VIXIO
Regulatory Intelligence

Real-Time Risk, Real-World Liability: The New Global Standard for AML

March 2026

About This Report

This report is part of Vixio Regulatory Intelligence's Outlook series, which provides subscribers with forward-looking insights and consolidated research on key segments of the global payments industry.

This edition is designed to provide high-level intelligence on anti-money laundering regulation in 2026.

Authors

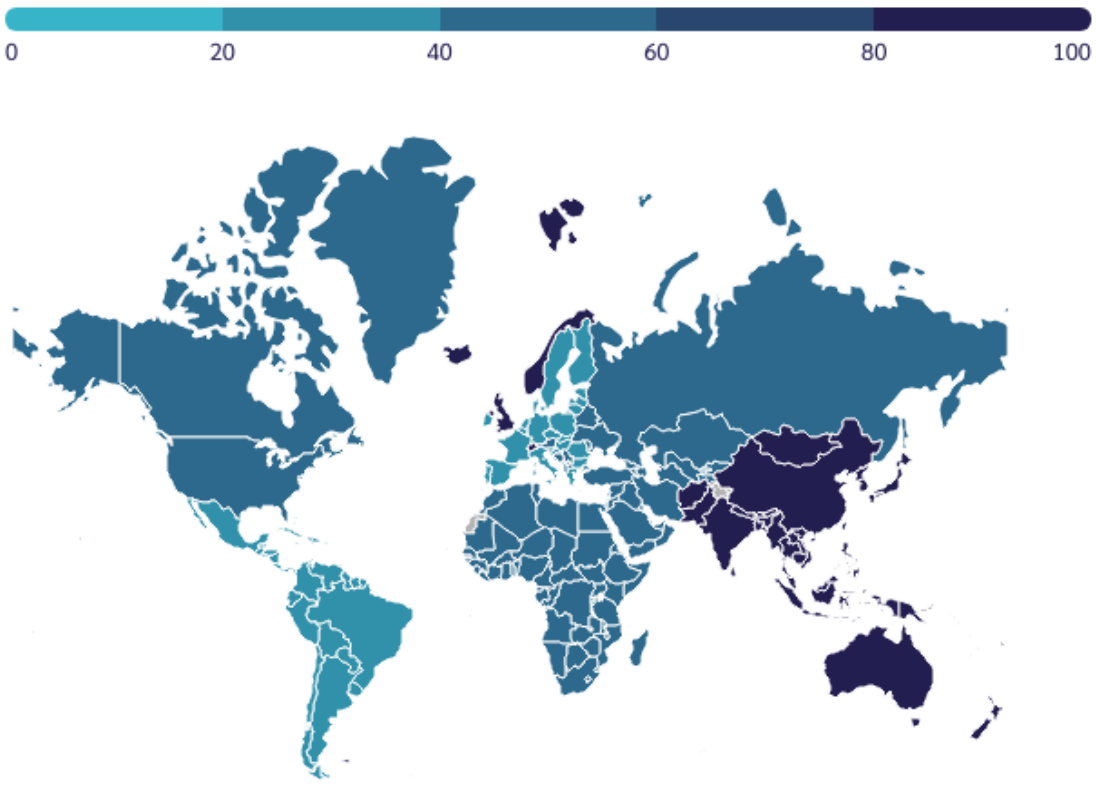
Writing/Editing:
Adam Parkinson | Editor
Allegra Lapetina | Senior Regulatory Lead
Alex Davies | Analyst
Armani Rahman | Analyst
Ranjini Ghosh | Analyst
George Gallwey | Senior Analyst

Design:
Sonia Nimley, Hiriyti Bairu | Content Operations Team

Contents

Introduction: Reshaping Oversight for a Digital-First World	04
Global AML Modernisation Timeline	07
Regulation to Watch	08
The EU: The Single Rulebook, Unified Oversight and Heightened Liability	10
The US: Moving Stablecoins From the Periphery to the Core	13
Australia: A Structural Reset of the AML Architecture	16
South Africa: Digital Payments Growth and the Rising Cost of Compliance	19
Latin America: Payments Innovation, Dollar Dependency and Uneven Enforcement	21
About Vixo	24

Horizon Scanning Update



Number of AML modernisation updates by region, March 2025 - March 2026

As of March 25, 2026

Introduction: Reshaping Oversight for a Digital-First World

The era of static financial crime compliance is coming to a close. For decades, global anti-money laundering/counter-terrorism financing (AML/CTF) frameworks have been designed and implemented for a world of relatively slow, intermediary-driven banking transactions.

Today, however, that system is being overhauled in a wave of global AML reform.

As real-time payments, stablecoins and decentralised finance (DeFi) move from the periphery to the core of the global economy, regulators are having to comprehensively modernise their oversight regimes.

This goes beyond a routine update to the rulebook – it is a structural reset designed to close the gap between the speed of modern financial innovation and the limitations of legacy monitoring.

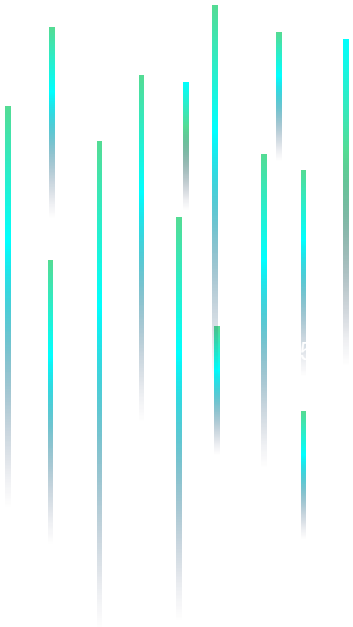
Speed, Complexity and Convergence

The main catalyst for the global overhaul of AML regulation is the sheer pace of digital finance. Traditional frameworks that rely on the safety net of delayed settlement are ill-equipped to manage the borderless, instantaneous nature of stablecoin transfers or high-speed domestic payment rails.

Another factor is the convergence of fraud and money laundering. In a world of instant payments, the time between a fraudulent transaction and the subsequent laundering of those funds has shrunk to seconds.

For compliance professionals, the reality of digital-first operations is that the window to detect and stop a crime has narrowed from days to milliseconds.

> *For compliance professionals, the reality of digital-first operations is that the window to detect and stop a crime has narrowed from days to milliseconds.*



A Global Sample of Modernisation Challenges

To understand the trajectory of this evolution, Vixio has examined five key jurisdictions that represent the different modernisation challenges currently facing the global financial system.

	Primary AML Modernisation Step	Key Goal	Technology Focus	Compliance Impact
 EU	Centralisation: creation of the Anti-Money Laundering Authority (AMLA) and the single rulebook.	To eliminate regulatory arbitrage and uneven national enforcement.	Harmonisation: standardising data formats to enable EU-wide monitoring.	Shift to a centralised model, with high-risk firms facing direct EU supervision by 2028.
 US	Integration: bringing stablecoins under the Bank Secrecy Act (BSA) via the GENIUS Act.	To bring digital assets within the regulatory perimeter.	Auditability: emphasis on real-time, on-chain monitoring and integration with suspicious activity report (SAR) workflows.	Stablecoin issuers must adopt bank-level governance and automated reporting.
 Australia	Structural reset: extending oversight to "Tranche 2" sectors.	To close structural gaps and align with Financial Action Task Force (FATF) standards for professional services.	Outcomes-based reporting: upgrading the Australian Transaction Reports and Analysis Centre's (AUSTRAC) portals to handle a massive influx of new sector data.	An expansion of the regulated population, with a focus on a demonstrable uplift in controls.
 South Africa	Credibility: rapid updates to avoid being returned to the FATF greylist.	To signal international legitimacy to global investors and correspondent banks.	Digital verification: pushing for automated customer due diligence (CDD) and biometrics to manage fintech growth.	Extended record-keeping (seven years) and a shift to data-backed, defensible risk policies.
 Latin America	Infrastructure uplift: leveraging instant payment rails (Pix, Bre-B).	To manage tension between retail innovation and US dollar dependency.	Fraud/AML integration: using artificial intelligence (AI) and machine learning (ML) to detect fraud and money laundering concurrently on instant rails.	High pressure to align with US sanctions, with compliance as a strategic determinant.

VIXIO Regulatory Intelligence

Strategic Resilience Over Technical Adherence

For the compliance function, the key issue is not simply that AML regimes across jurisdictions are changing rapidly, but how organisations are expected to respond.

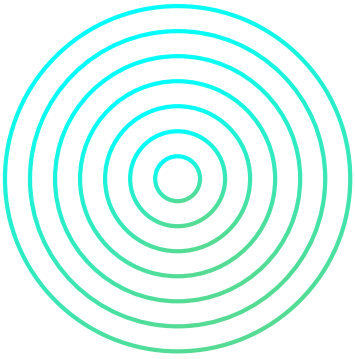
It is vital to avoid prioritising quick-win technical implementation over the more fundamental governance, personnel training and model validation required to make compliance systems defensible during future audits.

One key challenge will be managing the regulatory squeeze, as the significant capital requirements for updated data architecture and personnel trigger a market shakeout. The strategic decision firms have to make is no longer simply whether to automate – they must – but whether to build, buy or partner for their risk infrastructure.

Another challenge is that the historical separation of fraud and AML teams is now a liability for financial institutions. Firms that maintain a siloed approach will struggle to meet the outcomes-based expectations of regulators that increasingly consider fraud a key entry point for money laundering.

Finally, as technology-driven supervision (SupTech) and the use of AI become standard, compliance teams will need to prioritise model explainability and defensibility, taking a risk-based approach to determining which activities and decisions are automated.

Compliance officers must be able to demonstrate that they understand and can defend the logic behind automated decisions to satisfy increasingly tech-savvy regulators.



> *The convergence of high-speed digital finance and fundamental regulatory reform is redefining compliance, and just sticking to the letter of the new rulebook is insufficient.*

Compliance as a Strategic Moat

The various modernisation initiatives underway in jurisdictions around the world are not just changes in laws and regulatory frameworks – authorities are implementing a foundational change in the compliance infrastructure.

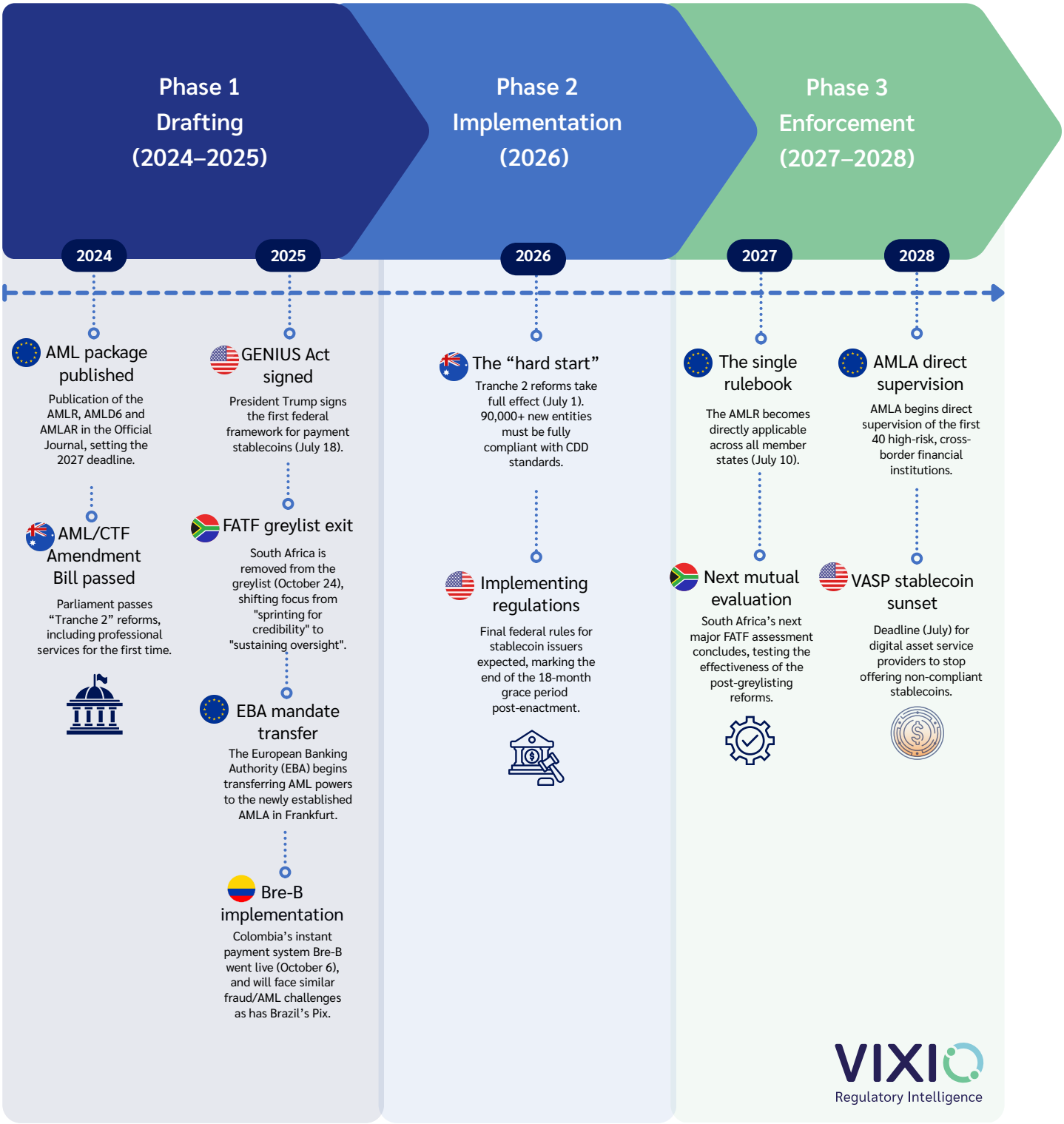
The convergence of high-speed digital finance and fundamental regulaxtory reform is redefining compliance, and just sticking to the letter of the new rulebook is insufficient.

Traditional AML structures are built to report on what happened yesterday, but modern rails require a framework that can both intervene in what is happening right now and mitigate or defend against what might happen in the future.

Firms need to build adaptive, flexible and tech-driven monitoring functions, moving beyond a cost-centre mentality to treat compliance as a fundamental factor in the organisation's ability to compete, grow and even exist.

By embedding continuous, defensible oversight, organisations can not only navigate this change, but transform their compliance infrastructure into a formidable competitive moat, securing market access and growth in the world's most innovative financial ecosystems.

Global AML Modernisation Timeline



Regulation to Watch

Jurisdiction	Notable Date	Summary	Legislation	More Info
 Australia	Implementation deadline **March 31, 2026** for existing regulated entities. Implementation deadline **July 1,** 2026 for newly regulated entities.	The regime extends AML and customer due diligence obligations to additional services that are recognised by FATF as posing high risks. The amendments aim to update AML legislation to better reflect changing business structures.	Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024	The reform also intends to reframe and clarify the requirements of an AML/CTF programme and enable AUSTRAC oversight. Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill Australia Unveils Sweeping AML Reforms
 Chile	Entered National Congress **May 2023**. Second constitutional stage in **2025–26**.	A bill to create an economic intelligence system coordinating intelligence units.	Bill to Create the Economic Intelligence Sub-System (AML Support Mechanism) (Boletín 15975-25	The bill seeks to strengthen AML detection and prevention of organised crime-linked illicit financial flows, expanding data sharing and early warning for suspicious economic activities.
 EU	The regulation is set to apply from **July 10, 2027**.	The regulation lays down rules concerning the measures to be applied by obliged entities to prevent money laundering and terrorist financing, beneficial ownership transparency requirements, and measures to limit the misuse of anonymous instruments.	Regulation (EU) 2024/1624 (Anti-Money Laundering Regulation – AMLR)	AMLR reforms the EU's AML landscape by placing its obligations in a directly applicable regulation. The regulation also sets out empowerments for AMLA to draft regulatory technical standards further setting out the requirements contained in AMLR. EU's AML Overhaul To Bring Unified Rules And Central Supervision
 EU	Published by the European Commission on **June 28, 2023**. Final publication is expected in **mid-2026**.	The regulation sets out strict requirements for payment and electronic money institutions to implement fraud prevention measures and establishes direct liability for failing to implement such measures.	Proposal for a regulation on payment services	This regulation effectively replaces Directive (EU) 2015/2366 (revised Payment Services Directive – PSD2) by placing the requirements applicable to payment institutions and electronic money institutions in a directly applicable regulation. PSD3 And PSR Set To Reshape Open Banking And Payment Security In The EU EU Edges Closer To New Payments Framework With PSD3 And PSR Agreement

Regulation to Watch

Jurisdiction	Notable Date	Summary	Legislation	More Info
EU	Consultation launched on **February 9, 2026.**	As part of its mandate to develop regulatory technical standards (RTS), AMLA has launched a consultation on three draft RTSs, including an RTS to establish the criteria for identifying business relationships, occasional transactions and linked transactions, which form the structural basis upon which customer due diligence obligations apply.	Consultation paper on the draft RTSs	The consulted upon RTS are: The draft RTS on business relationships, which establishes criteria for identifying business relationships, occasional transactions and linked transactions, which form the structural basis upon which customer due diligence obligations apply. The draft RTS on customer due diligence, which builds on the AML Regulation framework and sets out how obliged entities verify customer identity and conduct ongoing monitoring in a risk-sensitive and proportionate way. The draft RTS on enforcement, which establishes a common supervisory approach to assessing, categorising and responding to breaches of institutions' AML/CTF obligations.
South Africa	Consultation launched on **January 14, 2026.**	The bill marks a decisive moment in the country's attempt to modernise its AML regime under the sustained pressure of FATF greylisting.	Draft General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Bill, 2025	The draft bill seeks to strengthen South Africa's AML/CTF framework by enhancing supervisory powers, expanding information-sharing mechanisms, and aligning domestic legislation with evolving international standards.
US	Introduced **October 20, 2025.**	The legislation raises the currency transaction report and suspicious activity report thresholds under the Bank Secrecy Act.	Streamlining Transaction Reporting and Ensuring Anti-Money Laundering Improvements for a New Era Act (STREAMLINE Act)	Major AML Reform On Horizon As US Seeks To Cut Compliance Burden Regulatory Influencer: The STREAMLINE Act and a New Era of AML Compliance

The EU: The Single Rulebook, Unified Oversight and Heightened Liability

The era of fragmented financial crime compliance in Europe is over. For years, financial criminals have exploited uneven supervision and enforcement across member states, taking advantage of regulatory arbitrage to evade detection.

Coupled with a string of high-profile financial crime scandals and the growth of decentralised finance (DeFi) and crypto-assets, it has become clear that the old, directive-based patchwork framework is no longer fit for purpose.

To remediate systemic vulnerabilities and counter the speed of modern financial crime, the EU is executing a fundamental overhaul of the regulatory landscape.

Its revamped AML regime rests on three complementary legislative acts:

- Regulation (EU) 2024/1624 (the Anti-Money Laundering Regulation – AMLR).
- Directive (EU) 2024/1640 (the 6th Anti-Money Laundering Directive – AMLD6).
- Regulation (EU) 2024/1620 (the Anti-Money Laundering Authority Regulation – AMLAR).

In parallel, the proposed third Payment Services Directive (PSD3) and the new Payment Services Regulation (PSR), both currently awaiting final publication, are set to raise compliance expectations for banks and payment service providers (PSPs), particularly in relation to fraud mitigation and customer protection.

Collectively, these measures mark a step change in the EU's regulatory expectations, requiring financial institutions to rapidly reassess their AML and fraud-prevention frameworks under a more centralised, unified and demanding regime.

AMLR

By consolidating all AML requirements into a single, directly applicable rulebook, the authorities are giving firms greater clarity and ensuring a consistent approach across the EU, eliminating the cross-border differences that plagued previous, directive-based frameworks.

Greater uniformity across EU member states is a game changer, and means firms will find that the AML regime operates the same in, for example, Malta and the Netherlands.

However, firms will also need to be prepared for significantly stricter regulatory requirements.

The additional hurdles involve:

- Stricter due diligence requirements, including on beneficial owners.
- The expansion of obliged entities.
- A cap on cash payments.

AMLAR

With the establishment of the Anti-Money Laundering Authority (AMLA), the EU's regulatory framework is shifting toward a centralised model. Although approximately 40 high-risk institutions will fall under direct supervision by 2028, AMLA is already shaping the future compliance landscape through a concentrated wave of secondary legislation and critical industry consultations.

AMLA is currently preparing draft Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) that will substantially reshape compliance expectations. Key focus areas include:

- Financial intelligence units (FIUs) information exchange: Standardising how FIUs share data across borders.
- Supervisory triggers: Establishing the specific cross-border reporting triggers and risk-profiling methodologies that will determine which entities fall under direct AMLA oversight in 2028.

According to AMLA's Single Programming Document for 2026–2028, the authority intends to publish 22 RTS, ITS and guidelines by H2 2027. This represents an unusually concentrated wave of secondary legislation that will operationalise the AMLR's high-level obligations into detailed, enforceable requirements.

Each consultation therefore constitutes not merely a procedural step, but a strategic opportunity for firms to influence how key principles, including proportionality and risk sensitivity, are reflected in the final technical standards.

AMLD6

In contrast to AMLR, the directive sets out a series of mechanisms which must be put in place by member states for the prevention of money laundering and terrorist financing (ML/TF).

Although its provisions do not directly affect firms, its effects greatly complement the initiatives set out in AMLAR and AMLR, shaping the regulatory landscape that firms must follow.

Key changes include:

- Central beneficial ownership registers which must be held by each member state.
- The establishment of bank account information registers.
- Enhanced cooperation between FIUs.

PSD3/PSR

Alongside the new AML framework, the forthcoming PSD3 and PSR will significantly recalibrate the regulatory landscape for payment and electronic money institutions.

Although primarily focused on the provision of payment and e-money services, the draft legislation introduces a materially strengthened liability regime for fraudulent payments.

In particular, where a PSP fails to implement effective and proportionate fraud-prevention measures, it may be held directly liable for reimbursing customer losses — a model comparable to the UK's authorised push payment (APP) fraud reimbursement framework.

The UK experience illustrates the scale of exposure: fraud-related losses rose 12 percent to £257.5m in H1 2025. If a similar trajectory emerges in the EU, banks and PSPs will need to ensure both operational readiness and robust control frameworks.

Beyond liability, the draft acts introduce enhanced fraud-prevention obligations, including:

- Mandatory transaction monitoring systems designed to detect and mitigate fraud risk in real time.
- Structured information exchange between PSPs to facilitate the sharing of fraud-related intelligence.
- Reporting of fraud statistics, increasing supervisory visibility and market transparency.

Taken together, PSD3 and the PSR signal a move to a more prevention-focused supervisory approach, underpinned by clear accountability where controls fall short.

As the EU transitions toward a centralised supervisory model with stricter liability and uniform technical standards, firms must proactively align their internal controls to meet these more rigorous expectations.

Reshaping Expectations

Collectively, the application of the single rulebook, a centralised regulator, greater consistency among FIUs and direct liability for fraud related losses represent far more than a routine update to the compliance handbook – we are seeing a fundamental transformation of the EU's financial crime system.

The previous regime's hallmark was uncertainty, with national divergences creating gaps that the European Commission acknowledged, notably in paragraph 6 of the PSR proposal, as being insufficient for cross-border oversight.

With stricter AML requirements now enshrined in directly applicable EU regulations, the era of regulatory arbitrage is ending. For financial institutions, the transition leading into 2027 is a critical window to overhaul legacy compliance frameworks, upgrade internal controls and align operations with this newly unified oversight model.

> *AMLA is already shaping the future compliance landscape through a concentrated wave of secondary legislation and critical industry consultations.*

Beyond the new fraud and AML requirements requiring proactive measures from firms, the impact of direct supervision will be consequential. By 2028, AMLA will officially select up to 40 high-risk financial institutions that will be subject to direct supervision.

To be selected, an entity must operate in at least six member states and demonstrate a high residual risk profile based on the authority's specific methodology for assessing customer types, products and geographic exposure.

Selected institutions will face stricter scrutiny and greater sanctions for non-compliance, with maximum fines being up to 10 percent of an obliged entity's annual turnover, under Article 22(6) of AMLAR.

However, answering to a single supervisory authority will significantly ease the cross-border communication and implication burdens that have plagued these large institutions under the existing, fragmented system.

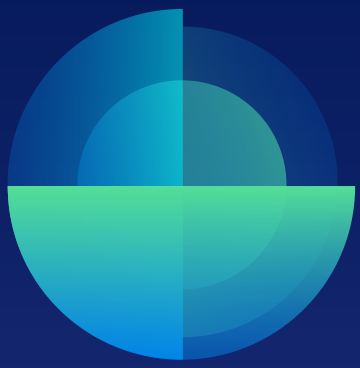
Similarly, through AMLA's indirect oversight, non-directly supervised entities will benefit from greater uniformity across FIUs and national AML regimes. However, as with any newly established central authority, some transitional and implementation challenges are to be expected.

Ultimately, this new era will reward early adopters that treat these legislative acts as a catalyst for modernisation. Firms will need to operate within a significantly more demanding and harmonised AML regime, with less flexibility and greater enforcement risk than ever before.

By embracing the standardisation of the single rulebook and actively engaging in AMLA's ongoing consultations, firms can help shape the standards by which they will be judged.

Those that lean into this centralised model will not only mitigate their regulatory risk, but also gain a significant edge in speed, security and customer trust within the world's largest integrated financial market.

Vixio Regulatory Influencers



Vixio's Regulatory Influencers deep dive into imperative regulatory changes across the globe. Discover what the world's regulatory leaders are up to and use Vixio's unique insights to understand market developments and accelerate your decision making. Read these and more:

Vixio's Verdict: Unpacking the EU Anti-Money Laundering Authority's Future Plans

Regulatory Influencer: The STREAMLINE Act and a New Era of AML Compliance

The US: Moving Stablecoins From the Periphery to the Core

US regulators are being forced to revisit long-standing anti-money laundering (AML) compliance frameworks as the rapid growth of stablecoins and crypto-related activity exposes the limits of traditional controls.

Systems designed for slower, intermediary-driven banking transactions are being tested by instant, borderless digital asset transfers that can move at a speed and scale that legacy monitoring frameworks were never built to address.

As such, supervisory attention is increasingly turning towards stablecoins and other crypto-related activity, representing a shift that reflects a broader effort to modernise the AML regime and address emerging risks tied to digital assets.

Rather than treating crypto as peripheral, regulators are moving to incorporate it more directly into the existing financial oversight structure.

Integrating Stablecoins into the Core

For years, crypto firms have operated within a patchwork system of federal and state regulation.

At the federal level, the Financial Crimes Enforcement Network (FinCEN) has largely relied on its authority under the Bank Secrecy Act (BSA) to issue interpretive guidance clarifying when crypto activities triggered money service business (MSB) obligations.

At the state level, oversight has flowed through money transmission laws, which largely reference adherence to federal AML regulations.

The passage and subsequent implementation of the Guiding and Establishing National Innovation for US Stablecoins Act (GENIUS Act) marks a pivotal moment in the regulatory treatment and oversight of cryptocurrency. It represents the first federal framework specifically designed to regulate stablecoins and establish nationwide standards for their issuance, supervision and oversight.

As rulemaking progresses, entities operating in the crypto space face a shrinking window to align governance and compliance frameworks with the act's licensing requirements, which are currently under consultation.

Although the GENIUS Act creates a licensing framework for domestic payment stablecoin issuers and standards for participation in the US payment stablecoin market, it also explicitly subjects stablecoin issuers to the BSA. It clearly obligates them to establish effective AML and sanctions compliance programmes with risk assessments, sanctions list verification and customer identification.

Regulators are making it clear that oversight is not just on paper. Enforcement actions, such as FinCEN's $3.5m penalty against Paxful, a convertible virtual currency (CVC), peer-to-peer (P2P) trading platform, for deficiencies in its AML programme, show that authorities are prepared to hold crypto firms accountable.

Paxful was found to have facilitated more than $500m in suspicious activity, enabling transactions with countries including Iran, North Korea and Venezuela, as well as with Backpage.com, a website seized by the Department of Justice in 2018 for facilitating prostitution and sex trafficking.

Such actions highlight that authorities are serious about enforcement, not just guidance, and organisations should be clear that the consequences of non-compliance may not be limited to significant financial penalties, but could also include licence revocation, remedial actions and reputational damage.

Crypto firms increasingly need to treat compliance as a basic condition of doing business, as failing to meet regulatory expectations can bring not only substantial financial penalties but also the loss of both legal and social licence to operate.

Bringing stablecoin issuers clearly within federal supervisory authority marks a meaningful shift whereby stablecoins are increasingly treated as payment instruments with financial integrity implications, rather than niche crypto products. In practice, this moves stablecoin activity closer to the core of the financial system.

A Shift in Oversight for Banks

At the same time, regulators appear to be adjusting their approach to traditional banks. In February 2026, FinCEN issued an order granting exceptive relief to covered financial institutions from certain obligations under its 2016 customer due diligence (CDD) rule.

According to the regulator, the action reflects its "commitment to modernizing the BSA framework while maintaining safeguards against illicit finance".

FinCEN's order follows an October 2025 update issued by the Office of the Comptroller of the Currency. In the update, the regulator announced it would eliminate mandatory examination activities not required by statute in order to reduce supervisory burdens for community banks and align with a risk-based supervision framework.

The change in oversight is not limited to rules and regulations. In testimony before Congress in September 2025, FinCEN's director Andrea Gacki explicitly articulated a modernisation strategy for the BSA, emphasising that "financial institutions must be permitted to direct more attention and resources toward higher-risk customers and activities, consistent with an institution's risk profile, rather than toward lower-risk customers and activities".

Meanwhile, the Streamlining Transaction Reporting and Ensuring Anti-Money Laundering Improvements for a New Era Act (STREAMLINE Act), currently pending in the US Senate, has a stated aim of modernising the BSA by reducing reporting requirements that have not kept pace with modern risks.

With mature AML programmes already in place at many large banks, US regulators are directing supervisory focus towards areas where risks are evolving more quickly, including digital assets.

Taken together, these developments suggest that regulators are less focused on expanding prescriptive requirements for established banks and are instead applying a targeted, risk-based approach.

The emphasis is moving from volume of documentation to demonstrable risk management outcomes. In practice, this means closer scrutiny of how promptly investigations are resolved and whether CDD is meaningfully implemented.

Compliance teams will need to evidence not only that policies exist, but that controls are operating as they should, deficiencies are identified and corrected quickly and senior management can articulate how AML risks are being reduced.

Banks that cannot demonstrate this operational effectiveness may find themselves subject to deeper supervisory reviews and facing enforcement penalties.

> *Crypto firms increasingly need to treat compliance as a basic condition of doing business, as failing to meet regulatory expectations can bring not only substantial financial penalties but also the loss of both legal and social licence to operate.*

Operationalising AML Modernisation

Clearer rules around stablecoins and crypto may support broader institutional participation, but the opportunity primarily favours companies prepared to meet increased supervisory expectations.

Companies operating in the digital asset space should anticipate deeper scrutiny and continue strengthening technology-enabled, risk-based compliance frameworks aligned with regulators' modernisation efforts. Preparation now will determine which companies can operate credibly within a more formalised regulatory ecosystem.

With the GENIUS Act placing stablecoin issuers clearly within the scope of the BSA as financial institutions, crypto firms need to revisit how they evaluate risk, likely by bringing their internal risk-rating frameworks more in line with how banks assess payment products.

The exercise should go beyond simply updating a risk assessment and instead reflect a shift towards bank-level supervisory expectations.

Given FinCEN's modernisation push, crypto firms should expect it to pay closer attention to their CDD practices. Compliance teams would benefit from assessing current internal compliance policies against the 2016 CDD rule expectations, even if previously operating under MSB-focused FinCEN guidance.

Proactive teams will build compliance frameworks that mirror bank-level suspicious activity report (SAR) governance, positioning the company for closer supervisory oversight, not just today's MSB-level requirements.

For many firms, this could mean an overhaul of internal compliance policies, as building compliance frameworks at this level is resource intensive and operationally disruptive. It may require substantial investment in personnel, data infrastructure, transaction monitoring technology and independent testing.

Lastly, if stablecoin issuers are treated as financial institutions, governance must be paired with compliance. Practical steps include elevating AML reporting cadence to the board, documenting board approval of the AML risk appetite for digital asset products and outlining formal procedures for examiners access to records.

Long-term success in this evolving environment will depend on treating crypto and stablecoin operations like any other financial institution, not a peripheral player.

Companies that adopt bank-level risk management and compliance and governance practices, as well as embed AML monitoring as a continuous function rather than a period exercise, will be better positioned to meet regulatory expectations, operate credibly and grow their business with confidence.

Vixio Webinars

Industry experts covering topics from all angles.

Tune into Vixio Regulatory Intelligence's webinars to unlock the facts and thoughts from industry experts across the sector – covering topics such as APP fraud, AML compliance and the evolving landscapes of different jurisdictions.

Australia: A Structural Reset of the AML Architecture

Australia is implementing the most extensive amendments to its anti-money laundering and counter-terrorism financing (AML/CTF) framework since its introduction almost two decades ago.

The changes are designed to modernise an AML framework that no longer aligns with the speed, complexity and digitalisation of financial services, particularly in payments, fintech and crypto business models.

The reforms respond to three persistent weaknesses:

- Structural gaps in coverage, particularly the long-delayed inclusion of "Tranche 2" professions and service providers and the extension of Australian Transaction Reports and Analysis Centre (AUSTRAC) oversight to a broader range of high-risk sectors.
- Regulatory gaps with Financial Action Task Force (FATF) standards.
- Evolving financial crime risks, including real-time payments, virtual assets and sanctions evasion techniques.

For AUSTRAC, the objective of the amendments is to examine how AML controls work in practice, paying particular attention to how obligations differ across sectors.

What's In, What's Out?

The amendments introduce more prescriptive customer due diligence (CDD) obligations tailored to different customer types, aiming to reduce ambiguity in how identification and verification obligations should be applied in practice.

They also strengthen expectations around the identification of persons associated with the customer, beneficial owners and senior managers.

For payment and crypto service providers, this has direct implications for both onboarding and ongoing due diligence processes, particularly where automated or high-volume know-your-business (KYB) models are used.

The rules narrow the definition of domestic politically exposed persons (PEPs) compared with earlier exposure drafts. Domestic PEP classification is limited to the head of a local government council, excluding councillors generally.

The rules narrow the definition of domestic politically exposed persons (PEPs) compared with earlier exposure drafts. Domestic PEP classification is limited to the head of a local government council, excluding councillors generally.

This refinement signals a broader regulatory trend towards risk-based proportionality, where supervisory frameworks increasingly target positions with the greatest risk exposure.

The change suggests a recalibration of risk sensitivity, seeking to focus enhanced due diligence (EDD) obligations on roles more likely to prevent corruption risk. AUSTRAC's measures aim to prevent over-classification that could dilute the effectiveness of PEP screening.

Firms should update PEP databases and third-party data feeds to reflect the revised definition. Those relying on external screening vendors will need to confirm that domestic PEP categories have been recalibrated accordingly.

Automated onboarding and ongoing screening tools may need to be reconfigured to remove councillors from domestic PEP flags while retaining heads of local government councils. Risk scoring models linked to PEP status should also be adjusted.

In addition, firms should reassess customers previously classified as domestic PEPs under the previous definition to determine whether EDD measures remain appropriate under the revised definition.

Where AUSTRAC is refining AML/CTF definitions in this way, compliance teams should anticipate similar adjustments across other sector-specific AML expectations.

In particular, this approach may be reflected in obligations applied to payment institutions and crypto-asset service providers (CASPs), where AUSTRAC is amending requirements to withstand the distinct operational and financial crime risk profiles of these sectors.

Challenges for VASPs

Unlike traditional financial institutions, virtual asset service providers (VASPs) often combine retail trading, wallet services, staking and cross-platform transfers within a single ecosystem. PEP status may therefore influence not only onboarding risk ratings, but also access to services such as higher withdrawal thresholds or derivatives trading.

Schedule 8 of the rules introduces a more detailed and harmonised framework for value transfers, aligning Australia's AML/CTF regime with FATF Recommendations 15 and 16.

The amendments require firms facilitating value transfers to ensure that information relating to both payer and payee is transmitted with each transfer, regardless of whether the transaction is conducted through traditional payment channels or involves virtual assets.

Firms should update their transaction monitoring and payment processing systems to ensure that relevant information is consistently captured, verified and transmitted.

For virtual asset transfers, where data capture can be more complex, VASPs may need to undertake a more substantial structural uplift in system upgrades and enhanced controls to avoid non-compliant transfers.

Compliance teams will need to strengthen oversight of third-party vendors and correspondent or intermediary relationships, ensuring that contractual arrangements, technical integrations and ongoing monitoring mechanisms support the accurate transmission of required information.

This represents a move towards greater transparency across payment chains and reinforces regulatory expectations around the importance of data quality and end-to-end visibility of transactions.

Incorporating Sanctions Compliance

The amendments strengthen the integration of targeted financial sanctions within the AML/CTF framework by requiring reporting entities to develop and maintain policies that ensure designated services are not provided in breach of the Autonomous Sanctions Act 2011 and the Charter of the United Nations Act 1945.

The requirement to embed targeted financial sanctions into AML programmes means sanctions compliance must be incorporated into core AML governance, risk assessment and control frameworks.

CDD workflows must include real-time sanctions screening at account opening, including screening of beneficial owners, controllers and associated parties. Screening logic and escalation protocols should be embedded within know-your-customer (KYC) systems rather than handled manually.

Sanctions screening must operate at the point of payment execution, including cross-border transfers and higher-risk domestic transactions. Firms may need to recalibrate monitoring rules to capture indirect exposure risks.

The rule broadens the scope of the assessment of clients subjected to sanctions to "any assets", replacing the earlier wording of "money, property or virtual assets". This reduces the scope for regulatory arbitrage by preventing sanctioned persons from exploiting gaps between asset categories or shifting value into instruments or structures that fall outside the narrowly defined terms.

Firms should identify all asset classes they facilitate, custody or intermediate, including less traditional exposures such as tokenised assets, loyalty points or prepaid instruments.

They may need to update AML and sanctions policies that reference specific asset categories to reflect the broader "any assets" scope. Legal and compliance teams should ensure internal documentation does not unintentionally narrow the scope through legacy wording.

Proactively mapping sanctions exposures across a wider range of asset types should place firms in a stronger position as sanctions regimes expand and geopolitical risks evolve.

> *The reforms signal the expectation that firms can demonstrate clear visibility over ownership and control structures, rather than relying on minimal or standardised data collected at onboarding.*

The broadened language may also signal a regulatory expectation that firms assess sanctions risk in terms of economic value, not merely predefined asset categories. AUSTRAC may scrutinise firms that rely on overly literal or technical interpretations of asset definitions to limit the scope of screening.

Future enforcement may focus less on whether a specific instrument fits within a category and more on whether a firm's control framework meaningfully prevents sanctioned persons from accessing or benefiting from economic resources.

Enforcement Signals: Rising Expectations, Lower Tolerance

Vixio Horizon Scanning data from January 2025 through to February 2026 shows that, during that period, AUSTRAC conducted audits of Binance, Mercedes-Benz and Airwallex – firms that operate complex, high-volume or technology-enabled business models.

These audits signal a focus on the importance of effective AML controls, and AUSTRAC CEO Brendan Thomas has emphasised that AML/CTF compliance is not a back-office function and requires clear accountability.

AUSTRAC can be expected to maintain and potentially intensify this supervisory stance as the reformed AML/CTF framework comes into force. The combination of audits and enforcement actions suggests lower supervisory tolerances for implementation gaps, particularly where firms are unable to demonstrate robust AML controls.

Delivery Over Design

Despite the ambition of the reforms, their impact will depend on their implementation by AUSTRAC and the payment institutions and VASPs operating within the regime.

For firms, the immediate focus should be on execution rather than speculation. This includes conducting gap analyses against the new requirements, prioritising system and control enhancements and documenting implementation roadmaps with clear oversight.

The implementation timelines, March 31, 2026, for existing regulated entities and July 1, 2026, for newly regulated entities, leave a small window for firms to comply. For many this will require technology uplift, governance recalibration and workforce expansion.

Although the availability of implementation plans offers flexibility, over-reliance on deferrals, particularly among VASPs undergoing first-time or expanded regulation, may attract supervisory concern.

Transitional arrangements are unlikely to shield firms from scrutiny if foundational controls remain underdeveloped. Early AUSTRAC engagement is likely to focus on documented risk assessments, board-level oversight and demonstrable progress in implementation.

For firms, the risk is that compliance becomes a resource-intensive exercise focused on delivery timelines rather than a genuine enhancement of financial crime controls.

Although AUSTRAC's proactive engagement, guidance and supervisory clarity will shape how the amendments work in practice, payment institutions and VASPs will bear equal responsibility for translating legislative reform into measurable risk mitigation.

AUSTRAC is likely to emphasise outcomes-based supervision, where firms are assessed on their ability to demonstrate effective controls, instead of technical rule adherence. Firms will need to evidence that the reforms have resulted in tangible uplift, such as strengthened transaction monitoring and improved sanctions integration.

Ultimately, firms must move beyond formal compliance to show demonstrable, sustained improvement in financial crime risk management to ensure they are positioned to meet regulatory expectations.

South Africa: Digital Payments Growth and the Rising Cost of Compliance

South Africa's Draft General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Bill, 2025 marks a decisive moment in the country's attempt to modernise its AML regime under the sustained pressure of Financial Action Task Force (FATF) greylisting.

South Africa was taken off the FATF greylist in October 2025, which demonstrates that the country has taken meaningful steps to improve its risk profile – the next challenge is to stay off.

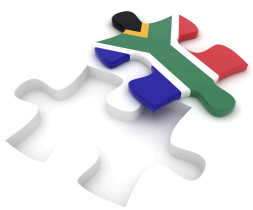
The bill amends several existing statutes and expands the powers of the Financial Intelligence Centre (FIC), and reflects a regulatory system trying to reposition itself for a financial landscape shaped by real-time payments, digital platforms and the growing convergence of fraud and money laundering risk.

This transition matters because South Africa's payments ecosystem is not limited to banks anymore. Research from the South African Reserve Bank shows that fintechs, non-bank payment service providers (PSPs) and intermediaries now sit at the heart of transaction flows, often operating at volumes and speeds that legacy AML frameworks were not originally designed to oversee.

The bill clearly sets out the South African government's ambition to ensure its AML regime is fit for today's challenges, but leaves open a critical question: whether expanded powers and tougher expectations will translate into consistent, effective supervision in practice.

Greylisting as Catalyst and Signal

FATF greylisting can be seen as the primary catalyst for the breadth and urgency of these reforms. The introduction to the bill explicitly states that it is designed to address deficiencies identified during South Africa's enhanced follow-up process and to demonstrate momentum ahead of the next mutual evaluation, expected to begin in mid-2026 and conclude in 2027.



Although the bill is at consultation stage at the moment, its proposed implementation in 2027 suggests that authorities may ramp up enforcement activities in the meantime to ensure the country stays compliant and off the FATF greylist.

The legislation plays a dual role: strengthening domestic AML controls while simultaneously signalling credibility to correspondent banks, investors and global regulators.

The expansion of the FIC's powers, particularly around information sharing and lifestyle audits, aligns South Africa with a global move towards more intelligence-led AML supervision.

Expanding authority is relatively straightforward, but deploying it in a targeted, proportionate way is harder. There is a risk that early enforcement targets easily identifiable compliance gaps, such as documentation deficiencies or reporting failures, rather than the deeper structural weaknesses that drive systemic financial crime risk over time.

Pulling Fintechs and PSPs into the Regulatory Core

A key feature of the bill is how it narrows the regulatory gap between banks and non-bank financial actors. By explicitly requiring institutions to identify and mitigate risks arising from new products, delivery mechanisms and emerging technologies, the reforms bring fintechs and PSPs closer to the core of the AML regime.

The amendments to the Financial Intelligence Centre (FIC) Act and Companies Act significantly increase financial risks for firms. Under the FIC Act, "accountable institutions" face stricter oversight, including mandatory lifestyle audits and an extension of the record-keeping period to seven years, with criminal and administrative sanctions for failing to report suspicious activities or comply with UN sanction lists.

The international standard set by FATF is a minimum of five years for keeping records, but South Africa has opted for a "gold standard" approach to address its specific grey listing concerns and the complexities of local white-collar crime investigations.

Simultaneously, the Companies Act introduces harsher penalties for failing to maintain registers of beneficial interest, allowing for potential deregistration and administrative fines of up to 10 percent of a company's turnover, with the statutory maximum fine increased from ZAR1m to ZAR10m ($60,000 to $600,000).

The cost of non-compliance is thus high, especially for firms operating on thin margins. However, staying compliant also carries tangible cost implications.

Obligations to meet higher evidentiary standards, embedding formalised product risk assessments before launch and preparing for deeper supervisory data access are all capital-intensive exercises, requiring investment in monitoring infrastructure, data architecture, compliance personnel and external advisory support.

Firms that cannot absorb or efficiently manage these obligations face difficult strategic choices, including slowing growth, narrowing product scope or seeking partnership or acquisition.

Over time, this may reshape the market, favouring firms with the resources to absorb compliance investment while putting pressure on leaner operating models built for speed and rapid iteration.

Deeper Supervisory Reach and Higher Evidentiary Standards

The bill significantly strengthens supervisory and enforcement capabilities, increasing both regulatory visibility and the consequences of weak controls. Expanded information sharing, longer data retention and sharper administrative sanctions make it more likely that historical onboarding, risk scoring and monitoring decisions will be scrutinised closely moving forward.

For firms operating high-volume, low-margin payment models, the longer record-keeping requirement increases storage, retrieval and audit obligations and raises the probability that historical customer due diligence, risk ratings and alert disposition decisions will be tested years after the fact. In a real-time payments environment, documentation discipline becomes as important as monitoring capability.

The bill also strengthens the FIC's ability to obtain and share information across public bodies and introduces lifestyle audits as an express function of the centre. This expands the state's capacity to triangulate financial intelligence across agencies, which should reduce miscommunication and ambiguity between regulators and regulated entities.

Fintechs and non-bank PSPs that onboard customers digitally will find that inconsistencies in source-of-funds assessments or beneficial ownership data may become more visible as datasets are linked.

Another notable shift is the explicit requirement that institutions assess and mitigate risks arising from new products, services, delivery mechanisms and emerging technologies before launch, formalising what has often been treated as best practice into a regulatory requirement.

Legislative Reform to Supervisory Measures

Cumulatively, these measures signal a move towards deeper supervisory reach and higher evidentiary standards. Rather than merely refining existing obligations, the bill represents a meaningful redefinition of South Africa's AML framework, recalibrating expectations in a way that will be felt most acutely by high-growth, technology-driven firms, although its implications extend across the broader financial services ecosystem.

Of course, the true test of the reforms will be how they are operationalised in practice, as much will depend on supervisory capacity, prioritisation and enforcement approach.

Businesses operating within South Africa's payments ecosystem should view this new AML modernisation regime as the beginning of a new supervisory phase. The focus is shifting from whether firms have policies in place to whether those policies are defensible, data-backed and consistently applied.

Over the longer term, higher compliance costs, deeper evidentiary standards and the credible threat of meaningful enforcement action will disproportionately affect smaller firms that lack scale.

These measures are likely to squeeze out smaller players, leaving the market to be dominated by larger, highly-resourced institutions capable of absorbing such heavy regulatory overhead.

The bill marks a transition toward a payments market where resilience, governance and financial crime capabilities will be continually tested.

Latin America: Payments Innovation, Dollar Dependency and Uneven Enforcement

AML modernisation in Latin America is being reshaped by rapid innovation, structural dependence on the US dollar and intensifying geopolitical competition over payments and settlement.

Latin American banks and cross-border payment and foreign exchange providers remain deeply reliant on US dollar clearing and correspondent banking relationships, reinforcing alignment with US supervisory expectations.

Cross-border wholesale payments for emerging markets, including those in Latin America, are typically processed through concentrated correspondent networks dominated by dollar clearing systems, with access becoming increasingly centralised in recent years.

Even as the region operates within a payments landscape shaped by US monetary dominance and China's efforts to expand the renminbi's footprint, Latin America has emerged as a global leader in instant payment innovation, most notably through Brazil's Pix, with additional advances such as Mexico's CoDi and Colombia's Bre-B.

Most jurisdictions in the region completed foundational AML reforms in the 2010s, under pressure from FATF and its regional body, GAFILAT. The current phase focuses less on drafting new laws and more on strengthening supervisory effectiveness, sanctions alignment and digital oversight.

Dollar Dependency and Sanctions Alignment

US dollar centrality continues to strongly influence AML implementation throughout the region. Data from the Bank for International Settlements (BIS) shows that globally, cross-border trade, high-volume remittances and foreign exchange flows depend heavily on US dollar clearing, with the greenback on one side of approximately 89 percent of all foreign exchange trades in April 2025.

As a consequence, supervisory expectations are influenced by enforcement signals and guidance from the US Financial Crimes Enforcement Network (FinCEN).

Regulators looking for alignment with FATF frameworks increasingly expect institutions to incorporate cross-border sanctions exposure, correspondent banking relationships and international standards into their AML risk assessments.

This expectation is rooted in FATF Recommendation 6 on Targeted Financial Sanctions, which requires jurisdictions to implement sanctions screening and freezing mechanisms within their AML/CTF systems, and in accompanying FATF guidance clarifying supervisory obligations.

Latin American supervisors have embedded these standards into domestic regulation. A leading example is the Brazilian central bank's Circular No. 3,978/2020, which formalised a risk-based AML framework aligned with FATF principles and requires institutions to conduct internal risk assessments covering cross-border exposure and correspondent relationships.

> *Across the region, payment service providers (PSPs), embedded finance platforms, foreign exchange operators and digital asset firms are now central to supervisory focus.*

The operational impact of the need for US regulatory alignment was evident in November 2025, when Mexico's Financial Intelligence Unit coordinated with the US to block entities linked to an international money laundering network, demonstrating cross-border sanctions and AML coordination.

The US' recent review of Brazil's Pix payment system highlights how real-time domestic payment infrastructure can carry international regulatory implications when embedded within dollar-clearing and correspondent banking networks.

As US sanctions regimes continue to expand and enforcement remains active, Latin American institutions operating within dollar-clearing networks are likely to face increased expectations around sanctions screening and escalation.

Payments Innovation and Fraud-AML Convergence

In Brazil, the Central Bank's 2024 limits on Pix transactions from unregistered devices signalled a willingness to embed fraud and behavioural risk controls directly into real-time payment infrastructure.

Brazil's virtual asset framework has since moved into full implementation, with Central Bank Resolutions No. 519, 520 and 521, effective from February 2026, establishing authorisation, foreign exchange oversight and AML requirements for virtual asset service providers (VASPs).

In 2025, Argentina's National Securities Commission operationalised the virtual asset provider registry established under Law No. 27,739, bringing VASPs within a formal supervisory framework.

The resolution requires mandatory Comision Nacional de Valores (CNV) registration prior to operation and imposes ongoing governance, internal control and reporting obligations. VASPs must implement documented AML/CTF programmes, appoint compliance officers, maintain customer identification and transaction traceability procedures, and submit periodic information to the CNV alongside suspicious transaction reports to the Financial Intelligence Unit (UIF).

By embedding VASPs within a supervised regulatory perimeter and empowering the CNV to suspend or revoke authorisation for non-compliance, the framework strengthens enforceability of sanctions and AML controls and aligns oversight more closely with FATF Recommendations 6 and 15.

In Peru, Resolution S.B.S. No. 02648-2024 brought VASPs fully within the AML framework, requiring documented compliance systems, customer and beneficial owner identification, and annual reporting to the Financial Intelligence Unit.

Mexico has complemented similar perimeter expansion with reforms, strengthening transparency and increasing institutional liability for monitoring failures in virtual asset and cross-border transactions.

Across the region, payment service providers (PSPs), embedded finance platforms, foreign exchange operators and digital asset firms are now central to supervisory focus.

FATF's digital transformation initiatives recognise that effective AML/CTF frameworks may in future rely on technological controls operating at scale and speed and be able to adapt to evolving risk patterns.

Both regulators and regulated institutions are exploring the use of advanced analytics, automated monitoring systems and AI-enabled tools to enhance scalability, improve risk identification and reduce reliance on purely manual controls.

For example, Colombia's Superintendency of Finance has implemented an AI-driven SupTech tool to automate the assessment of AML/CTF risk programmes, reducing manual workload and enabling supervisory prioritisation and more agile analysis.

However, such digital transformation across Latin America remains uneven. In less affluent or lower-capacity economies such as Bolivia, supervisory priorities continue to centre on strengthening foundational AML/CTF controls, rather than deploying advanced automated monitoring frameworks.

Structural Gaps, Fragmentation and Strategic Opportunity

A 2020 regional review by GAFILAT found that many Latin American jurisdictions had adopted legal frameworks aligned with FATF recommendations on beneficial ownership transparency. However, effectiveness lagged due to fragmented registries, limited digitisation, inconsistent updating of ownership information and challenges in cross-checking data across state authorities.

Recent reforms illustrate both progress and the persistence of implementation challenges. In Chile, Circular No. 2368 aligned supervisory expectations with updated Financial Analysis Unit rules, expanding PEP categories and reinforcing enhanced due diligence and beneficial ownership verification requirements.

Mexico's 2025 reform to the Federal Law for the Prevention and Identification of Operations with Illicit Proceeds tightened the definition of beneficial owners, expanded vulnerable activities and extended documentation retention obligations.

In El Salvador, a comprehensive 2025 AML/CTF legislative overhaul replaced a 1998 framework, strengthened the Financial Investigation Unit's database access powers, and formalised beneficial ownership identification within a newly coordinated national prevention system.

Together, these measures demonstrate institutional strengthening. However, the practical capacity of supervisors to investigate suspicious activity and sustain prosecutions, remains uneven across the region.

Brazil's supervisory architecture is anchored by the central bank's risk-based AML framework, providing a centralised financial intelligence structure, and integrated oversight of payment and VASPs.

In contrast, jurisdictions such as Bolivia are subject to ongoing FATF monitoring and continue to prioritise foundational supervisory capacity and investigative effectiveness. This divergence creates operational complexity for firms operating across multiple markets.

The Future of AML Supervision in Latin America

AML modernisation in Latin America is shifting from formal rulemaking towards infrastructure-level supervision and cross-border risk management.

For payment institutions, embedded finance platforms, foreign exchange providers and digital asset firms, this transition elevates compliance from a technical requirement to a strategic determinant of market access.

As the region navigates continued reliance on US dollar clearing, alongside growing ambitions for China-linked trade settlement and payment infrastructure integration, currency and corridor exposure are also becoming central components of supervisory risk assessments.

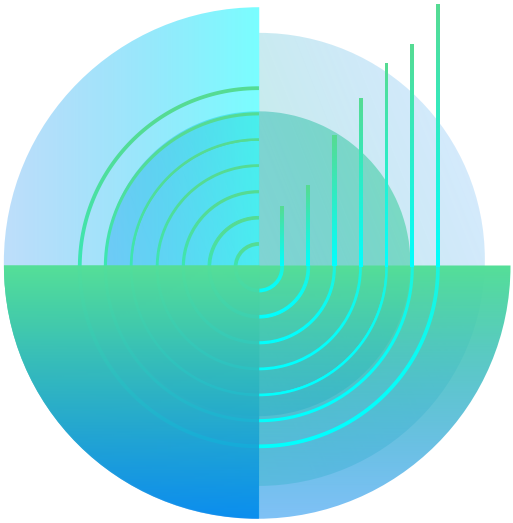
Firms should reassess the resilience of correspondent banking relationships, including dependency on specific clearing currencies and counterparties. Mapping sanctions exposure across key payment corridors and foreign exchange flows will become increasingly important, particularly where US dollar settlement or renminbi-linked trade flows are involved.

Organisations deploying automated or artificial intelligence-driven transaction monitoring tools should ensure robust model validation, documentation and explainability to withstand supervisory scrutiny.

In jurisdictions with uneven enforcement capacity, multinational firms may also need to strengthen group-level oversight to ensure consistent AML standards across markets.

Those that anticipate supervisory direction will be better positioned to sustain growth in a fragmented but strategically significant payments landscape.

> *The practical capacity of supervisors to investigate suspicious activity and sustain prosecutions, remains uneven across the region.*



Analyse. Anticipate. Accelerate.

About Vixio PaymentsCompliance

Vixio PaymentsCompliance is a fast, effective and user-friendly platform that supports compliance activities, removing time-consuming and resource-heavy manual searches and lowering associated costs. With PaymentsCompliance, customers can access real- time regulatory intelligence and updates in 140+ jurisdictions across the world through horizon scanning, expert analysis, and insights to better understand and prepare for changes in payments regulations.

Find out more at Vixio.com/vixio-platform

UK Office St Clare House, 30-
33 Minories London EC3N 1DD
Tel: +44 (0) 207 921 9980

US Office
1250 Connecticut Ave NW Suite 700
Washington, DC 20036
Tel: +1 202 261 3567

info@vixio.com

Vixio.com

Our deep understanding of the industries we serve, globally recognised analyst insights and easy-to-use technology are why Vixio PaymentsCompliance is trusted by some of the largest names in payments and other industries, including:

PayPal DISCOVER ByteDance

Disclaimer

This report has been created by Vixio PaymentsCompliance, a product of Vixio Regulatory Intelligence. Information contained within this report cannot be republished without the express consent of Vixio PaymentsCompliance.

Vixio PaymentsCompliance does not intend this report to be interpreted, and thus it should not be interpreted, by any reader as constituting legal advice. Prior to relying on any information contained in this article it is strongly recommended that you obtain independent legal advice. Any reader, or their associated corporate entity, who relies on any information contained in this article does so entirely at their own risk. Any use of this report is restricted by reference to Vixio PaymentsCompliance's terms and conditions.

© Compliance Online Limited (trading as Vixio) 2026