



Analyse. Anticipate. Accelerate.

# Enforcement Outlook: Asia-Pacific, Europe and North America

October 2025

# About this Report

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

This edition is intended to provide high-level analysis of enforcement activity across Asia-Pacific, Europe and North America in H1 2025, with forward-looking insights to help clients understand regulators’ priorities and avoid sanctions in the future.

## Contents

Introduction	3
Horizon Scanning Updates	6
Comparison By Jurisdiction	7
Comparison By Breach	12
Comparison By Product/Service	18
Spotlight: US Enforcement	21

## Authors

### Writing/Editing:

Adam Parkinson | Editor  
Jimmie Franklin | Senior Journalist  
Louise Coleman | Chief of Staff  
Armani Rahman | Analyst

### Content Operations/Design:

Hiriyti Bairu  
Sonia Nimley |  
Content Operations Team

## Notable Numbers

29

number of enforcement actions issued for AML violations alone in Europe in H1 2025

€400,000

penalty imposed on Paysera in Lithuania for acquiring e-money institution Contis without regulatory approval



£42m

fine issued to Barclays in the UK over major failures in handling financial crime risks

€88.2m

fine paid by Credit Agricole Corporate & Investment Bank in France relating to a criminal investigation into dividend-arbitrage trades



48

the number of US states that combined to impose an \$80m penalty on Block Inc. over violations of the Bank Secrecy Act (BSA) and anti-money-laundering and counter-terrorism financing (AML/CTF) rules

# Introduction

Vixio tracks enforcement activity in Asia-Pacific, Europe and North America, monitoring financial penalties, licence revocations and other sanctions imposed on banks and payments firms.

Our [2024 Enforcement Outlook](#) examined data on European enforcement activity collected during the first half of last year, highlighting the most active regulators, the most common breaches and the products and services most frequently sanctioned.

This year's report extends coverage to Asia-Pacific and North America, identifying emerging regional trends.

Regulators in jurisdictions around the world continued to rely on financial penalties during H1 2025, highlighting the potential cost to firms of failing to meet regulatory requirements.

Fines are effective because they create an immediate financial impact and may also influence investor confidence. In addition, heavy fines in particular signal to the market that breaches carry serious consequences.

Another advantage is that the threat of fines can drive internal compliance by incentivising firms to strengthen their governance, risk management and control frameworks.

Compared with other enforcement tools, fines are scalable, flexible and relatively straightforward to apply, which helps to explain why they are such a central feature of global regulatory enforcement strategies.

Nonetheless, regulators did opt for other forms of enforcement at times, such as licence suspensions and remedial orders, indicating a focus on intervention and collaboration as well as just deterrence.

## The old world on the move

Europe recorded the highest enforcement activity in H1 2025, with 123 actions (compared with 48 in Asia-Pacific and 46 in North America). This was almost double the 67 cases in H1 2024, suggesting firms in the region have yet to embed a genuine compliance-first culture.

The level of enforcement activity in Europe reflects the maturity of the industry in the region, which includes the 27 EU member states and the UK, and the scale should remind firms of the need to stay on top of compliance.

The region's regulators continued to favour imposing financial penalties in the first half of this year, with fines accounting for 80 of the total cases, or 65 percent. There were also 17 licence revocations and two suspensions, 14 remedial orders and four restrictive measures.

In H1 2024, more than 80 percent of enforcements were financial penalties, and the remainder consisted of licence revocations, warnings and orders to rectify the violations.

The growing use of licence revocations, suspensions and remedial orders suggests European regulators may be taking a more interventionist and preventative approach, using a wider range of tools to correct deficiencies rather than simply penalise them.

Although regulators continue to employ financial penalties, the 15 percent drop year-on-year in the proportion of fines imposed suggests they are becoming more of a last resort, to be applied only when firms fail to remediate issues or demonstrate systemic weaknesses.

Although the number of US enforcement actions in H1 2025 was relatively low at 46, the impact was amplified by multi-state actions. These are a feature of the US system, in which an investigation that begins in one state is joined by others.

A notable example is the [\\$80m settlement](#) reached by Block Inc. with 47 states and the District of Columbia for anti-money laundering (AML) violations in January 2015.

Multi-state actions increase financial exposure, operational complexity and reputational risk, as companies may initially believe they are under scrutiny in only certain jurisdictions, but find the investigation expanding nationwide.

This dynamic underscores the need for firms to treat early regulatory engagement and compliance remediation as a matter of national importance, and not just focus on state-level activity.

## Taking on AML failings

Across all regions, anti-money laundering (AML) failings were the most common breach in H1 2025. This reflects a global trend, with AML-related updates now representing an increasingly significant proportion of regulatory activity in jurisdictions around the world.

With financial crime prevention becoming a core priority for supervisory authorities, organisations operating in high-risk sectors such as banking and payments must review their AML compliance processes, as the financial and reputational consequences of non-compliance can be costly.

The growing focus on AML continued the pattern seen in Europe in H1 2024, when AML failings made up more than half of all enforcement activity: 36 cases, including 29 fines.

In H1 2025, Europe recorded 29 AML-related actions, broadly flat compared with the previous year. In Asia-Pacific, AML breaches also accounted for the highest proportion of the region's enforcement actions, with 13 penalties, followed by conduct of business violations with nine.

The picture in North America was more mixed, with AML accounting for ten of the region's 46 enforcements, marginally behind conduct of business violations at 11, and just ahead of reporting failings at eight.

The launch of the EU's Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) is set to change the way AML is regulated in Europe, increasing scrutiny on payment organisations and potentially leading to an uptick in enforcement.

In Asia-Pacific, regulators such as the Monetary Authority of Singapore (MAS), AUSTRAC and the Hong Kong Monetary Authority (HKMA) continue to ensure payment service providers (PSPs) and fintech firms are applying robust AML controls.

In the US, federal authorities initiated only three AML enforcement actions in H1 2025, with two resulting in monetary penalties and one in a remedial order. However, multi-state enforcement amplified the impact, most notably in the \$80m settlement with Block noted above. This case illustrates how even a small number of AML actions can carry significant financial and operational consequences when states coordinate.

Although the number of AML enforcements varied by region, the focus on financial penalties and systemic remediation underscores the global priority regulators place on AML compliance. Firms should strengthen monitoring and reporting frameworks and keep pace with regulatory developments to avoid enforcement action.

## Banking on enforcement

Banks accounted for a slightly larger share of enforcement actions than the other entities Vixio tracked in H1 2025 in Europe, which include e-money firms, payment processors, payment institutions and crypto-asset service providers.

Across regions, enforcement generally focused on banks and PSPs. North America exhibited the most variation in entity types, with e-money firms, payment institutions, payment processors and money transmitters all facing significant sanctions.

This highlights both the diversity of regulated entities in the US and the broad application of regulatory oversight across the payments ecosystem.

The breadth of enforcement may be a trend that spreads to other regions – regulators elsewhere have also begun to pay more attention to non-bank institutions in recent years. For example, the Bank of Lithuania and the Malta Financial Services Authority (MFSA) have both increased their scrutiny of payment and crypto-asset firms.

## Room for improvement

In H1 2025, regulators around the world identified failures in key areas such as customer due diligence, transaction monitoring, suspicious activity reporting and politically exposed person (PEP) screening, and imposed penalties accordingly.

Firms should factor these findings into their compliance reviews and avoid scaling back effective, well-resourced programmes.

Fines for similar breaches varied significantly across Europe, North America and Asia-Pacific, reflecting differing enforcement philosophies and market structures.

*“Banks accounted for a slightly larger share of enforcement actions than the other entities Vixio tracked in H1 2025 in Europe.”*

In Europe, EU member states maintained their robust approach to AML compliance. For instance, [Bunq](#), a Dutch neobank, was fined €2.6m by the Dutch Central Bank (DNB) in May 2025 for repeated AML failures between 2021 and 2022. Similarly, in March 2025, the Bank of Lithuania fined [Revolut](#) €3.5m for AML deficiencies.

These cases illustrate Europe’s trend of imposing moderate to high penalties for AML and consumer protection violations, often ranging from €2m to €20m per case.

Although there were fewer enforcement actions in the US in H1 2025, some substantial penalties were imposed. In addition to its \$80m multi-state fine, [Block](#) was fined \$40m by the New York State Department of Financial Services for failing to adequately manage AML measures and know-your-customer (KYC) compliance. These substantial fines reflect the US emphasis on deterrence and accountability.

Enforcement in Asia-Pacific was comparatively limited and less financially impactful. For example, in Singapore, the MAS imposed [penalties](#) totalling S\$960,000 (\$742,000) on five major payment institutions for breaches of AML and counter-terrorist financing (CTF) requirements.

### Navigating the shifting regulatory landscape

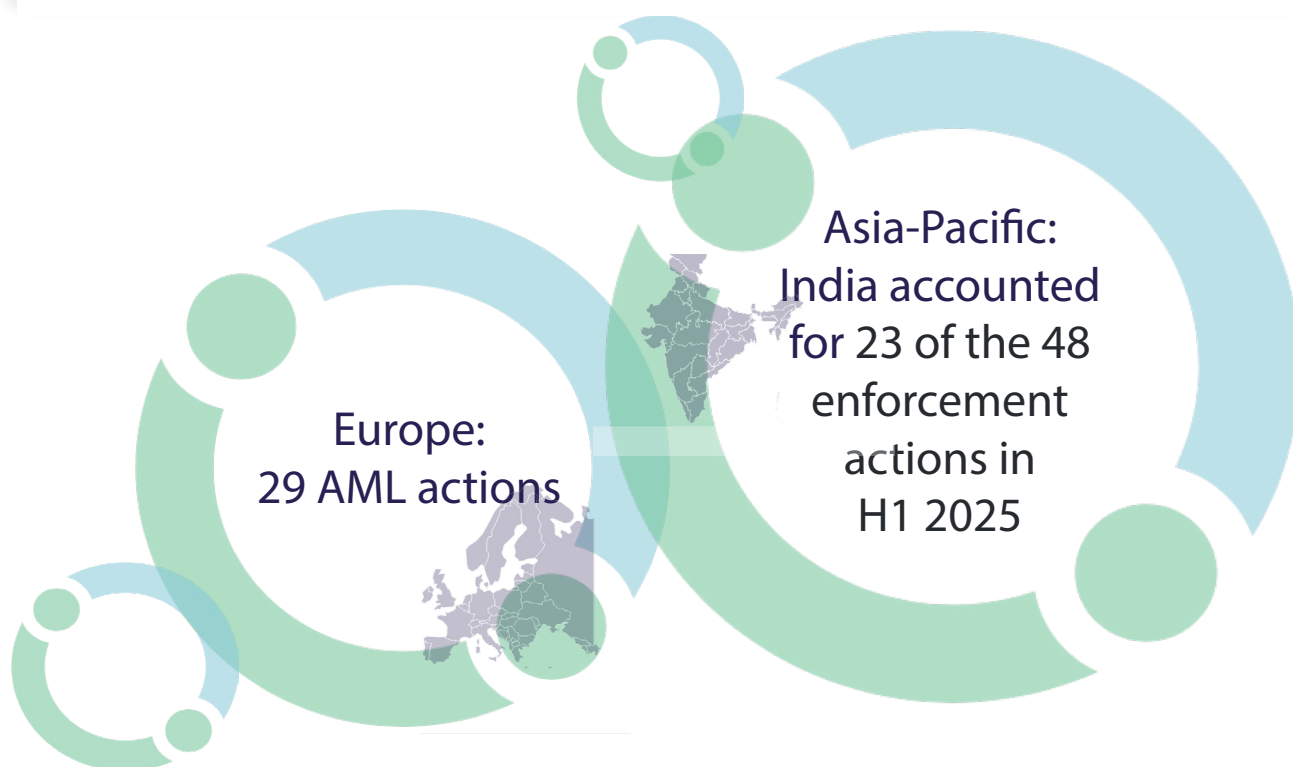
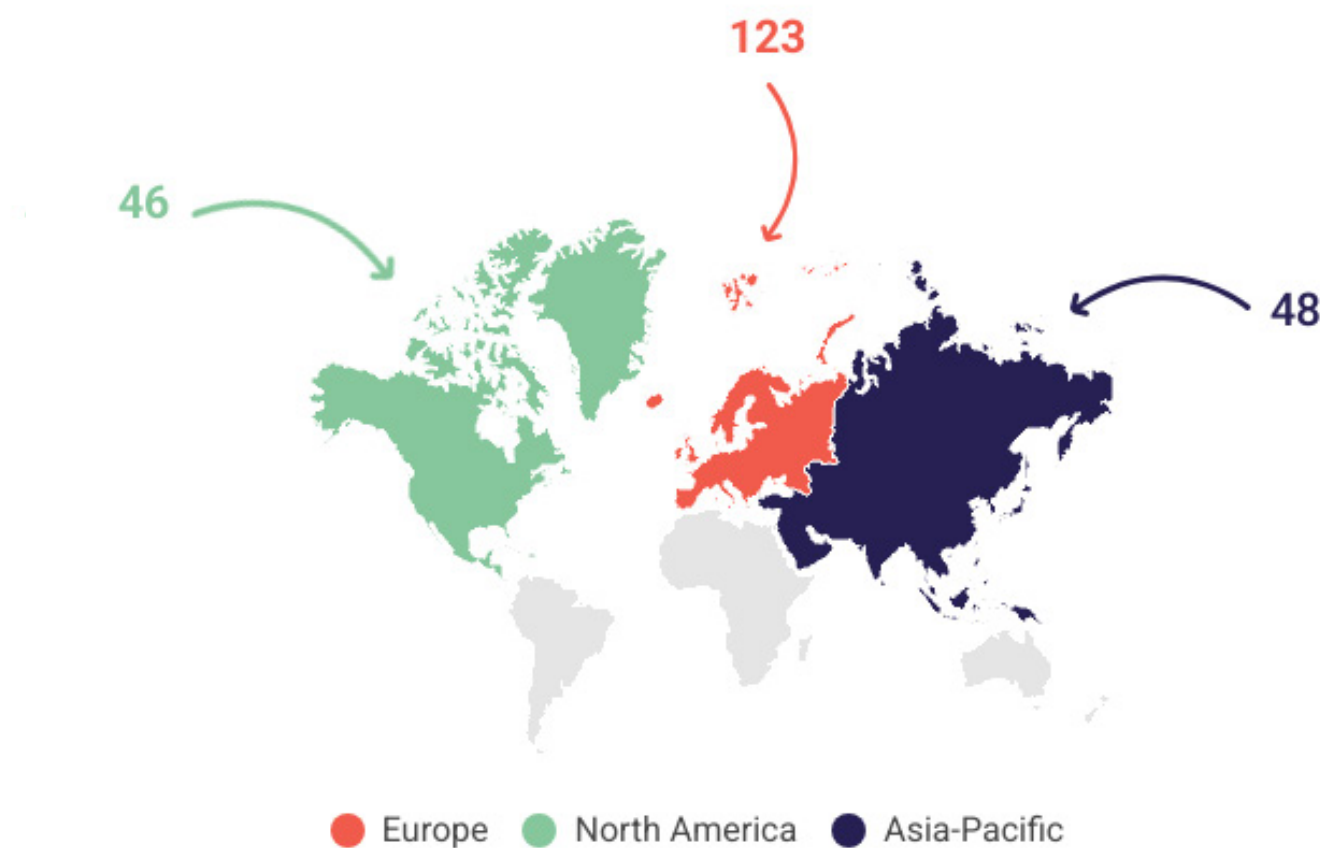
- » In H1 2025, European regulators recorded the highest enforcement activity, with 123 actions.
- » AML failings were the most common breach in H1 2025.
- » In Asia-Pacific, AML breaches accounted for the highest proportion of the region’s enforcement actions, with 13

These lower fines reflect a supervisory approach focused more on compliance improvement than punitive measures. Whereas Europe and the US continued to use fines as key enforcement tools in H1 2025, Asia-Pacific maintained a more corrective and less punitive posture, resulting in fewer and smaller penalties for similar breaches.

As enforcement evolves across regions, firms that embed resilience, transparency and accountability into their operations will be best placed to navigate the shifting regulatory landscape.

# Vixio 2025 Horizon Scanning Updates

Number of enforcement actions (by region)



## Comparison By Jurisdiction

European regulators recorded the highest number of enforcement actions in H1 2025, at 123, compared with 48 in Asia-Pacific and 46 in North America.

Europe's payments enforcement activity comprised a high number of AML and consumer protection actions, including significant fines for banks and PSPs.

In Asia-Pacific, enforcement activity was more limited in terms of numbers, but still focused predominantly on AML compliance, with 13 cases all resulting in financial penalties and a continued emphasis on supervisory engagement rather than punitive measures.

As noted in the introduction, although the number of US enforcement actions in H1 2025 was relatively low, the impact was amplified by multi-state actions, in which an investigation that begins in one state is joined by others.

Vixio's analysis shows that regulators around the world are active, and that the payments landscape is evolving rapidly, making regulatory arbitrage a risky strategy.

Rolling out a light-touch compliance framework may seem cost-effective initially, but it can become expensive if rules tighten or if non-compliance in one jurisdiction triggers enforcement or reputational consequences elsewhere.

A safer approach is to prioritise compliance from the outset, embedding robust standards throughout processes and setting high internal benchmarks.

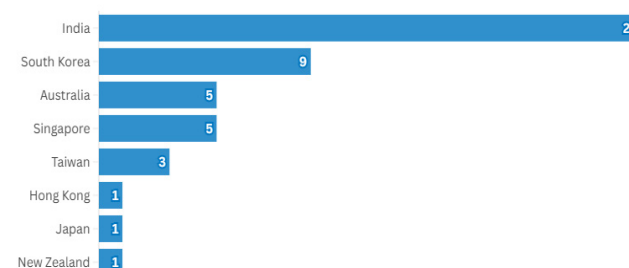
Applying these standards consistently across jurisdictions reduces the risk of enforcement, simplifies operations and ensures alignment with evolving global requirements.

Although this approach may involve higher upfront costs, it mitigates regulatory, financial and reputational risks; supports sustainable growth; and

future-proofs firms against tightening AML, digital asset and consumer protection rules.

### Asia-Pacific

Fig. 1: Enforcement actions in Asia-Pacific by jurisdiction, H1 2025



VIXIO  
Regulatory Intelligence

Regulatory enforcement in the Asia-Pacific region was relatively limited in H1 2025 compared with the US and Europe. Many authorities focused on implementing new payments and digital asset frameworks, emphasising supervision and industry engagement rather than punitive action.

During the first half of the year, several Asia-Pacific authorities were still in the consultative or implementation phases of new frameworks. For example, Australia has been engaged in a programme of [payment system modernisation](#) and Hong Kong has been developing a new [stablecoin regime](#). This shifted attention from penalties to policy refinement and industry engagement.

Enforcement outcomes are also less frequently publicised, and the region's market structure, which is dominated by established incumbents, offers fewer opportunities for large-scale breaches. Overall, oversight remained active but produced few headline cases during the period.

India led the Asia-Pacific region for enforcement in H1 2025, accounting for 23 of the 48 actions tracked by Vixio – nearly half of the total. South Korea ranked second, with just nine cases.



The Reserve Bank of India (RBI) imposed fines on 21 banks and payment institutions for a range of compliance shortcomings. These included know-your-customer (KYC) failures, due diligence lapses, conduct of business breaches and deficiencies in operations, governance, reporting and lending.

In June 2025, for example, the central bank [fined Fino Payments Bank Limited](#) INR2.96m (\$34,178) for breaching its Operating Guidelines for Payment Banks by exceeding the regulatory ceiling for end-of-the-day balances.

There were also directional breaches, in which entities did not comply with the RBI’s supervisory instructions.

Fines were most frequently imposed for operational failures and due diligence shortcomings, reflecting the regulator’s focus on operational resilience. Regulated firms should maintain robust internal policies, including up-to-date risk registers, regular staff training and thorough review of due diligence procedures, using screening technology effectively.

The Monetary Authority of Singapore (MAS) fined five payment institutions for anti-money laundering (AML) breaches, reinforcing its tightening stance on financial crime risks.

Although this may appear a modest level of activity for a major financial hub, it is roughly on par with some established European jurisdictions for similar breaches, particularly where regulators prioritise supervisory engagement and remediation over headline fines.

In Singapore, a notable feature of enforcement is the focus on individual accountability, with regulators often taking action against directors or compliance officers for lapses in controls.

This approach reinforces personal responsibility while maintaining the overall stability of the sector, rather than imposing large institutional fines as is more common in the US or parts of Europe.

The MAS’ activity in H1 2025 built on the [2024 National Anti-Money Laundering Strategy](#) published in November last year, which set out plans to maintain Singapore’s reputation as an “open” and “trusted” financial centre.

The emphasis on AML in H1 2025 reflects this strategy, underlining the need for firms in Singapore to maintain effective compliance processes to avoid regulatory action. The enforcement activity across Asia-Pacific’s banking and payments sectors suggests that regulators are emphasising resilience, governance and consumer protection.

Singapore was not an outlier in its focus on AML: such breaches accounted for the bulk of the region’s enforcement actions, with 13 penalties, followed by conduct of business breaches with nine.

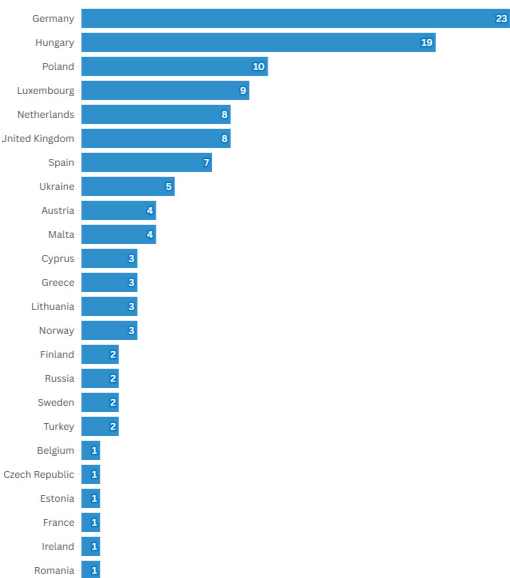
The figures underline the seriousness with which regulators are focusing on AML compliance and reflect heightened scrutiny of financial crime controls.

Regulators in jurisdictions such as Australia, Singapore and Hong Kong are evolving their frameworks to address key concerns such as money laundering, fraud and the growth of digital assets.

Firms operating in the region should implement robust monitoring and reporting frameworks to avoid enforcement action. They should also carefully monitor regulatory developments to ensure they remain aligned with evolving requirements.

## Europe

Fig. 2: Enforcement actions in Europe by jurisdiction, H1 2025





Regulators across Europe recorded 123 enforcement actions during H1 2025, with financial penalties accounting for 80 of these cases.

In addition, there were 17 licence revocations and two suspensions, 14 remedial orders and four restrictive measures.

The largest fine in Europe in H1 2025 was the [€15m penalty](#) imposed on ABN AMRO by the Dutch Central Bank for violating the Netherlands' bonus ban, paying bonuses to seven second-tier managers between 2016 and 2024.

The scale of the fine reflects the long duration of the breach, the bank's systemic importance and the regulator's aim to send a strong deterrent signal.

For financial organisations, it underscores the critical need for strict compliance with remuneration rules, robust internal governance and careful oversight of all management levels.

The case also reinforces that European regulators are willing to impose substantial penalties to enforce structural risk controls, making adherence to bonus and governance frameworks a top priority.

Germany and Hungary had the highest number of actions, with 23 and 19 respectively, together accounting for more than a third of the 123 cases.

In March 2025, Germany's financial supervisory authority, BaFin, initiated its first enforcement action under MiCA, [ordering crypto firm Ethena](#) to halt the issuance of its USD asset-referenced token (ART).

This marked a significant step in MiCA's enforcement phase. The framework, which came into force in June 2023, aims to establish a harmonised regulatory environment for crypto-assets across the EU. It includes provisions for transparency, disclosure, authorisation and supervision of transactions involving crypto-assets.

The initial enforcement actions, such as the one against Ethena, suggest that regulators are adopting a stringent approach to ensure compliance with MiCA's provisions. These actions serve as a warning to other crypto-asset service providers about the importance of adhering to the regulatory framework.

Looking ahead, regulators across the EU will continue to monitor and enforce compliance with MiCA, potentially leading to more enforcement actions. This proactive stance underscores the EU's commitment to creating a secure and stable environment for crypto-assets, aligned with broader goals of financial integrity and consumer protection.

*"Banks, being generally more established and numerous, were the primary focus of European enforcement actions in H1 2025, accounting for more than half of the entities penalised."*

However, banks, being generally more established and numerous, were the primary focus of European enforcement actions in H1 2025, accounting for more than half of the entities penalised.

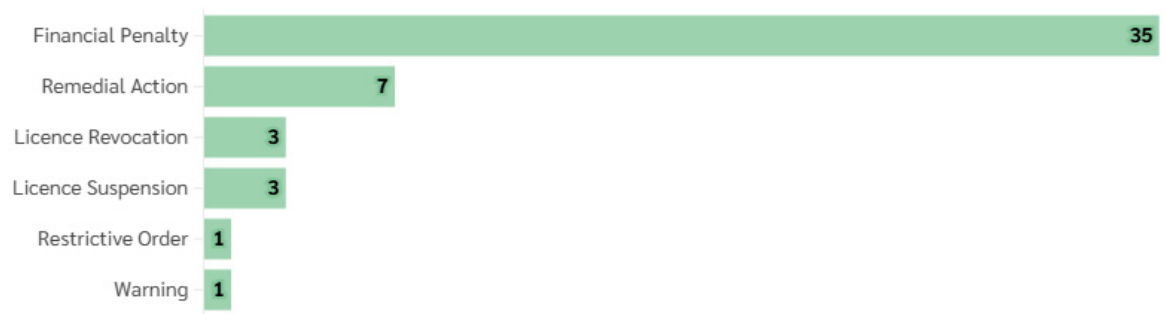
In contrast, e-money firms, payment processors and payment institutions made up just over a fifth of those sanctioned.

Regulators' focus on banks, particularly for AML and fraud breaches, reflects ongoing concerns about systemic vulnerabilities. At the same time, the payments sector is becoming increasingly diverse, leaving no room for complacency, as enforcement is expanding beyond traditional banks to encompass a broader range of firms

Financial services organisations operating in Europe should intensify compliance efforts, conduct thorough risk assessments, reinforce AML systems and monitor evolving regulatory requirements to prevent future penalties.

# North America

Fig. 3: Enforcement actions in North America by action, H1 2025



In H1 2025, North American regulators focused their attention on conduct of business (11), AML (10) and reporting failures (eight), with additional attention on consumer protection (six) and data protection and cybersecurity (six).

Regulators relied heavily on financial penalties, highlighting the potential cost to firms that do not meet regulatory requirements.

At the state level, enforcement activity was distributed across the country, with the most cases in Florida (nine), followed by California (four), North Carolina and Texas (three each).

As in other regions, AML remained the dominant risk area. Multi-state actions and penalties issued by FinCEN, state regulators and the Federal Deposit Insurance Corporation (FDIC) targeted weak transaction monitoring, reporting gaps and inadequate risk frameworks.

Money transmitters and payment firms saw enforcement actions concerning prudential standards, safeguarding and accurate reporting, with several licence suspensions and revocations emphasising the consequences of persistent failures.

For example, in March 2025, the North Dakota Department of Financial Institution (DFI) issued a [consent order against BAM Trading Services](#), doing business as Binance.US, for breaching prudential, AML and customer protection rules.

Under a consent order, the firm agrees to take specified corrective actions, such as strengthening AML programmes, enhancing risk management and improving governance, without admitting or denying wrongdoing.


The order is legally binding, and non-compliance can trigger further penalties. The DFI’s action highlights both its focus on crypto platform oversight and the broader use of consent orders as a flexible enforcement tool to ensure firms remediate regulatory deficiencies while maintaining operational continuity.

State regulators in New York, Texas and North Carolina also issued such penalties against firms that failed to adequately secure systems and customer data.

In January 2025, the New York State Department of Financial Services (DFS) issued a consent order against [PayPal](#) for multiple infractions, including inadequate implementation of cybersecurity policies and insufficient qualified personnel to oversee core cybersecurity functions. As part of the order, the regulator imposed a \$2m fine.

At the federal level, the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC) imposed penalties for misleading advertising, inadequate disclosures, and substandard complaint-handling processes.

In addition, the FDIC took a series of enforcement actions against banks, highlighting the regulator’s concerns regarding conduct of business and governance failings.



## North America: Most variation in types of entities subject to enforcement action

For example, in January 2025, it executed a consent order with [Crescent Bank](#) for unsafe or unsound banking practices and legal violations, requiring the bank to undertake several remedial steps, including an independent review of its current expected credit loss (CECL) and underwriting model risk management (MRM) framework.

The North American data indicates that firms should strengthen AML controls and build robust cybersecurity and data governance frameworks to mitigate the risk of sanctions, which can range from financial penalties to licence revocation.

The current US regulatory environment is challenging for banks and payment firms to navigate, owing to ongoing deregulation, increasing fragmentation of state-level rules and uncertainty around regulatory priorities.

Organisations operating in the jurisdiction should maintain well-resourced compliance functions capable of interpreting applicable rules. They should also preserve strong communication with state and federal regulators to minimise the risk of non-compliance.

## Comparison By Breach

European regulators maintained a strong enforcement stance in the first half of 2025. Enforcement against breaches categorised as “other” were the most frequent area of non-compliance, followed closely by AML issues and then at a greater distance by failures to meet reporting obligations.

The enforcement actions categorised as “other” covered a wide spectrum of breaches, including disclosure failures, weak internal controls, violations of banking and investment legislation and shortcomings in safeguarding.

Of note, no two enforcement actions within this group were taken for the same reason, underlining the breadth of regulatory scrutiny and the diverse ways firms can fall short.

This reinforces a clear message: compliance must be comprehensive. Although European regulators remain heavily focused on AML, they are equally prepared to act on deficiencies in other areas, meaning there is little room, or justification, for taking risks with compliance.

During H1 2025, European regulators issued 29 enforcement actions for AML violations, with 25 resulting in financial penalties. This underscores the EU’s continued tough stance on AML non-compliance.

AML’s status as the EU’s foremost supervisory priority in 2025 has been reinforced by the launch of the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). The body is expected to be fully operational by the end of the year, after supervisory powers are transferred from the European Banking Authority (EBA).

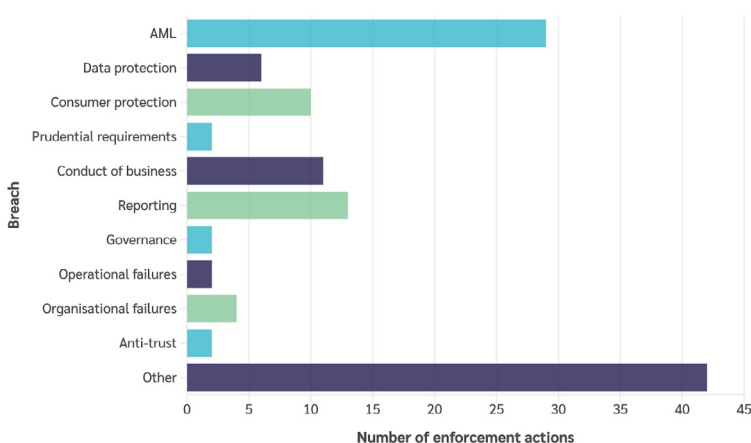
In parallel, the EU has begun rolling out its harmonised “single rulebook” through the [AML Regulation](#) (EU) 2024/1624 and the [6th AML Directive](#). These measures are intended to establish consistent standards across member states.

Together, they aim to close long-standing regulatory gaps and reduce the number of enforcement actions against banks, payment service providers (PSPs) and investment firms.

### The AML enforcement cases Vixio tracked most frequently cited:

- » Customer due diligence failures: Inadequate updating of customer information, weak ongoing monitoring of business relationships and lapses in know-your-customer (KYC) checks.
- » Transaction monitoring deficiencies: Failure to apply financial safeguards for high-value transactions.
- » Reporting shortcomings: Delays or failures in submitting suspicious activity reports (SARs).
- » Weak internal controls: Deficiencies in AML governance, policies, and risk management frameworks.

Fig. 4: Enforcement actions in Europe by breach, H1 2025



## AML by jurisdiction: Europe

Ukraine, Germany and Lithuania together accounted for just less than 50 percent of AML-related enforcement actions in Europe during H1 2025.

In Ukraine, the National Bank reprimanded banks and payment institutions for a range of AML issues. The most prominent was inadequate due diligence on existing and new customers, leading to fines for four firms.

In the first half of 2024, Germany and Lithuania recorded the highest number of AML enforcement actions in Europe, with German authorities issuing four measures and their Lithuanian counterparts issuing three.

Most sanctions stemmed from inadequate reviews or failures to submit SARs, deficiencies in KYC procedures and weaknesses in internal AML frameworks, particularly around conflicts of interest. Germany and Lithuania remained the most prevalent enforcers of AML-related deficiencies in H1 2025.

Both jurisdictions appear to be facing the same types of breaches as in H1 2024, with limited evidence of meaningful progress in strengthening institutional compliance.

This persistent pattern may indicate a need for stronger supervisory intervention, more rigorous enforcement measures and targeted capacity-building within financial institutions to ensure sustainable improvements in AML compliance.

The enforcement landscape in H1 2025 demonstrates that, despite extensive EU-level reforms, institutions still fall short on core AML obligations. Failures in customer due diligence, transaction monitoring, suspicious activity reporting and PEP screening remain the most frequent grounds for penalties.

These breaches highlight a deeper issue: firms are not consistently embedding a compliance-first culture in their approach to financial crime prevention. Beyond the financial costs, such violations carry

significant reputational risks, particularly for banks and payment institutions that customers depend on for safe and reliable services.

Repeated enforcement actions erode trust, damage client relationships and undermine market confidence. Ultimately, these shortcomings stem less from errors in interpreting regulatory requirements than from ineffectively implementing compliance frameworks.

These jurisdictional differences highlight the challenge AMLA will face in achieving a fully harmonised supervisory regime, even with the introduction of the EU's single rulebook.

## Reporting failures: Europe

In the first half of 2025, reporting failures were the second most frequently sanctioned individual breach in Europe, with 13 enforcement actions, 11 of which resulted in fines. Failures ranged from late submission of required documentation to inaccurate data and other shortcomings in AML-related reporting.

Hungary's central bank, the Magyar Nemzeti Bank (MNB), accounted for around a third of these penalties (four). Such failures risk undermining trust in the country's financial sector, prompting closer scrutiny from EU supervisory bodies and raising the likelihood of intrusive remediation plans or licence restrictions.

Beyond regulatory repercussions, continued deficiencies in reporting also damage market confidence.

Investors and counterparties depend on reliable data as a foundation for transparent operations. When reporting systems repeatedly fail, questions are inevitably raised about governance, data integrity and the seriousness with which institutions approach compliance.

For Hungarian firms, this heightens reputational risks at a time when both domestic and EU authorities are tightening expectations.

In Germany, BaFin also issued two enforcement actions for reporting failures in H1 2025: one resulted in a financial penalty, the other in a formal warning.

This may reflect regulatory scrutiny of data quality, governance and internal reporting controls, particularly as supervisory frameworks become more risk-based and data-driven.

For financial service providers, this trend signals that even non-financial breaches, such as disclosure gaps, can trigger sanctionable action, with potential consequences for both compliance costs and supervisory relationships.

Germany's enforcement of reporting failures is being shaped by several overlapping forces.

After high-profile supervisory failures (most notably the [Wirecard scandal](#)), BaFin has committed to becoming more proactive and vigilant. [Statements](#) by the president of BaFin in June 2025 suggest that the regulator is more willing to challenge firms robustly when disclosures, control environments or transparency obligations are not met.

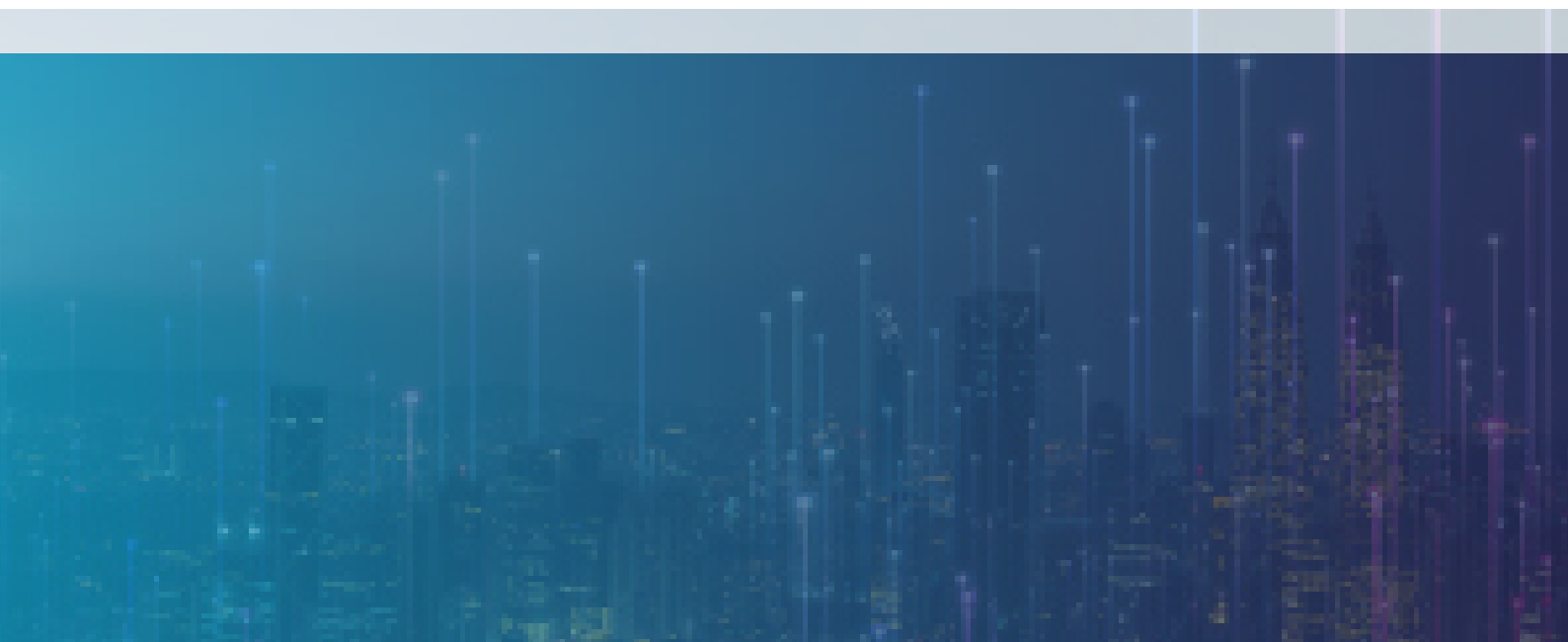
The use of warnings in addition to fines indicates a tiered approach: regulators are seeking to correct behaviour early, but also to use fines as deterrents where problems are more severe or persistent.

Firms with weak reporting systems may experience delays in gaining regulatory approvals, suffer loss of investor confidence (which may affect their

ability to raise capital) or face higher compliance costs.

In industries or sectors where trust in data is increasingly valued, those that fail to meet reporting obligations face heightened scrutiny and more severe market consequences.

*"In the first half of 2025, reporting failures were the second most frequently sanctioned individual breach in Europe, with 13 enforcement actions, 11 of which resulted in fines."*





## AML enforcement: Asia-Pacific

Across Asia-Pacific, the most prominent enforcement actions have also centred on AML, with 13 cases recorded, all of which resulted in financial penalties.

### The enforcement cases Vixio tracked most frequently cited the following issues:

- » Inadequate monitoring of business relationships and insufficient scrutiny of transactions.
- » A lack of clear oversight and leadership by senior management in relation to AML/CTF responsibilities.
- » Deficiencies in carrying out effective customer due diligence.
- » Failures in the identification and verification of customer identities.

## AML by jurisdiction: Asia-Pacific

In H1 2025, five of the 13 AML-related enforcement actions across Asia-Pacific were issued in Singapore, underscoring the jurisdiction's focus on financial crime controls.

AML is explicitly framed as a national priority in Singapore, with the government publishing its [National Anti-Money Laundering Strategy](#) in 2024.

The strategy emphasises that combating money laundering is of national importance. This serves not only to safeguard the financial system from illegal activities and illicit fund flows, but also to reinforce Singapore's standing as a trusted international financial centre and business hub.

It builds on the updated [Money Laundering National Risk Assessment](#), which consolidated years of observations on emerging threats and broader risk reviews to improve

Singapore's understanding and mitigation of financial crime risks.

This provides a forward-looking framework to guide proportionate, risk-based measures and ensure Singapore's AML regime remains robust and adaptive.

Reinforcing this message, the Monetary Authority of Singapore's (MAS) [Enforcement Report](#) makes clear that tackling AML breaches remains a top supervisory priority. The regulator has committed to continue issuing guidance to financial institutions on effective AML/CTF practices.

In Asia-Pacific, as elsewhere, the rapid expansion of cross-border flows, digital payment channels and the growing role of crypto-assets have opened new avenues for illicit finance, making financial institutions more vulnerable.

Many firms are still wrestling with legacy compliance gaps, particularly in areas such as transaction monitoring, customer due diligence and senior management oversight.

Enforcement actions, often accompanied by large penalties, are also used as a signalling tool, reminding institutions that AML compliance is a non-negotiable baseline for operating in the financial system.

At the firm level, these enforcement actions carry tangible consequences. Financial institutions face the immediate burden of monetary penalties, alongside the often heavier costs of remediation, such as hiring additional compliance staff and investing in upgraded monitoring systems.

The macro-level impact is equally significant. Consistent, visible enforcement raises the overall standard of AML compliance across the market, encouraging banks and payment firms to strengthen internal controls.

However, this can lead to industry consolidation. Smaller firms may find the cost of compliance unsustainable and opt to either exit the market or merge with larger players.



## AML enforcement: North America

In the first half of 2025, Vixio recorded enforcements across a wider spectrum of breaches in North America than the other regions, with conduct of business, AML and reporting violations the key areas of activity.

This may reflect the differing priorities in the US, where the impact of the second Trump administration on the regulatory landscape has been significant.

Focusing on AML, US federal authorities initiated only three enforcement actions in H1 2025, with two resulting in monetary penalties and one in a remedial action.

However, one of the most significant actions in H1 2025 was [Block's \\$80m multi-state settlement](#) with 47 US states and the District of Columbia for AML violations.

The fact that nearly every state-level regulator coordinated in a single enforcement action underscores the regulatory seriousness and cross-jurisdictional scrutiny facing payment and financial service providers.

From a reputational perspective, the scale of coordination matters as much as the penalty. When so many state regulators participate in the same settlement, it creates a perception of systemic failure rather than isolated misconduct.

This reputational damage carries longer-term consequences, such as third parties reassessing contractual risk, and future licensing or product approvals could face added friction.

For comparison, in H1 2024 US regulators brought 45 enforcement actions against financial institutions, of which 30 primarily concerned reporting obligations and AML breaches.

However, as noted above, in the US, large-scale enforcement can occasionally result from coordinated multi-state actions. This means that a single case that involves multiple state regulators rather than one federal authority can create outliers in enforcement data without indicating an increase.

The decrease in the overall number of enforcement actions likely reflects the broader deregulatory agenda, with authorities such as the Consumer Financial Protection Bureau (CFPB) adopting a markedly less interventionist approach.

### The enforcement cases Vixio tracked most frequently cited the following breaches:

- » Failing to submit suspicious activity reports (SARs) in a timely manner.
- » Improper record-keeping, particularly of customer identification and verification documents.
- » Failure to maintain effective AML programme policies.

## AML by jurisdiction: North America

Federal deregulation under the Trump administration is creating gaps in oversight, prompting individual states to assume greater responsibility for financial market supervision.

In April 2025, a [leaked internal memo](#) sent by CFPB chief legal officer Mark Paoletta revealed the agency is actively stepping back from certain enforcement areas to give states more authority.

Florida issued three financial penalties for AML-related breaches in H1 2025. On paper, this makes it one of the most active state-level enforcers. Again, however, the fines themselves remain modest, ranging from \$3,000 to \$45,000.

This raises a critical question: if the financial impact is negligible, are firms truly being deterred or merely treated to a cost-of-doing-business reminder?

California imposed two enforcement actions for AML breaches in H1 2025, both remedial in nature. This may point to a more corrective strategy aimed at reshaping compliance behaviour rather than simply punishing failures.

Within just months, the Trump administration's policies have resulted in a noticeably more business-friendly regulatory environment. However, deregulation at the federal level is inherently unstable. What one administration scales back, another can quickly restore or even tighten.

For that reason, firms cannot afford to become complacent in their AML controls simply because federal authorities have stepped back.

In the absence of a consistent federal precedent, institutions increasingly bear the burden of self-regulation. Firms should maintain robust internal AML governance aligned to their risk profile and operational complexity, irrespective of current enforcement trends.

By embedding resilient AML frameworks now, firms insulate themselves from political swings. Whether the next administration is Republican or Democrat, organisations with strong controls in place will be prepared, rather than caught off guard.

Regulators may be stepping back in terms of headline-making enforcement, but the obligation to maintain rigorous AML controls has not disappeared;

it has simply shifted from external pressure to internal accountability.

## AML wrapped

AML enforcement was the defining global trend Vixio identified during H1 2025, cutting across regions and sectors.

Regulators in North America, Europe and Asia-Pacific are converging on a common priority: addressing weak financial crime controls.

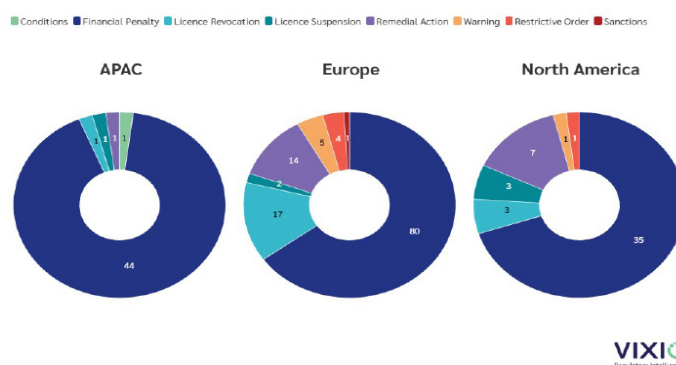
Enforcement actions reflect a sustained focus on supervisory oversight, backed by penalties, remedial orders and reputational consequences.

The call to action is clear: act now. Compliance frameworks must not exist only on paper; they must be operationalised, tested and continually strengthened to respond to evolving risks.

Institutions that delay until regulators intervene risk preventable damage. By contrast, those investing proactively in AML compliance reduce enforcement exposure and strengthen their standing as trusted participants in the global financial system.

For more on enforcement in the US, please see the [Spotlight](#) section.

Fig. 5: Number of Enforcements by Action, H1 2025



# Comparison By Product/Service

Vixio's research shows that banks are consistently the entities most likely to face enforcement action worldwide, particularly in the EU and Asia-Pacific. In North America, although banks have been heavily targeted by regulators, e-money firms, payment institutions, payment processors and money transmitters have also faced significant enforcement action.

This may be in part due to the multi-state actions taken against companies such as [Wise](#) and [Block](#), as well as the attention that the US government has given to money transmitters and money servicing businesses that work cross-border in countries such as Mexico.

In addition, the US state of Florida has imposed a number of relatively small fines on payments firms. It has been particularly focused on reporting violations, and has taken action against firms including [Wex Payments](#) and [Rapid Cash](#).

In the UK, one of the most significant fines issued in the first half of this year was against [Barclays](#), which paid £42m over major failures in handling financial crime risks. In Europe, Credit Agricole Corporate & Investment Bank [agreed](#) to pay €88.2m to settle a French criminal investigation into dividend-arbitrage trades designed to help foreign investors avoid withholding taxes.

In Germany, meanwhile, Deutsche Bank's DWS asset-management arm was [fined](#) €25m by prosecutors for so-called "greenwashing", making misleading claims about the ESG credentials of its investments.

In the US, enforcement actions so far this year have been smaller but still notable, including recent fines related to the [Flood Disaster Protection Act](#). However, none have surpassed \$20,000, and they are seemingly more symbolic than impactful.

## The focus on banks

There are numerous reasons why banks and credit institutions remain top of regulators' enforcement agendas globally.

Banks tend to face more enforcement actions than their counterparts due to a combination of structural, regulatory and practical factors.

These firms hold deposits, issue credit, act as clearing or correspondent institutions and are deeply interconnected with the wider financial system.

This systemic role means failures in areas such as anti-money laundering (AML), governance, risk management or liquidity can have much more wide-ranging effects, and likely trigger regulators to apply more stringent oversight.

Banks are also subject to a far broader set of obligations than most non-bank entities.

For example, far-reaching prudential rules on capital, liquidity and leverage sit alongside consumer protection, deposit insurance, AML, counter-terrorist financing (CTF) and sanctions compliance.

There is also more history in this space. Banking is one of the oldest regulated sectors, and its usage among populations certainly surpasses that of payments products or investments.

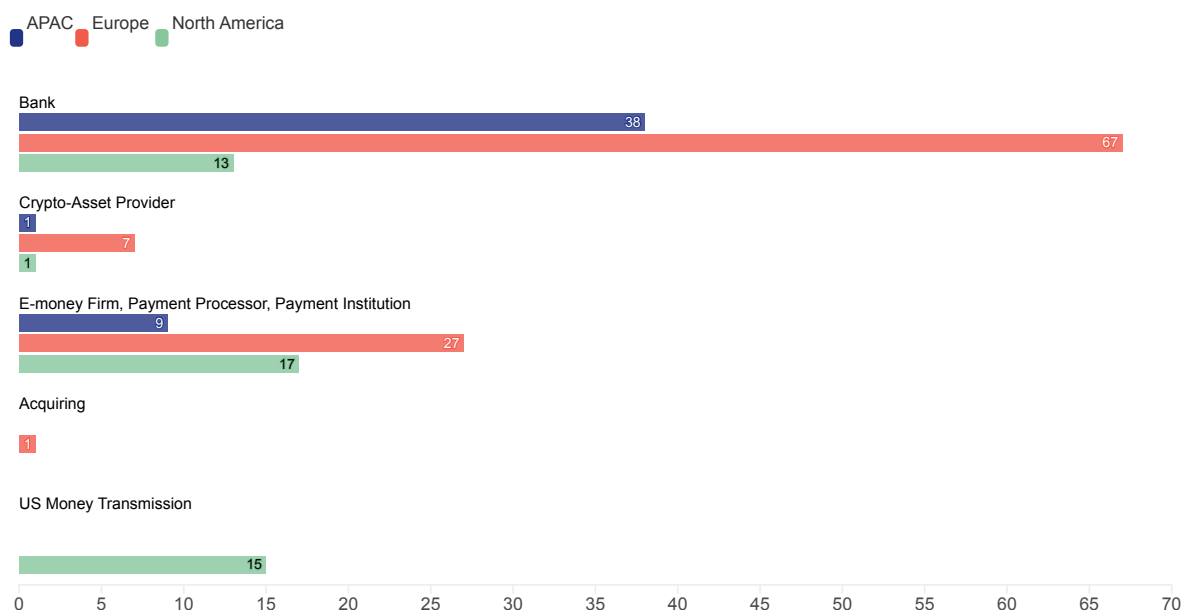
Because of this, supervisors have been able to craft and build up extensive inspection regimes, data collection tools and enforcement processes over the decades.

By contrast, non-banks such as fintechs, e-money firms or crypto businesses are often governed by newer or evolving frameworks, so enforcement has lagged behind.

In addition, regulators may have more sympathy for these much less systemic firms, or perhaps just fewer resources to take action.

Banks' scale and complexity increase both the opportunities for breaches and the chance of detection, and their systemic importance requires more frequent reporting, internal audit and compliance functions.

Fig. 6 Enforcement actions by entity type, H1 2025



This gives regulators greater visibility and more evidence to act upon. And when infractions do occur, the scale of potential harm, whether to customers, financial markets or the integrity of the system, often results in larger penalties and higher-profile cases.

## Targeting non-banks

Although it is still the case that banks face considerably more financial penalties and compliance requirements, the pattern may not last indefinitely.

As regulation of crypto-asset firms, e-money institutions and payment providers becomes sharper and more consistent, enforcement actions in those sectors are likely to rise.

Frameworks such as the EU's [Markets in Crypto-Assets \(MiCA\) Regulation](#) and the UK's Consumer Duty may end up being used to monitor and enforce more closely against firms outside the banking sphere.

Some regulators have also begun to pay more attention to payment firms and crypto-asset firms in recent years. For example, the Bank of Lithuania and Malta Financial Services Authority (MFSA) have both been active in this space.

The Bank of Lithuania is noted for its strict oversight of the Baltic country's large fintech sector.

Recent fines have included one against Paysera, which was given a [€400,000 penalty](#) for acquiring 100 percent of another e-money institution, Contis, before the end of the statutory assessment period and without regulatory approval.

Paysera had failed to supply sufficient information on the acquirers' reputation, financial reliability, AML/CTF risks, management plans and prudential compliance, leading the central bank to object to the deal.

In a [separate decision](#), the Bank of Lithuania revoked the licence of UAB PanPay Europe after finding gross and systematic AML/CTF failings, weak transaction monitoring and poor data controls, meaning the firm must cease providing financial services and return client funds.

Meanwhile, the MFSA has sent a series of Dear CEO letters targeting payments, e-money and crypto firms on matters such as misleading websites, safeguarding of funds and appropriate terrorist financing controls.

In the US, the authorities have become increasingly concerned about the role of payments firms in human and drug trafficking in the region, as a series of notices from FinCEN show.

In September 2025, for example, the agency issued two actions. First, it [re-issued](#) a modified Geographic

Targeting Order (GTO) aimed at combating cartel and other criminal activity along the southwest border.

The order requires certain money services businesses in specified ZIP codes and countries to file Currency Transaction Reports for cash transactions of \$1,000 to \$10,000, replacing the previous \$200 threshold that expired on September 9.

It also released a [notice](#) intended to help financial institutions detect and disrupt financially motivated “sextortion”. The notice explains how perpetrators, often abroad and using VPNs, target victims via social media and demand payments through peer-to-peer (P2P) platforms, money orders or convertible virtual currency kiosks.

It highlights AI-enabled image manipulation, outlines red-flag indicators for suspicious activity, and instructs institutions to include “FIN-2025-SEXTORTION” in suspicious activity reports (SARs).

The notices emphasise that payment services are under increased pressure from the US government.

The activity of regulators in jurisdictions around the world indicate both their priorities and the areas where they will continue to enforce and give firms the opportunity to remediate and solve any compliance issues before it gets to the point where they face a financial penalty.

In the coming year, things are unlikely to change much in Europe and Asia-Pacific, with enforcement likely to continue at a similar cadence.

However, firms should monitor whether the UK or EU member states decide to act over any more recent regulatory frameworks.

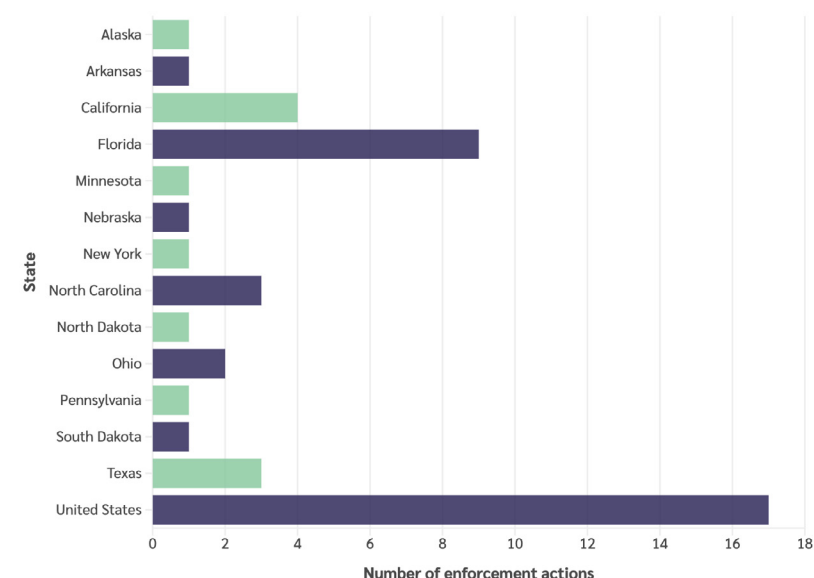
Legislation such as the Consumer Duty in the UK and the [Digital Operational Resilience Act \(DORA\)](#) in the EU provide tools for regulators to scrutinise both banks and non-banks on their compliance.

In the US, there could be a shift at the federal level, due to the change in priorities. For example, firms should be prepared to face greater scrutiny over issues such as debanking, with [reports](#) over the summer suggesting that a crackdown on this is likely.

This could mean that financial institutions face pressure in areas that were of less interest to previous administrations.

## Spotlight: US Enforcement

Fig. 7: Enforcement actions in the US by state, H1 2025



Source: Company data



During 2025 so far, there has been a striking shift in financial regulation enforcement in the US. Federal oversight has declined, with the Consumer Financial Protection Bureau (CFPB) in particular taking a step back and state regulators increasingly filling the void.

This shift is unsurprising. The Trump administration, and the Republican Party more broadly, have long opposed the CFPB and the type of enforcement action pursued under previous administrations.

Since the beginning of the second Trump administration, the CFPB has sharply reduced many of its core enforcement activities, dismissing lawsuits, reversing settlements and scaling back investigations.

The agency dropped [five enforcement actions](#) on a single day in February 2025, in what seemed a clear statement of intent. It subsequently withdrew a key consumer protection lawsuit against peer-to-peer (P2P) platform [Zelle](#).

Federal regulatory enforcement more broadly has fallen sharply, with some analyses indicating a 37 percent [decline](#) in enforcement action in H1 2025.

A visible sign of this retreat is the CFPB's [withdrawal of 67 guidance documents](#) in May 2025, including interpretive rules, policy statements, advisory opinions, bulletins and circulars.

### The rise of state enforcement

However, as the federal enforcement apparatus has retracted, state regulators have signalled their readiness to step up.

States license and supervise non-bank financial service providers, including money transmitters, digital payment apps and remittance firms. As such, they are well positioned to enforce state financial laws, and in some cases, elements of federal law where permitted.

As noted, in January 2025, 47 states plus the District of Columbia imposed an [\\$80m penalty on Block Inc.](#) over violations of the Bank Secrecy Act (BSA) and anti-money laundering and counter-terrorism financing (AML/CTF) rules. The company was also required to hire an independent consultant, report findings to states and correct deficiencies.

Separately, New York [fined Block \\$40m](#) for similar Cash App compliance failures. Wise has also faced [coordinated state enforcement](#) over AML/CTF shortcomings.

These actions reflect an organised framework of networked supervision via groups such as the Conference of State Bank Supervisors (CSBS) and the Money Transmission Regulators Association (MTRA). This allows multiple states to coordinate investigations, share resources and agree on remediation.

The rollback of CFPB guidance and interpretive rules, combined with its narrowing of enforcement priorities, creates a challenge for regulated firms.



Without strong guidance – and with many cases dropped or paused – there is less clarity about what conduct will draw enforcement action, creating both risk and opportunity for firms.

States retain broad powers under their own laws to enforce consumer finance and AML/BSA standards. More progressive jurisdictions, such as New York, that are broadly aligned with the CFPB's traditional philosophy are likely to move quickly to adopt stricter laws or interpretations.

## Fragmentation and complexity

For firms, the risk of inconsistent obligations is growing. Although the federal government has adopted a pro-business stance with a less interventionist approach to regulation, firms still face enforcement from state authorities.

A feature of the federal system is that a decision or practice acceptable in one state might be actionable in another.

This makes it vital that firms monitor not only federal regulation, but also state developments.

*“For firms, the risk of inconsistent obligations is growing.”*

Firms should be wary of responding to federal deregulation by scaling back effective and well-resourced compliance programmes.

With guidance withdrawn and federal priorities narrowed, state regulators are more likely to set their own enforcement agendas. This could lead to a more fragmented regulatory landscape, but also to legal challenges over the limits of state power.

The CFPB's enforcement pullback from both actions and interpretive guidance has opened the door for states to play a more central role. Multi-state actions, such as those against Block and Cash App, are emblematic: as the federal regulator retreats, collective state power is rising in consumer protection and AML/BSA enforcement.





## Regulatory Intelligence

### About Vixio PaymentsCompliance

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

Find out more at [Vixio.com/paymentscompliance.com](https://vixio.com/paymentscompliance.com)

#### UK Office

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

#### US Office

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

[info@vixio.com](mailto:info@vixio.com)

[Vixio.com](https://vixio.com)

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



DISCOVER



#### Disclaimer

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

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

© Compliance Online Limited (trading as Vixio) 2025