

GLOBAL FINANCIAL REGULATORY HIGHLIGHTS REPORT

Q3 2025

FOREWORD

Welcome to the third quarterly financial regulatory highlights report. The report provides seeks to provide a 360-degree perspective of the key financial regulatory developments during Q3 2025 with an emphasis on policy and supervision priorities.

The report is structured thematically by the major pillars of financial regulation. Each section presents a synopsis of the major developments supported by specific examples from across major geographies. The primary objective of the report is to provide a fact-based overview of the main directions.

Information reflected in the report was collected via Regxelerator's AI-powered intelligence platform Regxplora, which automatically collects updates from ~700 financial regulatory bodies, central banks, standard setters and national ministries of finance and treasuries on a 24/7 basis.

For more information and free access to Regxplora, visit platform.regxplora.com.

TABLE OF CONTENTS

01	Prudential Risk & Financial Stability
02	Cyber & Operational Resilience
03	AML & CFT
04	Consumer Protection
05	Artificial Intelligence
06	Digital Assets & Tokenization
07	Payments
08	Climate & ESG
09	Suptech
10	Other developments
11	Leadership changes

PRUDENTIAL & FINANCIAL STABILITY

Risk landscape

Against a weakening economic outlook and uncertainty, the prudential risk landscape continues to show a mixed picture.

Across core prudential metrics, authorities report that banks and insurers remain well capitalised and profitable despite the volatile backdrop. The ECB's 2025 stress test concluded that the euro area system is "resilient against a severe economic downturn scenario" with the aggregate CET1 ratio standing at 12.0% under an adverse path.

Point-in-time supervisory data reinforces this view, with the ECB reporting a Common Equity Tier 1 ratio of 16.05%, a return on equity of 9.85% and an NPL ratio of 2.24% in the first quarter, while stage-2 loans decreased quarter-on-quarter. Data for the second quarter by the European Banking Authority strengthened this picture further with CET1 at 16.3%, higher LCR and NSFR, ROE up to 10.7%, and stage 2 loans declining to 9.4%

In insurance, EIOPA's end of July dashboard also found that "risks in the European insurance sector are stable at a medium level" supported by robust capitalisation, improved non-life underwriting and broadly steady life investment returns, even as vigilance is maintained on liquidity indicators and lapse behaviour. The European Securities and Markets Authority (ESMA) H1 market review also points to overall resilience in funds despite the most pronounced volatility since the COVID-19 episode, with market infrastructures remaining robust in recent stress tests and cleared markets functioning without disruption.

At the same time, supervisors remain cautious. The European Supervisory Authority's (ESAs) Joint Committee stresses that "geopolitical risks are cross cutting and impact various aspects of financial institutions' operations", advising continued scenario analysis and strong provisioning policies as markets absorb tariff announcements and defence spending shifts. ESMA underlines that "any unexpected geopolitical developments could risk driving sudden market corrections" after the April volatility, with high or very high risks across markets and continued leverage and liquidity vulnerabilities in parts of the fund sector, including sustained real-estate fund outflows in some jurisdictions.

To further substantiate the prudential angle, the Joint Committee links the April swing to tariff announcements that drove a sharp widening in corporate spreads, particularly in high-yield, and notes that again-elevated equity valuations leave scope for sudden repricing; it also flags possible foreign-currency funding vulnerabilities as EU banks hold close to 30% of exposures and 21% of funding in foreign currencies

EIOPA also flags an upward outlook for market risk given persistent fixed-income volatility, and the potential disconnect between equity prices and fundamentals. In banking, profitability cushions are narrowing at the margin as net interest margins declined to 1.53% in Q1 and "continued to tighten" in Q2.

Outside Europe, prudential authorities echoed a similarly mixed view characterized by resilience and vigilance. In the UK, the July Financial Stability Report judges the banking system well capitalised with robust liquidity and maintains the countercyclical buffer at 2%, while noting that April tariff announcements drove market turbulence and that risky asset valuations remain vulnerable to sharp corrections. In the United States, the Federal Deposit Insurance Corporation's (FDIC) Q2 2025 Quarterly Banking Profile reports industry ROA at 1.13% with net interest margin broadly unchanged, asset quality metrics generally favourable despite pockets of weakness, domestic deposits rising for a fourth consecutive quarter, and the number of problem banks declining to 59.

In Australia, the Australian Prudential Regulation Authority's (APRA) September release shows authorised deposit-taking institution's total capital ratio stable at 20.4%, LCR at ~130% and NSFR near 116%, with 30–89-day arrears at 0.55% and non-performing loans at 1.07% even as commercial property exposures rose year on year.

Recovery and resolution

During the quarter, European authorities further focused on making recovery and resolution more execution-ready by publishing operational guidance, streamlining planning standards and building common testing frameworks. In banking, the Single Resolution Board (SRB) launched a consultation on updated operational guidance for separability and transferability that clarifies deliverables such as the separability analysis and transfer playbooks across all transfer tools and issued operational guidance setting out a standardised resolvability self-assessment that will feed a multi-year testing programme and future planning cycles. The European Banking Authority (EBA) complemented this with a new chapter of its Union Resolution Handbook that defines a taxonomy and lifecycle for simulation exercises to strengthen authorities' operational capacity, and opened a consultation to simplify and consolidate the regulatory technical standards on resolution plans and the functioning of resolution colleges to improve readiness and cross-border coordination.

In insurance, the European Insurance and Occupational Pensions Authority (EIOPA) advanced implementation of the Insurance Recovery and Resolution Directive by consulting on technical standards for resolution colleges and on minimum reporting forms and templates for resolution planning, aligning requirements with a phased and proportionate approach toward the 2027 application date.

The UK updated its domestic framework as the Bank of England finalised revisions to its Minimum Requirement for Own Funds and Eligible Liabilities (MREL) policy, with changes taking effect from 1 January 2026.

At the global level, the IMF published a technical note on exceptional public solvency support that distils conditions, instruments and governance good practice for last-resort interventions, providing an international benchmark for authorities refining their crisis toolkits.

Regulatory simplification and streamlining

Across prudential policy, authorities continued to signal a shift towards greater simplification, streamlining and proportionality in regulatory requirements and supervision in an effort to reduce burden and compliance cost while preserving sufficient supervisory insight. Areas targeted during Q3 stretch multiple areas including (1) regulatory reporting reduction and data rationalisation; (2) capital framework simplification and recalibration, (3) more granular tiering of requirements. Example initiatives include the following:

Regulatory reporting reduction and data rationalisation	Capital framework simplification and recalibration	More granular tiering of requirements
The UK PRA proposes deleting 37 bank reporting templates and consolidating FINREP requirements, targeting ~GBP 26 million annual savings from 1 January 2026	New Zealand's RBNZ consulted on lower capital requirements for deposit takers, removing AT1 and refining standardised risk weights to better align capital with risk	The ADGM FSRA finalised prudential changes for lower-risk firms, removing Expenditure-Based Capital Minimum for Category 4 firms that do not hold client assets or insurance money, supported by a higher capital base
Germany's Bundesbank and BaFin proposed abolishing the "million-euro" credit reporting regime by 30 December 2026, relying instead on AnaCredit and securities statistics	APRA initiated a consultation paper to implement its decision on removing AT 1 from banks' minimum capital requirements, including eliminating the concept of Tier 1 capital and recalibrating Common Equity Tier 1	APRA will formalise a three-tier banking framework to support greater proportionality, covering large banks, medium banks (other significant financial institutions) and small banks (non-SFIs)

In line with this shift, the European Central Bank's Single Supervisory Mechanism (SSM) is also taking targeted measures. This includes an overhaul of the Supervisory Review and Evaluation Process (SREP) into a multi-year, risk-focused process with shorter, earlier decisions, clearer Pillar 2 outcomes and a tiered follow-up model to support simpler supervision while maintaining appropriate safeguards. Additionally, the SSM is also cutting procedural burden through faster, more proportionate approvals, testing a 10-day fast-track for sufficiently simple securitisations and reducing average processing times for fit and proper assessments.

CYBER & OPERATIONAL RESILIENCE

In line with previous quarters, cyber risk and by extension operational resilience, remain front and center from a risk perspective, reinforced by ongoing geopolitical tensions and rapid digitalization. The European Supervisory Authorities (ESAs), in their Autumn Risks and Vulnerabilities report, warn that cyberattacks persist, including successful intrusions, and are growing in sophistication. High concentration in third-party IT providers and deep operational dependencies increase exposure and can amplify contagion and the potential systemic impact of incidents.

In terms of cyber risk incidents, Q3 2025 recorded fewer events than earlier in the year, with approximately 14 recorded incidents as of the preparation of this report compared with about 18 in Q2 and 25 in Q1. Overall, the profile shifted toward direct fund theft and large data compromises, illustrated by reserve-account diversions in Brazil's payments and banking sector and major data exposures at Vietnam's credit bureau, Lotte Card, and Allianz Life, while a smaller supply-chain breach at WealtheSimple reinforced persistent third-party risk. In digital assets, activity remained frequent but at mid-sized scales, with losses at GMX, CoinDCX, and BtcTurk in the 40 to 50 million range rather than the nine figure and billion dollar events observed in H1. Ransomware persisted but was concentrated in a single high-impact case at Seoul Guarantee Insurance that disrupted services for several days. Most notably, the threat actor profile tilted more clearly toward financially driven crime. The first half included several state linked or politically motivated operations, yet in Q3 the majority of activity appears to have been motivated by profit seeking groups such as ransomware crews and data theft syndicates. Only two outliers carried a geopolitical tone, namely the Cyber Anarchy Squad action against a Russian platform and the suspected Lazarus involvement in CoinDCX.

Against this backdrop, authorities actively drove forward the policy and supervisory agenda with measures during the quarter focusing on three broad themes.

Third-party and cloud risk

In Europe, the ECB finalised its Guide on outsourcing cloud services, clarifying expectations under DORA for board accountability, pre-contract risk assessment, multi-region or multi-provider strategies for critical functions, backup and recovery testing, among other things. In parallel, the ESAs issued a public Guide on DORA oversight that explains how Joint Examination Teams will designate and supervise critical ICT third-party providers through monitoring, information requests, investigations, and inspections, and how lead overseers and joint forums will coordinate follow-up. Complementing this, the EBA opened consultation on new Guidelines for sound management of non-ICT third-party risk, extending the framework beyond outsourcing Outside the EU, South Africa's FSCA and Prudential Authority set interim expectations for cloud and data offshoring and signalled a forthcoming cross-sector Joint Standard that will harmonise requirements and deepen supervisory scrutiny.

Testing

The Bank of Italy published an exploratory survey of the domestic cybersecurity-testing market, finding a dynamic but concentrated provider landscape. The analysis points to the need for greater standardisation, accreditation and resource development to meet rising demand for threat-led testing.

Intelligence sharing and incident reporting

The Central Bank of Kenya established a Banking Sector Cybersecurity Operations Centre to provide threat intelligence, incident response, forensics and investigations to regulated institutions. The Bank of Mauritius announced plans for a threat-intelligence sharing platform via a request for proposal, with the goal of providing the central bank and market operators timely and common access to actionable intelligence. In Abu Dhabi, the Financial Services Regulatory Authority finalised amendments requiring authorised firms to implement a cyber risk management framework integrated with overall risk management and to report material incidents within 24 hours.

Across the Pacific, the Australian Prudential Regulation Authority (APRA) reinforced expectations for cyber resilience towards the superannuation sector as part of a CEO roundtable following the cyber attack in April this year which compromised over 20,000 accounts across several major financial institutions. The Authority called for immediate uplifts in authentication, incident response and industry coordination and urged faster information sharing through the national financial sector playbook.

At the global level, the IAIS launched consultation on a draft Application Paper outlining objectives and a supporting toolkit to strengthen operational resilience across the insurance sector.

Spotlight: Key cyber incidents in the financial services sector by region during Q3 2025 (not exhaustive)

Region	Incident description	Impact
Asia	Hackers deployed ransomware against Seoul Guarantee Insurance (SGI), Korea's largest guarantor insurer, disrupting access to core operational systems.	~4 days disruption of SGI's online services were, delaying insurance policy issuance/verification nationwide
	Hackers breached India's CoinDCX's internal systems and stole \$44 million from an operational hot wallet, moving funds through blockchain bridges and mixers	~\$44 million theft from CoinDCX's treasury, prompting suspension of Web3 and DeFi connectivity services
	Attackers exploited an unpatched payment server at Lotte Card in South Korea, installing malware to exfiltrate nearly 200 GB of customer and card data.	Exposure of 2.97 million Lotte Card customer records, making it one of South Korea's largest financial data breaches
	ShinyHunters breached Vietnam's National Credit Information Center by exploiting an end-of-life platform vulnerability, stealing 160+ million credit records	Exfiltration of over 160 million Vietnamese credit bureau records
South America	Hackers infiltrated C&M Software – a tech provider bridging small banks to the Central Bank of Brazil's systems – using login credentials sold by an insider	~R\$800 million (~\$140 M) was illicitly transferred out of banks' reserve accounts
	Hacker group CyberTeam temporarily took offline Equifax S.A.'s Infocheck and Informconf website in Paraguay in a network denial of service attack	Temporary unavailability of Infocheck's website for part of the day, disrupting access to credit checks
	Brazilian Bank Tribanco suffered a cyber-heist after attackers penetrated reserve accounts and diverted funds, with rapid laundering into crypto assets.	Illicit transfer of bank funds from Tribanco's reserve accounts, presumed to be in the millions of reais
North America	A malicious 'Document Viewer' app on Google Play covertly dropped the Anatsa banking trojan - malware designed to steal financial credentials - onto user devices	Theft of an undisclosed number of banking credentials across multiple U.S. and Canadian banks,
	Attackers infiltrated Allianz Life Insurance Co. of North America through a third-party CRM, using social engineering to gain access to cloud-hosted client data.	Compromise of personal data for ~1.4 million customers, including sensitive identifiers (SSNs, government IDs)
	Wealthsimple was hit by a supply-chain attack through a compromised third-party software package that exposed limited client data	Exposure of ~30,000 Wealthsimple client records (<1% of total), including government IDs and SINs
Europe	Hackers compromised the hot wallet of BtcTurk's, one of Turkey's largest cryptocurrency exchanges, withdrawing crypto assets including large volumes of Ethereum.	~\$49 million theft of digital assets from BtcTurk's hot wallets
	The pro-Ukraine group Cyber Anarchy Squad struck Investment Projects, destroying parts of its IT systems and leaking internal databases.	Outage of Investment Projects' online platform and leak of internal company data
Global	A hacker exploited a price calculation flaw in decentralized exchange GMX's V1 smart contract using a re-entrancy attack to withdraw assets	~\$42 million in crypto theft, most of which was converted into ETH and stablecoins and dispersed to new wallets

Spotlight: Preparing for the impact of quantum computing

Since the start of the year, authorities have been moving toward more proactive awareness-raising regarding the impact of quantum computing on financial services, more explicitly identifying quantum computing as a potential threat to financial stability and security and establishing a sense of urgency around advancing mitigation measures. Amid these heightened risk signals, more structured transition planning toward a quantum-safe financial infrastructure is taking shape. In July, the Bank for International Settlements (BIS) published a quantum-readiness roadmap outlining a phased approach for migrating from current cryptographic systems to quantum-resistant alternatives.

The paper explains that quantum computers pose varying levels of risk to different encryption methods. Shor’s algorithm presents the most serious threat, as it can break RSA and ECC, which underpin secure communications and digital signatures. In contrast, Grover’s algorithm weakens symmetric encryption but can be mitigated by lengthening keys. The paper also warns that many legacy systems still rely on outdated protocols such as TLS 1.2, which cannot be upgraded to quantum-safe standards and must be replaced entirely. The paper’s evaluation of quantum-safe solutions reveals that while post-quantum cryptography - new mathematical problems that even quantum computers cannot solve - is ready for use today, it comes with major practical challenges:

Massive increase in data requirements The new encryption keys are 4–40 times larger than current ones (jumping from 256 bytes to over 1,000 bytes for public keys, and from 64 bytes to over 2,400 bytes for digital signatures), creating storage and transmission burdens	Transition complexity far exceeds simple replacement Payment terminals struggle with larger keys. Historical transitions like SHA-1 to SHA-2 took decades despite being simpler
Alternative quantum technologies remain experimental Quantum key distribution, which uses quantum physics to detect eavesdropping, requires expensive dedicated fiber optic cables and cannot verify identities. Other quantum solutions for protecting data during processing remain in research labs	Governments disagree on implementation strategy NIST believes the new algorithms alone are sufficient, while German and French security agencies insist on using them alongside traditional encryption for extra safety while the National Security Agency rejects quantum key distribution as too expensive compared to post-quantum algorithms

Against this backdrop, the paper presents a dual-track roadmap where system-wide coordination and individual institutional implementation must proceed in parallel. The paper proposes that both systemic and institutional efforts should follow three phases. At the systemic level, central banks should lead stakeholder education and risk assessment (engagement), coordinate decisions on protocol phase-out dates and technical standards (planning), then monitor system-wide progress through stress testing (execution). Individual institutions should mirror these phases: building internal awareness through executive leadership and cross-functional teams, developing cryptographic inventories and migration strategies, then executing implementation starting with high-priority systems.

The paper recommends two principles underpin all transition activities. Cryptographic agility—the ability to rapidly switch between encryption algorithms—should be built into both systemic standards and institutional implementations to protect against evolving quantum threats. Defense in depth requires layering independent security mechanisms (pre-shared keys, post-quantum algorithms, two-factor authentication) ensuring backup protection if one layer fails.

Practical experimentation effort

Alongside more strategic and structural planning, standard setters and authorities are also accelerating experimentation efforts:

Project Leap (Phase 2)

the BIS Innovation Hub also launched Phase 2 of Project Leap in collaboration with the Bank of Italy, Bank of France, and Deutsche Bundesbank as well as Swift and Nexi-Colt. Phase 2 of the Project builds on the outcomes of the project’s initial phase and concentrates on enhancing the quantum resilience of payment systems. It tests the use of post-quantum cryptography in a European payment system by sending liquidity transfers between Project Leap’s central bank participants using post-quantum digital signatures.

MAS Quantum-Safe Communications Sandbox

The Monetary Authority of Singapore (MAS) – in collaboration with private sector partners – has released a technical report on a proof-of-concept sandbox for quantum-safe communications in the financial sector. The initiative aimed to assess the use of Quantum Key Distribution (QKD) for secure communications. The findings indicate that QKD can significantly enhance the security of communication networks, particularly for financial institutions, by securing connections between data centers and premises.

AML & CFT

Global AML and CFT policy work should have a greater tilt towards operationalization with several comprehensive practical resources released by FATF in collaboration with global partners. Work on mitigating the unintended progress of its standard also took further shape with the release of a new dedicated procedure for handling potential adverse impacts on non-profit organizations.

Global policy developments

Practical National Risk Assessment Toolkit and Cooperation Handbook

In early September, the FATF launched a comprehensive Money Laundering National Risk Assessment toolkit providing countries with practical resources and methodologies to develop and strengthen their risk-based approach to assessing money laundering risks in line with FATF Standards. The toolkit comprises three main annexes offering different analytical tools:

ANNEX A

Quick guides for four priority areas - corruption, virtual assets and service providers, legal persons and legal arrangements, and the informal economy – that set out risk scope, key risk questions and considerations, and share relevant case studies

ANNEX B

Aggregation of cross-country risk information, including analysis of major predicate offences from 147 mutual evaluations, proceeds-of-crime estimates, and categorisation frameworks for threats and vulnerabilities using a PESTEL lens

ANNEX C

Compilation of assessment tools from the World Bank, International Monetary Fund, and Council of Europe with an outline of the methodology for risk assessment under each tool and links to other sources that may inform the risk evaluation

In parallel, the FATF – in cooperation with the Egmont Group, INTERPOL and the United Nations Office on Drugs and Crime (UNODC) - published a dedicated Handbook on International Cooperation on Money Laundering Detection, Investigation, and Prosecution Handbook. Intended as a practical guide, the handbook maps the operating landscape for international co-operation in money-laundering detection, investigation and prosecution, examining operational challenges, evolving needs and effective co-operation channels, and setting out best practices, tools and mechanisms that jurisdictions can adopt, distinguishing between formal and informal cooperation types complete with practical case studies.

New procedure to address unintended consequences affecting Non-Profit Organisations

In parallel, the FATF introduced a procedure to address unintended consequences from misapplying its standards to non-profit organisations, laying out a structured approach for countries, the IMF, and the World Bank to raise concerns. Notably, when two or more parties report that a country's NPO rules unduly disrupt legitimate activity, the ECG Co-Chairs conduct a prima facie review with FATF Secretariat support; the Secretariat engages the country, reporting parties, relevant FSRB secretariats, and the NPO community, and compiles evidence from prior assessments, comparable cases, and other credible sources to test a clear substantive threshold.

New statements by the Wolfsberg Group on Effective Monitoring for Suspicious Activity and its Risk-Based Approach

In July 2025, the Wolfsberg Group published Part II of its Statement on Effective Monitoring for Suspicious Activity, offering a practical framework to move from rules-based monitoring to ML/AI approaches across three pillars: transition and validation, balancing model risk with financial-crime risk, and explainability. It builds on the 2024 Statement, which broadened the focus from automated transaction monitoring to Monitoring for Suspicious Activity. The Group also issued a dedicated Statement on the Risk-Based Approach, setting the core principles of proportionality, prioritization, and effectiveness that underpin both MSA documents. It defines proportionality as requiring financial institutions to design financial crime risk management programs appropriate to their specific size, scale, footprint, and customer base rather than applying universal standards.

Continued elevated virtual asset risk concerns

Amid the growing adoption, AML and CFT-related risk concerns over crypto-assets, including stablecoins, remained elevated and continued to be key areas of policy and supervisory focus across geographies in Q3. Building on issues highlighted in its sixth Targeted Update on Virtual Assets and Virtual Asset Service Providers released in June, the FATF flagged further concerns through a comprehensive update on terrorist financing risks.

The report identified widespread deficiencies in the effective investigation and prosecution of TF cases and highlighted increasingly hybrid and decentralised financing methods, including the use of digital platforms and virtual assets. Notably, the report finds that terrorist misuse of virtual assets is rising, though difficult to quantify, as features enabling pseudonymous, rapid and cross-border transfers make them attractive, including peer-to-peer movements that occur directly between private wallets without an intermediary subject to AML and CFT controls. Abuse is concentrated in online donations and crowdfunding on social and messaging platforms, often via in-app wallets with weak customer due diligence and is reinforced by a shift from bitcoin toward lower-fee, lower-volatility stablecoins such as USDT. To complicate tracing, actors use mixers that commingle and redistribute funds to mask origin, anonymity-enhancing coins like Monero that conceal transaction details, single-use addresses that limit linkage, decentralised exchanges that allow direct token swaps without central order books, and unhosted wallets where users control keys outside regulated custody.

The FATF also highlights hybridisation – blending digital transfers with informal value-transfer systems such as hawala – where facilitators hold virtual assets “in trust” before cashing out, which makes conversion points critical yet vulnerable given reliance on virtual asset service providers, crypto ATMs, and informal or unregistered exchangers. Although public blockchains can aid investigations, effectiveness is constrained by pseudonymity, obfuscation tools, off-chain activity, and dependence on a limited set of analytics providers-

In the face of the growing risk concerns and challenges, standard setters and national authorities continue to review options for deployment of technology to enhance risk detection. In the United States, following the enactment of the new GENIUS Act, the ACT the Department of the Treasury issued a request for comment on innovative methods and technologies such as APIs, AI, and blockchain technology that financial institutions currently use or could potentially adopt to detect and mitigate illicit finance. At the state level, New York’s Department of Financial Services issued a notice encouraging covered banking organizations engaged in virtual currency-related activity to integrate blockchain analytics, including wallet screening, source-of-funds verification, ecosystem monitoring and counterparty risk assessment, into their compliance programs. At the global level, the Bank for International Settlements (BIS) has released a bulletin exploring an alternative approach to AML compliance for crypto-assets circulating on permissionless public blockchains, recognizing limits of intermediary-based controls. It proposes leveraging public transaction histories to assess crypto-asset provenance and assign AML “compliance scores” (including for stablecoins) that would be checked at banking off-ramps to block illicit inflows.

Spotlight: EBA’s perspective on ML/TF related affecting the EU’s financial sector

In late July, the EBA released its fifth Opinion on ML and TF risks, which finds that crypto-asset services remain a key risk concern with high and in parts rising exposure as activity and authorisations expand and residual risk in the sector outpaces inherent risk. It highlights several points for attention:

Rapid expansion drives risk exposure

Rapid expansion keeps risk high. Authorised crypto-asset service providers (CASPs) grew 2.5-fold to 2,525 between 2022-24, driving larger transaction volumes, leaving supervisors judge ML/TF risks as high

Control gaps at the core

Inspections continue to find deficiencies in understanding of customer-specific ML/TF risk and KYC and beneficial-owner verification, pointing to systems/controls not yet commensurate with firms’ risk profiles

Perimeter risks and weak governance

Some entities attempted to bypass licensing or registration, and several cases raised concerns about senior management integrity and the transparency and adequacy of governance arrangements

Interlinkages spread risk

Growing crossover with e-money and payment institutions and banks, often via outsourcing or group structures, blurs accountability and creates unclear operational boundaries for crypto-to-fiat services.

Shift in terrorist-financing vectors

While overall TF risk is broadly stable, law-enforcement observations show movement from bitcoin toward stablecoins and e-money tokens, with peer-to-peer channels and self-hosted wallets increasing obfuscation.

RegTech blind spots heighten exposure

Over-reliance on outsourced, poorly tested monitoring and screening tools has produced a surge in material weaknesses, leaving crypto and other sectors with unchecked alerts and systemic blind spots

CONSUMER PROTECTION

Consumer protection initiatives during Q3 remained focus on priorities visible earlier in the year including the progression of Buy Now, Pay Later (BNPL) regulatory oversight, finfluencer activity and the combat of the increasing fraud and scam activity. Alongside these, sales practices as well as complaint and redress management crystalized as new attention points across several geographies.

Buy Now, Pay Later

Further to the developments during Q1/Q2, which saw Australia, the UK, and the United States bring BNPL products within existing consumer credit frameworks, authorities maintained their focus on regulating BNPL during Q3. Malaysia's Senate approved the landmark Consumer Credit Bill 2025, establishing a dedicated Consumer Credit Commission to oversee BNPL providers alongside other previously unregulated credit activities.

In Germany, the Federal Government approved legislation proposed by the Ministry of Justice and Consumer Protection to transpose the EU Consumer Credit Directive into national law, extending consumer credit protections to BNPL models and interest-free loans for the first time. The law requires mandatory creditworthiness assessments before contract conclusion, aligned with real estate loan standards, while eliminating the written form requirement for general consumer credit contracts to enable digital and online completion.

Finfluencer activity

Following the significant global push against finfluencers witnessed during Q2 including the "Global Week of Action Against Unlawful Finfluencers," a coordinated initiative during early June by nine regulators, and the release IOSCO's final report on finfluencers, Q3 saw further targeted activities.

The Monetary Authority of Singapore published the Guidelines on Standards of Conduct for Digital Advertising Activities that establish expectations for responsible digital advertising practices by financial institutions and their appointed third parties, including online content creators. As part of this, the MAS has developed a practical guide titled "7 must-knows when sharing financial information online" that clarifies key regulatory considerations for content creators, including circumstances requiring MAS licensing for providing financial advice or dealing in capital markets products, verification procedures for legitimate financial institutions, and disclosure requirements for sponsored content.

Likewise, the UK Financial Conduct Authority opened a consultation in July after the government legislated to bring third-party BNPL lenders inside the FCA's perimeter from July 2026. Building on the Consumer Duty, the FCA proposes proportionate creditworthiness assessments, clearer pre-contract and ongoing disclosures, tailored borrower support, and capped late fees. Meanwhile, the Dutch AFM highlighted ongoing risks in BNPL growth, emphasizing concerns over inadequate credit checks and supporting stricter regulatory thresholds for mandatory creditworthiness evaluations ahead of its November 2026 supervisory takeover.

The Canadian Investment Regulatory Organization (CIRO) released a qualitative research report highlighting how personal relationships and online networks shape the experiences of new do-it-yourself (DIY) investors. Drawing on 45 in-depth interviews with new and seasoned DIY investors as well as financial content creators, the study confirmed that social media plays a key role for both information and validation with investors frequently using platforms like YouTube and Reddit to learn basic concepts, discover new opportunities, and cross-check recommendations.

Finally, active enforcement of illegitimate finfluencer activity also remained a priority. At the end of September, the Alberta Securities Commission imposed sanctions on a finfluencer after finding that his posts on platforms such as YouTube and X failed to disclose affiliations with four Alberta issuers as mandated and that he lacked formal education in finance despite presenting himself as knowledgeable in the field.

Redress and Complaints Management

Q3 also saw substantive focus on modernizing consumer redress and complaint handling. In the UK, the FCA and the Financial Ombudsman Service proposed reforms to prevent backlogs and give firms greater predictability by improving coordination through a transparent referral process and a lead-complaint mechanism for novel issues, setting clearer expectations for early reporting and wider implication triggers, and requiring better prepared cases before investigations begin. A parallel government consultation would adapt the “fair and reasonable” test so outcomes align with FCA standards where rules are material, create tools to pause handling to manage mass redress events, introduce an absolute ten-year time limit for bringing cases to the Ombudsman with limited exceptions, and allow firms and consumers to seek a FCA view before a final decision.

In Canada, the CSA advanced a framework to give the Ombudsman for Banking Services and Investments binding authority, paired with a new oversight model that uses designation orders and a multijurisdictional memorandum of understanding to balance independence with accountability. The refined two-stage process would require external decision makers at the review stage when a recommendation of CAD 75,000 or more is contested. Separately, the Financial

Consumer Agency of Canada (FCAC) reported gaps at small and mid-sized banks in defining and recording complaints, meeting the statutory 56-day resolution clock, producing complete quarterly reports, and issuing substantive written responses.

Meanwhile in New Zealand, the Financial Markets Authority (FMA) has urged companies to enhance their processes for handling customer complaints. Research conducted by the FMA revealed that less than one-third of individuals feel confident about how to lodge complaints against their financial service providers. Many potential complainants are deterred by perceived barriers such as uncertainty about the outcome and the complexity of the process

Reinforcing this shift toward transparent and timely redress, Australia’s ASIC confirmed it will publish public dashboards for internal dispute resolution, proceeding with publication of internal dispute resolution data at the firm level. The dashboards, which will include privacy safeguards, clearer comparisons and explanatory context, are intended to enhance accountability and complement the Australian Financial Complaints Authority’s firm level external dispute resolution data..

Sales and Culture

During Q3, several authorities signalled renewed focus on sales culture. In Australia, ASIC concluded its review of direct sales of life insurance and, in a letter to CEOs called on life insurers and distributors to strengthen product design and monitoring, using complaints, claims and cancellation data, link remuneration and performance to compliance and customer outcomes rather than volume, extend quality assurance to all sales and retention calls, streamline cancellation processes, and improve oversight of emerging compliance technology. ASIC acknowledged some progress, including lower lapse rates and wider use of call monitoring, but highlighted rising claims disputes and uneven governance. Separately, ASIC issued a consumer alert on pushy superannuation switching, warning about high-pressure tactics, cold calls, free offers to find and consolidate lost super, limited disclosure and unlicensed advice, and launched a campaign aimed at consumers targeted by comparison pitches.

In Canada, the OSC and CICO published survey findings from 2,863 mutual fund dealing representatives in bank branches that point to persistent sales pressure and conflicts. Twenty five percent of respondents said clients are sometimes recommended products that are not in their interests while sixty eight percent reported experiencing sales pressure at least sometimes, with the widespread use of performance scorecards viewed as increasing pressure and shaping recommendations. The review also found knowledge gaps, including weak understanding of management expense ratios and reports that clients sometimes receive incorrect information. The authorities have moved to a second phase to obtain firm level data on compensation, incentives and controls and to determine whether further action is needed to ensure client interests come first

Scams and fraud

The quarter also featured a continued intensification of global efforts to counter scams and fraud, with authorities expanding their toolkits across prevention, detection, and disruption. Initiatives ranged from national education campaigns and cross-sector alliances to the rollout of AI-powered fraud detection and collaborative platforms for intelligence sharing.

Alongside these initiatives, authorities also continued to invest in governance structures supporting anti-scam and fraud measures. In Hong Kong, the Monetary Authority (HKMA), Securities and Futures Commission (SFC), Insurance Authority (IA), and Mandatory Provident Fund Schemes Authority (MPFA) jointly launched the Anti-Scam Consumer Protection Charter 3.0, collaborating with major technology and telecom firms. Charter 3.0 introduces six principles targeting improved financial scam reporting, advertiser verification, internal monitoring of financial content, robust enforcement of platform terms, and increased public education. In New Zealand, the Ministry of Business, Innovation and Employment (MBIE) established the cross-sector Anti-Scam Alliance, bringing together government agencies, banks, telecoms, digital platforms, and consumer groups. The Alliance will enhance intelligence sharing, create a national anti-scam strategy, update industry codes, and promote public awareness.

Prevention

India's SEBI launched an investor awareness campaign on All India Radio specifically targeting stock trading frauds on social media platforms, with broadcasts across 234 stations nationwide

Colombia's Financial Superintendency launched the "¡Alerta! Ofertas Fraudales" microsite providing information on different types of scams and self-assessment tools for citizens

Canada has formed a coalition involving the government, law enforcement and major financial, telecom, and tech firms to form the Canadian Anti-Scam Coalition (CASC), launching a nationwide scam education campaign

Detection

South Korea's FSC announced plans for an anti-vishing AI platform to gather suspicious account data across financial sectors and enable instant information sharing and AI-based pattern analysis for preventive blocking

Swift and 13 international banks demonstrated AI-powered fraud detection doubling real-time fraud identification rates using privacy-enhancing technologies and federated learning on 10 million test transactions

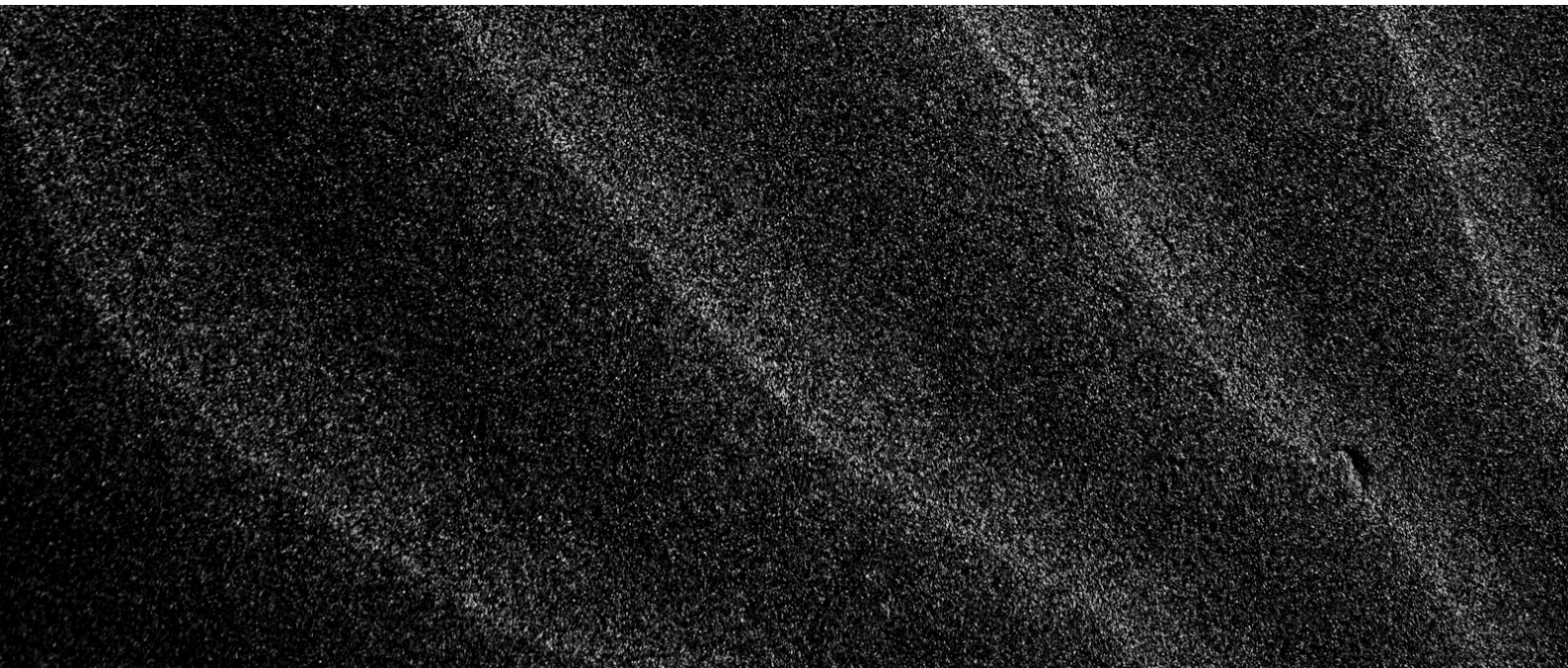
Hungary's National Bank launched the initial phase of its new Central Fraud Detection System, which leverages AI to identify fraudulent activities involving bank transfers and is part of a broader set of anti-cyber fraud measures

Disruption

Australia's ASIC expanded its investment scam takedown capability to include social media ads, removing over 14,000 scam websites in two years and averaging 130 malicious site takedowns weekly

Singapore implemented multiple restrictions for scam mules limiting access to banking services, mobile line subscriptions, and Singpass/Corppass services for individuals involved in mule-related offenses

Indonesia's OJK - in collaboration with 21 government agencies - established the Indonesia Anti-Scam Center which processed 225,281 reports and blocked 72,145 accounts holding IDR 349.3 billion



ARTIFICIAL INTELLIGENCE

AI continued to command policy and supervisory attention during Q3. Continuing from the first half of the year, authorities continued to focus on market engagement and responsible innovation via sandbox environment and other capacity building programs. New legislative proposals and supervisory guidance further shaped expectations regarding AI oversight and explainability.

Market development initiatives

Initiatives to facilitate responsible adoption of AI and support capacity building remained a focal point, too, in Q3. In August, the Hong Kong Insurance Authority launched the AI Cohort Programme. Comprising an inaugural group of seven insurers, the Cohort commits to establishing an AI Centre of Excellence in Hong Kong to serve as a regional hub for AI innovation, supporting AI talent development through capability-building initiatives; and contributing to knowledge sharing with the industry and regulators. In the UK, the Financial Conduct Authority (FCA) concluded the feedback phase to its April 2025 engagement paper proposing AI Live Testing. Respondents welcomed the initiative as a constructive mechanism for understanding AI model performance under real-world conditions. The FCA has commenced the first cohort of AI Live Testing, planning to work with approximately 5-10 participating firms starting in October. The initiative forms part of the FCA's broader AI Lab, which comprises five components.

Spotlight: The UK FCA's Five Pillar AI Lab Approach

Supercharged Sandbox	AI Live Testing	AI Spotlight	AI Sprint	AI Input Zone
Collaboration with Nvidia offering firms access to accelerated computing, enhanced datasets and more advanced tooling / AI enterprise software	Dedicated program allowing successful applicants to test AI systems in real-world conditions, with regulatory support and oversight	Space for showcasing real-world insight and practical understanding into how firms are experimenting with AI in financial services	Dedicated event held in January 2025, convening a diverse set of stakeholders inform our regulatory approach to AI and support innovation	Survey on the future of AI in UK financial services including promising and impactful use cases held during Q4 2024 / Q1 2025

In the United States, House Financial Services Committee Chairman French Hill introduced H.R. 4801 at the end of July 2025, a bipartisan bill for the establishment of AI Innovation Labs. The bill would require every federal financial to operate an AI Innovation Lab, which functions as a supervised sandbox for time-limited AI test projects by regulated firms. Firms would be required to apply with a description of the AI use case and a detailed compliance strategy, specifying how risks will be managed, and why the approach serves the public interest, improves efficiency or compliance, and poses no systemic, AML/CFT, or national-security risk.

Policy initiatives

In addition to market development activities, a marked concentration in policy development by standard setting bodies from the insurance and actuarial domain was visible in Q3. In July, the IAIS published an Application Paper on the Supervision of AI that explains how existing Insurance Core Principles apply to AI systems and sets out a risk-based, proportionate supervisory approach, providing practical guidance on governance and accountability, robustness and security, transparency and explainability, and fairness, ethics and redress, illustrated with jurisdictional case studies.

In August, the EIOPA released its Opinion on AI Governance and Risk Management, clarifying how existing Union insurance legislation should be applied to AI systems that fall outside the AI Act's high-risk perimeter and setting supervisory expectations for proportional risk assessment, data governance, human oversight and third-party controls across the insurance value chain. In parallel the International Actuarial Association also released three draft papers for consultation —the AI Governance Framework, Testing of AI Models and Documentation of AI Models—which together propose a comprehensive actuarial control cycle for AI.

Spotlight: Addressing AI Explainability Challenges

As part of broader work to advance AI policy and the operationalization of a suitable supervision regime, explainability moved into focus during the quarter. Notably, the BIS Financial Stability Institute has published an Occasional Paper examining how regulators can address explainability challenges arising from financial institutions' increasing adoption of artificial intelligence models, particularly in critical business applications. The paper examines the tension between the high performance yet low explainability of advanced AI models and evaluates existing model risk management frameworks and outlines several recommendations to overcome identified challenges.

Challenges to AI explainability

Advanced AI models—particularly deep neural networks and large language models (LLMs)—are inherently difficult to explain. Their predictions stem from complex, non-linear architectures with vast numbers of parameters, trained on opaque datasets and driven by probabilistic token generation. Although post-hoc tools such as SHAP, LIME, and counterfactual explanations exist, they face well-documented limitations. These include inaccuracy, instability under minor input variations, poor generalizability, lack of verifiable ground truths, and vulnerability to manipulation that can produce plausible yet misleading outputs.

These technical limitations clash with supervisory demands. Explainability expectations vary across audiences, including boards, supervisors, and customers, but most regulatory frameworks do not differentiate accordingly. Adaptive or self-learning models blur the line between ordinary operations and model changes, complicating approvals and monitoring. Proprietary or third-party systems often restrict access to internal mechanics, limiting independent validation and forcing reliance on sensitivity analysis or benchmarking. For generative AI, the challenges are even greater: benchmarks are immature, fairness and explainability techniques remain underdeveloped, and many use cases lack definitive ground truths.

Current model risk management (MRM) provisions such as governance, documentation, validation, monitoring, and independent review were originally designed for more transparent models. When strictly applied to modern AI, they are difficult to satisfy, especially in high-impact or capital-related contexts.

Potential Adjustments to MRM Frameworks

The authors recommend updating MRM frameworks. Supervisors should require firms to set explainability standards tailored to each use case and scaled by risk and materiality. In high-impact applications, inherently interpretable models should be preferred. Where complex models are used, firms should apply multiple complementary explanation methods, document assumptions and limitations, and ensure explanations are suitable for different audiences.

Model selection should be evidence-based. Firms should justify added complexity over simpler alternatives and demonstrate consistent performance improvements across diverse scenarios. Where trade-offs between performance and explainability are accepted, model use should be conditional on the implementation of safeguards that mitigate associated risks. These may include regular stability and repeatability testing, outcome monitoring with defined performance thresholds, enhanced data governance, human oversight, and mitigations such as fine-tuning or retrieval-augmented generation. Circuit breakers should be in place to deactivate models rapidly if performance degrades.

Supervisors should define what counts as a material change in adaptive AI models, set proportionate validation expectations for third-party tools, and make clear that firms remain accountable. Where AI outputs materially affect individuals, firms should provide accessible explanations and offer recourse. For regulatory capital use authorities could limit their scope to specific risk categories or apply stricter input/output floors to retain the benefits of high-performing models while managing risks.

Concurrently with the paper, the BIS Innovation Hub also launched Project Noor. A collaboration between the BIS Innovation Hub Hong Kong Centre, the Hong Kong Monetary Authority and the Financial Conduct Authority, Project Noor seeks to equip financial supervisors with tools to independently evaluate the transparency, fairness, and robustness of AI models used by financial institutions. It will involve prototyping of explainable AI (XAI) techniques combined with privacy preserving techniques to translate complex model logic into plain language and intuitive visuals, thereby offering insight into the factors that have influenced a decision and the decision's sensitivity to change factors.

DIGITAL ASSETS & TOKENIZATION

The momentum in digital assets that has built up since the start of 2025 further persisted with significant efforts in advancing policy and supervisory frameworks visible across geographies. While stablecoins remained a focal point across the board, policy priorities at the national level were largely shaped by local agendas and the degree of maturity of existing regulatory frameworks.

Asia-Pacific

Across Asia-Pacific, policy priorities concentrated among other things on cyber-resilience, custody and governance, as well as AML/CFT controls. The Hong Kong's Securities and Futures Commission issued binding guidance to licensed trading platforms for the safeguarding of client digital asset following identified cyber-resilience lapses, while Indonesia's Financial Services Authority published expansive cybersecurity standards promoting zero-trust architecture and enhanced incident response requirements. Malaysia's Securities Commission also consulted on new safeguards for licensed exchanges, including strengthened cold storage, governance, and listing processes.

In Australia, AUSTRA introduced conditions on cryptocurrency ATM providers to mitigate money laundering, terrorism financing, and other illicit financial activities after a dedicated cryptocurrency taskforce identified instances of non-compliance with relevant measures. Under the newly imposed conditions, providers must cap cash deposits and withdrawals at AUD 5,000, strengthen customer due diligence procedures, and display mandatory scam warnings on their terminals.

Separately, the Hong Kong Monetary Authority finalized and activated its new licensing regime for stablecoin issuers, effective since August 1, with the release of the final Guideline on Supervision of Licensed Stablecoin Issuers, the companion Guideline on Anti-Money Laundering and Counter-Financing of Terrorism, as well as two explanatory notes covering the licensing process and transitional arrangements for pre-existing issuers.

Meanwhile, other Asian counterparts focused on perimeter management: The Reserve Bank of Fiji announced that, with effect from 30 August 2025, the provision of virtual asset services in Fiji is illegal and considered a criminal offence. In contrast, the Central Bank of the Philippines announced the indefinite extension of the moratorium on the issuance of new licences to virtual asset service providers with effect from September 1.

Europe

In Europe, ESMA further advanced the operationalization of MiCAR with the release of the finalised guidelines on the knowledge and competence of staff at crypto-asset service providers who provide information or advice, setting minimum thresholds for qualifications and experience. In parallel, the EU's new anti-money laundering authority, AMLA, explicitly signalled that with the inception of its supervisory powers on 1 July 2025 it will place particular focus on compliance of crypto-asset service providers with AML/CFT controls. Meanwhile,

In the UK, Q3 2025 saw the Financial Conduct Authority launch the consultation, setting out how existing FCA Handbook standards will apply once new legislation brings specified crypto-asset activities into scope. The paper proposes applying high-level standards and cross-cutting rules such as the Principles for Businesses, SYSC, conduct of business, product governance, operational resilience, complaints handling and access to the Financial Ombudsman Service to firms conducting activities including qualifying stablecoin issuance, custody, operating trading platforms, intermediation and staking.

In Switzerland's FINMA issued guidance clarifying the appropriate financial statement disclosure of crypto-based assets under the DLT Act, phasing out older fiduciary treatment in favour of updated custody classifications and new supervisory reporting channels.

Middle East

In the Middle, the Abu Dhabi Global Market's Financial Services Regulatory Authority (FSRA) has efforts underway to further refine its established digital assets regime with two new consultations in September. This includes a consultation on the regulatory framework fiat-referenced tokens (FRT). Building upon December 2024 amendments that introduced FRT issuance as a standalone regulated activity, the proposals seek to address remaining gaps in the regulatory treatment of FRTs and align with emerging business models in this space. Under the proposed framework, foreign-issued FRTs would be assessed based on criteria including adequate reserves, traceability, issuer jurisdiction and regulatory framework, while domestic ADGM-issued FRTs would be automatically accepted for use. The framework expands the scope of the Regulated Activity of Providing Custody to include FRTs alongside virtual assets and additionally introduces FRT Intermediation as a new activity under Providing Money Services to capture firms that buy and sell FRTs as a standalone business. The second consultation addresses the staking of virtual assets and sets out a tailored perimeter and obligations for Authorised Persons, such as virtual asset custodians and virtual asset managers, who engage in staking using clients' virtual assets under proof-of-stake protocols. It clarifies permissible activities, differentiating staking from other yield-generating mechanisms and proposes due diligence, disclosure, client reporting, and notification requirements.

In Qatar, the Qatar Financial Centre in early September announced plans for a blockchain-based proof of concept for Islamic finance under its Digital Assets Lab. The proof of concept is intended to demonstrate a blockchain-based digital receipt system, designed to improve transparency, efficiency, and regulatory compliance in Shariah-compliant asset-backed finance.

North America

Mid-July marked a critical milestone with the new Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act being signed into law by the President while the House of Representatives approved the bipartisan Digital Asset Market Clarity (CLARITY) Act, laying the groundwork for the much-demanded regulatory certainty. Complementary to this, the President's Working Group on Digital Asset Markets released a roadmap outlining recommendations for the further evolution of the regulatory framework and the ecosystem build-out at large. Federal authorities built on the momentum with a series of targeted measures. The Commodity Futures Trading Commission (CFTC), among other things, opened a "crypto sprint", debuting consultations on listing spot crypto-asset contracts on designated contract markets and seeking stakeholder input on leverage and margin rules, while simultaneously piloting the acceptance of tokenised collateral (including stablecoins) for derivatives margin to improve capital efficiency. To reinforce this trajectory, staff of the SEC and CFTC also issued joint guidance confirming that regulated venues may already facilitate trading in certain spot crypto products, provided robust surveillance, clearing and transparency arrangements are observed. The SEC on its part, also continued further to delineate the perimeter of permissible activities: a Corporation Finance statement concluded that narrowly defined "liquid staking" arrangements and associated receipt tokens do not, in themselves, constitute securities, and Commission orders authorised in-kind creation and redemption for bitcoin- and ether-based ETPs in digital-asset markets. Separately, The Federal Deposit Insurance Corporation (FDIC), Federal Reserve Board (FRB), and Office of the Comptroller of the Currency (OCC) have jointly issued a statement clarifying how existing risk-management and compliance principles apply when banking organizations provide safekeeping for crypto-assets

Caribbean

In Bermuda and the Cayman Islands – both markets with established and recognized digital asset regimes and a sizeable pool of licensed entities – the emphasis during the quarter has been on refining licensing procedures and clarifying supervisory expectations. The Bermuda Monetary Authority (BMA) issued a comprehensive Guidance Note detailing its expectations for entities applying for licenses under the Digital Asset Business Act, particularly emphasizing corporate governance and second- and third-line control frameworks, alongside specific requirements tailored to various business models. The Guidance explicitly addresses proportionality considerations based on license types and the nature, scale, and complexity of regulated entities. Moreover, the Authority a dedicated thematic review for the digital asset business sector as an information gathering exercise to identify key patterns, trends and areas of emerging risk across the industry.

The Cayman Islands Monetary Authority, through a dedicated Supervisory Circular, reiterated its compliance expectations for virtual asset service providers regarding anti-money laundering and countering financing of terrorism and as part of that also highlighted key findings from recent on-site inspections and desk-based reviews, pointing to identified deficiencies in customer risk assessments, oversight of technological solutions, customer due diligence - especially concerning politically exposed persons - sanctions screening procedures, and board-level oversight of compliance functions.

Persistent concerns

These efforts notwithstanding, authorities have continued to maintain a cautious position and voiced concerns over observed market behaviours and developments. In September, French AMF, Austrian FMA, and Italy's CONSOB have jointly proposed targeted improvements to strengthen the MiCAR framework following challenges identified during its initial months of implementation, highlighting significant differences in supervisory approaches across national jurisdictions and inadequate protections against sector-specific risks, particularly regarding European intermediaries' access to third-country platforms operating without MiCA protections. Their four key proposals include (1) transferring direct supervisory powers over significant crypto-asset service providers to ESMA to prevent regulatory arbitrage, (2) mandatory requirements for European intermediaries to execute orders only on MiCA-compliant platforms, (3) implementation of independent cybersecurity audits, and (4) the establishment of a centralized one-stop shop for token offerings - measures aimed at addressing the concentration of 90% of crypto trading on ten global platforms seeking to leverage European passporting from single member states.

Echoing similar concerns, Dutch Financial Markets Authority Chair Laura van Geest in an interview stressed that although the European Union's Markets in Crypto Assets Regulation introduced mandatory licensing, the current regime remains insufficient, emphasizing that crypto assets have no underlying value and that minimal information and distribution requirements leave consumers vulnerable to impulsive trading and market manipulation.

In addition to these structural concerns, authorities across have also further intensified warnings including over continued concerns over unregulated activities. The Hong Kong Monetary Authority and Securities and Futures Commission issued a joint statement in mid-August addressing market movements linked to stablecoin announcements and social media speculation and raising the risk of potentially manipulative practices.

ESMA in a statement in July, cautioned investors about the potential 'halo effect' where association with regulated entities may cause investors to overlook risks from unregulated products offered by regulated crypto-asset service providers while Slovenia's Securities Market Agency warned explicitly against aggressive cryptocurrency marketing that highlights quick profit opportunities without adequately disclosing risks. At the global level, the World Federation of Exchanges called for regulatory action against tokenization of equities by unregulated brokers and crypto platforms over significant investor risks.

PAYMENTS

Q3 2025 saw continued acceleration in payment system modernisation, with sustained momentum around instant payment infrastructure, regulatory consolidation, and regional connectivity. Alongside this, CBDC experimentation and policy articulation progressed steadily across jurisdictions with several key milestones reach.

Expansion of Instant and Digital Payment Systems

Q3 saw the continued expansion of instant and digital payment infrastructure. In the EU, the Instant Payments Regulation progressed, requiring all euro credit transfer providers to support 24/7 SEPA Instant payments with 10-second settlement at no extra cost. The European Central Bank also introduced new requirements on cyber risk, outsourcing, and governance for major euro payment systems. In Canada, Payments Canada completed the Real-Time Rail technical build and began full system testing. A public consultation on the associated legal framework showed strong support for centralized fraud prevention and called for clearer rules on finality and irrevocability. Emerging markets also progressed on various fronts. In August, Barbados launched its national instant payment system initiative BimPay, targeting a March 2026 roll-out. The new system will enable payments between individuals, businesses, and Government on a 24/7/365 basis and will be designed to be fully interoperable. Meanwhile, Iraq enabled wallet-to-wallet and wallet-to-merchant remittances widening access to low-cost digital remittances, while Saudi Arabia's central Bank launched a new e-commerce payments interface that links the national "mada" debit network with global card networks and supports payment card tokenization.

Regulatory Oversight

Several jurisdictions also evolved their regulatory oversight structures during quarter. In Canada, the Bank of Canada on September 8 began supervising nearly 1,500 payment service providers for compliance with requirements for managing risks and safeguarding end-user funds under the Retail Payment Activities Act. Canada's Department retains responsibility for coordinating the national security screening of the applicants.

In the UK, HM Treasury opened a consultation on merging the Payment Systems Regulator (PSR) into the Financial Conduct Authority (FCA) following its March decision to dissolve the PSR. The objective is to streamline oversight under the FCA while maintaining the designation regime and applying the FCA's strategic and competition mandates to payments. This aligns with the UK's broader payments transformation. In July, authorities also confirmed a new delivery model under the National Payments Vision whereby public authorities set strategy, a new industry Delivery Company leads procurement and development, and Pay.UK continues to operate existing rails. This reset is intended to supports the UK's next-generation retail infrastructure and support coordination between public and private stakeholders.

Cross-Border and Regional Payment Connectivity

Cross-border payment integration continued to gain traction, most notably across Asia and Africa. Indonesia and Japan launched QR payment interoperability, enabling Indonesian users to pay Japanese merchants in local currency via domestic apps. Indonesia, Malaysia, and Thailand also expanded their Local Currency Transaction Framework by appointing more cross-currency dealers, enhancing MYR-IDR-THB trade liquidity. Africa advanced regional integration with the launch of PAPSS's African Currency Marketplace, enabling direct local currency FX transactions and reducing reliance on hard currencies and correspondent banks.

Cash Preservation and Digital Inclusion

Preserving access to cash remained a focal point, too. In Australia, the Council of Financial Regulators and the Competition and Consumer Commission (ACCC) consulted on a national cash distribution framework, addressing declining usage while ensuring access for vulnerable groups and resilience during outages. The Reserve Bank of New Zealand on its part launched its annual cash use survey to track trends and guide long-term redesign of the cash system. In the UK, the Parliament noted that the Bank of England will track cash acceptance as part of its consumer survey, allowing the Government to monitor cash acceptance levels as a precautionary measure as cash acceptance is presently not mandated by law. In Austria, the National Bank announced a collaborative initiative with the Austrian Association of Municipalities to install up to 120 new cash dispensers in rural areas with insufficient access to cash services to ensure cash availability, particularly in regions lacking bank branches or existing cash machines.

Spotlight: Key CBDC Developments

Q3 saw continued solid progress across national Central Bank Digital Currency (CBDC) projects in both developed and developing markets. In parallel to the national developments, the Bank for International Settlements (BIS) also published its 2024 survey on CBDC adoption. Drawing on responses from responses from 93 central banks, the survey reveals that while 91% of the 93 surveyed central banks remain engaged in CBDC exploration, actual implementation remains limited with only three live retail CBDCs (Bahamas, Jamaica, Nigeria) and no launch of a wholesale CBDC to date.

The data furthermore shows that wholesale CBDC projects have progressed to more advanced stages than retail CBDCs globally, with 38% of advanced economy central banks running wholesale pilots compared to 15% for retail, while emerging market economies show greater divergence by increasingly focusing on either retail or wholesale rather than pursuing both simultaneously. Central banks cite preserving the role of central bank money amid declining cash use alongside rising asset tokenization as a primary motivation, with cross-border payment efficiency driving wholesale CBDC development and domestic payment improvements motivating retail CBDC work.

AUSTRALIA

In July 2025, the Reserve Bank of Australia and Digital Finance Cooperative Research Centre announced the selection of 24 use cases for Project Acacia's next phase. These use cases will involve real money and asset transactions as well as proof-of-concept simulations across asset classes such as fixed income, private markets, trade receivables, and carbon credits. Settlement assets will include stablecoins, bank deposit tokens, and pilot wholesale CBDC. ASIC is providing regulatory relief to facilitate the testing. Testing will occur over a six-month period, with findings expected in early 2026.

TÜRKİYE

In September, the Central Bank of the Republic of Türkiye invited private sector participation in its Digital Turkish Lira Project ecosystem, enabling banks, payment institutions, and electronic money institutions to propose innovative use cases for testing in the sandbox. Building upon first phase findings, the second phase specifically targets advanced use cases such as tokenization, programmable payments, user-controlled digital identity, interoperability with existing systems, and machine-to-machine payments. A second phase progress report is planned to be released later in the year.

UNITED STATES

The House of Representatives passed the "Anti-CBDC Surveillance State Act" in mid-July, prohibiting Federal Reserve banks from issuing a CBDC either directly or indirectly through intermediaries. The legislation also bars the Federal Reserve Board and Federal Open Market Committee from testing, studying, developing, or implementing a CBDC or using one for monetary policy.

EUROPE

The European Union marked a major milestone in September with the release of findings from its digital euro innovation platform's first iteration, which engaged ~70 market participants from February to May 2025. The initiative operated through two complementary workstreams: visionaries explored conceptual applications while pioneers conducted technical testing in a simulated digital euro environment. Based on the work, conditional payments - transactions that trigger automatically when predefined conditions are met - as a key innovation driver that could transform payment experiences across multiple sectors.

UNITED ARAB EMIRATES

The Central Bank of the UAE released a policy paper detailing the strategic vision, architecture, and phased implementation of its Digital Dirham. It confirmed retail and wholesale tokens will be direct liabilities of the central bank via a two-tier, wallet-based system managed by licensed financial institutions. A bespoke distributed-ledger platform has already been integrated with the reserve banking system, enabling automated issuance, redemption and transfers. Additionally, a retail pilot has inter alia tested fractionalized asset settlement, tourist wallets with instant VAT refunds and programmable social-benefit payments.

UNITED KINGDOM

The Bank of England has published a design note outlining its product strategy for a potential digital pound, proposing a phased rollout beginning with an 'Initial stage' featuring peer-to-peer payments via aliases, online merchant acceptance, and instant settlement. More complex functionalities including point-of-sale integration and conditional payments would follow in a 'Near stage'. A separately released design note addressed interoperability models within the public-private framework whereby the Bank would operate core infrastructure while regulated intermediaries would deliver retail services.

BAHAMAS

At the September 2025 CB+DC Conference, the Central Bank of The Bahamas reported that it is building a fast payments platform fully interoperable with the SandDollar, mandating direct participation by all retail domestic payment providers and bringing the Government on as a participant, with minimal additional technical work expected for providers already on the SandDollar.

CLIMATE & ESG

Climate and broader sustainability policy advanced across multiple fronts in the quarter. At the global level, the Financial Stability Board (FSB) released the 2025 update of its Roadmap for Addressing Financial Risks from Climate Change – the latest update since 2023 – as part of its reporting to the G20 Finance Ministers and Central Bank Governors, highlighting the major completed actions since 2024 and outlining planned work under the four pillars of the roadmap.

Within the context of the G20's Sustainable Finance Working Group, the NGFS also doubled down on transition planning with two new notes. The first note, "Climate Target Setting and Transition Plans" provides guidance on how financial institutions can establish robust climate-related targets within their transition plans in alignment with business strategies and risk management frameworks while the second note, "Interactions Between Climate Scenario Analysis and Transition Plans," examines the synergies between climate scenario analysis and transition planning. Separately, the IAIS, in collaboration with the World Bank Group, shared a paper with the Working Group with focus on natural catastrophe (NatCat) protection gaps. The paper highlights the global challenge posed by NatCat protection gaps and addresses the increasing frequency and severity of NatCat events, such as hurricanes and floods, and the unsustainable economic and social toll they impose.

Spotlight: FSB's Planned work under the Roadmap for Addressing Financial Risks from Climate Change¹

Block 1: Disclosures

- ISSB prioritisation of IFRS S1/S2 implementation support including education, TIG and capacity building
- Transition-plan disclosure guidance with IOSCO review and GEMs capacity-building network

Block 2: Data

- IMF pilot to evaluate availability and collection of granular climate-related financial data for ~50 economies
- Continued work to close cross-jurisdiction and sector data gaps that hinder forward-looking climate risk metrics

Block 3: Vulnerabilities analysis

- FSB development of forward-looking metrics and analyses on physical risk and insurance protection gaps
- IMF enhancement of climate-risk methodologies in surveillance with a 2025 update

Block 4: Regulatory and supervisory practices and tools

- Scaled capacity building via BIS FSI, IAIS EMDE support, IMF FSAP training and World Bank guidance
- Stronger focus on adaptation and protection gaps including BCBS extreme-weather work

Spotlight: Progressing EU Simplification Efforts

During the quarter, the EU advanced the Omnibus I simplification agenda in several areas. In early July, the European Commission adopted a delegated act to streamline application of the EU Taxonomy, reducing administrative burden while preserving core environmental objectives, with changes set to apply from 1 January 2026. In parallel, the Commission adopted a targeted "quick fix" to the first set of European Sustainability Reporting Standards (ESRS) to extend phase-ins and ease selected disclosures for early reporters under the CSRD, providing immediate relief for wave 1 companies. EFRAG complemented this with a 60-day consultation at the end of July on revised ESRS that propose material

simplifications, including a reduction of mandatory datapoints by 57 percent and an overall reduction of total disclosures by 68 percent.

Subsequently, at the end of September, the European Council formally adopted a regulation to simplify and strengthen the Carbon Border Adjustment Mechanism as part of Omnibus I. The measure introduces a de minimis mass threshold that eases entry-level compliance for smaller import flows. According to the Council, the new threshold will exempt 90% of importers from CBAM while still covering 99% of CO2 emissions from iron, steel, aluminium and cement imports.

¹ Not exhaustive

Standard setters and authorities also continued to translate transition risk into macro-prudential and central bank toolkits. The Network for Greening the Financial System (NGFS) published an occasional paper examining the macroeconomic implications of carbon-intensive energy price changes through a dedicated model comparison exercise. The ECB announced the embedding of a new “climate factor” in the Eurosystem’s collateral framework to shield its refinancing operations from losses that could arise if climate-related transition shocks erode the market value of pledged assets.

Beyond these developments, policy efforts at the regional and national level progressed on broadly three fronts:

Taxonomy development

Malaysia, through its Joint Committee on Climate Change, advanced on a unified Malaysian Taxonomy aligned with the ASEAN Taxonomy. In parallel, Hong Kong consulted on Phase 2A of its sustainable finance taxonomy, expanding sector coverage to manufacturing and information and communications technology, increasing the number of defined activities and embedding transition features such as interim targets, sunset dates and a new objective on climate change adaptation

Disclosures and Assurance

In Australia, ASIC published a set of FAQs that interpret new Corporations Act 2001 provisions requiring sustainability report to be subject to assurance. The FAQs specify auditor eligibility

and sets out independence, rotation, appointment, removal and resignation rules. They also confirm limited assurance during the phase-in with full audits from July 2030.

In South Africa, Financial Sector Conduct Authority entered a cooperation programme with the International Finance Corporation to craft a national roadmap for ISSB adoption, develop ISSB-aligned regulations, and produce implementation tools for boards and train supervisors. Within Europe, EBA issued a no-action letter to provide clarity on the application of ESG Pillar 3 disclosures during the ongoing review.

Product integrity and claims

A third strand focused on product integrity and claims. The EBA opened consultation on revisions to its product oversight and governance guidelines for retail banking products to integrate ESG features, strengthen target-market and distribution expectations and require processes that detect and manage greenwashing across the product life cycle. ESMA complemented this with practical guidance setting out four principles for sustainability-related claims in non-regulatory communications, with practical examples focused on the use of ESG credentials such as labels and awards, to support clear, fair and not misleading claims.

Outside the EU, the Bermuda Monetary Authority proposed enhanced fund-level sustainability disclosures and restrictions on misleading fund names, including substantiation of objectives, strategies and benchmarks, with a transitional period to embed the new standards.

Spotlight: New Insights from Supervisory Work

Authorities and standard setters across several geographies also deepened their understanding of the maturity of implemented measures through targeted supervisory reviews. Findings highlight continued deficiencies in several areas:

Strong variations in the incorporation of climate-change risks into insurers’ Own Risk and Solvency Assessment (ORSA)

EIOPA highlights significant divergences in materiality assessments and modelling approaches across jurisdictions, as well as persistent data shortages that often require insurers to rely on simplified or qualitative techniques. It also points to widespread difficulty in extending scenario analysis beyond standard ORSA time horizons due to the gaps and modelling uncertainties.

Capacity, data gaps and methodological limits weakening the decision usefulness of climate-risk scenario assessments

OSFI and AMF’s 2024-25 standardized climate scenario exercise found constrained baseline capacity across many institutions, limited geocoding and hazard mapping, poor flood-insurance and adaptation tracking, and scarce counterparty/property emissions and energy data, weakening physical and transition assessments. Methodological limits further reduce decision usefulness as top-down scenarios and static balance assumptions obscure institution specific vulnerabilities and second order effects.

Deficient identification, specificity and evidencing in climate-related disclosures

Within the context of its 2025 climate-related disclosure review, the New Zealand FMA identified that many climate statements lack entity-specific, decision-useful disclosure: risk and opportunity identification and assessment are often incomplete or non-specific, materiality is blurred by long lists (including immaterial or industry-irrelevant items), time horizons are omitted, and scoring or colour-codes are provided without explaining criteria.

SUPTECH

GENERAL DEVELOPMENTS

During the quarter, authorities have continued advancing their digital agenda through a diverse set of SupTech initiatives. In the United States, the CFTC announced the implementation of Nasdaq's market surveillance platform to strengthen its market surveillance and fraud detection capabilities. The SEC launched a dedicated new AI task force, led by the newly appointed Chief AI Officer Valerie Szczepanik, to drive agency-wide adoption of AI tools and systems. Separately, it also rolled out a new interactive statistics and data visualizations webpage that consolidates time-series charts, pie charts, and geographic heat maps on key capital market indicators. In Europe, the Single Supervisory Mechanism in late September held its annual Banking Supervision Innovators Conference, showcasing a broad portfolio of tools – including generative AI powered solutions – to support activities such as the development of briefing notes, fit and proper assessments, bank-supervisor interactions such as during stress testing exercises as well as facilitate more effective information and knowledge management.

Spotlight: EBA Report on the Use of AML/CFT SupTech tool

In addition to national initiatives, in August the EBA released a new report assessing the current use of SupTech tools by competent authorities for AML/CFT supervision across the EU. Based on data collected through a November 2024 survey of competent authorities and a January 2025 workshop hosted as part of the EBA's Forum of EU AML/CFT supervisors, the report analyzes 60 SupTech projects or tools reported by 31 competent authorities from across 25 EU Member States and three third countries.

Overall adoption trends and example reported use cases

The report identifies that AML/CFT SupTech adoption remains at an early stage but with increasing uptake, as most tools or projects were initiated within the last three years and currently stand at varying stages of maturity: 47% already in production, 38% under development, and 15% still in exploratory or ideation phases. Overall, the 31 responding competent authorities have worked on a total of 60 SupTech projects or tools to date, using 13 different technologies and applying these tools to address 13 types of AML/CFT supervision tasks or processes. Authorities participating in the survey, highlighted inter alia the following specific use cases:

On-site inspections

- Tool to centralise inspection planning and enhance audit trails, thereby addressing information management gaps
- Tool to support AML/CFT remediation tracking, consolidating data to support more effective monitoring and reporting
- Tool to manage large datasets and streamline supervision using process mining, NLP, and AI, with focus on crypto cases

Risk assessments

- Tool to automate risk assessments and improve risk accuracy by clustering algorithms and through semantic search
- Tool to support ML/TF risk management by improving planning, assessments, and inter-authority communication
- Tool to monitor crypto transaction risks which relies on blockchain analytics to analyse crypto-related risks

Fit & proper assessments

- Tool to support fitness and propriety assessments by translating documents, structuring data, and generating a risk score

The report furthermore identifies various success factors for the adoption of SupTech in an AML/CFT context such as the development of common standards for data formats, structures and exchanges to enhance functionality between systems, the use of synthetic data generation to create realistic training datasets while limiting data privacy concerns and establishing concrete metrics directly tied to supervisory objectives to assess performance and added value of SupTech tools.

OTHER DEVELOPMENTS

Spotlight: Responding to evolving public and private market dynamics

Q3 Since the start of 2025, regulatory authorities globally have converged on addressing the systemic implications of private markets' rapid expansion, with efforts intensifying further during Q3, reflecting recognition that private markets represent a permanent structural shift requiring targeted oversight.

Assessments released during the first half of the year identified several concerns. Australia's ASIC, in a dedicated consultation paper on private and public market dynamics in February, stressed opacity and information asymmetries, conflicts of interest, valuation challenges, leverage vulnerabilities as well as fees and expenses as risk areas warranting attention. Findings from a UK FCA multi-firm review examining the robustness of valuation processes for private market assets across UK asset managers, alternative investment fund managers, and investment advisers found significant variations in the level of functional independence within valuation processes and that some valuation functions were limited in their control and oversight effectiveness. Moreover, the review identified seven key areas where valuation-related conflicts are likely to arise while pointing out that many of firms currently do not comprehensively identify and document these.

Since mid-year, efforts have further shifted toward more active market intervention with the goal of addressing identified risks while preserving the economic benefits of private markets. The World Federation of Exchanges (WFE) launched a multi-pronged campaign, issuing papers in June and July warning that unchecked private market growth, aided by favourable regulatory treatment, posed risks to market integrity and financial stability. The WFE recommended developing harmonized transparency standards across both public and private market types, reviewing the regulatory and tax regimes that currently favour private capital, and implementing supervisory reporting requirements for secondary trading. The Federation specifically called for quantifying and assessing secondary trading platforms' interaction with public markets, scrutinizing bundled private credit and equity arrangements, and ensuring that regulatory and tax policy does not introduce distortions between market segments.

Most recently in September, ASIC released the findings from a commissioned review of Australia's private credit funds sector to complement the insights from its public consultation. While findings highlight the potential benefits of private markets in an Australian context, they also reiterated many of the previously raised risk concerns including opaque remuneration and fee structures, inadequate management of related-party transactions, and inconsistent valuation practice, supporting the case for clearer industry standards. In response, ASIC announced a forward-looking roadmap which involves the release of an outline findings and examples of better and poorer practices, guiding principles for the private credit industry and an expert reports on the future of Australia's capital markets and international data reporting and transparency practices in private markets.

Preserving the relevance of public equity markets

Amid changing public and private market dynamics and shrinking IPO pipelines, authorities are actively stepping up efforts to ensure public equity markets remain competitive and attractive to issuers and investors alike. Observed initiatives broadly fall into three areas:

Faster and more flexible IPO admission tracker

Spain's CNMV launched "BME Easy Access", reversing the IPO sequence by allowing firms to be admitted to trading first, then conduct placements gradually over an 18-month extendable period

ASIC introduced a two-year trial of a streamlined IPO timetable, shortening the pre-lodgement review period and permitting issuers to receive retail applications during the exposure period

Broadened access via new venues and instruments

Saudi Arabia's CMA created a regulatory framework for depositary receipts for foreign share, allowing foreign firms to register and offer these under the same conditions as local issuers

South Korea's FSC liberalized omnibus account rules, permitting overseas securities firms easier registration and enhancing foreign investor access to Korean stocks

Reduced prospectus and disclosure burdens

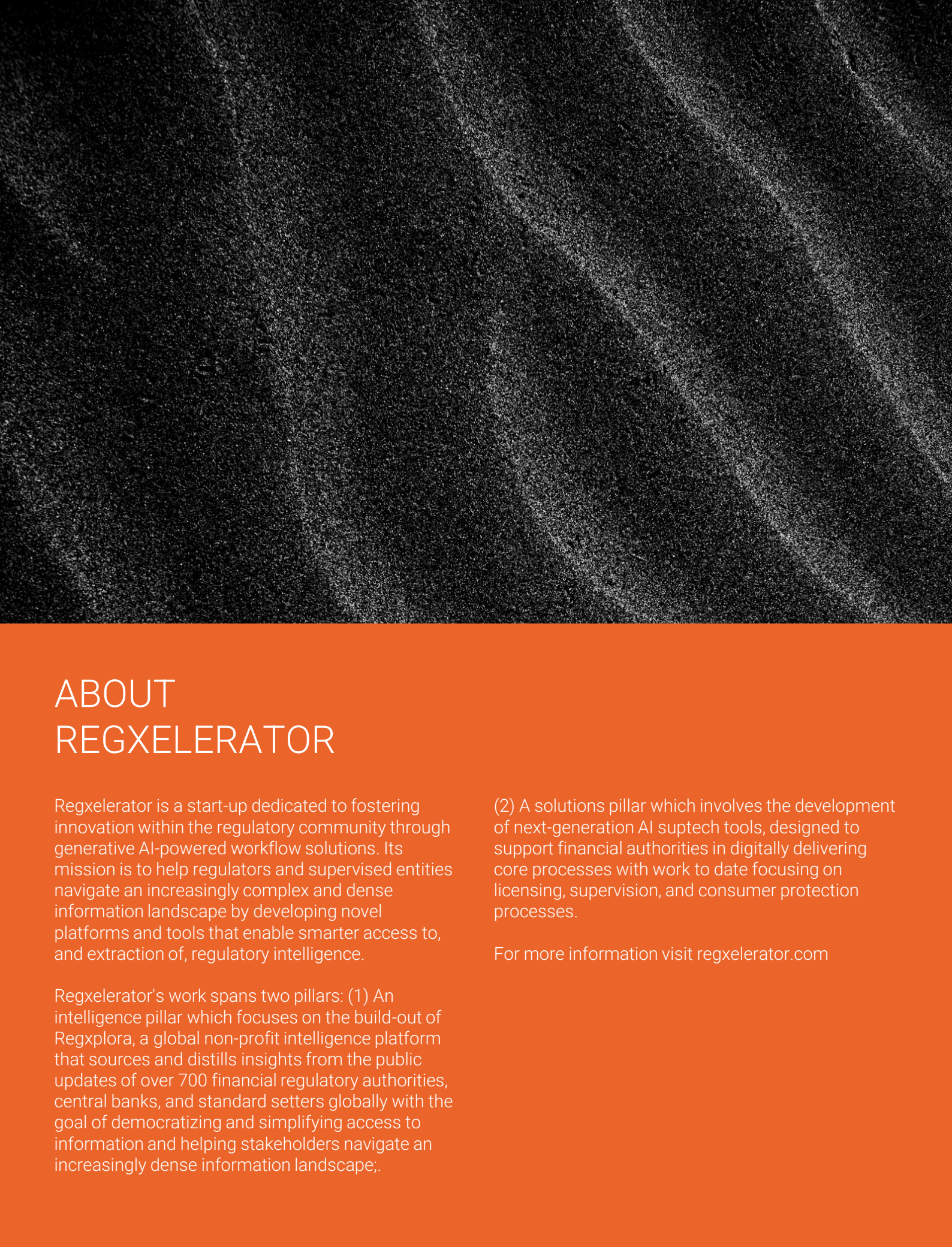
MAS has proposed streamlined IPO prospectuses that focus on essential investor information and simplified documentation for companies conducting secondary listings

The Canadian Securities Administrators issued orders to permit recent IPO issuers to conduct follow-on offerings quickly without additional prospectuses

LEADERSHIP CHANGES

Austrian National Bank	Governor	Martin Koche	New appointment
Reserve Bank of New Zealand	Governor	Anna Brehm	New appointment
Bank of Mauritius	Governor	Dr. Priscilla Muthoora Thakoor	New appointment
National Bank of Ethiopia	Governor	Dr. Eyob Tekalign Tolina	New appointment
U.S. Federal Reserve Board	Governor	Dr. Stephen Miran	New appointment
U.S. Office of the Comptroller of the Currency	Comptroller of the Currency	Jonathan Gould	New appointment
AMLA	Executive Director	Nicolas Vasse	New appointment
Austria Financial Market Authority	Executive Director	Mariana Kühnel	New appointment
Mexico CNBV	President	Ángel Cabrera Mendoza	New appointment
Canada Deposit Insurance Corporation	President and CEO	Gina Byrne	New appointment
ISDA	Chair	Amy Hong	New appointment
New York State Department of Financial Services	Superintendent	Adrienne A. Harris	Departure
	Superintendent (Acting)	Kaitlin Asrow	New appointment

In addition to these leadership changes, the European Banking Authority announced in September that José Manuel Campa will step down as Chairperson at the end of January 2026. Likewise, the Chair of the Australian Securities & Investments Commission, Joe Longo, confirmed that he will not seek reappointment when his term concludes on 31 May 2026.



ABOUT REGXELERATOR

Regxelerator is a start-up dedicated to fostering innovation within the regulatory community through generative AI-powered workflow solutions. Its mission is to help regulators and supervised entities navigate an increasingly complex and dense information landscape by developing novel platforms and tools that enable smarter access to, and extraction of, regulatory intelligence.

Regxelerator's work spans two pillars: (1) An intelligence pillar which focuses on the build-out of Regxplora, a global non-profit intelligence platform that sources and distills insights from the public updates of over 700 financial regulatory authorities, central banks, and standard setters globally with the goal of democratizing and simplifying access to information and helping stakeholders navigate an increasingly dense information landscape;

(2) A solutions pillar which involves the development of next-generation AI supotech tools, designed to support financial authorities in digitally delivering core processes with work to date focusing on licensing, supervision, and consumer protection processes.

For more information visit regxelerator.com