer profiling. Upholding fairness and transparency is essential to maintaining trust and regulatory compliance.

A key challenge in AI-based money laundering detection is preventing models from **disproportionately flagging** individuals or businesses based on race, nationality, or socioeconomic status.

Bias can arise from imbalanced datasets, outdated risk scoring methods, human input errors or even operator bias. Institutions should carry out fairness assessments and regular mode audits to spot and reduce bias in AML algorithms.

Transparent decision-making processes is crucial for ethical AI use. Additionally, **explainability tools**, such as SHAP (SHapley Additive exPlanations) values can help compliance teams understand why certain transactions or customers are flagged as high risk, promoting fairness and accountability in AML operations.

Trust and governance

Building trust in AI-powered AML systems requires **transparent governance frameworks and regulatory oversight**. Financial institutions have to make sure that **AML decision-making models are interpretable**, **auditable**, and **explainable** to both regulators and internal stakeholders.

Effective governance involves clearly defining roles and responsibilities for data management, holding teams accountable for data quality, and enforcing compliance with regulations. Collaboration between compliance teams, data scientists, and regulators helps create a culture of transparency and responsible use of AML solutions.

Additionally, integrating **human-in-the-loop mechanisms** allows automated AML decisions to be reviewed and overridden when necessary. This prevents errors and increases stakeholder confidence in AI-driven compliance solutions.

> “Both management and investigators themselves need time to build trust in AI. You have to **demonstrate that AI can match or outperform human results**. It’s best to start with smaller, understandable tasks and consistently validate AI outcomes with people to gradually build confidence.”

KBC Group Financial Crime Unit

5
Sticky legacy

Legacy tools for transaction monitoring in AML pose significant challenges. They produce large volumes of false positives, have limited accuracy in detecting suspicious activity, are costly to operate and maintain, and struggle to integrate with newer technologies. Overall, legacy transaction monitoring technology cannot meet the evolving demands of AML compliance and must be replaced with advanced solutions.

Batch-based processing

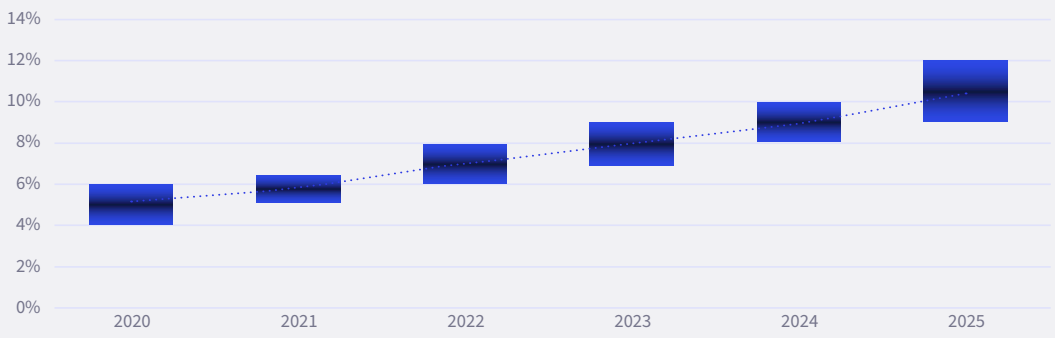
The outdated nature of these tools is clear in their batch-based processing, which operates ex post (reviewing transactions after they occur rather than in real time). This limits the ability to provide a comprehensive overview of AML risks across a portfolio, focusing instead on individual transactions.

As a result, **organisations struggle to gain a full understanding of their AML risk exposure**, making effective risk management difficult.

False positives

Legacy AML transaction monitoring systems often produce an **overwhelming number of false positives**, placing a **heavy burden on compliance teams**. Their rigid, rule-based design lacks the flexibility to accurately distinguish between legitimate and suspicious transactions. As a result, financial institutions must manually review a high number of triggers.

TRANSACTION MONITORING EFFECTIVENESS RATES



Chartis research

This inefficiency:

- Increases operational costs and leads to compliance fatigue;
- Takes time and resources away from high-risk activities;
- Impacts customer satisfaction, as legitimate transactions may be flagged and delayed unnecessarily.

To address these challenges, the industry is increasingly turning to **AI-driven models** that use **dynamic risk scoring** and **pattern recognition** to **reduce false positives**.

Poor effectiveness

Many legacy AML solutions can't keep up with the more advanced methods money launderers use today. They often rely on **static thresholds and rule-based logic**, which **don't adjust to new financial crime tactics**.

For example, criminals may avoid detection by breaking up large transactions into smaller amounts (known as "smurfing"), exploiting limitations of traditional monitoring systems.

> "New or more detailed scenarios require changes to underlying data sources. This, in turn, triggers maintenance work on data feeds into legacy FinCrime applications. **Past reliance on external non-SaaS providers creates heavy dependency** on the vendor and its upgrade cycles. Whether the upgrades are useful or not, this leads to **high costs and delays**."
>
> KBC Group Financial Crime Unit

These legacy tools also **lack advanced capabilities like advanced network analysis**, making it harder to uncover money laundering rings and hidden connections. As a result, financial institutions remain reactive rather than proactive, increasing the risk of regulatory fines and reputational damage.

To address these shortcomings, modern AML systems now use machine learning models that continuously refine detection parameters based on emerging threats.

High costs

Legacy AML tools are not only ineffective but also carry **high operational**, **maintenance**, **and upgrade costs**. Outdated software requires constant patches, updates, and manual intervention to stay compliant with evolving regulatory requirements.

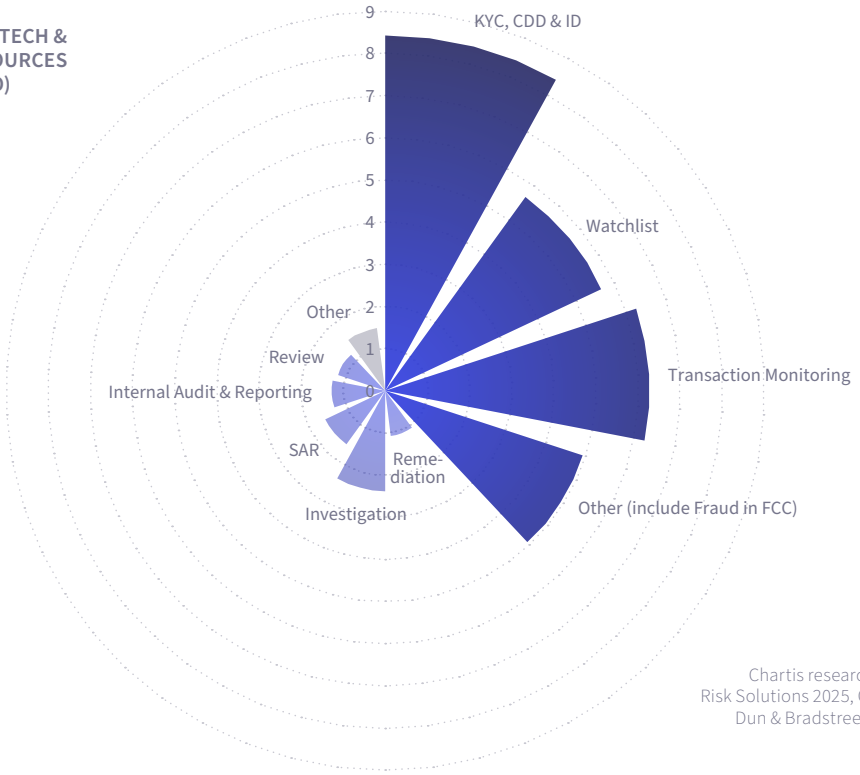
Maintaining **on-premises systems**, including hardware, licensing, and specialised staff, adds a significant financial burden. These systems often need **extensive customisation to meet new regulations**, leading to long implementation timelines and increased reliance on external vendors.

Institutions that continue to use these costly legacy tools risk falling behind competitors who adopt **cloud-based**, **scalable AML platforms**. Modern AML solutions, especially those powered by AI, offer **significant efficiency gains through automation and real-time monitoring** – but they are not without cost.

Implementing AI-driven systems can involve substantial upfront investment in infrastructure, data integration, model training, and governance. Additionally, ensuring transparency, fairness, and regulatory alignment in AI models requires ongoing testing, validation, and skilled oversight.

Ultimately, the shift to modern AML platforms can reduce long-term operational costs and improve effectiveness, but institutions must carefully weigh the total cost of ownership, including both legacy burdens and the complexities of advanced technologies.

SPENDING ON TECH & RELATED RESOURCES (BILLION EURO)



Chartis research: Data from LexisNexis Risk Solutions 2025, Oxford Economics 2024, Dun & Bradstreet 2023, The Banker 2024

Complex integration

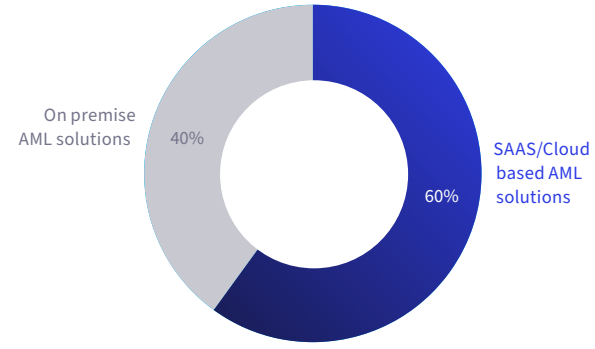
Traditional banking systems were **not designed to support real-time transaction monitoring or advanced analytics**. This makes the **integration of modern AML solutions** with existing legacy infrastructure **extremely challenging**.

Many financial institutions operate fragmented IT ecosystems with **scattered data sources**, requiring extensive middleware development and costly API integrations.

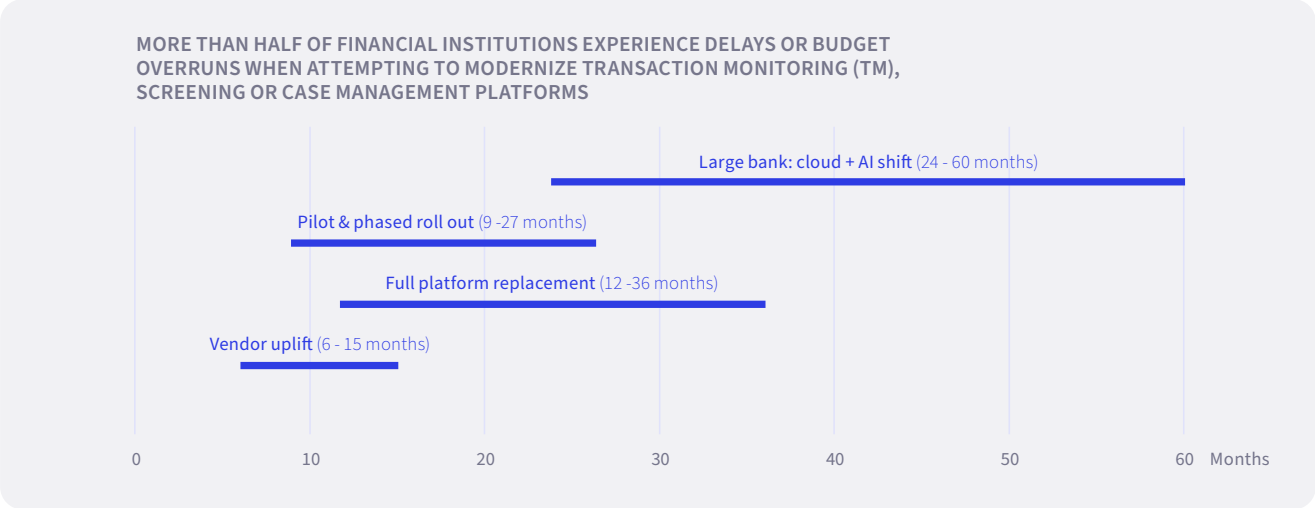
Additionally, legacy platforms often have **rigid architectures** that are **incompatible with AI-driven solutions**, requiring major system overhauls. These integration challenges slow innovation and delay the adoption of more effective detection tools.

> “Developing, validating and running an AI model is a lot more expensive than running a simple scenario. But when you consider that a **single model may have tens or even hundreds of scenarios**, each requiring regular performance analysis, recalibration, back-testing, and validation, the situation can look very different.”
>
> KBC Group Financial Crime Unit”

RATIO ON PREMISE VERSUS SAAS/CLOUD BASED AML SOLUTIONS



Chartis research: FATF (2021), LexisNexis Risk Solutions (2025)



Chartis research: 1LOD (2025), Deloitte (2024)

To address this, some institutions adopt **hybrid models** where **AI-enhanced solutions run alongside existing systems** until a full transition becomes possible.

Solution selection

The **AML market** is **crowded with vendors** claiming to offer proven, mature AI-supported solutions, making it hard for financial institutions to choose the right technology partner. Many providers promise cutting-edge AI-driven tools, but it can be **difficult to separate real innovation from marketing hype**.

Some vendors rebrand traditional rule-based systems as "AI-powered," even though they don't have actual machine learning capabilities. Financial institutions **have to deal with varying levels of regulatory approval, system transparency, and explainability when browsing solutions**. This process can feel like finding a needle in a haystack, as many offerings appear similar but vary greatly in effectiveness.

To overcome this, financial institutions should:

- Conduct thorough proof-of-concept trials;
- Benchmark vendor solutions against real-world transaction data;
- Prioritise solutions offering clear auditability, adaptability, and proven risk reduction.

> "To select the right vendor, you need to focus on **performance**, **understanding of needs** and **complexities**, **ease of data integration** (both in and out) and a **clear roadmap** for other use cases such as fraud and embargo."

KBC Group Financial Crime Unit

Market trends

1 Advancements in AI and intelligent systems

AI-driven solutions enhance AML efficiency and effectiveness by reducing false positives, automating risk assessments, and detecting complex criminal networks. The techniques below should not be seen as separate, stand-alone solutions but as building blocks that can be combined or introduced gradually as trust and expertise grow.

Improved alert ranking and augmentation

Traditional AML systems produce large amounts of alerts, many of which are false positives. AI-algorithms use predictive analytics and historical case data to **rank alerts by risk level**. This allows compliance teams to prioritise the most critical cases, manage backlogs and benefit from running AI and rule-based solutions side by side for comparison in a live environment.

Alert ranking assigns a numerical score to an entity based on urgency or intensity of investigation needed. A well-designed alert scoring system prioritises the riskiest customers, **so compliance teams can focus on high-priority cases**. Usually, a 0-100 scale is used, where 100 represents the highest risk.

The system evaluates transactions, entities, or activities using indicators like transaction patterns, customer profiles, and historical behaviour. Based on these parameters, an alert score is generated to **help compliance teams streamline case management**. **Higher-scoring alerts** are typically **routed to senior analysts**, while **lower-risk alerts** can be **reviewed by junior staff**.

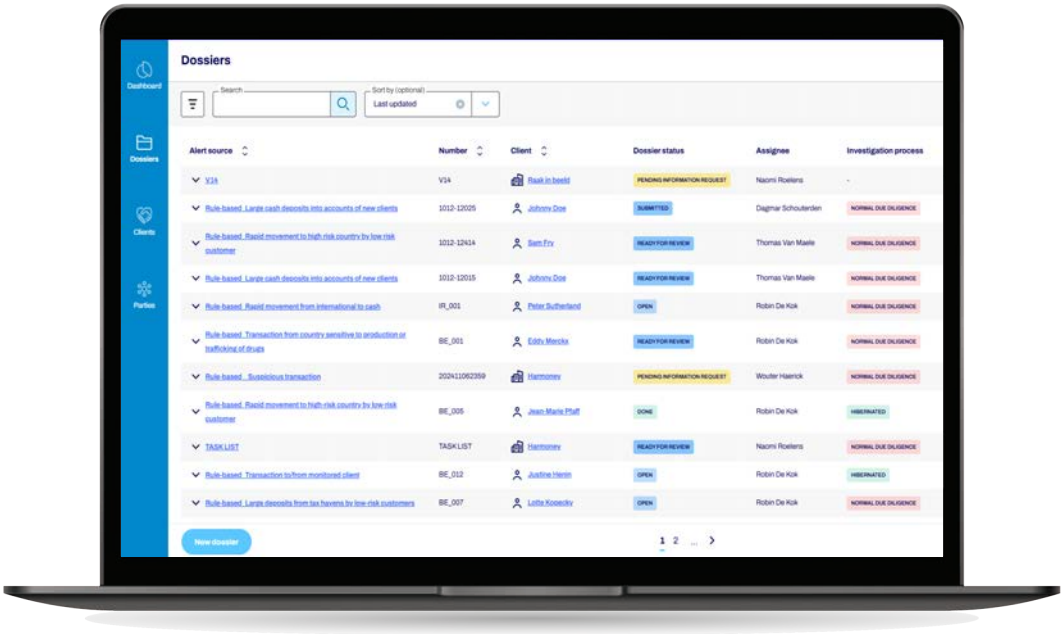
Risk-based investigation efforts

AI augments AML teams by **dynamically allocating investigative resources** according to risk severity. Rather than reviewing every case equally, AI models learn from past cases to focus time and expertise where it's needed most. Automated risk-scoring helps compliance teams prioritise cases.

> "After implementing AI in our AML KYT processes, **the number of triggers dropped** from a range of 65,000–85,000 to 50,000–70,000. Additionally, **AI generated 5,000 new relevant triggers** that were previously undetected, significantly improving our efficiency and effectiveness."
>
> Discai Client

Using a risk-based approach, financial institutions can **allocate resources more efficiently by focusing on high-risk cases** while **minimising efforts on false positives**. Instead of using a uniform investigative approach for all alerts, institutions leverage AI-driven

SCREENSHOT OF CASE MANAGEMENT APPLICATION OF HARMONEY, AN ECO SYSTEM PARTNER OF DISCAI



models to **dynamically adjust the level of due diligence** based on risk severity. Higher-risk cases get more scrutiny, while lower-risk alerts may have less due diligence or be temporarily put on hold.

This shift allows banks to move away from the traditional "sledgehammer approach", which often led to unnecessary disruptions for low-risk customers, towards a more refined "tweezer approach" that applies targeted measures only where necessary. Supervisory bodies, such as the Dutch Central Bank (DNB), stress the importance of this transition, encouraging financial institutions to tailor their compliance efforts based on rigorous risk assessments.[14]

Advanced analytics and AI-powered automation help institutions **optimise investigative workflows**, letting compliance teams concentrate on actual suspicious activities.

Complex pattern detection

Legacy tools struggle to spot hidden relationships in money laundering. **AI-powered anomaly detection and graph learning** connects separate transactions and actors to uncover illegal networks. Instead of just using static transaction thresholds, AI-driven models study **transactional behaviours**, **identifying suspicious activity across multiple accounts and entities**.

Machine learning models can add nuance to rule-based transaction monitoring alerts and help **detect more complex forms of money laundering** that traditional systems may miss.

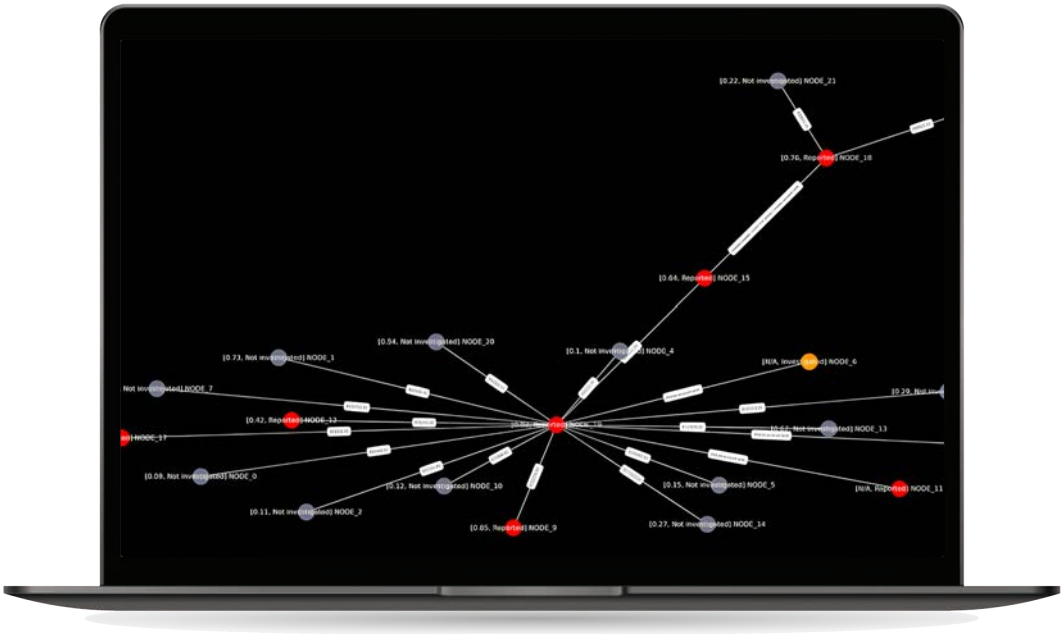
For instance, **a network of money mules** might remain under the radar if all participants use small amounts and don't trigger any scenarios individually. However, AI models can identify and investigate these complex networks, **using capacity that is unblocked because of reduced due diligence and hibernation processes**.

Automated content generation

The rise of **Generative AI (GenAI)** has transformed financial crime prevention, particularly through **automation of compliance reporting and regulatory processes**.

One of the most promising applications of GenAI in the AML domain is the **drafting of Suspicious Activity Reports** (**SARs**). Large Language Models (LLMs) support compliance teams by generating structured summaries that describe customer

AI MODELS CAN IDENTIFY AND INVESTIGATE COMPLEX NETWORKS



14. De Nederlandsche Bank: Van herstel naar balans: een vooruitblik naar een meer risicogebaseerde aanpak van het voorkomen en bestrijden van witwassen en terrorismefinanciering. (From recovery to balance: a look ahead to a more risk-based approach to preventing and combating money laundering and terrorist financing.)

> We aim to provide the investigators with a **pre-drafted summary of the client and the case history**, combined with alert explainability.
>
> KBC Group Financial Crime Unit

FICTIOUS EXAMPLE OF A SUSPICIOUS ACTIVITY REPORT

Reporting institution:
ABC Bank Ltd.
Compliance Department
123 Compliance Street, Brussels, Belgium

Date of report:
6 June 2025

Subject information:
- **Name:** John Doe
- **Date of birth:** 15 March 1985
- **Nationality:** British
- **Account number:** 123456789
- **Customer since:** January 2023

Nature of suspicious activity:
Unusual cash deposits and international wire transfers inconsistent with the customer's known profile.

Description of activity:
Between 1 April and 15 May 2025, the subject made **multiple cash deposits** totalling **€95,000** across different branches in Brussels. Each deposit was just **below the €10,000 reporting threshold** and occurred within short intervals (often on the same day).

The funds were then transferred to **three different accounts in Eastern Europe**, including one in a high-risk jurisdiction identified by the FATF. The customer claimed the funds were from "freelance consulting," but didn't provide **any supporting documentation**.

Reason for suspicion:
- Structuring "smurfing" to avoid reporting thresholds;
- Inconsistency with customer's declared occupation and income;
- Use of high-risk jurisdictions;
- Lack of transparency and documentation.

Action taken:
- SAR submitted to the BE FIU (CFIT/CFI)

Attachments:
- Transaction history;
- Customer identification documents;
- Internal compliance notes.

Prepared by:
Jane Smith
Senior Compliance Analyst
ABC Bank Ltd.

profiles, past investigations, risk assessments (from rules-based or AI-driven models) and overall findings. This automation significantly reduces the time needed to write reports, while maintaining accuracy and consistency.

Beyond SAR generation, GenAI is also **enhancing regulatory change management**. By analysing new regulations, LLMs can interpret legal texts, identify overlap with existing policies, and even create new policies to bridge compliance gaps. This **streamlines policy revision processes**, helping financial institutions stay aligned with the latest regulatory changes. GenAI can also deduplicate existing compliance documentation, improving operational efficiency in heavily regulated environments.

Some **advantages of GenAI in AML**:

- It is fast, consistent and adaptable.
- It minimises human error.
- It ensures that reporting aligns with the latest regulatory requirements.
- It allows investigators to focus on high-risk cases rather than administrative tasks.

However, financial institutions have to make sure that AI-generated reports are understanable and meet regulatory expectations for auditability and explainability. **Human oversight remains essential** to validate AI-generated content, with the goal of complementing rather than replacing expert judgement. As AI continues to advance, using GenAI in AML operations will become a key advantage, helping firms stay compliant at scale while improving the effectiveness of financial crime prevention.

Smart AI agents

AI agents are the next step in AI-powered AML operations, offering a smarter and more efficient way to detect money launderers and stay compliant. These systems **go beyond basic automation**: they **proactively gather and analse relevant data**, **streamline investigative processes**, and **help maintain regulatory adherence**.

One of its main functions is the **automatic retrieval of crucial information**, such as:

- Historical customer investigations;
- Associated risk patterns from similar entities;
- External news sources;
- Structured transaction aggregations.

AI could also **provide insights into company structures**, including shareholder and director information, providing investigators with a complete picture of the entity being examined.

Effective **AI-powered case management systems** use entity resolution techniques to correctly link external data sources to customer profiles. This way, investigators receive the most relevant information at the right time, allowing faster decisions and improved efficiency. AI agents can dynamically assign alerts to the most appropriate workflow based on risk factors, investigator expertise, and predefined compliance protocols.

Despite their potential, the **adoption of AI agents in AML operations remains limited**. Many financial institutions are cautious about full integration due to concerns around regulatory compliance, explainability, and adaptability to nuanced risk environments.

Still, AI agents offer a strong path forward. Banks can encode their internal policies, regulatory obligations, and risk appetite into structured instructions. By leveraging best practices and predefined workflows, AI agents can automate key steps like case assignment, data retrieval, reporting, and transactional analysis while staying flexible enough to handle unique customer risk profiles.

Implementing AI agents is expected to greatly improve the efficiency of AML operations, increasing compliance accuracy and cutting down on manual work. As AI technology advances, using AI agents **will become essential for intelligent compliance**, helping financial institutions stay regulatory compliant in a more complex financial world.

General and super intelligent AI

This whitepaper does not explore General and Super Intelligent AI, as much about these technologies remain **uncertain** and **speculative**.

However, staying alert to developments in this area is important to manage complexities, maximise benefits and reduce risks associated with these technologies.

General and Super Intelligent AI could bring both **major opportunities and potential threats**. Although the timeline and progress are uncertain, monitoring the shift from narrow AI applications to more advanced systems is crucial. Narrow AI, which excels in specific tasks, serves as a foundation for understanding and anticipating the capabilities of more generalised AI.

By following these changes, stakeholders can better prepare for the transformative impact of General and Super Intelligent AI, while prioritising ethical considerations and safety measures.

2
Enhanced client insights

Traditional AML approaches have typically focused on individual transactions, but money laundering increasingly occurs across complex networks. Trends in the sector point to more holistic strategies that emphasise dynamic, risk-based client profiling, analysis of relationships across accounts and entities, and integration across previously siloed systems.
These developments enable earlier detection of suspicious behaviour and more robust compliance practices.

Transaction-centred monitoring

Traditional AML systems have historically focused on **monitoring individual transactions** in isolation or aggregations. This approach often leads to many false positives and false negatives, **resulting in fragmented risk assessments**.

Transaction-centred monitoring uses **predefined rules and thresholds** to flag potentially suspicious activity, but criminals adapt to avoid detection. AI and machine learning now play a critical role in improving transaction monitoring by spotting hidden patterns, anomalies, and structuring techniques.

360° client view

A holistic client view **goes beyond just monitoring transactions**. It assesses customer risk using **multiple data points**, including past transactions, behaviour patterns, and external risk indicators. By combining data from various internal and external sources, financial institutions can build a complete risk profile for each customer. This helps them assess more accurately whether activities match expected behaviour.

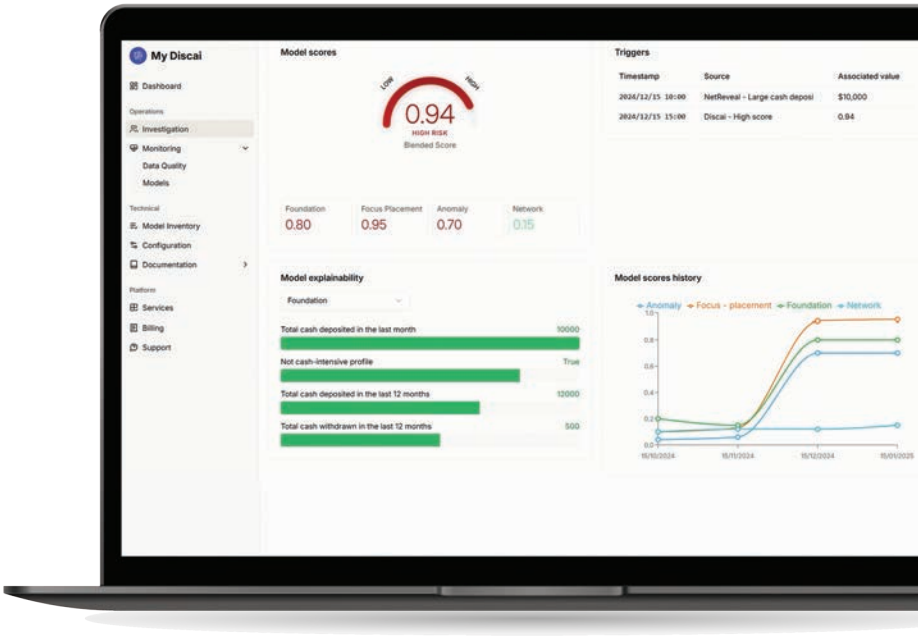
For example, if a retail client who usually makes small local transactions suddenly starts sending small or large sums to offshore accounts, the system can flag this deviation for review.

1 alert is typically generated per **700-3.300 transactions**, highlighting high volumes and potential over-alerting.

Only **1** in **4-10 alerts** becomes a case, showing significant alert triage.

Just **5-10%** of **alerts**, or **1** in **10-20 cases**, lead to a suspicious activity report (SAR), reflecting a steep drop-off from alerts to regulatory filings.

Chartis research: Deloitte (2024), 1LOD (2025), Flagright (2024)



SCREENSHOT OF DISCAI'S AML KYT CLIENT PROFILING

Bank network view

Money laundering is rarely isolated. Rather than focusing on individual transactions, a network-based approach examines connections between accounts, entities, and transactions to uncover complex schemes.

Through **AI-driven network analysis**, institutions **can detect hidden relationships** among entities that seem unrelated or accounts from other financial institutions. Visualisation and analysis of flows at a network level can help banks detect collusion, layering techniques, and coordinated financial crimes more effectively.

Combined monitoring and screening

Financial institutions have **traditionally** used **separate systems for AML, fraud detection, and sanction screening** – yet money launderers often take advantage of the gaps between these systems. By creating a unified framework, institutions can develop a more complete risk management strategy.

This allows **AI-powered platforms** to **cross-check suspicious transactions across different compliance domains**, improving detection accuracy. In addition to improving detection capabilities, **integrating fraud**, **AML**, **and sanction screening can cut costs** by rationalising data feeds, storage, and case management.

> "AI is currently limited to its own data, but **an overarching system could identify patterns across institutions without violating customer confidentiality**. Added experience from investigators and insights from sources like the Financial Intelligence Unit (FIU) and National Bank will help to identify suspicious behaviour and further tighten the net around the professionalised organisations engaging in money laundering as a service."

Frans Thierens
Anti-Money Laundering Compliance Officer (AMLCO) at KBC Bank

For Frans Thierens' take on how AI reduces the complexity of modern AML, read the full interview in the annex.

> What I would love to see is a broader scope of cooperation, particularly on developing best practices for risk management and monitoring. That includes **enriching banking data with information from other institutions and the public sector** to make our way of working more effective.

Michael Wittenburg
Senior General Manager Compliance at KBC Group

For further insights from Michael on the successes and challenges of AI in AML strategies, refer to the full interview in the annex.

(International) insight sharing

Collaborative intelligence sharing among banks and across jurisdictions is **one of the most promising steps forward in AML**. Money laundering often involves cross-border transactions, making it crucial for institutions to share risk insights while respecting privacy regulations.

Singapore's **COSMIC** (Collaborative Sharing of ML/TF Information & Cases) initiative facilitates information sharing among major financial institutions, so they can detect and prevent money laundering more effectively.

The **European Union's latest AML package**, and particularly **Article 75**, wants to enable cross-sector and cross-border information and intelligence sharing by **creating information sharing partnerships**. This regulation would give public and private participants regulatory responsibilities when necessary. This way, they can share their understanding of strategic threats and information on particular criminal networks in a properly governed and safe way.

Article 75 – Partnerships in AML (EU AML Regulation 2024/1624)

***Article 75** of the **EU Anti-Money Laundering Regulation (EU) 2024/1624** introduces a formal legal basis for the creation and operation of **public-private partnerships (PPPs)** in the fight against money laundering and terrorist financing.*

These collaborations show that joint AML efforts are recognised to lead to better crime prevention. By using secure data-sharing methods and privacy-protecting technologies, banks worldwide are joining collective intelligence frameworks to strengthen global efforts against money laundering.

3
Proactive risk prevention

AML strategies are moving from reactive to real-time: financial institutions are adopting event-driven architectures and predictive analytics to detect suspicious activities before escalation.

AML efforts have typically been reactive, responding to financial crime after suspicious activities are detected. By shifting towards proactive AML strategies, institutions aim to prevent money laundering and fraud before they occur or before escalation. Potential threats can be identified early using real-time transaction monitoring, behavioural analytics an AI-driven risk assessments.

Fraud and sanction examples

As money launderers and sanctioned entities keep changing their tactics, financial institutions need to anticipate risks proactively. **AI-powered models** can **detect subtle changes in transactional patterns**, identifying fraud attempts before they escalate.

For example, a recently retired couple made a transaction to a shell company in Dubai, which was flagged by the monitoring system. When asked, they said it was for a crypto investment. Although they didn't admit it, the transaction was suspected to be fraudulent, and they were informed accordingly.

Event-based architecture

Event-based architectures revolutionise the way financial institutions approach anti-money laundering.

This innovative approach:

- Enables the **processing of real-time triggers**;
- Allows for **dynamic adjustment of risk models** based on emerging threats;
- And thus marks a **big change from traditional batch-based** compliance checks.

As event-based architecture enables **instant transaction analysis**, financial institutions can respond more swiftly to potential threats. This real-time capability is crucial today, because financial threats are dynamic and call for quick intervention.

Moreover, **integrating external data sources** (like geopolitical developments and law enforcement alerts) makes financial crime detecting even more effective. By incorporating diverse data streams, financial institutions understand the risk landscape better, resulting in more informed decisions.

The move to an event-based architecture is a logical step forward, as everything related to the banking business is becoming more event-driven. This approach is **completely in line with the regulation of instant payments**, ensuring that financial institutions stay compliant and efficient.

Event-based architecture not only **improves** the **accuracy** and **timeliness of AML efforts** but also gives financial institutions the chance to **proactively address** emerging threats. Agility and responsiveness remain crucial.

Investigation throughput time

One of the biggest **challenges in AML investigations** is the **time** needed **to process and review suspicious activity reports**. AI-driven automation and workflow improvements greatly reduce the time investigators spend manually checking alerts. By automatically gathering and organising relevant case data, AI helps compliance teams resolve investigations more quickly.

> “Overall, the goal and current trend is to **shorten throughput time through efficiency gains**. However, there are some hard limits, such as “outreach”, which is partly beyond our control.”

Successful AI use

Creating value in combating financial crime involves many factors and should be customised to fit each financial institution's specific needs.

This value can take many forms, such as:

- **Uncovering hidden patterns** in suspicious activities;
- **Improving employee satisfaction** through streamlined processes;
- **Reducing operational costs** by automating routine tasks.

To achieve these benefits, **human involvement must be balanced with AI adoption**, keeping a human-in-the-loop approach to maintain accountability and trust. **Explainability of AI models** is essential to build trust among stakeholders.

A **clear vision and robust architecture** are essential for effective data management, infrastructure, and model risk management. Institutions need a **complete control framework** to stay safe from potential threats and ensure the integrity of their systems and models. **Proper AI governance** is the final piece of the puzzle, guiding ethical and responsible use. By combining these elements, institutions can maximise the value of their AML efforts, creating a safer and more efficient financial system.

1
The human factor

As mentioned before, AI adoption in AML requires skilled professionals to interpret AI insights, safeguard model explainability, and guard regulatory compliance.

Understanding and adoption

To start using AI in AML, it's crucial to understand what it can and cannot do. It's essential to demystify AI for all stakeholders and stress that it is meant to support, not replace, human expertise. **Education programs and pilot projects** are key to demonstrate AI's capabilities and limitations. By running pilot initiatives, institutions can showcase tangible benefits and ease concerns about AI's role in AML.

> "The saying "**Repeat a lie often enough and it becomes the truth**" comes to mind with AI models. I'd be cautious about using a model that only explains itself by pointing to past decisions. True explainability should be based on clear, descriptive elements."

At an individual level, AI adoption depends on how useful and easy someone thinks it is. These are some key factors influencing adoption:[15]

- **Perceived ease of use**: Employees need to find AI tools easy to use without much effort.
- **Job relevance**: AI should help employees with their daily tasks and make their work better.
- **Output quality**: Employees trust and use AI only if its results are accurate and reliable.
- **Result demonstrability**: Employees should be able to see how AI improves their investigations.
- **Perceived enjoyment & computer self-efficacy**: People are more likely to use AI if they feel confident and enjoy using it.

Cross-functional collaboration is needed for successful AI implementation in AML. Compliance teams, business process transformation teams, model validation teams, data engineers, legal advisors, and operations specialists have to work together to guarantee that AI-driven solutions meet both regulatory requirements and business goals.

AML Compliance Officers (AMLCOs) need to be actively involved in the validation of AI models, to make sure that outputs are clear and fit existing compliance frameworks. Institutions that embrace multi-disciplinary collaboration can build AI-powered AML solutions that are both effective and scalable.

Senior management and leadership support is crucial for a successful data-driven AI strategy. Their commitment secures needed resources and promotes a culture of innovation and trust. Leaders can champion the vision by aligning AI initiatives with business goals, helping to overcome resistance and address ethical challenges.

15. Based on insights dissertation Joke Cherlet on Increase in the adoption of AI models – using explainability

Trust

AI models need to be **explainable** and **observable** for successful AI adoption: compliance teams need to understand how decisions are made. Observability mechanisms like **monitoring model performance**, **tracking decision-making pathways** and providing **clear audit logs** create trust. Transparency builds acceptance with both investigators and regulators alike, reinforcing compliance with AI-driven AML practices.

Employee satisfaction

AI can improve employee satisfaction by **reducing repetitive tasks**, such as reviewing false positives. This lets analysts focus on complex investigations that need human intuition and judgement. **AI also creates new roles**, like AI risk managers and model governance specialists, providing opportunities for career growth. Institutions that proactively invest in training employees on AI-driven compliance tools will see higher engagement and better retention in their teams.

Accountability

It's clear that AI can improve AML efforts, but **humans should remain accountable**. AMLCOs need to be authorised to make the final decision, so AI-driven outcomes can be properly reviewed before action is taken. Regulators also expect institutions to document AI-related decisions, demonstrating that AI outputs are overseen by humans. Establishing clear accountability frameworks aligns AI-driven compliance strategies with ethical and regulatory standards.

2
Modern FinCrime architecture

Institutions need to create AI risk management frameworks to monitor model performance, mitigate bias, and maintain data integrity.

Enterprise-wide risk assessment (EWRA) and beyond

An Enterprise-Wide Risk Assessment (EWRA) is an important component of AML Risk Management. An **EWRA evaluates and mitigates risks** that may impact a bank's profitability, stability, and reputation. Traditionally, financial institutions follow a **risk-based approach**: high-likelihood, high-impact risks receive more scrutiny, while lower-risk areas need less oversight. AML risk mitigation starts at customer onboarding with KYC checks, sanction screening, and authentication, helping verify that customers and transactions align with the institution's risk appetite.

Beyond traditional AML risk factors (like products, customers, channels, and geographies), banks now also face **new risks** tied to data, AI models, and digital systems. External software providers must meet security and data protection standards while fitting into banks' risk frameworks.

Responsible AI use, transparency, and secure digital infrastructure should all be part of AML risk management to reduce exposure from tech-driven tools and third-party systems.

Data vision, architecture and control

In AML activities, including transaction monitoring, fraud detection, and sanctions compliance, a **strong data management vision** is essential. This means having a clear strategy for **how data is collected**, **stored and used**, in line with business goals and regulatory demands.

A **solid data architecture** underpins this vision, letting data flow smoothly between systems, integrates well and remains easily accessible. It enables seamless interoperability between various systems and applications, facilitating the extraction of valuable insights.

A key part of this architecture is **entity resolution**: the process of accurately identifying and linking data related to the same entity across different sources. This process combines all relevant information, helps reduce duplication and improves the accuracy of analysis.

Another important element is managing **positive labels for supervised learning**. These labels (SARs) help train AI models to recognise patterns and predict future occurrences by indicating suspicious instances.

Proper **data classification** is also **critical for anomaly detection**, where AI systems identify deviations from normal behaviour that may signal suspicious activities.

Managing all these components well makes AI applications more reliable and effective in AML.

Effective AML solutions depend on high-quality data. Poor data quality can lead to faulty risk assessments and ineffective transaction monitoring. But rather than slowing innovation, financial institutions can use AI data quality controls (like anomaly detection in event-based KYC processes) to improve accuracy.

Key data quality areas include:

- **Trustworthiness**: Using reliable data sources;
- **Consistency**: Keeping data definitions and structures stable;
- **Correctness & completeness**: Reducing missing or incorrect values;
- **Governance**: Assigning ownership and implementing monitoring processes;
- **Purpose alignment**: Making sure data fits AML needs;
- **Real-world representation**: Training models on data that reflects actual behaviour.

Regular monitoring of data quality helps catch and correct issues like data drift, outliers, and missing patterns, especially in AML transaction monitoring.

Infrastructure risks

Modern financial institutions need to **balance open digital ecosystems with solid security frameworks**. Cyber threats like data breaches and system intrusions, can cause serious financial and reputational damage. **Industry standards**, such as ISO, SOC certifications, **and** the **Cloud Security Alliance (CSA) Cloud Controls Matrix**, offer structured ways to strengthen digital resilience.

Key risk management areas include:

- **Threat & vulnerability management**: Proactively identifying and mitigating cybersecurity threats;
- **Supply chain security**: Safeguarding the integrity of third-party services;
- **Incident response**: Developing solid frameworks for security breach investigations;
- **Identity & access management**: Enforcing strict authentication (e.g., MFA);
- **Logging & monitoring**: Implementing real-time surveillance for anomalous activities.

A **strong cybersecurity foundation** helps financial institutions avoid disruptions and protect their reputation.

AI model risk

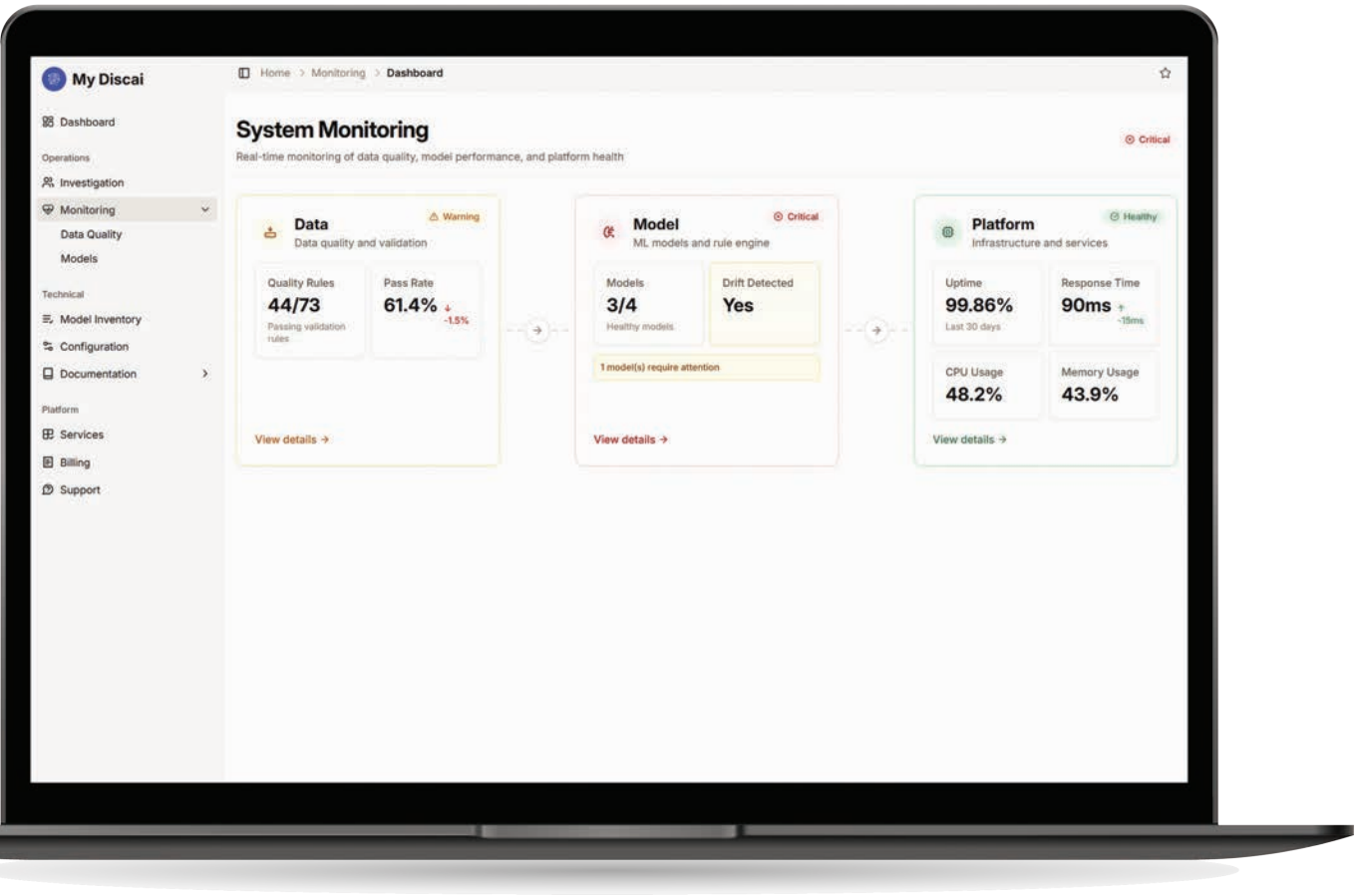
Financial institutions increasingly use AI models for AML, but **managing model risk is essential**. The European AI Act requires **AI models to be transparent**, **unbiased**, **and auditable**.

Banks must assess and validate these models based on:

- **Purpose definition**: Clearly identifying the intended use;
- **Risk classification**: Categorising AI models as high-risk, limited-risk, or minimal-risk;
- **Model inventory & governance**: Documenting all AI-driven models, including performance metrics, retraining schedules, and compliance status;
- **Initial & regular validation exercises and ongoing monitoring of**:
  - Input data evaluation: assessing data quality, completeness, and relevance.
  - Bias & fairness: ensuring AI-driven decision-making doesn't discriminate.
  - Model design review: analysing the logic, algorithms, and statistical techniques.
  - Performance monitoring: tracking precision, recall, and detection effectiveness to avoid model drift.
  - Audit & governance: implementing review processes for regulatory alignment.

A clear and well-documented AI risk management strategy helps institutions use AI effectively while staying compliant, ethical, and resilient.

SCREENSHOT OF DISCAI'S AML KYT PLATFORM MONITORING



3
Solid governance

Effective AI-driven AML depends on robust governance. Clear policies, cross-functional oversight, accountability, and transparency help models perform reliably, comply with regulations, and adapt to evolving risks.

Governance in practice

A strong governance framework sets clear **policies** for developing, deploying and monitoring AI models.

It also requires institutions to create **cross-functional governance teams that oversee AI models**, making sure they perform well and meet compliance standards. The teams should be made up of **people from different areas** like compliance officers, risk managers, data scientists, model owners, and legal experts.

Accountability is fundamental. Organisations have to define clear lines of responsibility, to guarantee human review of AI-generated outputs before regulatory actions are taken.

Explainability and transparency are crucial as well. AI-driven AML decisions need to be able to be interpreted and justified. Regulators require AML models to be auditable: institutions should be able to demonstrate how an AI model reached a decision. Techniques like model documentation, transparent algorithms, and explainability tools are key to meeting these rules.

Governance frameworks also need mechanisms for ongoing **performance monitoring and model validation**. AI models can degrade over time because of new criminal tactics, regulatory changes, and evolving customer behaviour. Regular audits, data drift analysis, and bias detection techniques are needed to keep models accurate and fair.

Finally, **continuous learning and adaptation** should be encouraged. AI in financial crime prevention is changing fast, so governance structures need to be agile and adapt to new technological advancements, emerging threats and regulatory changes.

Strong governance helps financial institutions tackle the complexities of modern AML and remain compliant and trustworthy.

> “To **establish solid AI governance**, you need to:
>
> - **Clearly identify model owners** (the main users or beneficiaries);
> - **Make sure the owners fully understand how the models work**, the input/output data and business context;
> - **Have an independent validation team** review the model;
> - **Make sure decision-making about model use includes oversights** – owners can’t decide alone if a model is fit for use.”

KBC Group Financial Crime Unit

Discai's proven AML KYT solution

AI built on banking expertise

Discai is a subsidiary of universal bank insurance player KBC Group, created to bring trusted, in-house AI solutions to the financial sector. Built within one of Europe's leading bank-insurance groups, Discai combines real banking experience with advanced technology. Its award-winning solutions are designed to meet regulatory requirements while improving day-to-day efficiency and effectiveness.

Enhanced monitoring with KYT

At the core of Discai's offering is its **AML Know Your Transaction (KYT) solution**: an AI-powered tool that truly transforms transaction monitoring. Already rolled out across KBC's five core countries, the solution replaces legacy systems and introduces a model-driven approach to AML.

The tool combines customer and transaction data to provide **near real-time risk scoring**. This helps teams make quicker and more accurate decisions. Institutions using KYT have seen a **40–60% increase in efficiency** and twice as many relevant cases being reported, without compromising risk controls.

Trusted technology

Discai's solution is cloud-based and modular. This means it can be easily integrated into existing systems or used alongside current tools. Its technology is tested, scalable, and aligned with regulatory expectations. Importantly, it avoids the risks often associated with acquiring unproven FinTech solutions.

As part of KBC Group, Discai offers long-term support, deep regulatory knowledge, and the stability of a trusted financial institution.

Get in touch

Discai enables financial institutions like yours to strengthen their AML capabilities with minimal disruption. To explore how our technology can support your compliance strategy, visit **www.discai.com** or contact us at **info@discai.com**.

Book your demo

Experts speak

Interviews

INTERVIEW

Michael Wittenburg outlines the **wins** and **failures of AI within AML strategies**

As the USA and the EU find themselves heading in very different directions with their AML efforts, one thing is clear: collaboration is more necessary than ever. In this conversation, Michael Wittenburg, Senior General Manager Compliance at KBC Group, outlines the current approaches to AML from a global perspective. He also explores the potential successes and pitfalls of deploying AI technology within a more unified global AML strategy.

There is a market perception that the USA has historically played a significant role in AML efforts around the world. However, recent actions by the Trump 2.0 administration have raised concerns. Actions like pausing investigations and enforcement under the Foreign Corrupt Practices Act (FCPA), disbanding anti-corruption task forces, and non-enforcement of beneficial ownership reporting. What are your thoughts on this recent shift in strategy from the USA?

I don't believe that the US has been leading the fight against financial crime. While there are efforts at the state and federal levels, particularly in terms of combatting terrorism, the overall approach is fragmented, with a patchwork of local regulations.

How would you compare the US approach to the EU's current stance on AML?

They are complete opposites. I believe the EU is leading the way today with its new AML package and the AI Act. The former directive approach led to localised interpretation and implementation, which in turn facilitated regulatory arbitrage. By moving towards a more harmonised regulatory approach, the EU is taking a good step forward. However, the effectiveness of this updated approach will depend on the technical standards we receive, since those will define the how throughout the EU.

What do you think is needed to build a more effective AML strategy?

To be truly effective, we need to expand the collaboration between banks, regulators and executive powers. Banks only know one part of the story, so a more integrated approach involving all stakeholders is essential. That collaboration should not impose responsibilities on banks alone but rather ensure a multilateral process that can fight money laundering from various angles.

To make a real difference, it will be paramount to share insights and collaborate across participating entities. With examples like the UK's Joint Money Laundering Taskforce and Singapore's COSMIC platform, as well as the new Article 75 in the EU's AMLD6, what is your view on the likelihood of practical use cases of this article?

What I would love to see is a broader scope of cooperation, particularly on developing best practices for risk management and monitoring. That includes enriching banking data with information from other institutions and the public sector to make our way of working more effective.

What are the biggest challenges in terms of implementing these cooperation efforts?

One of the significant barriers is the constraints imposed by regulations like GDPR. For example, an attempt at joint transaction monitoring in the Netherlands was discontinued by those constraints. While information sharing is valuable, we need to be much bolder in our cooperation. Transparency and information are crucial in fighting financial crime, of course, but we must ensure there are safeguards in place to prevent abuse.

What would you consider an appropriate operating model and information exchange protocol between participants?

In my personal opinion, though not realistic today, a possible approach could be for banks to share relevant data with regulators or Financial Intelligence Units (FIUs). By combining data from different banks with information from FIUs, the regulator/FIU could create a much more comprehensive monitoring system. It would involve integrating various data sources to get a full picture and monitor financial activities more effectively.

Do you foresee a leading role from the private or public sector in this collaboration?

Both sectors have crucial roles to play. Public-private partnerships are essential in this fight. The private sector – financial institutions in particular – often serves as the first line of defence against money laundering. They bring important resources to the table, from substantial staffing and expertise to advanced technology and vast amounts of data.

The public sector, on the other hand, provides regulatory oversight and investigative powers. Effective collaboration between these sectors can enhance detection capabilities, improve risk assessments and ultimately strengthen overall AML strategies.

In the coming years, how do you see the evolution of capacity and skillset for AML teams in the first and second lines of defence?

A typical investigator is often alert-driven, focusing on individual alerts and transactions. Cross-functional thinking in investigations is challenging, especially given the frustration that can come from false positives. People need to feel that their investigations and notifications lead to meaningful outcomes. Currently, we are too focused on the small fish rather than the big ones. Investigators will have to embrace cross-functional thinking and become more data-driven, considering each transaction in a wider context.

AML teams are great at investigating individual alerts, but to truly understand if an alert is a part of something bigger, AML teams need better tools, resources and means. It's similar to law enforcement, really: you wouldn't send the FBI to every crime scene. Instead, you would dispatch local police to deal with standard cases and reserve advanced profiles for complex matters. Different levels of seniority and skills will be needed.

To be bold, I don't believe that first-line investigations will be largely replaced by technology. While new technologies can enhance our capabilities, human oversight remains crucial. The EU also emphasises the importance of human oversight in the future. Technology can assist in reducing the workload and improving accuracy, but it cannot fully replace the nuanced understanding and judgement that human investigators bring to the table.

What critical success factors are needed to create value when using AI in financial crime fighting, particularly in the context of transaction monitoring?

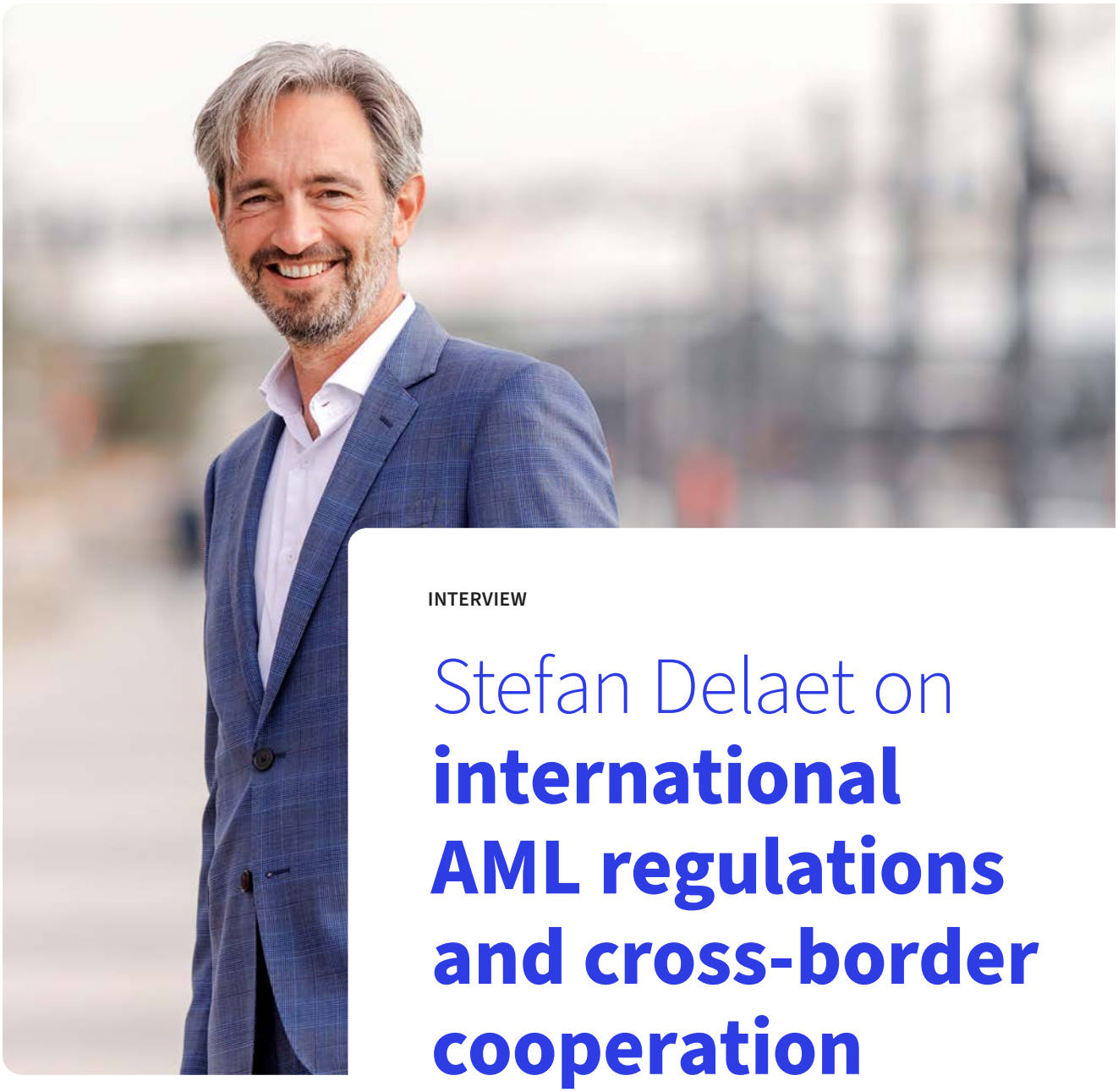
One of the major issues we see is that 80% of AI projects fail, whether they involve machine learning, deep learning or other technologies. These failures often stem from organisations not being ready in terms of mindset, strategy and foundational elements.

It's like buying the best airplane without knowing how to operate it: it's useless. The general problem is that AI systems are perceived to be a solution to all problems, but these systems need to be embedded within an overall strategy. You need to understand the root cause of the problem you want to solve before you can determine the best solution.

Many AI projects fail because organisations start to buy systems and develop models without first having the necessary foundation in place. Without a clear strategy and understanding of the problem they want to solve, those projects are doomed to fail. It's essential to know what AI is capable of and how it should be integrated into the overall strategy.

Thank you for your insights, Michael. It seems that AI holds great potential, though its success depends on a clear strategy, strong collaborative work and a solid understanding of its role in financial crime fighting.

Michael Wittenburg *became the KBC Group Senior General Manager Compliance in June 2024 after joining the group in 2023 as the General Manager Financial Crime Unit. He holds a doctorate degree in Policing, Crime and Security, alongside multiple master's degrees in areas of expertise such as Law, Governance, Risk and Compliance, as well as Counter-Fraud and Counter-Corruption.*



INTERVIEW

Stefan Delaet on **international AML regulations and cross-border cooperation**

AML is a complex challenge that requires international collaboration. We sat down with Stefan Delaet, General Manager Financial Crime at KBC Group, to discuss the impact of geopolitics, regulatory shifts, and AI on AML.

Let's dive right in. What do you think about recent articles about the pausing of the Foreign Corrupt Practices Act (FCPA), the disbanding of anti-corruption task forces, and the lack of enforcement around beneficial ownership reporting under the Trump 2.0 administration? How will these developments affect European AML lawmakers?

Since Europe introduced its first AML directive in 1991, it has gradually developed its own regulatory framework. This has resulted in the extensive single rulebook under the AMLR and the establishment of the Anti-Money Laundering Authority (AMLA).

On an international level, I believe the Financial Action Task Force (FATF) now has a much greater impact than the US. In total, over 200 countries and jurisdictions have committed to implementing FATF standards as part of a coordinated global response to prevent organised crime, corruption, and terrorism.

The Trump administration's current actions reflect an isolationist attitude aimed at protecting America from foreign threats and making America big again by limiting regulatory pressure on US firms and citizens. However, a mentioned, the EU has developed its regulatory framework and will continue to do so to preserve its internal market and its international trade position.

This graph from BCG Henderson highlights three significant trends: the United States leads in the creation of AI applications, China in their deployment, and the European Union in their regulation. How do you think geopolitics impact AML?
It is interesting, though not surprising, to see how different geographies follow different paths when it comes to embracing technology. Over the past decade, most new technologies have emerged from the 'land of the free' (the United States) driven by libertarian capitalism and the innovation engine of Silicon Valley. China, as a state-driven economy, has excelled at rapidly copying and deploying technologies across entire sectors and regions. Although lately, it is increasingly becoming a hub for development. Europe is literally in the middle and tries to make a careful trade-off between technology, politics, and consumer interest.

So in the fight against financial crime, what should take priority? Technology, people, or politics?
Well, it's clear: these three levers need to point in the same direction. Only then can we achieve sustainable change or development and move from a push-driven to a pull-driven market. Some argue that Europe is a political midget that lacks the courage to reduce regulations and therefore hinders the economy and evolution. Personally, I think that, apart from some regulatory exaggeration, Europe is actually quite sophisticated and capable – also in tech. At the same time, Europe is considerate of human rights, which is crucial for a strong democracy.

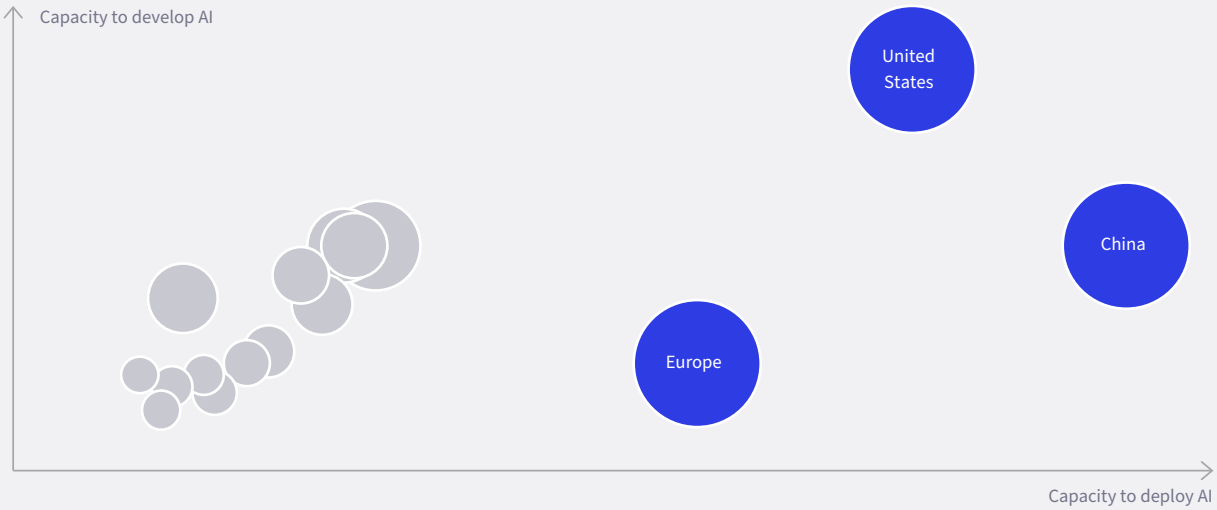
In other words, I believe that balancing the levers is in everybody's interest. Even if it sounds like a temporary setback to some people, I believe it's better than living in a society ruled by technocrats or autocrats. In the fight against money laundering, 'black-listing' of countries has long been a key tool. However, it's not the only one, and it can quickly become a political tool in current geopolitical times. Criminals are becoming more professional and tech-savvy, as they run their traffic through low-risk countries.

That means we cannot relax our rules or our investments in technology if we want to be effective in anti-money laundering and counter-terrorist financing.

Balance is clearly key.
Thank you for your time and for sharing your stance!

Stefan Delaet *is General Manager Financial Crime at KBC Group, with over 20 years of experience in leadership roles across strategy, finance, and risk. With his strong legal background, he brings a rigorous and principled approach to regulatory compliance and the fight against financial crime. His mission? To ensure that KBC remains resilient and ready for the future.*

AI DEVELOPMENT AND DEPLOYMENT WORLDWIDE



BCG Henderson Institute: Europa can catch up, but must act – today.
IMD World Competitiveness Centre, World Economic Forum; BCG Henderson Institute analysis.

INTERVIEW

Stefan Delaet on the evolving role of AML teams in today's digital world

As financial crime grows more sophisticated, AML teams have to evolve too. In this conversation, Stefan Delaet, General Manager Financial Crime at KBC Group, discusses the development of AML capabilities and staffing and recruiting options.

Stefan, tell us: how will capacity and skillset for AML teams evolve in the coming years? Which training and development plans are required for training and upskilling staff?
KBC has built a robust and high-performing AML framework, which has taught us a lot about what's needed for strong AML management. Efficiency through process and performance management is becoming increasingly important. Effectiveness is also high on the agenda, as criminals are becoming more organised and professional. That's why AML colleagues need to be flexible and agile in our detection and monitoring, much like in cybersecurity. We need detective mindsets to identify suspicious behaviours or transactions from the data and systems. Collaboration with stakeholders outside our organisation (such as regulators, FIUs, data and IT teams, our peers and competitors, the police and the justice system) will help us raise our game in the fight against financial crime.

How do digitalisation and technology influence the role of AML professionals?
Digital has become the new normal, meaning that the majority of transactions, onboardings, and client interactions now take place remotely. Because of this shift, AML teams need to be open to digital and IT tools. Machines will be able to process large volumes of information and enhance human capabilities. However, senior expertise will still be crucial for the final assessment, due to increasingly complex regulations and the sheer volume of data. This will require computational thinking, including an understanding of data flows and their logical, or illogical, outcomes.

According to AFC (Anti-Financial Crime) Tech expert Shlomit Wagman, the rise of AI means that more skilled AML professionals will be needed – not less. What is your opinion on this?
I believe what she says is valid. Training and development plans should emphasise continuous learning, combining both theoretical knowledge and practical skills. This includes training on the latest AML software and data analysis techniques, as well as keeping up to date with regulatory changes. Upskilling staff through certifications, workshops, and hands-on training is vital to keep up with the evolving AML landscape.

As I've already mentioned, I want to stress that common sense will remain crucial for analysing behavioural patterns and intent. That's not surprising, as every digital profile reflects a human being. Digital profiles often mirror the physical world, but the interactions occur at a much faster pace. It's almost like speed dating (laughs).

From an investigation perspective, where do you see the split between a first and second line of investigation in AML? What typical skills are needed for both?

In AML investigations, the first line of defence typically involves the initial alert generation and preliminary investigation. This includes tasks like transaction monitoring, customer due diligence (CDD), and initial risk assessment.

The primary objective here is to detect potential atypical behaviour early and flag them for further analysis. To do this, you need strong attention to detail, basic analytical skills, and familiarity with AML software. First-line professionals need to be adept at recognising patterns and anomalies in transaction data that could indicate money laundering.

The second line of defence, on the other hand, involves more in-depth analysis and decision-making. Findings from the first line are validated, more enhanced investigations conducted if warranted, and decisions made on filing suspicious activity reports (SARs) resp. adaptations in the monitoring approach.

The aim of the second line is to ensure that initial alerts are thoroughly investigated and that appropriate actions are taken based on the findings. To achieve this, advanced analytical skills, critical thinking, sound decision-making capabilities, and a deep understanding of regulatory requirements are essential. The ability to interpret complex data, grasp the broader context of transactions, and make informed judgements about potential risks is key to delivering strong results.

Here, I'd like to reiterate the need for increased trend analysis and information exchange in order to detect early attempts by criminals to bypass our systems. This is very similar to the prevention of cyberattacks. This will help us prepare for a future in which real-time monitoring becomes the norm.

How can companies structure their lines of defence to prepare for future AML challenges?

Regardless of how the division between the lines of defence is structured, it must be clearly defined and aligned with the maturity of each part of the organisation. At KBC, we have gradually expanded the tasks and responsibilities of the first line. In 2024, we even established a Group 1st Line Financial Crime Unit to streamline local standards and scenarios, and to take ownership of the applications. This approach ensures a consistent and effective AML strategy across the organisation, strengthening our ability to combat financial crime efficiently and effectively.

Most financial institutions are still exploring various options to address staffing issues. A recent report from PWC stated that "finding skilled staff is the most important factor for effective AML compliance" and that "more than 90% of the respondents stated that they are planning to increase the AML staff with 10% or more."

What is your take on various staffing options, like nearshoring, offshoring, outsourcing, automation, augmentation and so on?

The requirements for AML teams are indeed increasing, and your needs will depend on the maturity stage of your organisation. At KBC, we've gone through several stages, using all of these options at different points. Some years ago, we began by reinforcing both lines of defence through upstaffing. This was followed by centralising or nearshoring specific tasks and processes to Centres of Competence,. The strong capacity for standardisation within the nearshore centres also enabled us to automate more tasks yet with a human oversight.

In parallel, we started building models and we decided to use AI to enhancerule-based systems, which has reduced false positives and improved efficiency and effectiveness. This set-up offers a best of both worlds for now. It allows people to focus to further enhance the maturity of the AML programme.

Given the fast-changing world and requirements, the demand for qualified people will most likely remain high. With limited resources, organisations have to balance their investments in data, technology, and senior expertise. This will support plug-and-play strategies for dealing with spikes and simultaneously create more room for staff development and smarter ways of working.

In this context, seniority in the second line of compliance becomes a critical success factor. These professionals must bring real-life experience from first line investigations, possess an investigative mindset, and be capable of identifying emerging financial crime trends. Organisations should invest in targeted training programmes, external hiring, and internal mobility to ensure the second line is staffed with individuals who can challenge, guide, and elevate the first line. Their expertise ensures that both human and augmented resources are not only compliant but truly impactful. Senior second line experts act as strategic enablers, ensuring that the AML framework remains agile, effective, and future-proof.

At the end of the day, good AML management must be, or become, efficient and effective.

That's a very clear takeaway and goal to work towards. Thank you for your time!

Stefan Delaet *is General Manager Financial Crime at KBC Group, with over 20 years of experience in leadership roles across strategy, finance, and risk. With his strong legal background, he brings a rigorous and principled approach to regulatory compliance and the fight against financial crime. His mission? To ensure that KBC remains resilient and ready for the future.*

INTERVIEW

Frans Thierens on **AI** and how it **reduces the complexity of modern anti-money laundering**

Modern technologies are becoming more sophisticated, but so are modern money launderers and the organisations involved in financing international terrorism. In this conversation, Frans Thierens, Anti-Money Laundering Compliance Officer (AMLCO) at KBC Bank, digs into the advances and new complexities in anti-money laundering legislation. His responses highlight the important role of AI technology in identifying illicit transactions and suspicious patterns.

Frans, would you first walk us through the essence of transaction monitoring obligations in anti-money laundering (AML) regulation?

The primary focus of AML legislation is to detect atypical transactions that cannot be matched with the customer's profile. Belgian and European laws place the duty of vigilance on front offices: the people in direct contact with customers. In the context of a digital world, though, human alertness should be supplemented with automated monitoring systems, which can assist with identifying atypical transactions based on various considerations.

Traditionally, rule-based systems generate alerts based on parameters such as limits – for example, transactions coming from high-risk countries and exceeding a predetermined amount. However, those systems do not allow for profiling based on comparison with peers or other behaviors. Artificial intelligence (AI) can identify behaviors from large data sets and assign scores to customers, indicating their likelihood of involvement in money laundering.

Can you elaborate on KBC's use of AI in ALM monitoring? Why and how does AI come into play?

For now, KBC uses AI to augment and support rule-based systems, which has increased efficiency and effectiveness. AI

When criminal enterprises "create" money mules, they essentially fabricate elaborate artificial digital identities from scratch.

These mule accounts often involve the creation of a synthetic identity, built from real but stolen identities combined with entirely fake data. Mules can also be fully automated shell personas without any authentic human information or action behind them at all.

For example, a fraudster creates a fake identity, then opens a bank or crypto account in that name, using it to funnel money from scams or cybercrime operations. This continues for as long as the account remains uncompromised before switching to the next.

With this type of complex and sophisticated digital approach, money launderers have identified ways to reduce the risk of exposure or non-compliance that persuaded or coerced human mules may have presented in the past.

can also identify complex patterns, such as social fraud, by analysing additional features as a targeted approach to suspicious activities.

Profiling involves comparing a customer's transactions to their previous behavior and to the behavior of its peer group in order to identify variations and explain atypical transactions, like sudden international money transfers due to a job relocation. Employing an AI model to evaluate customer behavior fits within the spirit of the legislation.

Local regulators focus on timely reporting of transactions. Ex ante AML processing often clashes with the digital habits and possibilities offered to clients as well as with rapid processing requirements, like the European Payment Services Directive (PSD). Ex ante monitoring often targets fraud, requiring swift action, while money laundering activities are continuous and their complex patterns can only be observed over time.

Frankfurt was chosen from a list of 9 candidates to become the enforcement hub for the EU's fight against money laundering.

The German city was selected through a series of public hearings, which granted the new Frankfurt-based AMLA direct and indirect supervisory powers over obliged entities and empowered the Authority to impose sanctions and measures against money launderers and those engaged in the financing of terrorism.

Frankfurt is of course home to the European Central Bank and has long been a well-established international financial hub within Europe. In addition, local and national governments pledged their financial, logistical and political support. As such, Frankfurt was deemed to have the appropriate talent, logistics and infrastructure already in place to be able to spearhead critical initiatives, coordinate with local and international authorities, and facilitate anti-money laundering efforts at the highest level.

How have money laundering activities changed over time? How can AI help combat these newer, more sophisticated approaches?
The money mules of today are no longer selected but rather created. In the past, people like students, unemployed individuals, notaries and doctors were persuaded to make their accounts available to receive funds and act on the instructions of the money launderer or fraudster.

This new approach is further complicated by a combination of legal and illegal activities. AI technology can enhance the process of investigating dormant accounts and identifying patterns, such as for example multiple customers wiring funds to the same gold dealer.

Payments to social security, tax authorities, salaries and gold dealers may appear legal at a glance, but they require deeper investigation to reveal concerning patterns. Due to data restrictions, visibility is limited to the flow of data within one's entity, so activities at other institutions or in other countries add complexity to the process. The human mind is creative, but it unfortunately cannot capture every important detail from memory.

Embedded in the EU's Anti-Money Laundering Regulation (AMLR), Article 75 details how financial institutions and other obliged entities may form supervised partnerships. Its purpose is the ability to share customer information with the specific goal of combatting money laundering and the financing of terrorism.
Information sharing is permitted only for higher-risk cases or where further assessment is needed to determine risk.
Supervisory authorities must pre-approve partnerships, ensure data protection compliance, and may consult FIUs and data protection agencies. Only specified categories of customer and transaction data may be shared, and participating entities must maintain internal policies and records. The provision aims to support targeted, cross-border collaboration while remaining compliant with legal and privacy safeguards.

Moving forward, how do you anticipate AI will transform AML monitoring?
AI is currently limited to its own data, but an overarching system could identify patterns across institutions without violating customer confidentiality. Added experience from investigators and insights from sources like the Financial Intelligence Unit (FIU) and National Bank will help to identify suspicious behavior and further tighten the net around the professionalised organisations engages in money laundering as a service.
The EU Anti-Money Laundering Authority (AMLA) aims to centralise intelligence in Frankfurt in an effort to Europeanize national systems. While on an institutional level KBC lacks visibility on transactions at other financial institutions, Belgium's FIU has the authority to connect suspicious activities across multiple banks within the country. And at the European level, AMLA can require system access and overcome technical challenges to consolidate suspicious activities across borders.

What impact do laws and regulations have on the AML process?
Regulations, especially the GDPR, can admittedly complicate processes. In Belgium, tax authorities fought for years to gain visibility into accounts. Combining customer databases with transaction databases is complex. In the Netherlands, for example, GDPR hindered progress on a modest setup.
Article 75 of the new EU AML package offers hope, but it does require agreement from local regulators and data protection authorities. The concept is promising in theory but demands significant practical work.

Clearly, as laws and technologies continue to develop, the role of AI will only become more significant in facilitating vital AML efforts. Thank you, Frans, for sharing your knowledge and expertise.

Frans Thierens *is Anti-Money Laundering Compliance Officer (AMLCO) at KBC Bank. With a legal background and extensive training in financial crime compliance, he has been active in the field for multiple decades.*

INTERVIEW

A business ethics view: **Developing and deploying compliant and ethical AI models**

In this interview, one of the Compliance Advisors in KBC's Ethics unit sketches the ins and outs of developing, assessing, deploying and monitoring AI. He explains how AI can be used ethically in financial institutions and how these tools can remain compliant with changing regulations.

How does your financial institution integrate responsible behaviour into its AI strategy and ensure compliance with the AI Act?
Our strategy as a financial institution is based on the principles of responsible behaviour. Principles like acting with integrity and transparency and putting our customers at the centre are essential to the foundation of our organisation. We strive to treat our stakeholders and customers fairly and transparently when using AI. That is especially important in areas where algorithmic models can impact outcomes on an individual level, for example credit decisions and personalised financial services. In all of these cases, we apply the same principles of responsible behaviour that we would display in any face-to-face interaction.

We aim to integrate responsible behaviour into the way of working and output of our AI models. It is the key to building added value and trust in our AI solutions. The AI Act has become a regulatory necessity and we have already taken steps to prepare, starting with the 2020 EU White Paper on AI, which is based on the European strategy for AI initially outlined in 2018. We have integrated these principles into a trusted AI framework that allows to assess and mitigate risks in order to implement responsible AI.

Why does the KBC Group insist on overdelivering, compared to what is required from a regulatory standpoint?
Long before the AI Act came into force, we were already developing a minimum viable product that follows the principles outlined by the EU, putting us at a distinct advantage. We are committed to avoiding potential issues and misuse of technology, even in the absence of regulation.

Beyond complying with legislation, our approach is also focused on applying responsible behaviour to the output of our AI models. That is why we believe it is important to conduct impact assessments, which include identifying and addressing risks relating to discrimination, transparency, proper data usage, safety and oversight. We strive for explainability of our AI models, as well as maintaining accountability for their usage.

Can you elaborate on the decision-making process involved in developing and implementing the AI models that the KBC Group uses?
The trusted AI framework we apply helps us make clear and well-reasoned choices and ensures that the ultimate accountability lies explicitly with the business rather than the AI developers. Operating in a highly regulated sector, where regulators expect well-documented accountability, we strive for documented explanations on the different evaluation areas in our framework.

The approval process includes impact assessments. Whenever risks are detected during this process, it allows to reflect on possible mitigating measures to manage these risks.

This is not only applicable to machine learning but also to generative AI, where we can reduce certain inherent risks through advanced prompting.

How does your organisation ensure responsible governance and risk management in AI projects?
The standard governance of AI projects begins with an idea formulated by the business. Then, we assess whether AI can provide a solution. During the scoping phase, we estimate the costs, benefits and added value, and we complete a high-level impact assessment on the different evaluation areas to identify potential risks.

We have also been adapting the trusted AI framework to reflect the applicable regulatory requirements of the AI Act. It now includes a check for prohibited AI, and more developments are expected to follow. On the basis of the high-level impact assessment, a preliminary advice is automatically provided and contains clear actions for the creators.

Next, the modelling and piloting phase begins, an interactive process where AI models are tested and possibly adjusted. Throughout this process, the final impact assessment of trusted AI is completed, with more detailed questions to help assess the impact and address any identified risks. A final advice is drafted by the legal and compliance departments before the final decision on deployment is taken. This ensures that we can present a coherent and documented narrative to regulators and external parties.

Do you have any concrete examples?
One example of our approach is CV screening. The KBC Talent Acquisition team use AI for support, but always maintain the human touch to ensure fair treatment of all applicants. AI will never autonomously decide on a recruitment. That decision remains one made by the recruiter together with the manager.

During the modeling and piloting phase, technical fairness checks are performed. Before an AI model is deployed, the final advice and the trusted AI impact assessment are reviewed. This document contains the benefits of the AI model, the risks, and the advice from the legal and compliance departments.

All information about the AI model is documented in the same tool, providing an overview of the impact assessments, advice and mitigations. After deployment a monitoring process follows, to ensure maintained model performance. By addressing any issues early on, we can avoid future problems.

The entire process is outlined and scheduled for review by the AI steering committee, where specific points can be further debated and the process formally receives approval and confirmation through thorough and proper documentation.

How does your organisation address the friction between innovation and ethical use of AI?
Surprising as it may seem, I see friction as an opportunity. By integrating the ethical aspect from the beginning and applying the five dimensions of responsible behavior, we can identify and mitigate many risks early on.

Although this initially takes more time, it pays off in the medium and long term. It creates trust, which is crucial when working with AI and Generative AI. People are sometimes wary of AI models, but by ensuring transparency and ethical considerations, we can carefully build trust.

Thank you for highlighting KBC's approach to AI integrations. With technology evolving fast, it's comforting to know that large financial institutions like the KBC Group are treading into the future in thoughtful ways.

Evaluation areas for new AI models

1. **Data protection and privacy**: This dimension focuses on GDPR and privacy, ensuring compliance with local and international data protection regulations.
2. **Diversity, fairness and non-discrimination**: Here, we look at fair treatment and prevention of discrimination and bias. We conduct statistical checks to see if there are deviations in treatment of, for example, age groups. In the case of any deviations, we perform causal checks to determine whether there might be logical explanations.
3. **Accountability and professional responsibility**: This dimension includes assessing the quality of the AI models, data quality, documentation, quality monitoring and accountability. We ensure that there is clarity on which business line is accountable for the AI model.
4. **Safety and security**: We assess how robust the AI models are, their technical vulnerabilities, interactions with third parties and the potential for internal manipulation. This helps us prevent security risks.
5. **Transparency and explainability**: Here, we ensure that AI models are explainable and that there is human oversight where necessary. This is especially important for models with a potentially high impact on customers.

A note from the author

Let me be clear: **AI is not a silver bullet**.

It is a **powerful enabler** – a crucial piece of the puzzle – that can strengthen AML efforts when applied responsibly and strategically.

AI needs care, **transparency**, and **oversight** to avoid problems like bias, excessive or missed alerts, and misplaced reliance on automation.

The reality is different: adoption in practice lags behind the perception. Many institutions are still working through the hard parts: **governance**, **integration**, and **building trust** in the systems they deploy.

This paper aims to strip away the hype and give a grounded, practical view of what AI can, and cannot, do in AML. It is enriched throughout with the valuable insights of KBC Group financial crime experts, whose hands-on experience and proven track record bring depth and practical perspective.

My thanks go to the KBC Group Compliance team for their insights. Their nuanced perspectives and in-depth knowledge have been central to shaping this whitepaper and keeping it focused on what matters in practice.

Let's move forward with clarity, collaboration, and a shared commitment to **build a safer financial system**.

Christophe Himpens *is a Strategic Advisor Financial Crime with 20+ years in financial services, driving regulatory, process, and data-driven solutions to combat financial crime.*

Your thoughts on AML?

About Discai

As part of KBC Group, a leading European financial institution, Discai delivers trusted AI solutions to combat financial crime. Backed by KBC's deep expertise in banking, compliance and data science, Discai combines technological innovation with regulatory rigour.

Its flagship AML KYT solution, developed in-house and successfully implemented within KBC entities, enhances the efficiency and effectiveness of AML processes. Discai's unique blend of domain knowledge and technological excellence empowers financial institutions to tackle the evolving financial crime landscape with confidence, while staying aligned with complex regulatory requirements.

Discai
Powered by KBC

info@discai.com | **discai.com**