FROM DETECTION TO PREVENTION: THE NEXT ERA OF ANTI-MONEY LAUNDERING

Whitepaper

FINTECH & PAYMENTS

JUNIPER RESEARCH

1.1 Introduction

The AML systems market is a rapidly-evolving industry which faces challenges such as changing regulations, heightened sanctions, and evolving money laundering methods.

Juniper Research defines anti-money laundering systems as:

'A set of solutions used to help companies prevent, detect, investigate, and report suspicious activity indicative of money laundering or terrorist financing, AML systems can facilitate faster and more accurate compliance and investigation.'

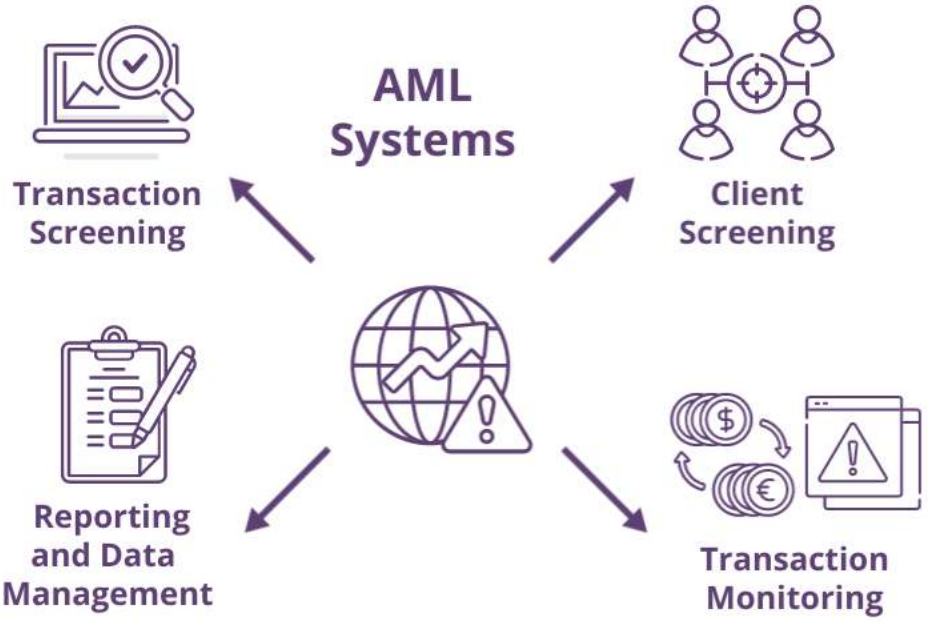
AML solutions help businesses combat the increasingly sophisticated methods that criminals move towards to avoid detection; leading to an increase in more advanced technology that can protect businesses against financial crime based on advanced technology, such as behavioural analytics. AML includes a set of policies, procedures, and technologies that prevent money laundering. Money laundering refers to the process of taking illegally obtained money and making it appear to have come from a legitimate source; putting the money through a series of commercial transactions in order to 'clean' the money. The term arose from regulatory regime, specifically to detail the concealing of financial movements for underlying crimes ranging from tax evasion, drug trafficking, public corruption, and the financing of terrorist groups.

There are many types of people who are able to commit money laundering, such as organised criminals, terrorist groups, corrupt heads of state, business leaders, and senior executives who manipulate or misreport financial data. The financial sector is struggling to keep up with an unprecedented rise in fraud and financial crime. It is becoming increasingly difficult to operate in the industry without being infiltrated by criminals at all levels. They are creative, connected, collaborative, and ready to take advantage of any opportunity they find inside or around business operations. As financial crime becomes more complex and interconnected, siloed systems and processes become less effective in detecting and preventing it. The changing nature of these practices makes it difficult for financial institutions to detect, prevent, and investigate crimes. Furthermore, the pandemic accelerated the transition to a cashless and digital world; opening new opportunities for financial crime and fraud. In the modern, complex environment, financial institutions are insufficiently prepared to manage these threats, which have always been of greatest concern for them.

There are multiple facets to AML systems:

- Client Screening: The process of assessing and verifying existing and potential customers, to then identify the associated risks with financial crime such as terrorist financing and money laundering. It involves checking against various databases, sanctions lists, customer identities, and backgrounds to determine and prevent criminal activities.
- Transaction Monitoring: The process of continuously monitoring customers' transactions between other individuals and entities, to detect suspicious or unusual activity that may indicate money laundering or other financial crimes.
- Transaction Screening: A real-time check of a transaction before or during processing to identify whether it involves high-risk individuals' entities or countries. The purpose of this system is to delay or block transactions that include sanctioned individuals or entities, adverse media/watchlists, politically exposed persons (PEPs), and countries on embargo lists.
- Reporting and Data Management: Reporting in AML refers to the generation and submission of specific reports to regulatory authorities and internal stakeholders, based on regulatory obligations and detected criminal activity. Some of these reports include Currency Transaction Reports (CTRs) on large deposits/withdrawals, Know Your Customer (KYC)/Know Your Business (KYB) reports, Suspicious Activity/ Transaction Reports (SARs/STRs), and audit/compliance reports. Data management refers to how the AML platform collects, stores, organises, integrates, and analyses the data from a collection of sources to support the monitoring of investigation and reporting.

Figure 1: Anti-Money Laundering Systems Market Landscape



Source: Juniper Research

1.2 Types of Digital Money Laundering

i. Cryptocurrencies

Cryptocurrencies and digital currencies are important instruments in cyber laundering. Mixing services, sometimes known as tumblers, are used by criminals to combine their illicit and legitimate money. Because of this, it is difficult for authorities to determine the original source of the funds.

Cryptocurrencies use a technology called blockchain to record every transaction securely and transparently; blockchains are public ledgers, which are chains of blocks containing transaction records. A blockchain is a decentralised ledger stored across many computers worldwide, called nodes, so no single entity controls it. Transactions are able to be verified by a process known as mining or staking, which prevents double-spending and fraud. Popular cryptocurrencies that individuals and entities use include Bitcoin (BTC) and Ethereum (ETH).

Criminals will exploit the capabilities of cryptocurrencies by moving money anonymously across borders quickly. They are able to convert illegal funds into cryptocurrencies to then use complex transactions such as mixers, tumblers, or decentralised exchanges to hide the funds' true origin; cashing it out eventually as 'clean cash'.

A growing trend among criminals is the act of cross-chain swapping. Structured chain hopping involves the splitting of funds and distributing them simultaneously across several blockchains. Multi-hop chain-hopping is the act of distributing assets from one asset to another, repeatedly. Both techniques are used to confuse investigators as they create a trail that is fragmented and hard to follow. They come with high fees and are very inefficient by design for criminals to carry out. These methods are gaining traction in high stakes' laundering operations: in one 2025 case, hackers suspected to be linked to North Korea stole $75 million from an unnamed exchange and bridged the funds in sequence from Bitcoin to Ethereum, then to Arbitrum, Base, and then finally Tron.

ii. Online Gaming and Gambling

Online gambling and gaming are becoming increasingly common ways for criminals to launder money and finance illicit operations, especially with legalised crypto-based gambling. The UK Gambling Commission (UKGC) has warned that crypto-based gambling poses serious threats to AML/Counter-terrorist Financing (CTF) vulnerabilities. Licensed operators have been known to launder proceeds from major digital thefts; one example being the 2025 Bybit Crypto hack which is the largest crypto theft ever known ($1.5 billion worth of Ethereum). The North Korean hacker group converted stolen crypto into anonymous tokens, such as gaming tokens used in blockchain games, or buying in-game items, to then later cash out winnings which appeared to be clean funds.

iii. Proxy Servers and Anonymising Software

Criminals will use Virtual Private Networks (VPNs) or The Onion Router (Tor) to mask IP addresses and country of origin to then be able to route transactions through them. This allows these individuals to obfuscate fund movement, which, in-turn, enables scaling and speed while reducing traceability. There are also capabilities to layer virtual assets via mixing services such as transactions; passing through privacy-focused cryptocurrencies to break blockchain traceability. Crimes running via these anonymous networks have increased reach and efficiency, often within cross-border schemes. These techniques are commonly combined with trade-based laundering, virtual assets, shell companies, and mule networks to hide traceability of fraudulent activity. A technological method known as 'proxy piercing' is used to unmask individuals who use proxy servers to hide their identity; identifying their true IP address and general physical location. It works by bypassing the mask, using advanced piercing tools, to discover the origin IP. Many more fraud detection systems use this technology in order to flag suspicious transactions and spot fraudsters.

iv. Romance Fraud

Romance scams are a form of online fraud where scammers create fake personas to establish a romantic connection with their victims. Scams often target vulnerable individuals who have recently experienced hardship. These scams are devastating for victims and, according to the Federal Trade Commission (FTC), losses to romance fraud totalled over $1.4 billion in 2023. These scams are also known to be one of the costliest to victims, with a median loss totalling over $2000 per person. Scam artists use dating apps or social media to gain trust, then exploit victims emotionally and financially; typically asking for money due to a fabricated emergency. This demographic is often deemed to be financially stable, and in the workforce, and may be going through major life changes such as a divorce or loss of a partner; making them particularly attractive targets for scammers.

v. Job Scamming

Money mule recruiters utilise fake online job adverts to target those who are looking for work, or individuals who are looking for ways to earn quick and easy money. Job scamming is a growing issue as fraudsters begin to leverage the use of AI to pose as employers, recruiters, and consultants; making it even more difficult for individuals to spot the warning signs. Most scammers will ask for money upfront and provide a variety of reasons as to why this needs to happen, with psychological tricks such as placing timeframes of completion to incentivise urgency: this can take the form of asking individuals to pay an admin fee before the application deadline. Many will also look to steal personal information such as ID; asking for photos and bank account details which can later be used for identity theft, to apply for bank accounts, or attempt to takeover individuals' existing accounts.

vi. Dark Web and Encryption

The dark web is an encrypted part of the Internet that hosts online content not indexed by conventional search engines. Also known as the 'darknet', its first structure was conceived by the US Naval Research Laboratory, in the mid-90s, as an anonymised and ciphered network for the ease of communication between US spies. The dark web is utilised as a key ecosystem for laundering money and distributing illicit goods. Some of the illicit uses include the buying and selling of drugs and weapons, stolen credit cards and IDs, fake passports, money laundering, cryptocurrency mixing, and more. There has been a market shift towards invitation-only access for these websites; making them much more difficult for law enforcement to infiltrate.

vii. Deepfake & AI-powered Financial Scams

These scams are not isolated or speculative: they present a real threat due to their scalability, accessibility, and capabilities of bypassing authentication systems. Deepfakes pose a fundamental challenge to financial institutions because fraudsters can impersonate trusted figures to execute unauthorised actions. The current cutting-edge AI deepfakes utilise two machine learning (ML) models which work against one another. The 'generator' algorithm is trained upon sample imagery, video, or audio to create new pieces of deceptive media, or to manipulate a pre-existing one. The 'discriminator' algorithm is trained on the basis of providing criticism on where the 'generator' has missed distinctive features in the sample, so it can go back and correct the inconsistencies. This is known as a Generative Adversarial Network (GAN). In February 2024, a finance employee participated in a

video conference which she believed to be with a senior executive, later finding out it was actually an AI deepfake, which led to a $25 million fraudulent transfer.

1.3 Drivers

The pandemic and rise of digital technology have exacerbated financial crime for financial institutions, economies, and governments around the world. Financial behaviour has been significantly altered by the COVID-19 pandemic; making it more difficult for banks to identify anomalies and behaviour that might constitute financial fraud. Because of the pandemic, many people have turned to online shopping, and fraudsters have taken advantage of this; while some businesses may have become more likely to engage in unethical practices. As a result, banks are more likely to be involved in financial crimes, especially when it comes to payments

1.3.1 Rising Levels of Online Crime and Money Muling

Online crime and money muling has become more than just individuals being paid to transfer illicit money: it has evolved into organised, cross-border digital networks that exploit people (often unknowingly) and facilitate large-scale fraud that challenges AML systems on a global scale.

Social engineering and digital exploitation has become a main issue: through the use of more sophisticated fraud mechanisms such as fake job ads, romance scams, and phishing, criminals end up luring vulnerable people into acting as mules via seemingly harmless and legitimate roles. Generative AI has also exacerbated this complicated issue as criminals use deepfake tech-enabled, hyper-personalised scams; making catching criminals much more difficult.

Furthermore, social media and messaging apps provide a channel for criminals to create fraud rings and use instant cross-platform co-ordination to hide and move funds faster than traditional surveillance could possibly detect. The cost-of-living crisis and economic desperation are a gateway to this sort of crime, especially with youth unemployment, and post-COVID financial stress can make people more susceptible to becoming mules. This is particularly the case in key regions such as Eastern Europe, Latin America, and parts of Asia, where 'quick cash' schemes have a high success rate.

Many banks around the world still rely on rules-based transaction monitoring that is unable to catch the subtle behaviour of mule accounts, such as the opening of new accounts with little history, and movements of high-value transactions through the account very suddenly. Mule herders tend to use low KYC fintech accounts, prepaid cards, and nested transactions to confuse AML systems. With cross-border mule networks expanding, they tend to target weak collaboration efforts from banks, jurisdictions, banks, and regulators. Mules now move money through Instant SEPA, crypto, neobanks, and challenger banks before the transaction is flagged, and accounts are often traded, rented, or stolen; enabling the use of layered laundering techniques that outpace regulatory efforts.

Most companies are realising the risks associated with digital platforms such as social media and eCommerce. Platform risks can have ripple effects across multiple organisational silos; causing fraud to spread. Combatting platform fraud requires a cross-functional, enterprise-wide approach since it affects the entire organisation.

One specific problem with social media is its use by criminals to recruit young people to act as money mules. In order to outsmart their victims, they exploit vulnerabilities and invest continuously.

1.3.2 Regulatory Expansion and Harmonisation

Regulatory expansion and harmonisation stands out as a principal driving force shaping today's AML market. Worldwide endorsement from the Financial Action Task Force (FATF), complemented with landmark regimes such as the EU's AML Packages and US Beneficial Ownership reform, is shifting markets towards greater cross-border enforcement, coherence, and elevated compliance expectations.

The establishment of the European Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA), created under regulation (EU) 2024/1620 and operational from July 2025, has the legal authority to directly supervise high-risk entities, including banks operating within a minimum of six member states and crypto firms. Initially, AMLA will oversee up to 40 selected entities, where they will co-ordinate joint supervisory teams with national regulators:

it can directly enforce EU laws when member states' oversight is deemed insufficient. The regulator holds great normative power including issuing regulatory standards, guidelines, and enforcement decisions, including fines of up to 10 million euros or 10% of annual turnover.

The single AML rulebook is a directly applicable AML regime across EU member states. Applying from July 2027, it replaces the previous fragmented national implementation with a uniform playbook. Additionally, it expands from obligated entities, including Cryptoasset Service Providers (CASPs) defined as an approved legal entity or person whose business is the provision of one or more crypto asset services, to clients, football clubs, real estate agents, and luxury goods traders; mandating Customer Due Diligence (CDD), risk-based approach, Ultimate Beneficial Owner (UBO) disclosure, and cross-border reporting.

FATF continues to apply pressure on jurisdictions to implement harmonised frameworks. Laws such as China's 2025 AML Law and India's expanded PMLA indicate that compliance with these global standards is being met. FATF Recommendation 24 helps to secure international norms surrounding UBO transparency, such as mandating up-to-date, accessible, and reliable data on beneficial ownership.

1.3.3 Technological Integration

The most transformative driver includes the technological integration of AI, Graph Analytics, and regtech. AI and ML are reshaping detection; moving businesses away from rules-based systems to predictive behavioural and real-time monitoring. Adoption is increasingly seen not only as an option for organisations, but as a mandatory tool for industry success, customer security, and to avoid legal and financial consequences.

1.3.4 Costs to Businesses

Companies now face soaring costs just to remain compliant with regulators: The average Tier 1 bank will spend $10-20 million annually on AML compliance staff alone. Presently, non-financial sectors are being forced to take a better stance on ramping up AML compliance, which tends to be a new and unexpected cost.

As long as they are receiving fines, institutions will also face operational disruptions and revenue loss. Fines, for the most part, come with business restrictions such as being barred from taking on new clients, entering markets, or even handling correspondent banking. In certain scenarios, AML failures will trigger investigations into executives; leading to board-level resignations and strategic overhauls. Furthermore, investors and acquirers are conducting deep AML due diligence before completing any deal: firms with a poor AML track record are considered high-risk assets.

Failing to meet AML obligations has led to many companies receiving massive fines in recent years; particularly notable within the banking and fintech sectors. Not only do businesses suffer financially, but they also experience damage to brand reputation, impact on share price, and trigger regulatory scrutiny in other jurisdictions. Some notable failings in recent years include TD Bank which, in October 2024, was fined a total of $3.09 billion from the Financial Crimes Enforcement Network (FinCEN) and the Department of Justice (DOJ) for Bank Secrecy Act violations, such as not detecting suspicious transactions, not reporting large or structured transactions, or having inadequate AML controls; with an additional $450 million penalty via the Office of the Comptroller of the Currency (OCC) with a cease and desist order. The bank failed to monitor transactions and allowed over $670 million to be laundered, including drug trafficking proceeds between 2018-2024. More recently, in February 2025, the cryptocurrency exchange OKX was fined over $504 million in fines and fees for knowingly violating AML laws and failing to carry out proper KYC proceedings.

In 2024, regulatory authorities around the world imposed over $4.6 billion in enforcement penalties related to AML/CFT breaches. This is a 30% decrease from the previous year, but still indicates persistent regulatory scrutiny and elevated costs for compliance failures. The banking sector took the majority of the share: accounting for about 70-80% of total AML fine value. The US was the leader in global sanctions: responsible for handing out 95% of global fines, with financial institutions headquartered in the US incurring $3.5 billion in fines. Evidently, worldwide jurisdictions have been noted to have lowered evidentiary thresholds, such as within Singapore; making it easier to convict mules and intermediaries. Sentencing guidelines in some jurisdictions, such as the UK, have maximum penalties of 14 years for these crimes: with average sentencing times increasing.

i. Evolving Digital Techniques

As technological advancements drive innovation, this also provides criminals with more digital methods to use to evade detections and commit fraud. Furthermore - and we advocate for regulators, banks, and other key players in the AML system to understand these methods - when designing AML systems, vendors should be aware of the emerging technologies being capitalised on by criminals, and the evolving methods and schemes they are using to launder money and manipulate victims online. By better understanding emerging typologies, AML system vendors can create solutions which are at the forefront of innovation; protecting customers as effectively and efficiently as possible. Reasons for following this approach include:

a) Adaptability

Money laundering techniques evolve as criminals exploit new technologies. AML system vendors must stay abreast of emerging technologies to adapt their solutions accordingly. Understanding these advancements enables vendors to update their systems and provide effective countermeasures against novel money laundering methods.

b) Enhanced Detection

Criminals often leverage cutting-edge technologies to hide their illicit activities. AML systems need to incorporate advanced analytics, machine learning, and artificial intelligence to detect complex patterns and anomalies in financial transactions. Understanding emerging technologies helps vendors develop more robust algorithms which can identify new money laundering tactics.

c) Global Reach

Money laundering is a global issue, and criminals exploit technological advancements to move funds across borders rapidly. AML system vendors must understand emerging technologies to design solutions that are effective on a global scale, taking into account the nuances of different financial systems and jurisdictions.

d) Cryptocurrency Integration

The rise of cryptocurrencies presents a unique challenge in terms of money laundering. AML system vendors need to understand blockchain technology and the intricacies of cryptocurrency transactions to provide solutions that can monitor, analyse, and detect suspicious activities involving digital assets.

1.4 Market Forecast Summary: Anti-money Laundering Systems

Total spending on third-party AML systems will grow by 121% by 2030; up from $33.9 billion in 2025. Gaps in transaction monitoring and beneficial ownership transparency are two key vulnerabilities driving spend.

With increasingly complex regulatory regimes, firms are turning to AI-driven screening and analytics to strengthen detection while addressing high false-positive rates. The report found that banks will account for 64% of AML spending by 2030, spurred by sustained exposure to regulatory oversight.

Juniper Research's recent AML Systems Market Competitor Leaderboard evaluated 18 key AML system vendors against a series of robust criteria, including segment coverage, service offerings, and various capacity and capability measures.

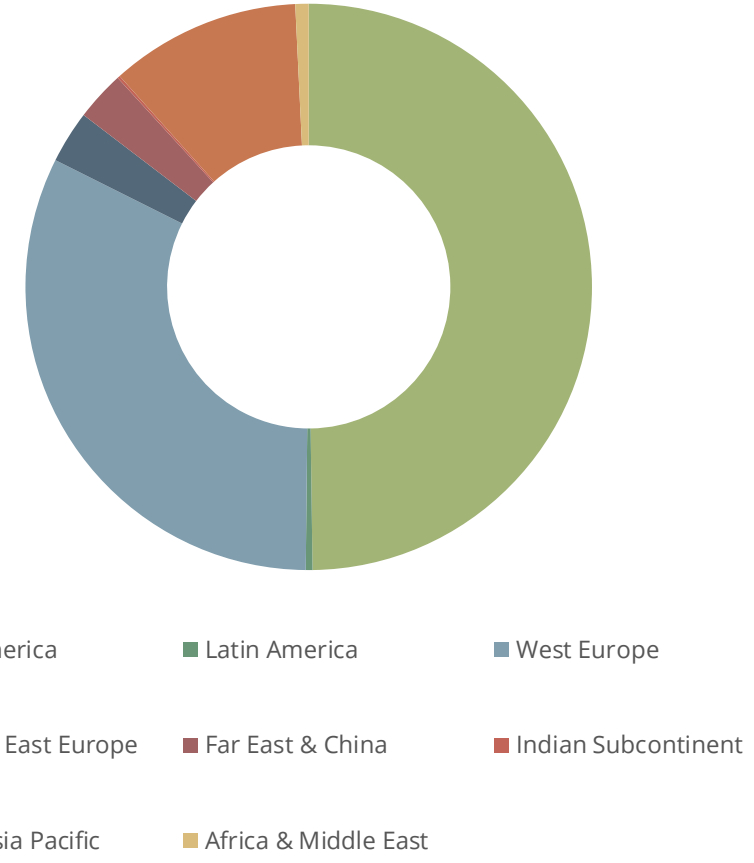
The top 3 vendors for 2025 are:

- LexisNexis Risk Solutions
- Oracle
- Experian

Juniper Research found that leading AML vendors are increasingly expanding their scope of offerings to optimally suit a range of business requirements. These include real-time data integration, transaction monitoring for cryptocurrencies and blockchain activity, cloud-based, API-first solutions for scalability, and explainable AI for regulatory compliance.

AML vendors must look to move beyond traditional compliance tools and deliver on intelligent, adaptable systems that can anticipate risks across diverse sectors. By providing sector-specific risk models and explainable AI, institutions can customise detection rules and justify decisions to regulators; ultimately, minimising the impact of financial crime.

Figure 2: Total Spend on Third-party AML Systems in 2030 ($75 billion), Split by 8 Key Regions



Source: Juniper Research

Order the Full Research

As regulatory frameworks tighten and financial crime becomes more complex, the demand for robust, AI-powered anti-money laundering (AML) solutions has never been greater.

This research delivers actionable intelligence that empowers financial institutions, regulators, and technology providers to stay ahead of evolving threats and capture emerging opportunities. Covering 60+ markets and 10 industry verticals, it goes beyond the numbers to reveal where adoption will accelerate, how vendors are innovating, and what strategies will define the next era of AML.

With detailed market forecasts, competitive benchmarking, and unique insights into regulatory shifts, the suite is designed to equip stakeholders with the knowledge they need to make smarter decisions, safeguard compliance, and capitalise on future growth.

Key Features

- **Key Takeaways & Strategic Recommendations:** In-depth evaluation of growth opportunities and emerging challenges in AML system adoption, supported by strategic recommendations for technology vendors, regulators, and financial institutions.
- **Market Dynamics:** Insights into the trends and challenges shaping AML adoption across industries. Includes analysis of the Country Readiness Index for 60+ markets, 10 industry verticals, and the latest regulatory developments. The report also explores technological innovations in fraud detection, the impact of growing regulatory involvement, and the challenges posed by increasingly complex financial crimes.
- **Benchmark Industry Forecasts:** Forecasts include total spend and adoption of AML systems across 10 industries – five financial (banking, fintech, insurance, investment, lending) and five non-financial (gaming & gambling, public sector, non-profit, real estate, legal). Metrics cover spend levels, number of companies deploying AML systems, and adoption trends by sector.
- **Juniper Research Competitor Leaderboard:** Independent capability and capacity assessment of 18 AML vendors. The Leaderboard distinguishes sector leaders, challengers, and disruptors; providing a clear view of market positioning.

What's in this Research?

1. **Market Trends & Strategies** – In-depth analysis of drivers and inhibitors shaping AML adoption, including the impact of regulation, technological innovation, and evolving financial crime tactics. Includes country-level evaluation via the Country Readiness Index.
2. **Competitor Leaderboard** - Independent evaluation of 18 leading AML system providers, benchmarked on innovation, strategy, and market impact.
3. **Data & Forecasts** – Detailed forecasts of AML system spend and adoption across 10 industry sectors, supported by 39,200+ datapoints.
4. **Interactive Forecast Excel** – Over 59,800 datapoints with scenario analysis tools; enabling users to stress-test strategies and compare against custom assumptions.
5. ***harvest* Online Data Platform** – 12 months' access to Juniper Research's data portal, including continuous updates, exportable charts, and visualisation tools.

Publication Details

Publication Date: September 2025

Author: Shane O'Sullivan

Contact: For more information contact info@juniperresearch.com

Juniper Research Ltd, 9 Cedarwood, Chineham Park, Basingstoke, Hampshire, RG24 8WD UK

Tel: UK: +44 (0)1256 830002/475656 USA: +1 408 716 5483 (International answering service)

http://www.juniperresearch.com