An eflow report

# 2026 Global trends in market abuse and trade surveillance

Maintaining market integrity amidst technological, economic and geopolitical shifts

# Executive summary

Welcome to the third edition of eflow's annual report on the global trends that are impacting market abuse and trade surveillance. Since we launched our inaugural report in 2024, our research has been read by more than 3,500 regulatory professionals around the world. This is not only an indication of the profession's relentless desire to build on its own expertise, but also reflects a unique period in which a diverse array of market forces have influenced regulation across financial services.

As in previous years, the report combines both quantitative and qualitative research to generate a truly holistic perspective of how firms are adapting to the challenge of preventing market abuse. Global enforcement statistics provide a useful backdrop to how regulators are holding firms to account. However, I always find that it's the insights we gather from interviewing more than 300 regulatory professionals that add an extra layer of context that numbers alone cannot provide.

This year's findings indicate this more strikingly than ever. On the face of it, financial penalties issued to firms for market abuse-related failures fell to their lowest annual level since 2019, at $310m. However, based on commentary provided by senior compliance professionals at organisations ranging from tier one banks to specialist investment firms, regulatory scrutiny remains a consistent and evolving pressure.

Some of the most eye-catching headlines that we explore throughout this report include:

- The use and adoption of AI has emerged as the dominant compliance risk for firms, cited by 69% of regulatory professionals. Regulatory uncertainty (65%) and geopolitical instability (54%) remain areas of concern, echoing last year's research.

- In relation to market abuse specifically, more than half of firms (53%) said that keeping pace with regulatory change was the concern that kept them up at night, highlighting the rapidly evolving backdrop that firms need to navigate.

- Despite the seemingly relentless integration of AI into so many aspects of our personal and professional lives, its use in the context of trade surveillance remains immature. Only 16% of firms have AI fully deployed as part of their trade surveillance strategy, while 29% say that they don't have a formal strategy in place or don't plan to use it at all.

When all of these factors are combined, it's difficult to overstate just how challenging it is for firms to navigate the current regulatory landscape. And this is before you consider the global impact of President Trump's second term in office and his administration's unpredictable approach to global trade, digital assets and regulation.

As I said in last year's executive summary, predicting the future is a dangerous game at the best of times, let alone against a backdrop of rapid technological evolution, significant market volatility, and a geopolitical climate that shifts from week to week.

Having said that, there are some clear trends that I expect to emerge or continue to develop over the next 12 months. These include:

- Enforcement action will continue to increase. Between 2019-2023, the annual volume of global enforcement fines was consistently beneath 50. In each of the last two years, that number rose beyond 100 as regulators switched their attention to smaller firms and high frequency enforcement. We expect this trend to continue as AI-assisted supervision and increased collaboration enables investigations to be progressed more efficiently than ever before.

- Cross-market surveillance will become a shared supervisory capability as new analytical approaches and improvements in investigative techniques enable firms to detect it consistently. While I don't envisage a sudden enforcement surge, I do expect cross-market surveillance to move beyond isolated breakthroughs.

- AI will resolve the build vs buy debate when it comes to trade surveillance technology. For years, firms have deliberated as to whether to build surveillance systems in-house or partner with a specialist vendor. While AI, in theory, enables firms to build their own technology more efficiently, the reality is that enterprise-grade deployment will increasingly tilt toward specialist partners able to deliver not just capability, but assurance and control.

Having been part of the regulatory scene in various guises for over 20 years, the pace of change seems to accelerate every year. However, one fact does remain constant – the role of regulatory professionals in maintaining market integrity is more important than ever.

**Ben Parker**

Chief Executive and Founder, eflow

# Contributors

## Ben Parker | eflow CEO & Founder

Ben Parker is CEO and Founder of eflow, one of the world's leading RegTech providers. Ben is an expert in financial services regulation and has a wide range of experience in tackling market abuse and developing the latest advances in trading surveillance. Having recognised the growing regulatory pressures that compliance professionals are facing, Ben's mission at eflow is to create a new standard for digital infrastructure that can allow businesses to get one step ahead.

## Alex Parker | Chief Technology and Product Officer & Founder

Alex is eflow's Chief Technology and Product Officer, as well as one of eflow's founders. In his role, Alex oversees eflow's team of dedicated product and infrastructure specialists, keeping abreast of the latest technological advancements and regulatory changes. Alex draws from more than 20 years of experience spanning digital infrastructure, consultancy services, and business analysis, having worked for firms based in both the UK and Australia.

## Nathan Parker | Industry Expert

Nathan is a thought leader in RegTech, FinTech, and Web3, with a track record of delivering high-impact research for global technology vendors and regulators. His expertise has been instrumental in helping RiskTech and RegTech firms develop and launch innovative solutions, ensuring market success both domestically and internationally.

## Michael Lawrence | Industry Expert

Michael is a technology researcher specialising in AI, risk, and compliance. Since 2017, he has focused on the RegTech market, advising major regulators and financial institutions on technology strategies, serving as a Product Manager for a digital marketplace for RegTech solutions, and producing extensive thought leadership. In 2024, he founded a boutique research firm to continue delivering deep industry insights.

Part 1

# The global backdrop

2025 was an unpredictable and volatile year. Markets were impacted by a constant churn of events – international conflicts, shifting trade dynamics, election cycles and uneven monetary policy – some persistent, others fading almost as quickly as they emerged. For firms, this made conditions difficult to interpret and even harder to plan against, creating a persistent sense of uncertainty that continues to influence risk decisions into 2026.

At the same time, the industry reached a technological inflection point. What many describe as a fourth industrial revolution is taking practical shape as artificial intelligence moves from experimentation to operationalisation across front, middle and back-office functions. Its potential utility in trade and communications surveillance is becoming clearer, but firms are grappling with how to govern it effectively to enable safe, scalable adoption.

For regulators, 2025 was a year of recalibration. Growth and risk agendas began to compete more visibly, particularly in major financial centres. But while the regulatory tone softened rhetorically toward simplification, competitiveness and innovation, market integrity remained a core focus area – and is still the backbone of well-functioning markets.

> *"There was a long period of stasis in this industry – things didn't really move until they had to. Now the pace of change has ramped up significantly."*
>
> ***Head of Trade Surveillance, Tier 1 Bank***

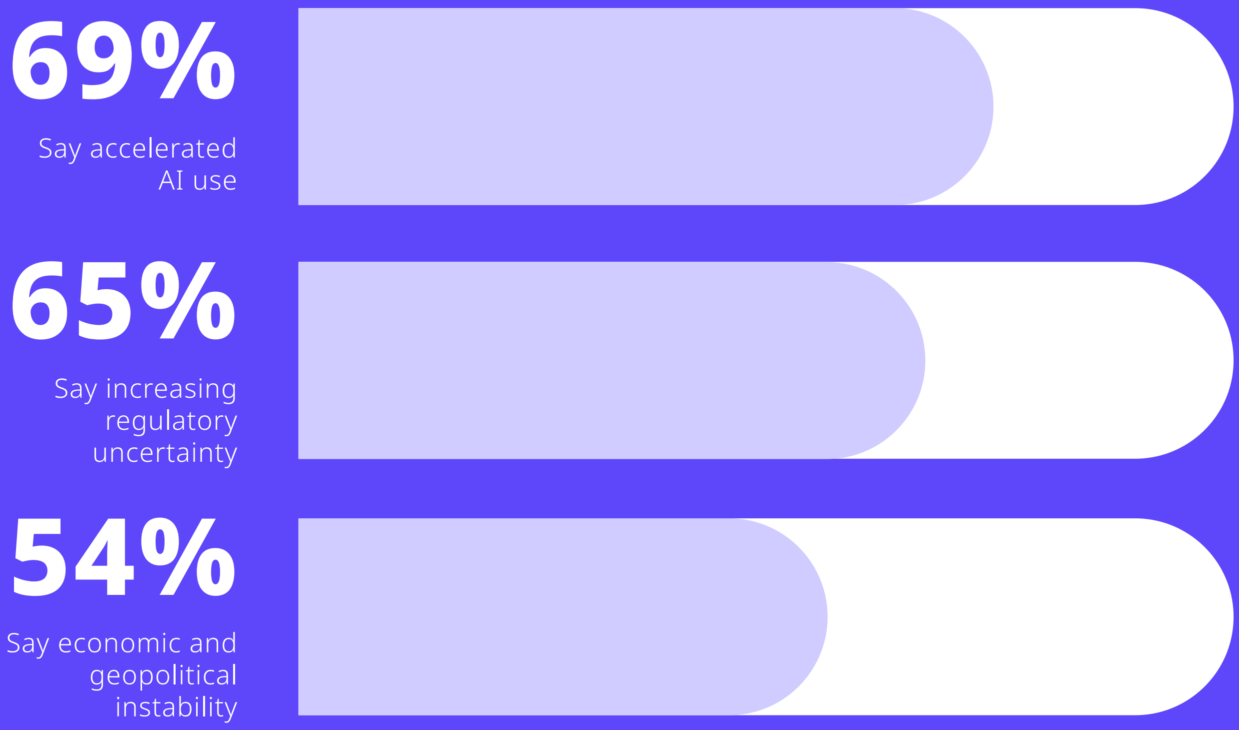
From an enforcement perspective, 2025 appeared to be a year of deceleration. Total fine values dropped to $310 million from a multi-billion dollar high in the previous year. However, to view this as a softening of the regulatory stance is to fundamentally misread the landscape. Instead, it signals a reprioritisation of enforcement effort. Supervisors have actively cleared a pipeline of smaller cases – often involving mid-tier firms and technical breaches – while concentrating resources on complex, high-impact misconduct.

Rulemakers are leaning more heavily into data-driven oversight and artificial intelligence, and as monitoring capabilities become more agile and incisive, scrutiny is intensifying, and pressure on firms to strengthen surveillance and risk management frameworks continues to build.

This outlook is echoed by compliance leaders across the world:

***Which market forces are most likely to cause compliance challenges in 2026?***

*Taken from eflow's global survey of 300 compliance decision makers.*



Part 2

# Historical market abuse enforcement (2019-2025)

## Quantitative overview

441

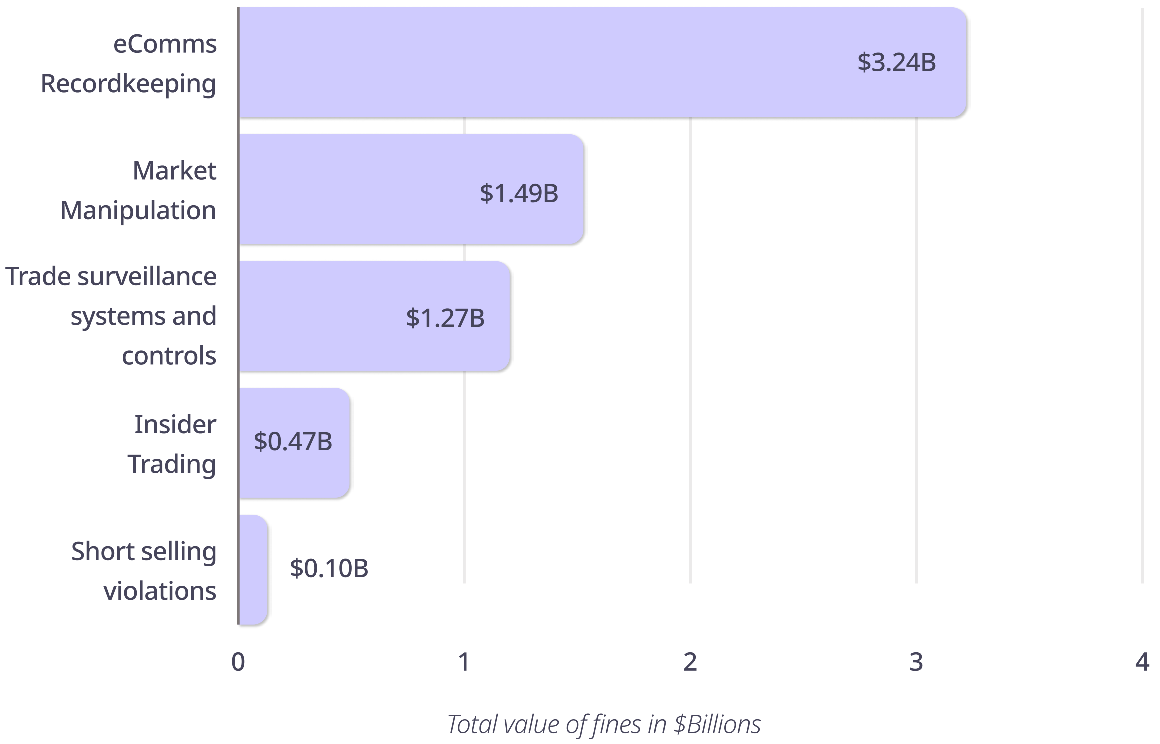
Total number of fines issued

$6.6bn

Total financial penalties issued

Market abuse is one of the most heavily regulated and actively enforced areas of financial regulation. Between 2019 and 2025, regulators issued 441 fines totalling $6.6 billion across multiple enforcement typologies. Notably, the majority of penalties arose from failures in surveillance, controls, and supervisory systems rather than isolated instances of misconduct. This underscores the systemic and operational focus of modern market abuse enforcement. These figures also exclude the substantial internal costs of remediation and ongoing compliance.

MARKET ABUSE ENFORCEMENTS BY TYPOLOGY - WHOLE PERIOD (2019-2025)



## Typology definitions

**eComms recordkeeping:** Any failure to record, monitor or analyse electronic communications.

**Insider trading:** The possession and use of confidential, non-public information, providing an unfair advantage when trading financial instruments.

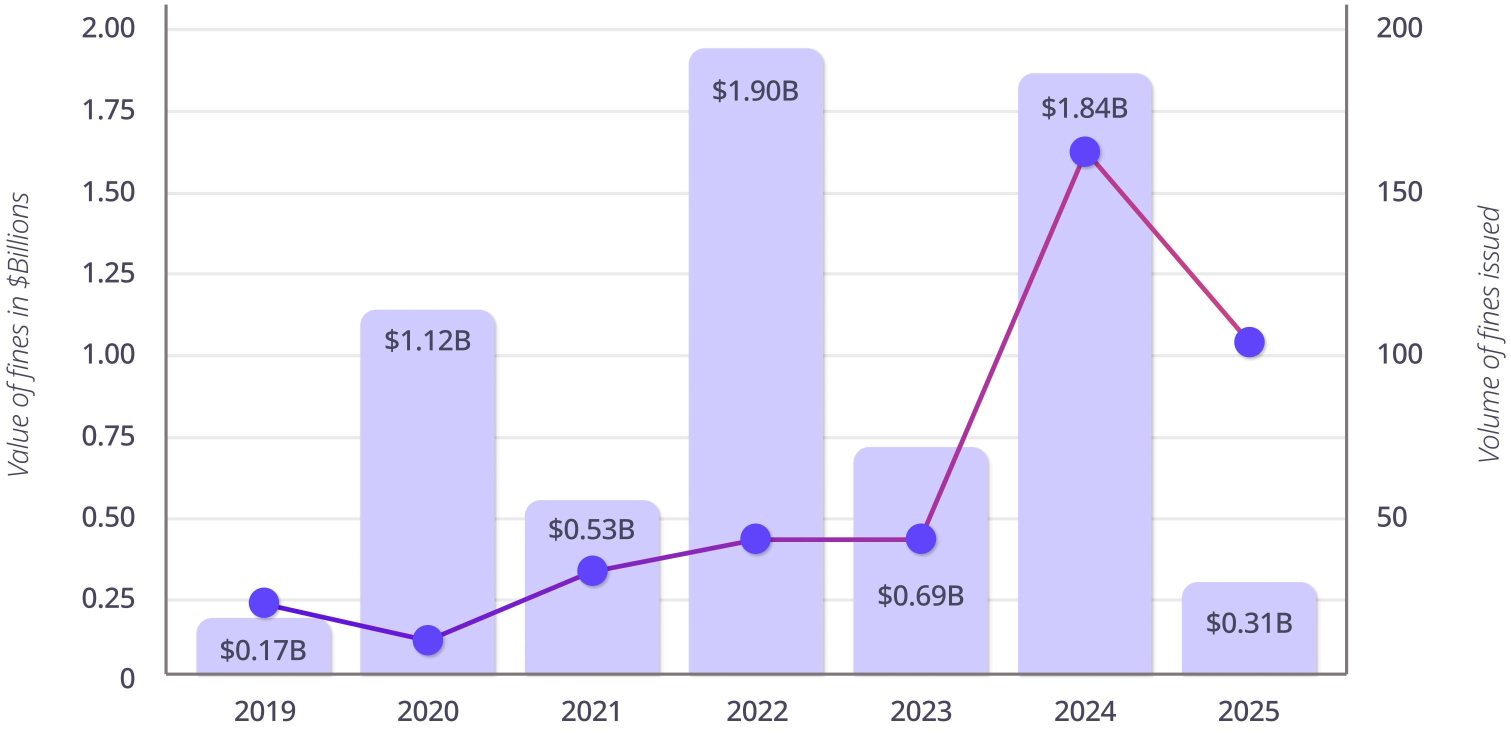
**Trade surveillance systems and controls:** Deficiencies in data, systems and controls required to monitor trading activities.

**Market manipulation:** The deliberate attempt to alter the free and fair operation of a market to create false/misleading appearances with respect to the price of an asset.

**Short selling violations:** Any transaction that breaches regulations regarding short selling.

## Annual enforcement trends

ANNUAL ENFORCEMENTS - VALUE VS VOLUME



The recent decline in the aggregate value of market abuse enforcement should not be interpreted as a reduction in regulatory scrutiny or ambition. Instead, it reflects the inherently uneven nature of enforcement outcomes, which are often driven by the timing and resolution of a small number of exceptionally large, complex cases rather than by fluctuations in underlying regulatory activity.

Historically, high-value enforcement years have typically been shaped by one or two outsized actions, while lower-value years reflect the absence of such cases rather than a slowdown in investigative effort. Large market abuse investigations are resource-intensive, frequently multi-year in duration, and require sustained coordination across supervisory, enforcement, and legal teams. As a result, enforcement values naturally oscillate as major cases are built, prosecuted, and ultimately finalised.

At the same time, enforcement capacity is finite. Periods of intense focus on large-scale investigations can temporarily constrain the regulator's ability to bring other major cases to conclusion, contributing to apparent lulls in headline enforcement values even as underlying risks continue to accumulate. This effect was reinforced in 2025 by broader institutional and political dynamics, including regulatory recalibration and operational disruption, without altering the long-term enforcement trajectory.

Importantly, this year's lower aggregate enforcement value sits alongside one of the highest volumes of enforcement actions on record. Regulators remain highly active, deliberately pursuing a larger number of smaller and mid-sized cases in order to free up capacity for future large-scale actions.

> *"I'm not sensing any deregulation at all. If anything, recent examinations have intensified. Regulators are more focused now – they know exactly which questions they want to ask."*
>
> ***Head of Surveillance, Global Bank***

## Case study: enforcement lag and resource allocation

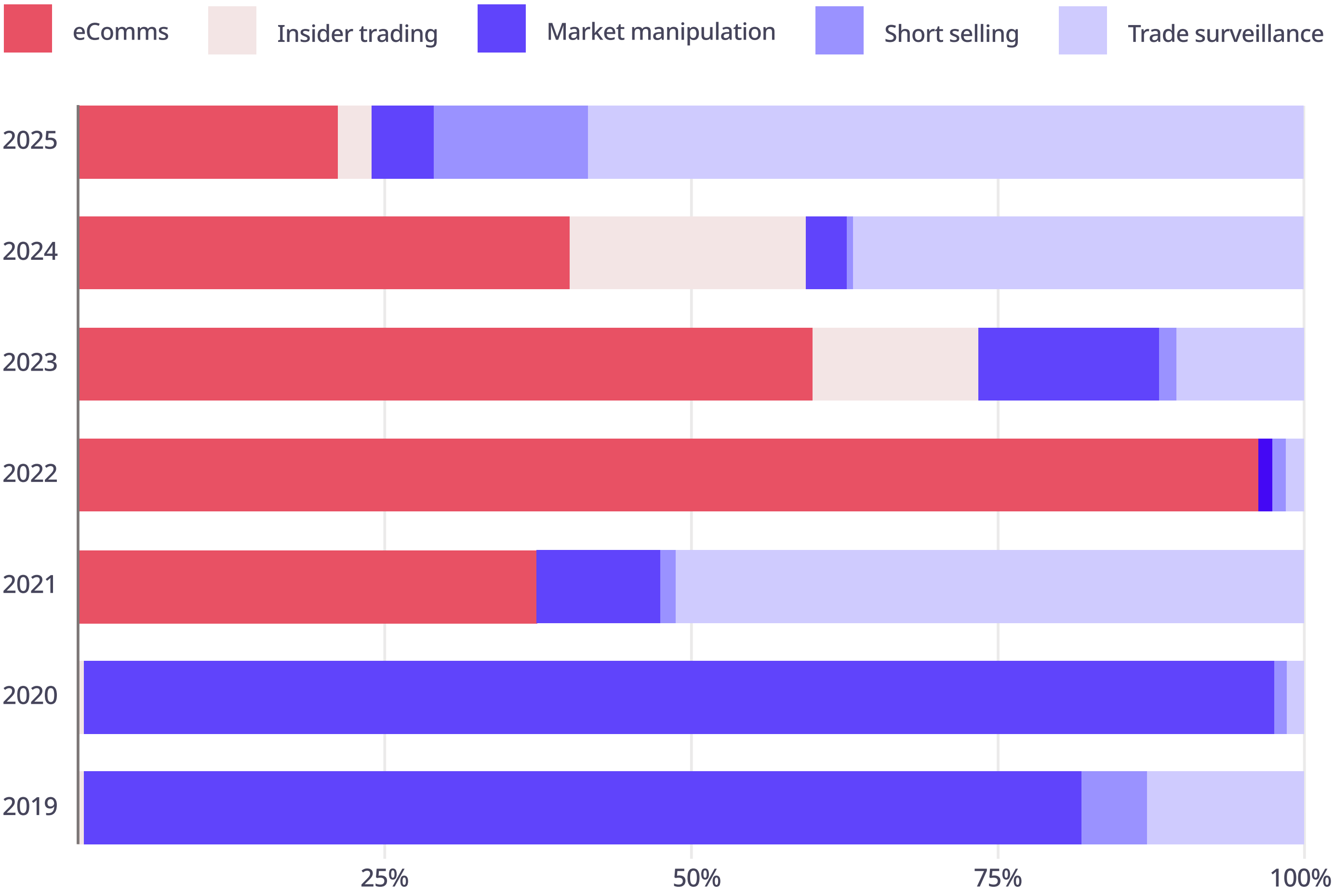
These dynamics are well illustrated by one of the largest joint market abuse enforcement actions finalised in 2024, arising from a coordinated regulatory crackdown against 26 firms on off-channel electronic communications. In this instance, enforcement outcomes were finalised and announced in August 2024, but the timing of those actions was largely incidental. The underlying investigations had begun much earlier, with multiple firms brought under scrutiny between September 2021 and October 2022 as part of a coordinated supervisory initiative.

Crucially, the investigations did not begin because the misconduct had newly emerged. The behaviour had been widespread and long-standing, with evidence in some cases dating back as early as 2015, awaiting discovery. Hence, the timing of eventual enforcement actions in 2024 did not reflect a sudden spike in misconduct or scrutiny, but the culmination of years of investigative effort, data review, and enforcement coordination across a large population of firms.

### Implications

Seen in this context, a year with fewer large enforcement outcomes does not signal reduced regulatory risk. If anything, it points to enforcement pressure being deferred rather than dissipated. Low enforcement today may imply higher enforcement tomorrow, and now is not the time to step back from modernising surveillance - in fact, it’s quite the opposite.

PERCENTAGE BREAKDOWN OF ENFORCEMENTSBY TYPOLOGY YEAR ON YEAR



In its 2026 annual regulatory oversight report, FINRA warned of serious, continued deficiencies in firms' trade surveillance frameworks. It is therefore no surprise that enforcements in that area continued to dominate in 2025, accounting for over 50% of the total enforcement value. Notably, short selling violations accounted for a larger share of annual enforcement than ever before, driven, in large part, by ASIC's first ever fine in this area.

Part 3

# 2025 enforcement deep dive

> *"2025 was less about going after the biggest firms with headline fines, and more about higher-frequency enforcement across smaller firms. The focus is still very much there."*
>
> ***Head of Surveillance, Global Bank***

**105**

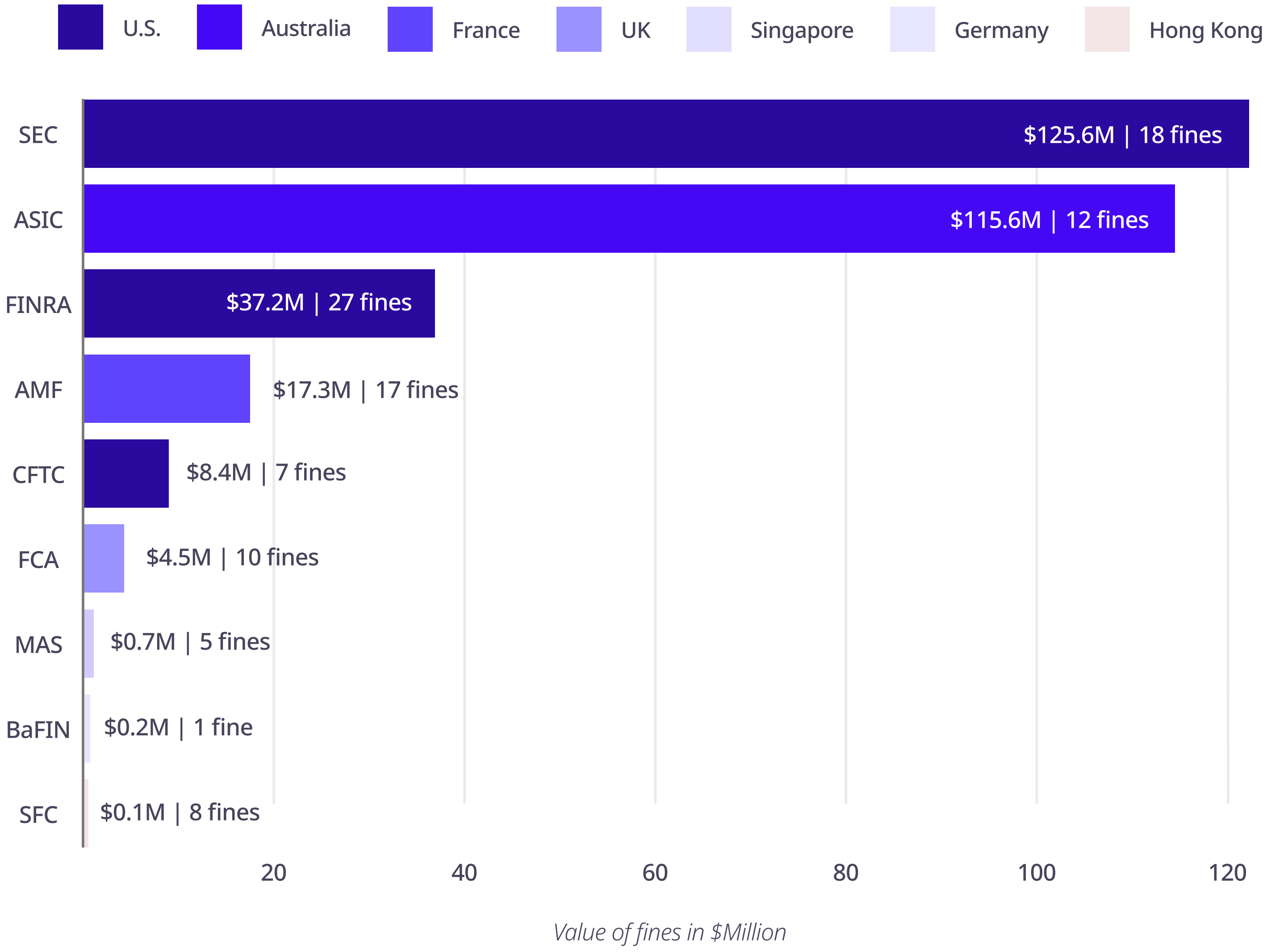
Total number of fines issued

**$310M**

Total financial penalties issued

Once again, U.S. regulators were most active in 2025, accumulating $170 million in fines across 52 closed cases. However, unlike previous years, there is significant representation of other regulators toward the top of this list. Namely, ASIC had a record-breaking year of enforcement, spurred by an $80 million penalty against ANZ for trading misconduct. Similarly, AMF more than doubled their annual enforcement value, overtaking CFTC in 2025.

## 2025 ENFORCEMENT VALUE AND VOLUME BY REGULATOR

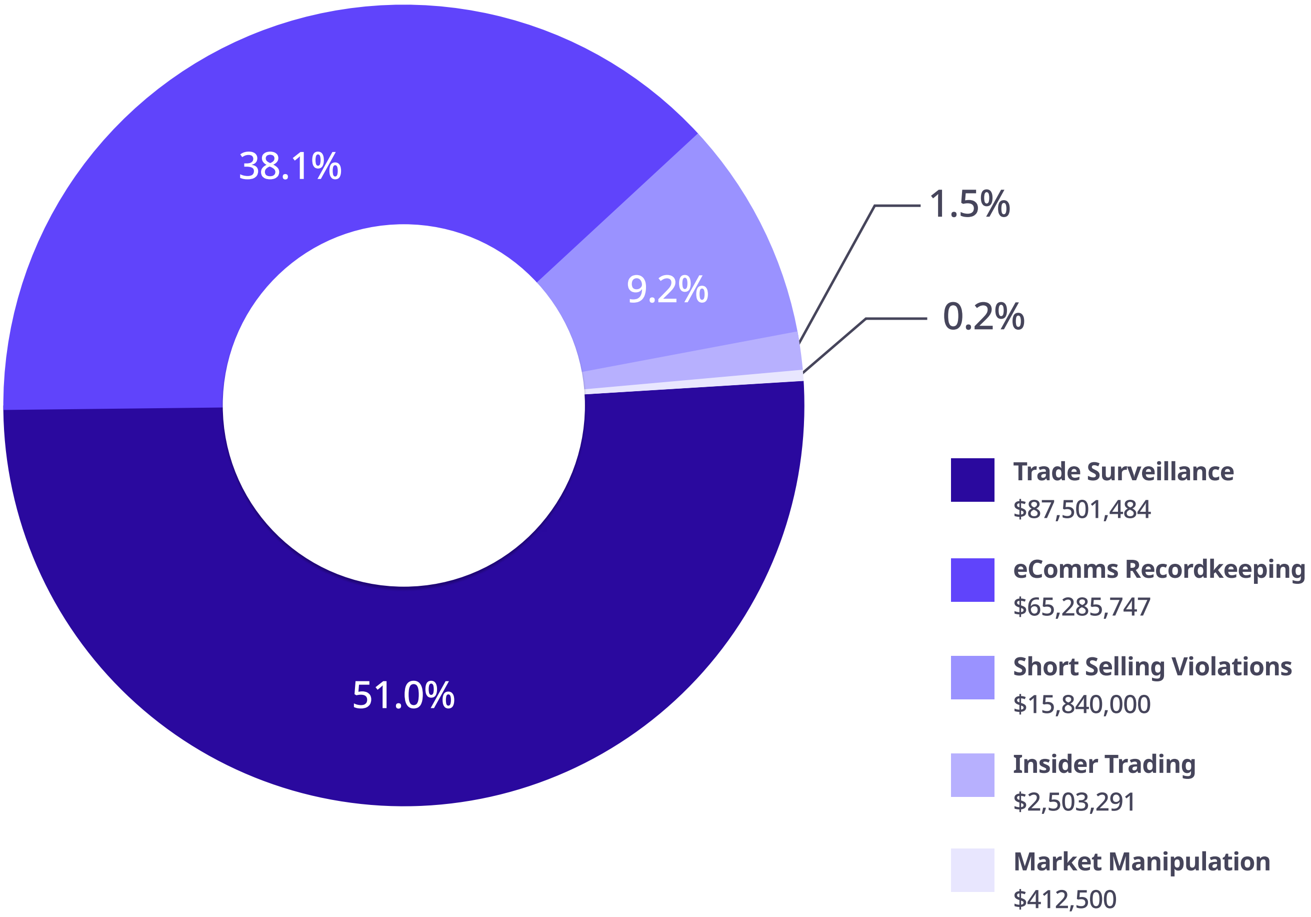


With their increased activity, and a drop in closed enforcements in the U.S., Australia and France had the highest enforcement value per dollar of market capitalisation.

# 2025 enforcements by region

## United States

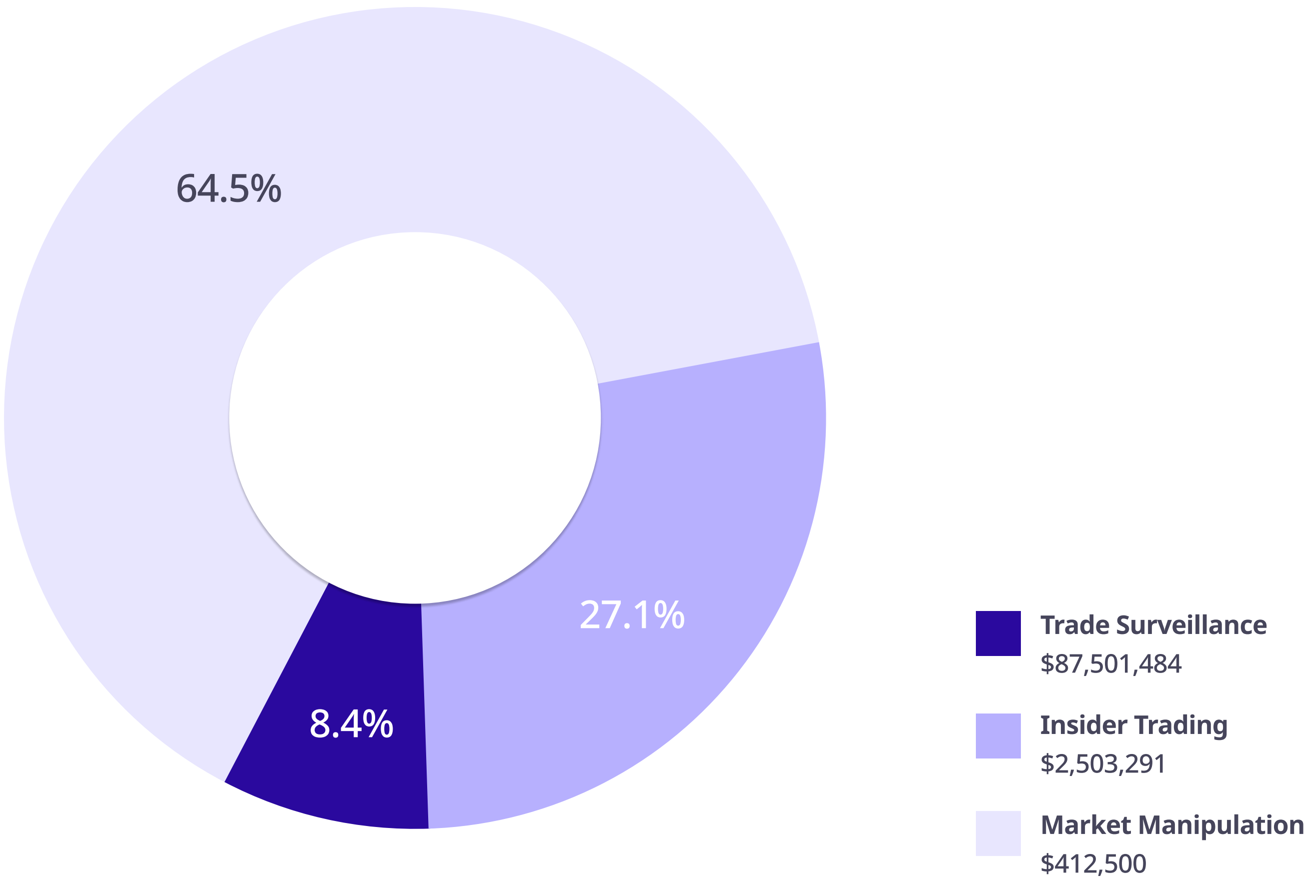
### BREAKDOWN OF U.S. ENFORCEMENT BY TYPOLOGY



For the second year running, the U.S. stands out for having recorded fines in all of our five regulatory typologies, reflecting its mature enforcement approach. This year, trade surveillance and eComms recordkeeping enforcements far surpassed all others in the U.S., and coincided with a key survey result: that U.S. respondents were by far the most likely (58%) to say that integrating trade and eComms surveillance is among the main challenges keeping them up at night.

## Europe

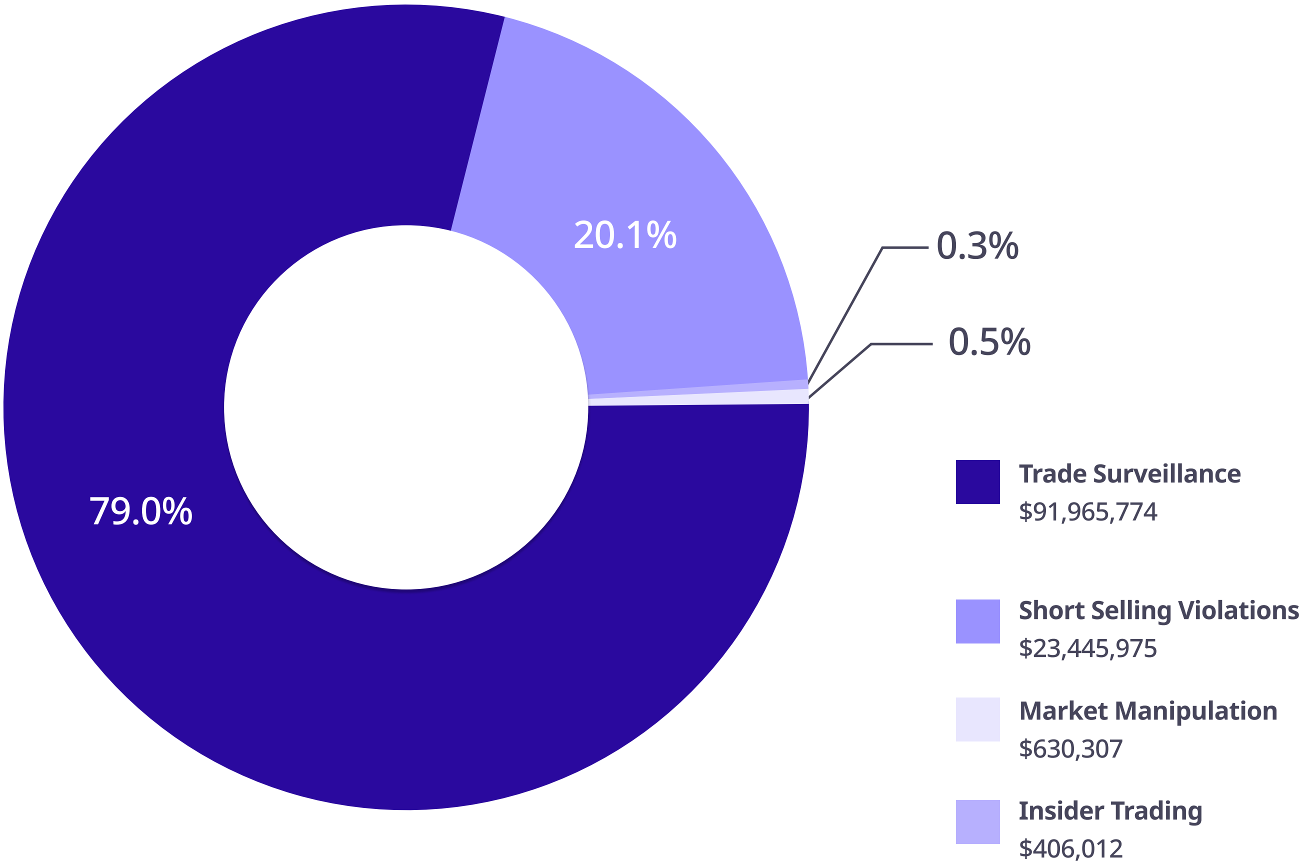
BREAKDOWN OF EUROPEAN ENFORCEMENT BY TYPOLOGY



Despite having a much smaller overall value, Europe was able to close a higher value of enforcement against serious, proven cases of market manipulation and insider trading than the U.S. This highlights a difference in enforcement priorities, which appear to be cyclical rather than structural given the year-over-year fluctuations. Again, practitioners in these regions are feeling this pressure – in our survey, European respondents were most likely to say that accurately identifying insider trading and market manipulation is the number one challenge keeping them up at night.

## APAC

### BREAKDOWN OF APAC ENFORCEMENT BY TYPOLOGY



Australia led a break-out year for enforcement in APAC, with higher total fines than any other region in trade surveillance and short selling violations. This not only stands out compared to other regions, but also when compared to itself just one year prior when annual trade surveillance fines were less than $6 million and there were no recorded short selling violations.

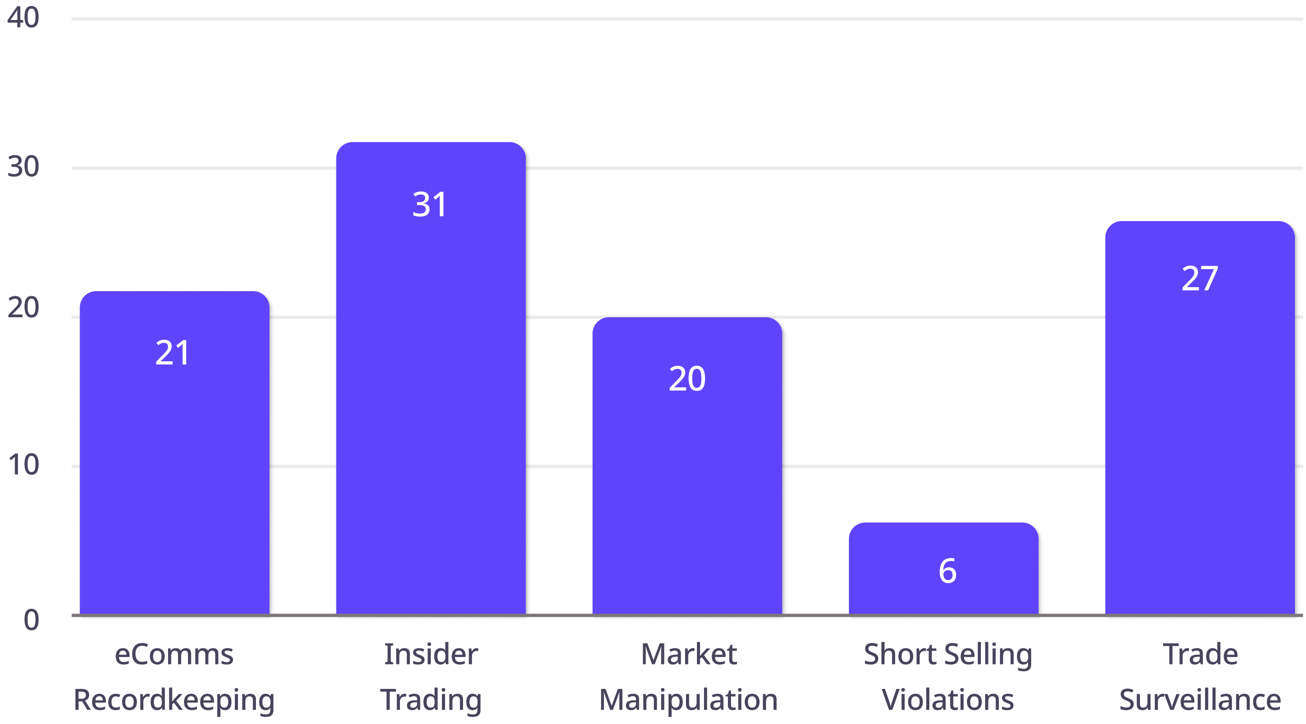
Part 4

# Market abuse typologies:

## Patterns, complexity and detection challenges

The 2025 enforcement profile highlights continued regulatory focus on surveillance effectiveness, insider dealing, and market manipulation. While familiar typologies remain prominent, supervisory attention is increasingly shifting toward control failures and more complex abuse patterns.

2025 ENFORCEMENTS: VOLUME BY TYPOLOGY



## The market manipulation playbook

> *"Market abuse isn't black and white anymore. Traders and firms are finding new, more nuanced ways to do things they shouldn't be doing – and surveillance has to evolve to keep up."*
>
> ***Head of Trade Surveillance, Tier 1 Bank***

Identifying genuine market manipulation remains one of the most persistent and technically demanding challenges for compliance teams. We are seeing a continued push for better detection of more complex, pattern-driven and cross-market behaviours.

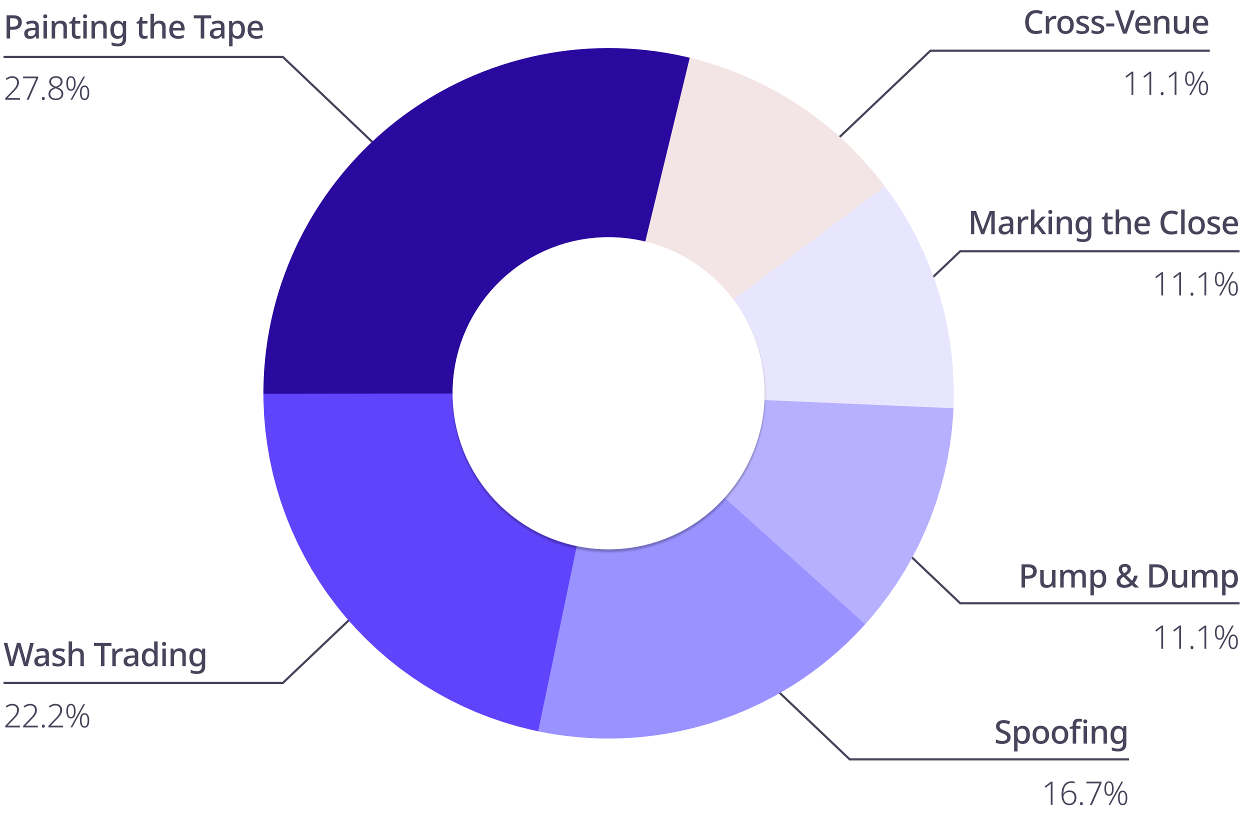
**42% of leaders say accurately identifying insider trading and market manipulation is what keeps them awake at night.**

### Proportion of market manipulation enforcements by subcategory

Viewed in aggregate, enforcement activity continued to cluster around well-established manipulation typologies like wash trading, marking the close, spoofing, and pump-and-dump schemes.

These cases were geographically dispersed across Asia-Pacific, Europe, and North America and largely reflect familiar, single-instrument patterns of misconduct that firms have long sought to address through traditional trade surveillance frameworks.

2025 ENFORCEMENTS: VOLUME BY TYPOLOGY



## Case study: Cross-border manipulation via reference price distortion

Two of the year's most technically intricate enforcement actions were issued by France's AMF. The first, a €10 million **fine** levied against U.S.-based fund EcoR1 Capital and its director. The case highlights how dual listings can create cross-border vulnerabilities when pricing in one market directly feeds into issuance terms in another.

The misconduct centred on Innate Pharma, primarily listed on Euronext Paris, which launched a Nasdaq ADS offering in 2019. The ADS subscription price was mechanically set using the five-day average of Innate's Paris closing price. During this window, EcoR1 sold heavily into the close on Euronext Paris, depressing the reference price and thereby lowering the ADS subscription price. This allowed the fund to acquire ADSs in the U.S. at an artificially reduced cost, exploiting the pricing link between the two markets.

## Case study: Cross-venue and cross-product manipulation via linked product pricing

Then, in February, **the AMF** concluded an enforcement action involving cross-product, cross-venue price manipulation.

The underlying shares were primarily listed on Euronext Paris, which served as the reference market for related warrants. However, equity trades were placed on German secondary venues outside Paris trading hours, during periods when prices from those venues were used as inputs for warrant valuation models. In each sequence, a trader would place share orders to move the underlying price, then exploit the temporary price shift to generate rapid profits in the linked warrants before prices reverted.

Cross-product and cross-venue manipulation remains the Achilles' heel of trade surveillance systems. It exploits structural gaps between venues, instruments, and pricing mechanisms, making it extremely difficult to detect.

> *"Cross-product manipulation is difficult because you first need to know which instruments are actually related – and that mapping constantly changes...this isn't like looking at one order book on one venue. You're trying to link behaviour across products, venues, maturities, and strategies – it's not black and white."*
>
> ***Head of Trade Surveillance, Tier 1 Bank***

**31% of leaders say cross-product and/or cross-venue manipulation keeps them awake at night.**

## Detecting cross-venue manipulation: Learnings from the AMF

Last year, we recognised regulators' ambition to improve detection of cross-asset and cross-venue abuse. Supervisors have since made significant investments in advanced analytics, including network analysis and cross-asset visualisations, alongside enhanced monitoring of fixed income and commodities markets to strengthen market integrity.

This year, the AMF has most clearly demonstrated how that ambition translates into enforcement. Both of the standout manipulation cases discussed above originated in France, with the second revealing a particularly sophisticated investigative approach.

Rather than starting with the equity orders themselves, the AMF worked backwards from suspicious warrant profits to cross-venue equity order behaviour.

### How the AMF identified the misconduct

- **Sequence-based pattern detection:** the AMF became suspicious of a group of traders making very fast profits on warrants late in the day, and those profits only happened when the share price briefly moved in a certain direction and then quickly snapped back.

- **Cross-venue causality analysis:** the AMF linked temporary best bid/offer shifts on German venues – driven almost entirely by one trader with extremely high cancellation rates – to downstream warrant pricing and profits.

- **Mechanical monetisation proof:** by combining timestamps, order-book states, and issuer pricing logic, the AMF demonstrated a closed profit loop (equity orders-  mid shift-warrant repricing-profit-order cancellation) repeated 250 times.  Those fake share orders briefly nudged prices just enough for warrant prices to change, the warrants were sold for a profit, and then the fake orders were pulled so prices went back to normal.

This heightened enforcement focus may also explain regional sentiment. French respondents reported the highest level of concern around cross-product and cross-venue manipulation (35%).

### Our takeaways

- Regulators are becoming increasingly adept at piecing together complex, cross-venue and cross-product behaviours, even where traditional surveillance tools fall short.
- Firms should not underestimate the value of seemingly "simple" internal alerts. In this case, the investigation began with a basic flag on unusual, repeated profitability.

> *"Bad actors don't trade in silos – and surveillance frameworks can't operate like this either. The question regulators are asking is: have you taken reasonable steps to see the full picture?"*
>
> ***Ben Parker - CEO, eflow***

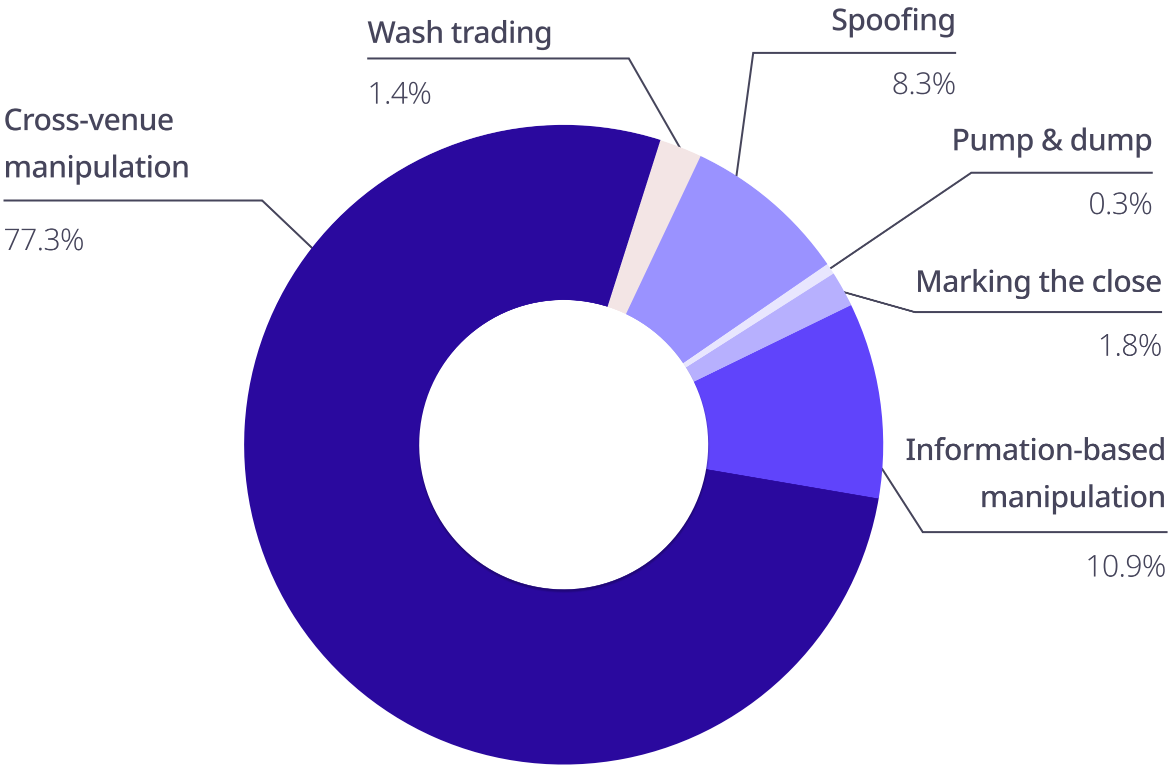
## Value of market manipulation enforcements by subcategory

Enforcement volume remained high in 2025, but overall value dropped significantly. This is largely a result of a disproportionate number of high-impact criminal convictions against individuals (70% of cases) – many of which had no associated financial penalty – rather than broad enforcement escalation against institutions.

The two aforementioned cross-venue enforcements represent the highest value market manipulation penalties this year. Outside of those, the actions completing the top five were:

- **FCA**: £381,000 in combined fines imposed on three individuals for spoofing in Italian government bond futures.
- **MAS**: S$440,000 in civil penalties levied against five individuals for painting the tape and unauthorised trading in equities.
- **MAS**: S$350,000 civil penalty imposed on a single individual for marking the close through repeated false equity trades.

2025 ENFORCEMENTS: VALUE BY TYPOLOGY

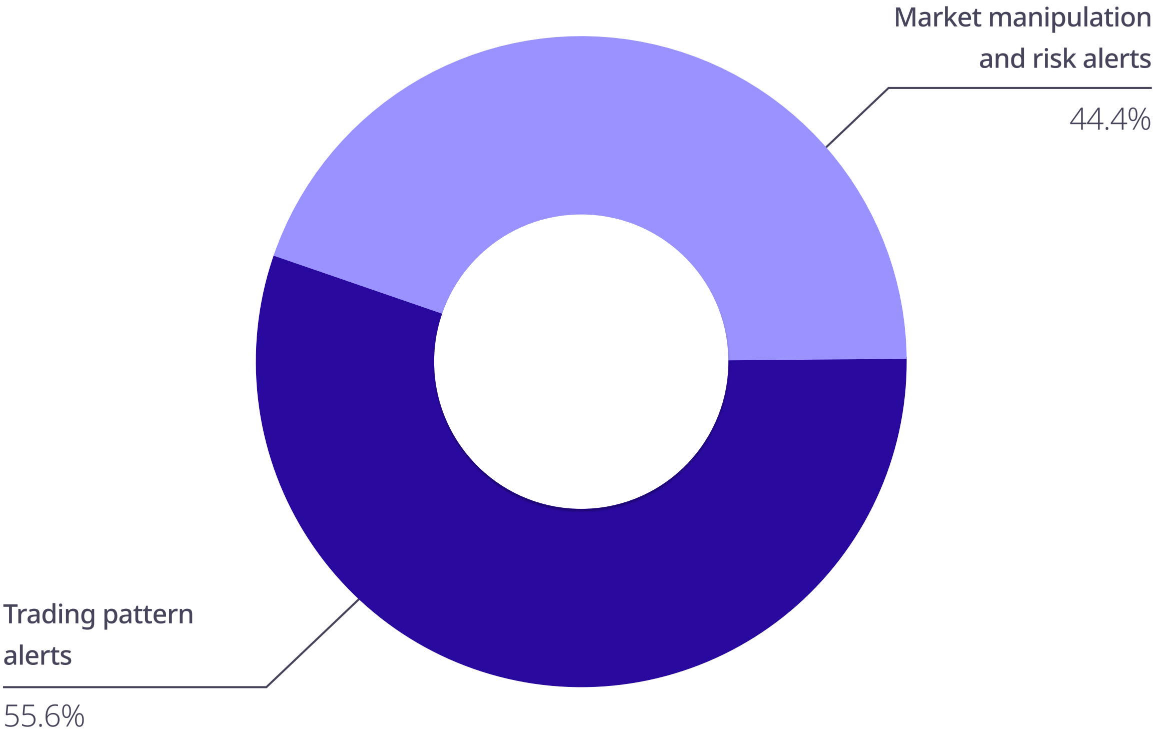


## Volume of static risk flags vs. pattern-based manipulation

Market manipulation risk alerts (MMR) represent defined market abuse or risk typologies (e.g. spoofing, wash trading, front running). Some can be triggered by a single event, others still rely on short-horizon pattern recognition. The defining feature is that these alerts map directly to a recognised form of manipulation or regulatory risk.

Trading pattern (TP) alerts identify behavioural trading patterns over time (e.g. marking the close, ramping, churning) that may not be explicitly illegal in isolation, but become suspicious when sequencing, timing, or repetition creates a misleading market signal.

TRADING PATTERN VS MMR ALERTS



### Data considerations

MMR alerts depend on high-quality point-in-time data, including orders, executions, prices, volumes, ownership links, and venue identifiers, with sufficient precision to assess size, structure, and proximity at the time of the trade.

TP alerts require richer historical and contextual data, including full order-lifecycle data, high-granularity timestamps, market data across extended time windows, participant identifiers, and often volatility or benchmark data to distinguish manipulation from normal market behaviour.

### Technology considerations

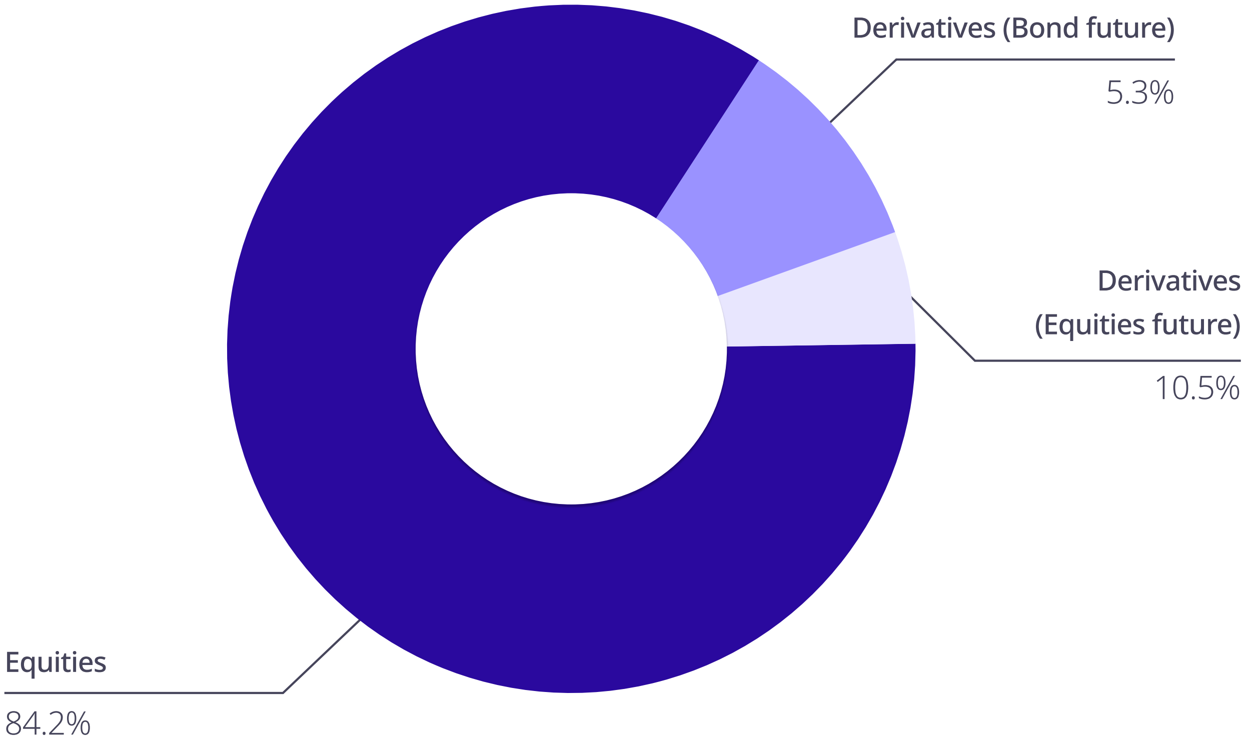
MMR capability is typically driven by deterministic rule engines with configurable thresholds, instrument banding, and cross-venue awareness, optimised for low latency and precision.

TP capability requires stateful analytics that aggregate behaviour over time, dynamically adjust thresholds, and manage complex alert logic at scale. Without this, firms either miss subtle manipulation or generate unmanageable levels of noise.

### What it means for surveillance teams

Firms should assess whether their trade surveillance frameworks are designed to flag known risks and are capable of detecting evolving, pattern-based manipulation that increasingly drives regulatory concern.

## Volume of market manipulation enforcements by asset type



Enforcement outcomes in 2025 remain heavily concentrated in equities, reflecting the depth, liquidity, and regulatory maturity of equity markets rather than the exclusive presence of misconduct. Derivative-related cases account for a smaller share of concluded actions, often where pricing is tightly linked to underlying equity markets.

# Insider trading

Insider trading is an area of intense and sustained supervisory pressure, but enforcement action is proving to be episodic rather than continuous, with total penalty values frequently driven by one or two outliers.

This is evident in the data. In the United States, enforcement volume under the SEC remained flat year-on-year, while total penalties fell sharply from approximately $250m to $2.5m. In Hong Kong, the lower enforcement value in 2025 follows a prior year dominated by a single high-value action.

2025 INSIDER TRADING ENFORCEMENTS BY REGULATOR YEAR ON YEAR

| Region | Regulator | 2024 Volume | 2024 Value | 2025 Volume | 2025 Value |
|---|---|---|---|---|---|
| Australia | ASIC | 1 | $0 | 4 | $194,182 |
| France | AMF | 3 | $630,290 | 14 | $4,695,808 |
| Germany | BaFIN | 1 | $554,750 | - | - |
| Hong Kong | SFC | 5 | $48,451,805 | 3 | $66,428 |
| Singapore | MAS | 1 | $51,836 | 2 | $145,402 |
| United Kingdom | FCA | 5 | $155,264 | 6 | $1,849,773 |
| United States | CFTC | 3 | $55,843367 | - | - |
| | FINRA | - | - | - | - |
| | SEC | 3 | $249,923,740 | 3 | $2,503,291 |

Enforcement statistics can materially understate risk. As noted last year, actual insider trading activity may be up to four times higher than the number of prosecuted cases, reflecting structural limits in detection and enforcement rather than low underlying misconduct.

Supervisory indicators reinforce this concern. The FCA's latest market cleanliness (MC) assessment shows continued anomalies, with 2024 figures above the five-year moving average. While not conclusive, persistent abnormal price movements ahead of announcements remain a useful proxy for potential insider trading.

Reporting trends point in the same direction. In 2024, the FCA received an outsized proportion of insider trading STORs relative to overall submissions: of 4,528 reports, 3,495 related to insider dealing and 581 to market manipulation.

## Regulator focus is shifting upstream: Information leakage and unlawful disclosure

Regulators are increasingly concerned not just with trading outcomes, but with how sensitive information escapes control in the first place, particularly during M&A activity. The FCA has highlighted multiple leakage vectors, including deliberate tipping of the press by individuals at issuers or their advisers, as well as inadvertent disclosure through careless "hinting" of market-sensitive information.

The FCA also signalled heightened risk amongst corporate finance firms that often hold highly price-sensitive information for extended periods. This elevates the risk around market soundings – interactions between issuers and investors used to gauge interest ahead of an announcement.

Similar concerns are clear in Asia; the SFC has called out market soundings as a core market abuse risk, introducing guidelines in 2025 that emphasise information flow control, senior accountability, and communications surveillance.

## Market sounding control expectations (FCA & SFC)

### Information handling and access

- Restrict market-sensitive information to authorised staff on a need-to-know basis
- Apply effective information barriers and prevent unauthorised disclosure or leakage
- Maintain accurate insider lists and access logs

### Governance and accountability

- Assign clear senior management ownership for market soundings
- Protect compliance independence and effective challenge
- Approve and document market sounding recipient lists, with clear rationale

### Process discipline

- Use standardised, scripted disclosures shared consistently with all recipients
- Limit the number and timing of soundings to what is necessary
- Confirm safe-harbour applicability where multiple brokers are involved

### Communications and surveillance

- Conduct soundings only over authorised, recorded channels
- Monitor voice and electronic communications for leakage risks

### Personal account dealing

- Enforce pre-clearance, holding periods, and breach escalation
- Monitor staff trading linked to access to inside information

### Record-keeping and review

- Retain auditable records of consents, disclosures, recipients, and access
- Periodically review controls to ensure they remain effective and proportionate

## Organised crime networks

Insider trading is no longer predominantly opportunistic or individual-led, but is increasingly orchestrated by organised crime groups (OCGs), often operating across borders.

In its 2025 Market and Risk Outlook, the AMF warned of the growing threat from insider networks who repeatedly obtain information illegally through corruption, coercion, or cyber attacks. They are more sophisticated, and have more resources for recruiting sources of information and then transmitting the information without a trace.

The FCA has called OCGs “the most serious threat to (UK) markets”, accounting for around 25% of all STORs.

## The regulatory response

Given the scale and cross-border nature of these networks, regulators are strengthening their own collaboration frameworks. The AMF emphasised intelligence-sharing as a core defence, including referrals to judicial authorities, cooperation with domestic and international regulators, and active participation in multilateral frameworks to speed up information exchange.

French authorities are also placing greater responsibility on firms themselves. The AMF and the French Anti-Corruption Agency have jointly issued a call for vigilance to companies that hold privileged information due to their market listing or financial activities. The guidance explicitly highlights the risk of private corruption and provides a list of organisational controls focused on information access and human vulnerability.

Trade and communications surveillance remain critical, but more so as investigative and escalatory tools, rather than the primary line of defence.

### Why this matters: preventing and detecting insider dealing

Firms need a joined-up control framework that stops information leakage at source and detects misuse when prevention fails.

At a practical level, this means managing three interdependent risk layers:

- **Controls at source:** organisational, people, and governance measures that limit who can access inside information, how it is handled, and when it can be shared.
- **Information-flow controls:** technical and procedural safeguards that allow firms to understand if, where, and how sensitive information is moving across communications channels.
- **Detection and escalation:** integrated trade and eComms surveillance designed to identify suspicious behaviour, corroborate signals, and support timely intervention and regulatory cooperation.

## Systems and controls: Common deficiencies

Enforcement actions in 2025 provide a clear window into where surveillance frameworks and supervisory controls are breaking down in practice. This section distils those findings to highlight where firms continue to struggle, and what regulators expect to see instead.

**Common deficiencies**

- **Asset class coverage gaps**: inconsistent surveillance across FX, equities, rates, credit, commodities, or ETDs.
- **Product-level coverage gaps**: spot products monitored, but derivatives, structured products, or OTC instruments excluded.
- **Typology blind spots**: alert logic is calibrated to a limited set of behaviours.

### Regulatory findings

- **UBS**: Incomplete and inconsistent trade surveillance across multiple asset classes, including FX, metals, rates, credit, and exchange-traded derivatives.
- **Canaccord Genuity Wealth Management**: Personal account dealing surveillance was outsourced to an affiliate and limited almost exclusively to insider trading, leaving broader manipulative behaviours undetected despite being formally in scope.

## Do not shift the blame to outsourced suppliers

**FCA Market Watch 84** highlighted increasing dependence on external vendors for trade reporting and explicitly rejected attempts by firms to attribute reporting failures to third parties.

The FCA explicitly stated:

*"Over-reliance on third-party vendors is not a defence."*

Continuing:

*"We have seen instances of poor-quality reports submitted by vendors on behalf of counterparties. Root causes include inaccuracies in vendors' data mapping, enrichment, and schema logic."*

Across transaction reporting and trade surveillance, the message remains the same: accountability lies with the firm. Regular review of vendor performance is paramount.

## Calibration thresholds and alert overload

### Common deficiencies

- **Unreasonably narrow thresholds:** genuine red flags are missed
- **Overly broad thresholds:** excessive false positives and alert fatigue
- **Lack of alert prioritisation and aggregation:** preventing risk-based triage

> *"Our legacy system generates too much noise. The goal now is fewer alerts, but much higher quality ones."*
>
> ***Head of Trade Surveillance, Tier 1 Bank***

### Regulatory findings

**Velocity Clearing**: Surveillance thresholds generated unsustainable alert volumes, overwhelming review capacity. Tens of millions of alerts went unreviewed or were closed without substantive analysis, rendering the control ineffective despite nominal coverage.

**TP ICAP**: Surveillance parameters were unreasonably narrow across multiple typologies. Marking-the-close detection was restricted to trades executed in the final five minutes of trading and exceeding 25% of daily volume, resulting in 45 missed red flags. Wash trade surveillance was limited to transactions occurring in the same millisecond, causing eight potential wash trades to go undetected. Layering and spoofing indicators were also missed due to restrictive alert logic.

**Robinhood**: Surveillance thresholds generated excessive false positives, overwhelming alert review teams and creating large backlogs of unresolved alerts, with limited ability to distinguish higher-risk activity from routine trading.

## Surveillance and supervisory procedure design failures

### Common deficiencies

- Vague, incomplete, or outdated written supervisory procedures (WSPs) that do not reflect current business models
- Unclear supervisory responsibility and role conflicts
- Supervisory processes misaligned with actual trading activity, product mix, or known manipulation risks

### Regulatory findings

- **Barclays:** Failed to establish and maintain WSPs reasonably designed to supervise employees' outside brokerage accounts, resulting in inadequate oversight of employee trading activity and associated market abuse risks.
- **United Capital Markets:** Did not maintain supervisory systems or WSPs reasonably designed to oversee equity and options trading by a senior executive, creating a clear self-supervision and governance failure.
- **Odeon Capital Group:** Relied on unstructured daily trade summary emails containing hundreds of fixed-income transactions, which could not be filtered, sorted, or analysed for patterns over time. The firm failed to detect at least 138 instances of potentially manipulative pre-arranged trading between 2019 and 2023.

## Data integrity and reporting system failures

### Common deficiencies

- Inaccurate or incomplete trade data feeding surveillance and reporting systems
- System configuration and logic errors left uncorrected over long periods
- Insufficient reconciliation and control oversight

### Regulatory findings

- **ANZ**: Misreported secondary bond market turnover, creating artificial pricing pressure and misleading the government about trading volumes. Conduct economically analogous to benchmark distortion despite being prosecuted under licensing and conduct obligations.
- **Sigma Broking**: Misreported nearly all transactions over five years due to incorrect system configuration, with governance and oversight failures allowing the issue to persist uncorrected.
- **Citigroup**: Failed to submit accurate large trader reports for several years due to a programming logic error and experienced regulatory recordkeeping failures.

### Emerging signals: Maintaining orderly trading under severe market volatility

In 2025, the Financial Conduct Authority fined the London Metal Exchange £9.2 million for failing to maintain orderly trading during extreme market volatility in its nickel futures market. The enforcement action followed severe price dislocation in March 2022, when nickel prices more than doubled in a matter of hours, ultimately leading to an eight-day market suspension and the cancellation of trades.

While not a traditional trade surveillance case – and therefore not included in the quantitative figures – the LME action is notable for its focus on systems, escalation processes, and human oversight under stress conditions. The FCA found that volatility controls (‘price bands’) were inadequately governed, escalation to senior decision-makers was ineffective, and junior staff lacked training to recognise disorderly market conditions beyond technical errors or rogue algorithms.

**It is the first enforcement action of its kind against a UK-recognised investment exchange.**

## Best practice

The aforementioned actions provide a clear blueprint for what regulators expect from effective trade surveillance systems and controls.

- **Surveillance coverage**: comprehensive across products, venues, and manipulation typologies, aligned to how and where trading activity actually occurs. Ensure that all orders and trades are monitored – including those cancelled or amended. Outsourced surveillance functions are subject to defined oversight, challenge, and accountability.
- **Calibration thresholds**: build dynamic thresholds that adjust to different market abuse typologies while accounting for the full spectrum of trading variables, including assets traded, actors involved, trading methods and venues accessed.
- **Supervisory frameworks**: WSPs are specific, current, and aligned to actual trading behaviour and risk exposure. Supervisory responsibilities are clearly assigned, with safeguards against self-supervision or role conflicts.
- **Data integrity**: Trade capture, transformation, and reporting systems are subject to regular testing and reconciliation. System configuration changes are governed, documented, and independently validated.

### Recalibrating thresholds

There is no explicit regulatory mandate on how often surveillance thresholds must be recalibrated, but continuous calibration is a recurring topic of discussion across the market. What regulators care about is whether calibration is reasonable, proportionate, and demonstrably aligned to a firm’s evolving risk profile.

Thresholds should be reviewed and adjusted whenever there is a material change in:

- trading behaviour or strategies
- products, asset classes, or venues
- business lines or operating models
- regulatory expectations or market conditions

# eComms recordkeeping

eComms recordkeeping enforcement in 2025 continued to originate in the U.S., but the composition shifted. FINRA accounted for 53.3% of enforcement actions by volume, compared with the SEC (31.1%) and the CFTC (15.6%).

This represents a near-complete reversal of the historic pattern. Since the start of the eComms enforcement cycle in 2020, the SEC has dominated activity, accounting for around 60% of enforcement actions over the past five years, compared with 22.1% for the CFTC and just 17.7% for FINRA.

The shift reflects a change in who is being scrutinised, not what is being enforced. Many large, globally systemic firms have been fined for eComms recordkeeping failures, and enforcement attention is increasingly moving down-market. This is evident in the enforcement firmographics, the generally smaller penalty sizes, and the increase in FINRA activity, whose remit naturally covers a higher proportion of small- and mid-sized broker-dealers than the SEC or CFTC.

Whether U.S. enforcement volumes remain elevated will depend on remediation outcomes. If recordkeeping improves, regulators may gain greater visibility into underlying misconduct and we may see enforcements shift to other typologies. If it does not, further waves of recordkeeping enforcement remain likely.

## Regulatory scrutiny is broadening beyond the U.S.

Regulators outside of the U.S. are now scrutinising eComms recordkeeping. In the UK, the FCA launched a multi-firm review into off-channel communications, focused on wholesale banks. While not an enforcement exercise, the review assessed whether firms' frameworks, surveillance, vendor oversight, and management information were delivering the outcomes required under SYSC 10A.

In France, the AMF has signalled a similar approach. In 2025, the regulator conducted a series of inspections focused on firms' ability to ensure full traceability of investment services, covering all electronic communications used by employees across voice and digital channels, irrespective of the technology or messaging platform involved (Bloomberg, Skype, WhatsApp and Teams are all called out). We can expect to see the outcome of some of those inspections in 2026.

### What good looks like, and where firms still fall short

The FCA identified strong practices in policy frameworks that explicitly covered new technologies, streamlined self-disclosure, and embedded clear escalation paths.

At a framework level, stronger firms had updated policies to explicitly cover new technologies (e.g. smartwatches), simplified self-disclosure processes, prohibited personal contact details in directories, and embedded clear escalation routes such as helplines.

Effective surveillance combined expanded lexicon (including emojis, voice notes, and video), channel-hopping detection, and the use of NLP and AI to reduce false positives.

However, weaknesses persisted, and the FCA specifically highlighted fragile third-party vendor controls, including outages and incomplete recordings. Management information (MI) quality varied widely, with weaker MI limiting senior management’s ability to assess control effectiveness.

## Short selling violations

After several years of relatively contained enforcement, 2025 marks a sharp escalation in the value of short-selling-related penalties. The number of actions remained modest (six in total), but the financial impact surged, driven overwhelmingly by two outsized cases making up for more than 75% of total penalty value: Macquarie Securities (Australia) and Robinhood Securities (United States).

SHORT SELLING VIOLATION ENFORCEMENTS YEAR ON YEAR

| Year | Short selling violations |
|---|---|
| 2019 | $8,606,120 |
| 2020 | $7,450,054 |
| 2021 | $5,148,629 |
| 2022 | $20,317,259 |
| 2023 | $10,000,000 |
| 2024 | $6,651,117 |
| 2025 | $39,285,975 |

## Macquarie Securities and short sale misreporting: a data integrity failure with market abuse implications

ASIC's action against Macquarie Securities (Australia) Limited marks a significant escalation in regulatory scrutiny of regulatory data quality. This is ASIC's first-ever short sale reporting case, culminating in an AUD 35 million penalty.

**Key facts:**

- At least 73 million short sales misreported between 2009 and 2024
- ASIC estimates the true figure may be as high as 1.5 billion
- Errors spanned more than 14 years and impacted over 300 securities
- In some cases, published short sale volumes were distorted by more than 50%

The failures were systemic, driven by long-standing system weaknesses and inadequate supervisory and technical controls. The conduct undermined the integrity of short sale transparency itself – a foundational input for market surveillance.

## Robinhood Securities: SHO failures in modern market structure

Robinhood Securities was fined $15 million for systemic Reg SHO violations linked to its stock lending, fractional shares, and recurring order programmes. Between 2019 and 2023, control failures led to more than 15 million principal short sales and over 58 million riskless principal short sales being mismarked as "long", alongside millions of trades improperly marked "short exempt" and fail-to-deliver positions not closed out as required.

### Our thoughts

- Regulators are treating inaccurate reporting and misclassification as threats to market transparency and surveillance effectiveness.
- High-volume, low-margin activity – like fractional shares, stock lending, and internalisation – can generate tens of millions of breaches if controls are misaligned.
- Legacy systems, incomplete position calculation, and weak data lineage are recurring root causes.

Part 5

# The evolution of market abuse

Several structural changes shaped market abuse risk in 2025, and they're set to have a more meaningful impact on firms' surveillance frameworks in 2026 and beyond.

At the product and market-structure level, digital asset adoption, tokenisation, and prediction contracts are expanding the venues and assets that need monitoring. In parallel, the composition of market participants is shifting. Retail activity now accounts for roughly 20–25% of U.S. equity trading in 2025, with materially higher peaks at points during the year.

The pace and drivers of investment decision-making are shifting as a result, with retail investors more likely to trade impulsively and under the influence of social media.

This section explores these themes in depth and discusses the surveillance implications for firms in 2026.

## DeFi, crypto and market abuse

Regulatory approaches to crypto market integrity have expanded and matured, with supervisors moving from defining the regulatory perimeter toward practical supervision, albeit with different regional priorities and regulatory philosophies.

In Europe, MiCA replaced disparate, national-level texts at the end of 2024. With the 18-month transitional period set to end on 30 June 2026, supervisors are currently focused on how oversight will operate in practice, particularly around market abuse detection and disclosure obligations.

In the U.S., policy debates continue to centre on innovation, token classification and jurisdictional clarity between the SEC and CFTC. The GENIUS Act, for example, treats stablecoins as part of mainstream financial infrastructure. By introducing licensing, reserve and AML requirements, the framework shifts elements of market abuse supervision upstream – from trading venues toward payment rails and settlement layers – reflecting a broader global trend toward infrastructure-level oversight.

> *"At a country level, if the U.S. is moving forward aggressively, you don't want to fall too far behind.*
>
> ***Head of Surveillance, Global Bank***

Across Asia, regulators are leaning into surveillance-led supervision. Singapore and Hong Kong are investing in investigative capabilities, blockchain analytics and social-media monitoring as core components of market integrity frameworks rather than optional enhancements.

> *"We're seeing a convergence between crypto and traditional finance, particularly in the UK and Europe. Expectations around alignment between MiCA, MiFID, and MAR are becoming clearer."*
>
> ***Alex Parker - Chief Technology & Product Officer, eflow***

## Digital asset surveillance expectations

When it comes to market abuse, ESMA's supervisory convergence work under MiCA is shifting the conversation from regulatory design toward practical supervisory oversight.

A core structural challenge is that many crypto assets do not have a traditional issuer that can be relied upon to safeguard market integrity. As a result, Crypto-Asset Service Providers (CASPs) are recognised as critical control points for detection, monitoring, and escalation. Supervisors are therefore expected to scrutinise CASPs' surveillance capabilities, governance arrangements, and investigative procedures in a manner increasingly analogous to MAR supervision in traditional markets.

> *"Once crypto is brought inside the regulatory perimeter, surveillance expectations come with it."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

## New surveillance perimeters

Digital asset market integrity cannot be supervised from a single data set. ESMA's guidelines state that monitoring should include publicly available data and, "to the extent possible", reconciliation of on-chain and off-chain activity.

Supervisory expectations also extend beyond trading activity. The guidelines encourage authorities to consider communications across web-based platforms, social media, blogs and other public channels, reflecting the heightened risk of misinformation and market manipulation in crypto markets.

## Defi-native abuse patterns

Market abuse in digital assets is evolving along two parallel tracks. First, traditional manipulation typologies are being transposed into crypto markets. Second, the mechanics of decentralised finance introduce infrastructure-level vulnerabilities that do not exist in traditional market structures.

Supervisors expect monitoring frameworks to evolve for crypto-specific manipulation vectors (front-running/sandwiching dynamics, etc.), alongside traditional patterns like wash trading/spoofing.

### Infrastructure-level abuse: MEV and DEX manipulation

Decentralised exchanges (DEXs) allow certain network participants to influence the order in which transactions are processed. This creates "infrastructure-level" abuse risks, commonly known as maximum extractable value (**MEV**), where actors profit by reordering, inserting or delaying trades during block production.

Typical examples include front-running (placing trades ahead of a known transaction to move the price) and sandwich attacks (trading immediately before and after a user's order to extract value). While these behaviours do not involve hacking the platform itself, regulators increasingly view them as a form of market manipulation because they exploit the market's technical architecture rather than traditional trading strategies.

## Considerations for firms

Crypto market integrity supervision is beginning to resemble traditional market abuse oversight.

Regulators are signalling that market integrity cannot be assessed through trade data alone. Surveillance expectations now extend across on-chain analytics, off-chain trading activity, social media signals and even settlement infrastructure. For firms, this represents a shift from venue-centric monitoring toward ecosystem-level surveillance.

Surveillance tooling itself will need to evolve. Traditional models built around price anomalies or order-book behaviour may struggle to detect infrastructure-driven risks such as MEV strategies or narrative-driven manipulation amplified through online communities. The growing emphasis on behavioural analytics, blockchain intelligence and cross-dataset correlation suggests that future surveillance frameworks will look more like hybrid intelligence platforms than standalone trade surveillance systems.

Firms are feeling the pressure. Year-over-year survey data shows digital assets and crypto markets rising sharply as a perceived compliance risk – from 29% in 2024 to 51% in 2025 – reflecting the rapid expansion of supervisory expectations and the growing complexity of monitoring decentralised market structures.

## 24/7 markets and asset tokenisation

Regulators are positioning asset tokenisation as a structural evolution of capital markets. The FCA and AMF cite potential benefits including:

- Faster settlement and operational efficiency
- Reduced intermediaries and reconciliation costs
- Improved transparency through shared ledgers
- More flexible market access

### Surveillance implications

The move toward tokenised assets introduces an “always-on” market environment. Continuous trading and near-instant settlement challenge surveillance models built around defined market hours, end-of-day reviews and venue-specific monitoring.

Core manipulation typologies remain largely unchanged, but the context in which they occur is evolving. Detection frameworks will need to adapt to:

- 24/7 trading activity across time zones
- Fragmented liquidity across tokenised venues and chains
- Faster price formation

For firms, the shift is less about entirely new abuse patterns and more about operationalising surveillance in real time as tokenisation brings elements of traditional finance onto blockchain infrastructure.

## Prediction markets and event-based trading

### Growth dynamics

Prediction markets have moved from crypto-native experiments into mainstream financial distribution. Platforms like Polymarket drove early growth, but traditional brokers like Robinhood and Interactive Brokers (IBKR) are now entering the space.

Global trading volumes have eclipsed the early days of crypto, ballooning from ~$100m per month in 2024 to over $13bn by the end of 2025. Some projections suggest volumes could approach the trillion-dollar mark in the coming years.

Robinhood CEO, Vlad Tenev has called it the ”fastest-growing business we’ve ever had”, and the CEO of IBKR believes global prediction-market volumes could eventually rival, or even surpass, equities trading.

## Market abuse risk

The fragile distinction between trading and gambling remains an open debate. However, assuming prediction markets continue to scale, we are looking ahead to the emerging market abuse risks.

## Insider-style information advantages

Prediction markets have turned everything from central bank policy to celebrity breakups into tradable assets. But where there is a payout, there is a temptation to cheat. In traditional equities, “insider trading” has a clear definition; in the world of event-driven contracts, that line is blurred. The vast surface area of these markets makes asymmetric information easier to find and harder to flag, sparking fears that the smart money may in fact be insider money.

One widely discussed example involved a trader placing substantial bets on prediction contracts tied to Google’s annual search rankings. These were highly granular questions about which personalities would rank highest and their precise positions. The trader achieved 22 correct outcomes out of 23, generating more than $1m in profit. While there is no proof of wrongdoing, the accuracy and specificity of the wagers raised questions about whether participants could exploit early signals or non-public insights in markets where oversight remains limited.

## High-profile market-moving events

Prediction markets tied to live events also introduce elements of risk akin to stock market disclosures.

During one Coinbase earnings call, contracts were created around the specific words Brian Armstrong (CEO) would say. After becoming aware of the markets, Armstrong deliberately listed all of the tracked terms at the end of the call, directly influencing the outcome of the bets.

In another interview, Armstrong debated the impact of insider information in prediction markets, citing situations in which it could be beneficial if the predictions were to serve us as a reliable indicator of future events.

When influential individuals can observe and potentially shape market outcomes in real time, the line between participation, signalling, and market manipulation becomes increasingly blurred.

## Potential wash trading

Researchers from Columbia University analysed trading activity to assess whether artificial volume was influencing prediction markets. Their study found “artificial trading” accounted for roughly 25% of all buying and selling on Polymarket over the past three years, although the level varied over time.

The researchers mapped out a large trading network and scored digital wallets based on how they behaved. They looked for patterns that did not resemble normal investing, for example, wallets that repeatedly opened and closed positions very quickly (a common wash trading signal). Accounts that mostly interacted with other suspicious wallets formed tight clusters, strengthening the likelihood that the activity was coordinated.

Many of the identified wallets generated large volumes of trades while making little profit or taking on real market risk – behaviour more consistent with artificial volume creation than genuine trading activity.

## What does this mean for firms?

As prediction markets begin to permeate traditional finance through technology-first brokers and established incumbents, broader adoption seems inevitable. For financial institutions, this is an emerging market dynamic that warrants close attention.

There are early signs that the industry is starting to respond. Prediction market platform Kalshi recently announced a significant expansion of its market surveillance and enforcement capabilities following scrutiny over potential insider-trading risks. The initiative includes the creation of a surveillance advisory committee, a partnership with a specialist trade surveillance provider, and the appointment of a new head of enforcement.

For firms, the key questions are strategic and operational:

- Does participation align with the firm's risk appetite and conduct obligations?
- Can existing surveillance detect manipulation driven by information flow, narrative influence, or event timing?
- Are governance controls sufficient where employees, issuers, or public figures could influence outcomes?

Surveillance will remain central, but effectiveness will depend on expanding beyond traditional price-pattern detection toward monitoring information flows, behavioural signals, and coordinated activity.

> *"Prediction markets are inherently difficult to monitor, but the expectation is still the same: surveillance should be in place to detect manipulation."*
>
> ***Ben Parker - CEO, eflow***

# Finfluencers

The rise of the "finfluencer" is one of the defining market conduct trends of the past five years. A new generation of retail investors – digitally native, mobile-first and highly responsive to peer-driven content – is increasingly consuming financial information through short-form video, livestreams and personality-led channels rather than traditional research notes or broker commentary.

Recent research from FINRA highlights the behavioural shift: younger investors are significantly more likely to rely on social media and influencers when making investment decisions. IOSCO has similarly warned that social media–driven investment activity presents growing risks to market integrity, citing global concerns around misleading promotions, undisclosed conflicts and cross-border enforcement complexity.

> *"One of the challenges is that many investors now get their advice from social platforms, where influencers can launch their own coins and simply tell followers to 'buy this.'"*
>
> ***Independent Market Abuse Expert***

## Risk and regulation

Finfluencer activity introduces a cluster of conduct and surveillance risks:

- Misleading or unbalanced disclosures, particularly around high-risk products such as cryptoassets, CFDs and leveraged trading.
- Undisclosed sponsorships or conflicts of interest, where compensation arrangements are hidden or poorly signposted.
- Pump-and-dump and coordinated manipulation schemes, amplified by algorithmic virality.
- Rapid retail mobilisation, where price movements follow social media momentum rather than fundamentals.

Supervisory response has been comparatively fast. The FCA recently led a coordinated international crackdown on unlawful finfluencers, signalling cross-border cooperation and intelligence sharing. In Hong Kong, the SFC brought its first case targeting social media–driven misconduct, underscoring that this is not a UK- or U.S.-centric issue but a global supervisory priority.

The direction of travel is clear:

- Marketing oversight and market abuse enforcement are converging.
- Social media is no longer a peripheral to market conduct risk.
- Firms are expected to supervise not only their own communications, but also third-party and affiliate activity linked to their products.

Ultimately, this trend converges with many others, as it demands increasing the scope of context considered when assessing market conduct.

## Our recommendations to firms: Managing new and existing risk

### Broaden the market abuse risk assessment

Everything must be contextualised. The risk landscape is evolving rapidly and firms should constantly assess whether their surveillance frameworks are fit for purpose.

What we're seeing:

- **Product-level assessments**: Firms are moving away from broad assessments (e.g., "Equities") to specific product levels and even trading methodologies (separating voice, electronic, and algo trading).

> *"Where firms previously assessed risk at an asset-class level, many are now moving to product-level assessments – and some are going even deeper by breaking risk down by trading methodology, such as voice, electronic, or algo trading."*
>
> ***Independent expert in Risk Assessments, Trade and Comms Surveillance***

- **Scale and complexity are driving technology adoption:** Greater granularity inevitably increases operational burden. Large-tier firms are now conducting hundreds of individual assessments across multiple regions, desks, and products. Manual spreadsheet-driven approaches are becoming unsustainable, accelerating the shift toward digitised risk assessment platforms and structured workflows.

> *"We're seeing risk assessments expand across regions, divisions, products, and trading models, which is driving a significant increase in the scale and complexity of assessments globally."*
>
> ***Independent expert in Risk Assessments, Trade and Comms Surveillance***

- **The industry is in the middle of a multi-year transformation cycle:** Firms reinvest effort each year to make the previous year's assessment even more targeted and granular.

## Maintain long-horizon surveillance data, defensible audit trails, and reconstructable trading records

> *"The markets keep fragmenting, the data keeps changing, and the question is always the same: what did you know, what did you do, and when did you do it?"*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

Investigations increasingly demand reconstruction of the full lifecycle of trading activity. Supervisors expect firms to demonstrate how decisions were made, how orders flowed through systems, and how behaviour evolved.

> *"Even something as conceptually simple as a wash trade requires you to reconstitute the full order trail across multiple systems."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

Technically, this means maintaining long-horizon datasets that link trade data, communications, reference data, and market context into a coherent audit trail. The ability to replay events – including timestamps, execution logic, and surrounding market conditions – is a core supervisory expectation.

> *"It's no longer enough to explain things verbally. Regulators expect you to back it up with physical evidence – governance records, audit trails, and proof of how decisions were made."*
>
> ***Head of Surveillance, Global Bank***

> *"People think, 'we built the trading system, so building surveillance should be simple.' But the problem I'm solving is completely different – it's figuring out what you did yesterday from incomplete breadcrumbs."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

## Broaden the dataset

Supervisors are increasingly signalling that market abuse cannot be detected through internal trade and order data alone. Expectations are expanding to include KYC data, historical behavioural markers, and third-party or publicly available intelligence on known manipulators.

Firms should document how external data is ingested, how it informs monitoring and escalation, and how it supports defensible decision-making. Regulators are also placing greater emphasis on cross-border patterns – including the use of overseas brokers and international networks – reinforcing the need for data models that support cross-venue and cross-jurisdictional reconstruction.

Finfluencer risk is pushing supervisors to look beyond traditional eComms and trade data to include signals emerging from public digital channels. Commentary from FINRA highlights how investing forums, finfluencers, and social sentiment tools are increasingly shaping trading behaviour, meme-driven strategies, and coordinated activity across markets.

Part 6

# The Regulator: How oversight is evolving

In 2025, authorities recalibrated their strategies, shifting from “prevention at all costs” to “rebalancing risk” to support growth. Standards have not been lowered; rather, oversight is becoming more efficient, targeted, and outcome-oriented.

We observed four interlinked themes:

1. Targeted rule simplification
2. Proportional enforcement focused on deterrence and material harm
3. Smarter oversight with better use of data and technology
4. A more tech-positive stance toward market participants adopting surveillance tools

## Targeted rule simplification

Regulatory reform in 2025 was about simplifying how and where rules are applied. While the tone and pace differ across geographies, the direction of travel is consistent.

> *“People now understand how market abuse affects pensions, interest rates, and investments. Dialling regulation back would hurt the public, not help them.”*
>
> ***Head of Trade Surveillance, Tier 1 Bank***

### United Kingdom

The FCA has been explicit in reframing regulation as an enabler of growth. Senior voices have emphasised the role of regulation as a market "stabiliser", supported by a regulatory agenda that is predictable, proportionate, and purposeful.

> *"When you're in compliance, having anything clearly defined is a huge help. The FCA provides a level-set that U.S. regulators often don't."*
>
> ***Head of Trade Surveillance, Tier 1 Bank***

Rule simplification is most clearly visible in the proposed transaction reporting reform. The FCA has adopted a "less but better" approach to regulatory data collection, reducing the number of reporting fields, removing overlapping or low-value requirements, and eliminating reporting obligations for millions of financial instruments that are not traded on UK venues.

### Transaction reporting reform

1. Reduce transaction reporting fields from 65 to 52
2. Remove reporting obligations for six million financial instruments only tradeable on EU trading venues
3. Remove foreign exchange derivatives from the scope of reporting requirements
4. Reduce the default back reporting period from five to three years
5. Require trading venues to populate fewer fields in their transaction reports
6. Reduce the number of instrument reference data fields from 48 to 37

The regulator is also doubling down on outcomes over prescription (e.g., the Consumer Duty Regime), giving firms greater flexibility in meeting regulatory objectives.

### European Union

ESMA has stated that simplification should not be confused with deregulation. Instead, the focus is on clarity and harmonisation.

> *"Deregulation is not real in market abuse. They're still adding things to MAR, not taking them away."*
>
> ***Head of Trade Surveillance, Tier 1 Bank***

ESMA has been driving simplification by rationalising complex, overlapping reporting frameworks. In June 2025, the supervisor launched a Call for Evidence on a comprehensive approach to simplifying financial transaction reporting, aimed at identifying the major cost drivers associated with regulatory reporting obligations under MiFIR, EMIR, SFTR, and other regimes.

Options under consideration include eliminating duplicative requirements and, more ambitiously, adopting a "report once" principle that would harmonise reporting templates across regimes while preserving the information necessary for effective oversight.

### United States

In the U.S., the early tone of 2025 suggested a sharper break from post-crisis regulatory orthodoxy. The return of Donald Trump brought an explicitly deregulatory narrative back to the forefront, reinforced by a series of executive orders calling for aggressive reductions in regulatory burden. These included proposals to remove two (or more) regulations for every new one introduced.

Deregulation has proven more targeted in practice. The SEC has signalled openness to reassessing rules where cumulative economic impact may not have been fully considered, including aspects of securities lending, short selling, and certain AML/CFT obligations for broker-dealers and mutual funds. At the same time, the SEC has been clear that "thoughtful and measured deregulation can unlock value" and "harmonisation and modernisation" is the ultimate goal, particularly where rule complexity creates inefficiency without improving outcomes.

Crucially, core market integrity functions have not emerged as primary targets for deregulation.

### Australia

In September 2025, ASIC published its Regulatory Simplification report, marking the first major milestone in a multi-year programme to reduce unnecessary regulatory complexity. Since the beginning of the year, ASIC has removed more than 9,200 pages of regulatory material, responding directly to longstanding industry feedback that regulatory sprawl was increasing compliance costs, stifling innovation, and obscuring regulatory intent.

The initiative focuses on clarity, accessibility, and usability, making rules easier to understand and comply with, while preserving strong consumer and market protections. This includes streamlining guidance, consolidating legislative instruments, redesigning how regulatory obligations are presented online, and modernising how firms interact with the regulator through digital lodgement and electronic execution.

### Regulation in flux: clearer rules or new challenges?

For firms, this shift does not translate into regulatory leniency. Even where simplification initiatives reduce duplication or improve clarity, the primary challenge remains managing regulatory change itself, particularly for organisations with a global footprint. Removing regulatory red tape is not a green light to reduce controls. Instead, regulatory change must be considered within a broader market abuse risk assessment, with control changes influenced by multiple factors.

Simplification creates opportunities for firms that adapt proactively – rationalising controls, modernising surveillance frameworks, and strengthening governance – but it also raises the bar by forcing firms to exercise clearer judgement over how regulatory outcomes are achieved and evidenced.

Our survey data highlights the challenge. Across all jurisdictions, “keeping abreast of regulatory changes” is the top concern keeping leaders awake at night (58% globally), rising sharply in Australia (74%) and the U.S. (63%).

> *“The concept of deregulation doesn’t really exist from where I’m sitting. The intensity hasn’t gone away – it’s just become more targeted.”*
>
> ***Head of Surveillance, Global Bank***

## Proportional enforcement focused on deterrence and material harm

Regulators are prioritising faster resolution of minor issues, sharper intervention where harm is real, and deterrence where it matters most.

### Focusing enforcement where it matters

The FCA will not pursue every minor breach, especially if firms self-identify and remediate issues. Instead, enforcement is being concentrated on cases that deliver “impactful deterrence.” This has translated into a streamlined enforcement portfolio: the same number of outcomes, delivered faster, with earlier alternative actions where full investigations are unnecessary.

Rather than waiting for harm to crystallise, regulators are acting early – restricting business lines, forcing offboarding of high-risk clients, sharing intelligence with other authorities, or prompting employment consequences through disclosures. The aim is to make markets structurally hostile to bad actors, not merely to punish them after the fact.

BaFin has formally anchored proportionality and risk orientation into its supervisory strategy, advocating reduced complexity, lighter requirements for lower-risk and smaller institutions, and faster, more transparent supervisory processes.

In the U.S., this same logic is visible in enforcement restructuring. The SEC has publicly committed to a "back to basics" enforcement agenda, refocusing on core areas such as insider trading, market manipulation, accounting fraud, and fiduciary breaches. Organisational changes, including the creation of a dedicated Market Abuse Unit, are designed to improve efficiency and target increasingly sophisticated misconduct, such as activity on alternative trading systems.

Meanwhile, the CFTC's "enforcement sprint" shows purposeful prioritisation in practice: clearing backlogs of low-level cases through fast-tracked settlements, while reserving investigative firepower for conduct that poses genuine client harm or market integrity risk. Recent outcomes show smaller fines, quicker resolutions, and tangible cooperation credit, paired with an explicit reallocation of resources toward more serious abuse.

### Expect sharper differentiation between "control gaps" and misconduct

Regulators are drawing clearer lines between fixable weaknesses in systems and controls, and persistent failures, poor judgement, or behaviour that undermines market integrity. The burden is moving upstream. Firms will be judged less on how they respond at the end of an investigation and more on whether they:

1. Escalate issues promptly,
2. Provide complete and accurate disclosures (not drip-fed facts),
3. Demonstrate remediation that genuinely reduces future risk.

### CFTC Cooperation Credit

The CFTC has introduced more granular self-reporting **guidance** which aims to remove uncertainty around the self-reporting trade-off.

By introducing a formal mitigation matrix, the Commission is clear that self-reporting, cooperation, and remediation will now be scored rather than vaguely considered. Firms now understand how certain behaviour translates into penalty reductions, and there will be fewer surprises at the end of an investigation.

The advisory draws a clear line between material violations that harm clients or market integrity, and lower-severity issues that can be responsibly identified, corrected, and prevented from recurring. Not all breaches deserve the same enforcement treatment, and regulators are increasingly recognising that through a more risk-based supervisory approach.

## Smarter data use and more sophisticated technology

Regulators have been signalling a shift toward more data-driven supervision for several years. What has changed more recently is the pace and depth of these initiatives. Since 2023, supervisory authorities have moved beyond incremental digitisation toward purpose-built data platforms, semantic layers, and AI-enabled supervisory tools.

## REGULATORY INITIATIVES PROMOTING SMART DATA

| Regulator | Initiative | Enhancements |
|---|---|---|
| SEC | Semantic layer over enterprise data | Transforms raw filings into meaning-aware data that can be reliably analysed by humans and AI, enabling scalable, AI-driven supervision and enforcement. |
| ESMA | ESMA Data Platform (2026) | Integrate data from various sources and expose dashboards and analytics so users (inc. NCAs) to improve risk monitoring and supervision. |
| FCA | SupTech and AI adoption | Investing in supervisory technology and AI while explicitly focusing on building internal data fluency, using technology to identify potentially abnormal trading. |
| AMF | Automated data processing and AI exploration | Automating regulatory data analysis and exploring AI and extraction tools, particularly in sustainability and non-financial reporting. |
| FINRA | FILLIP (internal LLM platform) | Deploying an internal LLM to support supervision, examinations, risk reviews, and document analysis; rolled out firm-wide in 2025 with ~40% weekly staff usage. |
| SFC | AI-enabled market and social media surveillance | Using AI to detect misleading information, coordinated manipulation, and emerging misconduct across markets and social media channels. |
| BaFin | ALMA (Automated Alarm and Market Analysis) | May 2024, BaFin integrated a machine-learning model trained on more than 1,500 historical cases of confirmed suspicious trading, enabling ALMA to better identify complex and subtle manipulation patterns. |

## A more tech-positive regulatory stance toward surveillance

> *"Our target-state architecture is evolving as regulatory expectations change – based on conversations with regulators, their expectations are being built directly into the platform."*
>
> ***Head of Surveillance, Global Bank***

Regulators' posture toward AI in surveillance technology has become noticeably more constructive as supervisory tone and engagement models evolve. Supervisors are encouraging controlled experimentation and adoption of new technologies, including AI and machine learning, where the objective is to improve detection outcomes and supervisory efficiency.

### eflow at the FCA Market Abuse Surveillance TechSprint

As part of the FCA's 2024 Market Abuse Surveillance TechSprint (MASTS), eflow showcased how machine learning can make market abuse detection more accurate and adaptive.

eflow demonstrated an AI-driven feedback loop that learns from historical surveillance outcomes – distinguishing high and low-value alerts and dynamically tuning detection parameters to remain fit for changing trading behaviours.

Using the FCA's real-world market dataset, eflow's model identified patterns where both traditional and ML-based methods agreed on high-risk behaviour, while also surfacing new risks that static, parameter-based systems missed.

**Watch eflow's FCA presentation here**.

The FCA has stated it will “support productivity improvements… through an increasingly tech-positive approach”. The regulator has also been explicit on the role of technology in “improving controls” and “reducing costs”.

Firms are encouraged to test AI and machine-learning-based surveillance methods through the FCA’s innovation labs. This innovation series has already helped over 200 financial firms test AI and machine learning technology services.

Similar attitudes can be seen from other global regulators:

- MAS has long promoted advanced analytics and AI through initiatives such as PathFin.ai and, in 2025, entered into a formal partnership with the FCA to jointly test AI solutions. The collaboration focuses on shared experimentation, responsible AI, and cross-border learning.
- In the U.S., FINRA has recognised that firms are already using generative AI across surveillance and compliance workflows, particularly for efficiency-driven use cases such as summarisation and information extraction. While its rules remain technology-neutral, the acknowledgement of real-world adoption reflects growing supervisory comfort with AI-enabled tooling.
- The AMF has stated its intention to examine how firms are using AI in market abuse detection. At the same time, it has highlighted persistent shortcomings in existing surveillance systems, reinforcing that innovation is welcome where it materially improves effectiveness and alert quality.

Regulators are becoming more technology-literate, more open to experimentation, and more explicit about the role of advanced analytics and AI in today’s surveillance systems.

## Balancing growth with market integrity: Industry perspectives

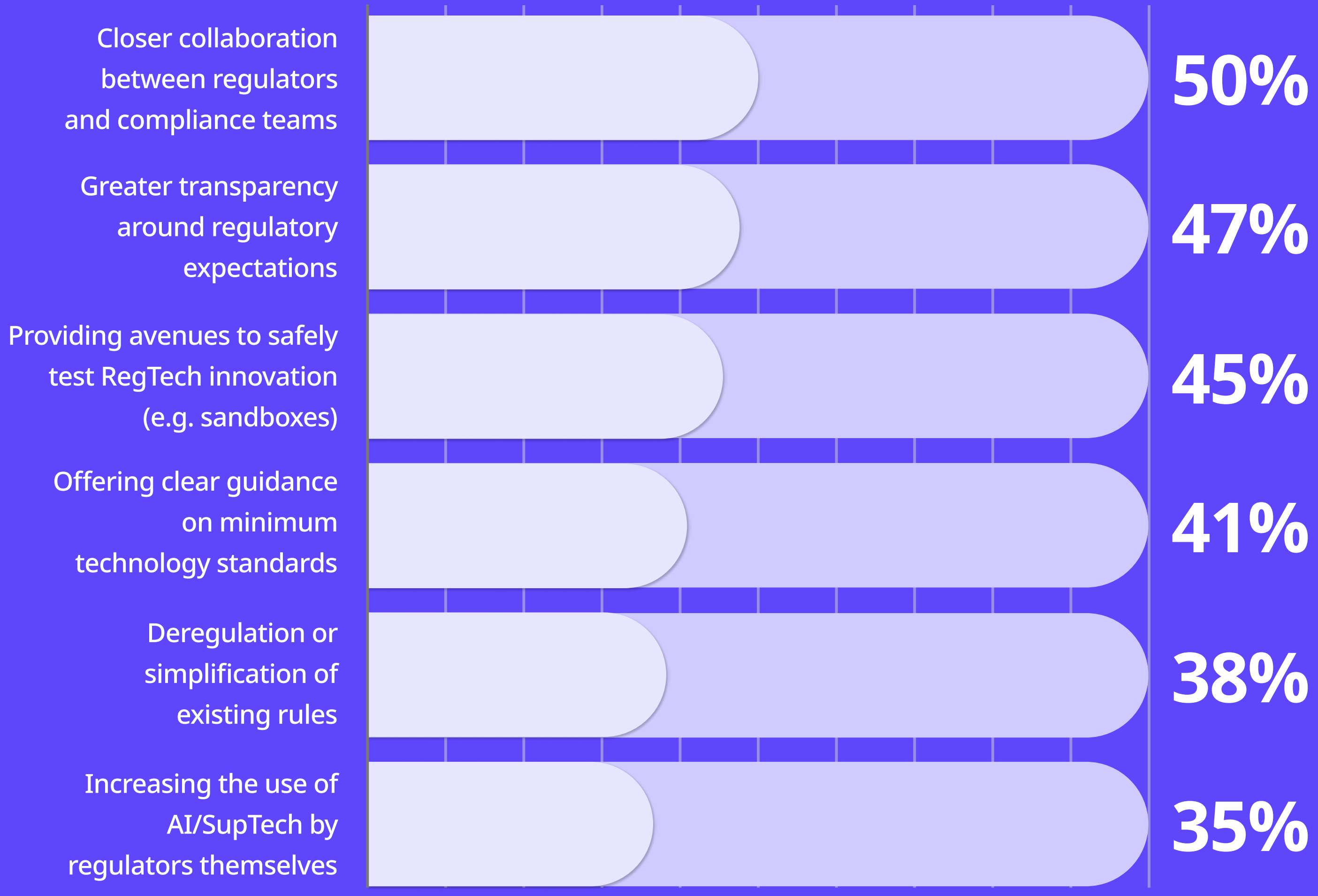
What stands out from market feedback is the call for smarter alignment. When it comes to market abuse, firms do not expect regulators to step back. They are asking them to lean in and engage with clearer expectations, closer collaboration, and structured pathways to test innovation safely.

The strongest responses point toward predictability and dialogue, which broadly validates the direction regulators have already taken through sandboxes, techsprints, and outcome-focused supervision. Preventing market abuse has to be a coordinated effort built on clarity, dialogue, and shared technological progress.

The data suggests a subtle gap. While supervisors continue to emphasise simplification and internal suptech adoption, firms appear more focused on practical clarity; how rules translate into real-world controls, and how enforcement expectations evolve as technology changes.

Our takeaway is this: balancing growth with market integrity will not come from reducing regulatory requirements, but from enabling firms to meet them more effectively, with regulators and industry operating as part of the same surveillance ecosystem.

***Which of the following regulatory measures would best promote the goal of balancing market integrity and market growth***



Part 7

# How surveillance technology moved forward in 2025

## Integrated surveillance

In last year's report, we argued that integrated trade and eComms surveillance would become non-negotiable as regulatory scrutiny intensifies and expectations of firms grow. And while regulators remain publicly agnostic on system architectures, they have continued to identify deficiencies that span both trade and eComms surveillance failures. In its $45 million case against Robinhood, the SEC found systematic recordkeeping breaches such as long-standing off-channel communications gaps, as well as inadequate retention of trade-related records among other serious breaches.

Our research also sheds light on the urgency within firms to integrate these sources. In our survey, 40% of firms reported that integrating trade and eComms surveillance was among the main challenges keeping them up at night in 2025, up from 37% one year ago. Anecdotally, interviewees also spoke of their frustrations of having these channels separated in the past, and their drive to utilise them together going forward.

> *"By now, trade and eComms surveillance really should play off each other."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

And, with regulators' growing willingness to scrutinise the full audit trail of a trade, integrating these channels will provide internal and external assurance that firms have taken all reasonable steps to identify market abuse.

> *"The biggest headache in surveillance isn't building typologies – it's getting the data models right so you can accurately reconstruct what actually happened."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

## Relational frameworks

At the close of 2024, we also predicted that firms would begin shifting from linear surveillance models toward relational frameworks capable of integrating AML data, PEP screening, eComms intelligence, and broader contextual datasets. The premise was that market abuse emerges through networks of people, accounts, communications, and financial flows that narrow rule-based systems struggle to capture.

2025 reinforced the need for surveillance programmes that incorporate external signals and cross-disciplinary intelligence rather than relying solely on trading patterns. These approaches are progressing but adoption remains uneven. Relational capabilities are emerging through phased enhancements with new data integrations and closer alignment between trade surveillance and financial crime teams.

### AML and market abuse enforcement crossover

Enforcement outcomes also demonstrate why relational detection matters in practice, particularly where market abuse intersects with broader financial crime risk.

One case brought to conclusion by the FCA involved a research analyst exploiting confidential, price-sensitive information to trade CFDs ahead of market announcements using accounts held by associates.

The underlying offense was insider dealing, but investigators identified financial activity consistent with laundering typologies. This case offers some crossover signals, separate from ordinary insider dealing, that traditional siloed monitoring may struggle to connect:

- Nominee and third-party account structures: Use of family members and associates obscured both MNPI-linked trading activity (market abuse risk) and beneficial ownership (AML layering risk).
- Derivatives as concealment tools: CFD positions enabled directional exposure without direct share ownership, complicating surveillance visibility while accelerating profit realisation.
- Post-trade financial flows: High-volume deposits, cross-border transfers, and unexplained cash movements reflected potential layering and integration stages extending beyond pure market abuse.

In theory, the firm could have detected the bad actor through either lens:

- Insider trading surveillance (suspicious timing of CFDs ahead of announcements)
- AML monitoring (unusual deposits, third-party accounts, cross-border flows)

But the strategic issue is not whether one control could have worked. It is whether relying on one silo materially increases detection risk, blind spots, and regulatory exposure. Either control might detect the misconduct, but neither is sufficient alone.

## eComms surveillance

Advances in large language models are compounding, and text-heavy domains are among the clearest beneficiaries. eComms surveillance sits squarely in that category. As NLP models become more context-aware, multilingual and capable of parsing nuance, the gap between keyword monitoring and genuine intent detection has narrowed significantly.

> *"AI is far more mature in eComms surveillance than on the trade side."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

Importantly, the evolution of eComms surveillance in 2025 has not been driven by model performance alone. It has also been shaped by the expansion of channels and context ingested.

In our survey, 38% of respondents ranked eComms Intent & Context Analysis among the highest-value AI use cases in their surveillance workflow. This value is driven by reconstructing narrative, linking tone, timing, counterparty dynamics and behavioural cues to potential misconduct.

FINRA's December 2025 report on social media-influenced investing highlights the growing role of AI-driven sentiment analysis tools across the market ecosystem. As detailed in Section II of the report, social media data aggregation and sentiment analysis are now used not only by investors to inform trading decisions, but by exchanges and regulators for market surveillance purposes. Exchanges are applying sentiment tools to detect broader social-media-driven trading trends, while regulators are leveraging social media analytics to support investigations into insider trading and market manipulation.

> *"Firms started with the most obvious channels – Bloomberg and email – then moved to LinkedIn, and are now moving further down the food chain to platforms like TikTok."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

This reflects a clear supervisory concern that social media, whether private communications, group chats, or public "finfluencer" content, can be weaponised to coordinate or amplify manipulation. The combination of virality, anonymity and algorithmic amplification introduces new conduct risks that cannot be captured by traditional, channel-limited monitoring frameworks.

For firms, this expands the perimeter of eComms surveillance beyond email and recorded voice into chat platforms, collaboration tools and, increasingly, relevant public social media signals. It also raises the bar for contextual understanding. As FINRA notes, sentiment tools must contend with sarcasm, coded language, multilingual content and data quality issues – precisely the domains where modern LLMs are beginning to demonstrate real capability gains.

## Artificial Intelligence

> *"AI is already part and parcel of most surveillance platforms – whether that's machine learning, NLP, voice-to-text, or large language models."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

TO WHAT EXTENT IS YOUR FIRM LEVERAGING AI FOR TRADE SURVEILLANCE?

| | Total | U.S. | UK | AUS | France | Germany |
|---|---|---|---|---|---|---|
| It is fully deployed across all relevant surveillance functions | **16%** | 17% | 20% | 23% | 8% | 12% |
| We are actively rolling out and piloting in specific functions | **31%** | 35% | 30% | 33% | 25% | 33% |
| We are actively planning deployment within the next 12-24 months | **24%** | 25% | 25% | 22% | 25% | 23% |
| We are exploring its use but do not have a formal strategy or plan yet | **20%** | 17% | 17% | 17% | 25% | 25% |
| No current or planned use - our firm doesn't have the relevant expertise in-house to leverage AI for trade surveillance | **8%** | 7% | 8% | 3% | 15% | 7% |
| No current planned use - although our firm does have the relevant expertise in-house to leverage AI for trade surveillance | **1%** | - | - | 2% | 2% | - |

Our data reveals a split reality. **Only 16% of firms report having fully deployed AI across their relevant surveillance use cases, and 29% are not currently planning for its use at all.** On the surface, this suggests hesitation.

Yet the data can just as easily tell a different story. **When including firms that are actively rolling out solutions or planning deployment within the next two years, 77% of the market is either already using AI or moving toward it.**

Unsurprisingly, interviewee sentiment mirrors this divide, with some more skeptical:

> *"Trade surveillance is still working out where AI genuinely adds value."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

And others more bullish:

> *"AI has use cases all the way through the alert lifecycle – from shaping your risk assessment and coverage strategy to supporting investigation."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

As 2026 begins, firms find themselves at markedly different stages of AI maturity in trade surveillance. For some, AI offers a chance to pull ahead through disciplined, high-value deployment; for others, there is a growing risk that hesitation translates into competitive and regulatory disadvantage.

## Finding value with AI

To understand where AI is delivering tangible impact, we asked respondents to rank the applications they consider most valuable to their trade and/or eComms surveillance efforts.

> *"As long as you stop short of expecting AI to think for you, it adds real value."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

## WHAT AI APPLICATIONS ARE MOST VALUABLE TO YOUR TRADE AND/OR ECOMMS SURVEILLANCE EFFORTS.

| | Total | Asset/Wealth Management | Fund Management | Broking | Banking | Prop Trading |
|---|---|---|---|---|---|---|
| Enhancing Detection of Known Abuse Typologies | 64% | 60% | 62% | 62% | 67% | 70% |
| Risk Scoring Alerts | 57% | 57% | 54% | 52% | 64% | 57% |
| Identifying Emerging or Unknown Anomalies | 55% | 54% | 60% | 62% | 54% | 43% |
| Actioning Low Risk Alerts | 47% | 54% | 49% | 38% | 48% | 44% |
| Identifying Emerging or Unknown Anomalies | 38% | 34% | 38% | 29% | 44% | 46% |
| Actioning Low Risk Alerts | 38% | 38% | 37% | 58% | 23% | 39% |

Perhaps unsurprisingly, the highest-ranked use case was enhancing detection of known abuse typologies through behavioural pattern recognition (64% overall). This reflects the industry's long-standing familiarity with statistical modelling and supervised learning.

Other statistical approaches, risk scoring and anomaly detection, come next. Again, this likely reflects the quantitative nature of markets as well as the skills and backgrounds of trade surveillance teams.

By contrast, use cases more closely associated with generative or agentic systems – such as copilot-style analyst support or advanced contextual interpretation – currently rank lower.

This reflects the progress made in industry today, not necessarily where ultimate value lies. While statistical use cases dominate present rankings, senior surveillance leaders highlighted other areas as being most transformational going forward:

### 1. Consistent, repeatable workflows

AI's ability to standardise triage logic, evidence assembly and reasoning pathways addresses one of surveillance's perennial challenges: variability in human judgement.

> *"AI is expected to handle data enrichment – pulling related emails (eComms) and trade data together into a uniform presentation for the analyst."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

> *"The real benefit is using AI as an assistant – to do the legwork of pulling data together – not as an independent validator."*
>
> ***Head of Trade Surveillance, Tier 1 Bank***

### 2. Data enrichment

> *"The real benefit is using AI as an assistant – to do the legwork of pulling data together – not as an independent validator."*
>
> ***Head of Trade Surveillance, Tier 1 Bank***

This reflects a shift from AI as decision-maker to AI as orchestrator – assembling structured and unstructured data into coherent investigative narratives.

> *"AI is expected to handle data enrichment – pulling related emails (eComms) and trade data together into a uniform presentation for the analyst."*
>
> ***Head of Surveillance, Global Hedge Fund Manager***

### 3. Eliminating clear false positives

> *"AI is effective for identifying a lot of false positives, and supports complex cases by summarising investigations, and pulling relevant trades and communications together into a single, consistent view."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

Our survey reveals an interesting correlation: firms in France (42%) and Germany (40%) were most likely to report significant challenges with false positives, and were also the least likely to have fully deployed AI (8% and 12%, respectively).

> *"AI can help remove obvious false positives, but it can't make subjective decisions. You still need the human element."*
>
> ***Head of Trade Surveillance, Tier 1 Bank***

## Barriers to adoption

The gap between AI value today, which is largely driven by techniques that have existed for decades, and AI value tomorrow, which adds a range of rapidly emerging capabilities, can be explained by a number of key barriers to adoption.

### 1. Data maturity gaps

AI is only as effective as the structure and governance of underlying trade and communications data, which is itself a stubborn, ongoing issue for surveillance teams.

Accelerated AI use is the most likely trend to cause compliance issues in the next year, as voted by 69% of respondents.

### 2. Skillset constraints

Combining AI engineering capability with market abuse expertise remains rare. 8% of firms have no plans at all with AI due to a lack of in-house expertise.

### 3. Cost and validation overhead

Model retraining, monitoring, maintenance and governance add ongoing operational burden.

### 4. Explainability and accountability

Regulators expect firms to stand behind system-influenced decisions.

> *"Regulators won't be comfortable with AI closing alerts on its own. You still need intensive QA, and the human remains accountable."*
>
> ***Head of Trade Surveillance, Tier 1 Bank***

These factors can weigh heavily on one side of the business case, and require leaders to have high confidence in the value being delivered.

> *"You have to be clear on what AI is meant to deliver – saving time, reducing cost, improving effectiveness. If you can't define that, you can't measure ROI."*
>
> ***Head of Surveillance, Global Bank***

These challenges have changed the build-versus-buy debate. As system and control deficiencies draw enforcement scrutiny, and as integrated trade and eComms surveillance becomes more complex, maintaining in-house AI infrastructure at regulatory-grade standards is becoming harder to justify. For more, read our prediction on the impact of AI on build-vs-buy.

Part 8

# Predictions

As we look ahead to 2026 and beyond, the financial markets landscape is poised for significant transformation. This section examines key developments that will shape market integrity and compliance in the coming year.

## Prediction 1: Cross-market surveillance will become a shared supervisory capability

2025 proved that complex pricing relationships and cross-product and cross-venue causality can be reconstructed to evidence more nuanced forms of manipulation. Yet the industry remains in a phase of building and experimentation. Over the next year, momentum will accelerate as regulators double down on analytics, intelligence sharing, and cross-border collaboration. Investigative techniques will diffuse more rapidly across supervisors and, increasingly, regulated firms.

For now, firms recognise the risk but lack the relational mapping or instrument linkage required to detect it consistently – 31% of compliance leaders are kept awake at night by cross-product or cross-venue manipulation risk. In the near term, regulators will continue to carry much of the investigative burden. But as analytical approaches mature and best practices spread, expectations will begin to shift upstream.

We don’t predict a sudden enforcement surge, but we do expect structural progress – regulator-led, ecosystem-driven. Cross-market surveillance will move beyond isolated breakthroughs toward a shared supervisory capability.

## Prediction 2: Prediction markets will move to the forefront of the regulatory agenda

Prediction markets will not remain a regulatory grey zone for long. The CFTC is under pressure to modernise oversight to reinforce legitimacy. With the initial proposal to prohibit trading on political event contracts withdrawn, the regulator is expected to advance more formalised event-contract rulemaking, framed around a “coherent interpretation of the Commodity Exchange Act” that supports responsible innovation while clarifying supervisory expectations. This process is likely to draw significant industry engagement.

Jurisdictional boundaries will remain a central challenge. Prediction markets have historically fallen within the CFTC’s remit, but the SEC has indicated that certain contracts may fall under securities regulation depending on structure and wording.

Globally, the picture will also remain uneven. While U.S. regulators focus increasingly on conduct and abuse risks, other jurisdictions are likely to move more cautiously. The UK and EU remain constrained by existing retail restrictions on binary options, creating a two-speed global market where fragmentation itself becomes a supervisory challenge.

Prediction markets are clearly moving into the broader market-conduct perimeter. Rather than waiting for complete regulatory clarity, firms engaging with these products should begin strengthening surveillance foundations now, anticipating closer scrutiny of trading behaviour, information flows, and market integrity risks.

## Prediction 3: The RegTech vendor ecosystem will consolidate

Platform providers will increasingly win over point solutions as integration demands rise. With surveillance expectations shifting toward full-lifecycle reconstruction, firms are less willing to assemble fragmented architectures themselves, instead gravitating toward fewer vendors and tighter integrations.

This dynamic favours providers capable of delivering end-to-end capability across data ingestion, analytics, investigation workflow, and case management. Expect suite buying and tuck-in M&A to accelerate, with larger vendors acquiring capabilities that close platform gaps.

Acquisitions are likely to cluster around data platforms and communications analytics, particularly where vendors can credibly support integrated trade and eComms surveillance and the broader contextual intelligence perimeter described earlier.

Pressure to embed artificial intelligence will act as a secondary catalyst. As regulators grow more explicit about the role of advanced analytics in effective surveillance – and as firms struggle to operationalise AI internally – vendors will face increasing pressure to demonstrate credible, production-ready AI capability. Rather than building complex AI layers from scratch, targeted acquisitions offer a faster path to deployment.

## Prediction 4: AI will resolve the build vs buy debate

For many years, firms have debated whether to build surveillance systems in-house or partner with specialist vendors. AI changes the terms of that debate. On the surface, generative AI strengthens the case for building. Prototyping is faster. Coding barriers are lower. Internal teams can spin up models, workflows and interfaces in weeks rather than months.

> *"We decided to build a new platform from scratch. In hindsight, I wouldn't do it again"*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

But building capability is no longer the hard part, and prototypes only go so far. Building and maintaining a platform fit for regulatory compliance is a full time job.

> *"I ended up spending far more time on UI design, workflows, and data plumbing than talking to the business about trading behaviour and intent."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

At the same time, AI is materially expanding what good surveillance looks like. Capability is compounding as models evolve rapidly.

> *"We reached a point where it was unrealistic to maintain our internal system. It's rules-based, and rules-based systems aren't fit for the way the landscape is evolving."*
>
> ***Head of Trade Surveillance, Tier 1 Bank***

Keeping pace with that evolution while managing model validation, explainability, data governance, security architecture and auditability, is the hard part.

> *"We spent most of the time upfront just figuring out how to get the data in correctly. If you don't trust the audit trail, the surveillance logic doesn't matter."*
>
> ***Global Head of Trade Surveillance, Global Asset Manager***

AI lowers the barrier to entry, but raises the bar for governance. When AI is involved in building or conducting surveillance, the layers of accountability multiply.

Over the next year, we expect AI to clarify the build versus buy debate: Firms may use AI to experiment and prototype internally, but enterprise-grade deployment will increasingly tilt toward specialist partners able to deliver not just capability, but assurance and control.

## Data maturity shifts the economics of build vs buy

Data architecture ultimately determines how flexible firms can be in deploying trade surveillance technology. Historically, implementing a surveillance platform could take a decade or more, driven, in large part, by the challenge of connecting fragmented data sources. In cases where central data pipelines are established, integration timelines can fall dramatically.

We don't predict vendor displacement, rather greater architectural flexibility. Firms with mature data foundations are less constrained by integration complexity and can evaluate surveillance tools based on effectiveness rather than connectivity alone. As a result, technology lifecycles may shorten, with surveillance platforms reviewed and refreshed more frequently as firms seek improved analytics, automation, and detection capability.

> *"Now, with consolidated data lakes and central repositories in place, switching platforms is far less burdensome because the data pipelines already exist."*
>
> ***Independent expert in Risk Assessments, Trade and Comms Surveillance***

## Prediction 5: Enforcement will increase and the high-volume baseline will harden

Between 2019 and 2023, annual fine volumes consistently remained below 50. In both 2024 and 2025, that figure exceeded 100. 2026 is likely to continue this trajectory as high-frequency enforcement becomes the default operating model. We also expect to see a structural shift in how enforcement is delivered.

Regulators are adopting a dual-track model, resolving minor breaches quickly to maintain market hygiene while reserving resources for complex, high-impact cases to deliver meaningful deterrence.

Throughout 2025, supervisors continued to build the infrastructure needed to support this approach. Sustained investment in data platforms, advanced analytics, and AI-assisted supervision, alongside closer cross-border collaboration and intelligence sharing, is enhancing their ability to detect misconduct, reconstruct behaviour, and progress investigations more efficiently.

In 2026, these capabilities will translate into outcomes. Enforcement will become more operationally scalable and evidentially robust, enabling regulators to surface a broader range of misconduct while accelerating case resolution.

# About eflow

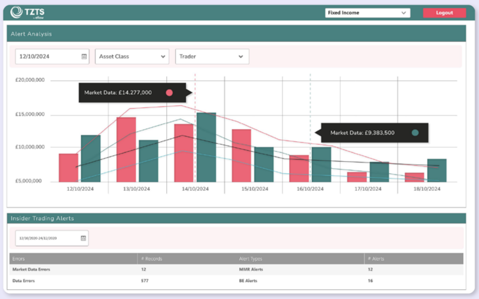
Since 2004, eflow has had a clear mission: to help financial institutions meet their regulatory obligations in the most robust and efficient way possible.

eflow technology is built on PATH, our robust and standardised digital ecosystem that integrates seamlessly with each of our specialist Regtech modules. This unique technological model offers firms the speed, convenience and efficiency of an off-the-shelf software solution, combined with a level of customisation that is typically only associated with a bespoke platform.

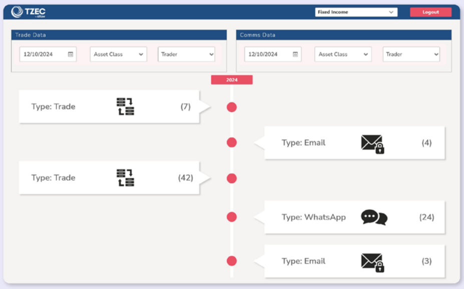
This means that as new regulatory challenges arise, as they inevitably will, you can rest assured that eflow's regulatory tools will already be one step ahead.

Explore our regulatory technology solutions at [www.eflowglobal.com](http://www.eflowglobal.com).

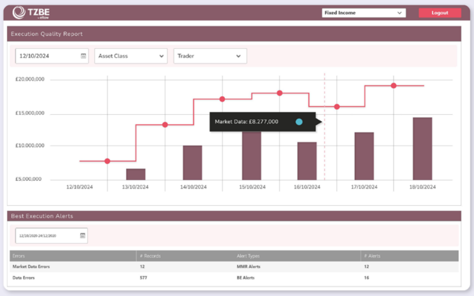
## Trade Surveillance



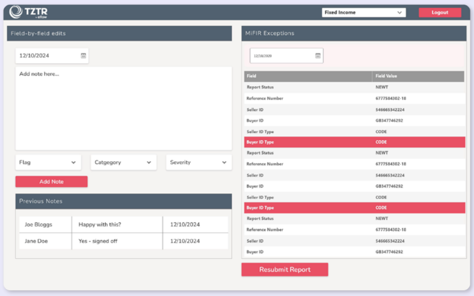
## eComms Surveillance



## Best Execution



## Transaction Reporting



# Appendix: Research methodology

This study builds on our 2024 research, combining qualitative and quantitative, primary and secondary research to produce unique insights into the market abuse landscape.

## Scope

### Time frame

- Q1 2019-Q4 2025

### Jurisdictions

The research encompasses eight key jurisdictions across three major regions, monitored through eleven regulatory bodies:

North America

- Securities and Exchange Commission (SEC, United States)
- Commodity Futures Trading Commission (CFTC, United States)
- Financial Industry Regulatory Authority (FINRA, United States)

Europe

- Financial Conduct Authority (FCA, United Kingdom)
- Autorité des Marchés Financiers (AMF, France)
- Federal Financial Supervisory Authority (BaFIN, Germany)
- European Securities and Markets Authority (ESMA)

Asia Pacific

- Australian Securities and Investments Commission (ASIC, Australia)
- Securities and Futures Commission (SFC, Hong Kong)
- Monetary Authority of Singapore (MAS, Singapore)

Global

- International Organization of Securities Commissions (IOSCO)

### Definitions

The research has focused on five enforcement categories, defined below:

- eComms Recordkeeping: Any failure to record, monitor or analyse electronic communications (e.g., emails, instant messages, voice recordings, and other digital communications) to detect, prevent, and respond to potential regulatory breaches or misconduct.

- Market Manipulation: The deliberate attempt to alter the free and fair operation of a market to create false/misleading appearances with respect to the price of an asset. Includes (1) selling or buying at the close of market with the purpose of misleading those who will act on closing prices, (2) Wash trading; selling the same financial instrument to create a false impression of market activity, (3) Spoofing and (4) Electronic Trading: Using electronic trading systems to enter orders at higher prices than the previous bid, or lower than the previous offer, and then removing them before they are actioned, with the purpose of giving the impression of greater demand or supply than there actually is.

- Insider Trading: The possession and use of confidential, non-public information, providing an unfair advantage when trading financial instruments. Includes (1) Front running / pre-positioning - transactions made for an individuals benefit in advance of an order, taking advantage of the knowledge of the upcoming order, (2) Takeover offers - using inside information from a proposed bid, knowing the implications on shares and (3) Acting for an offer - using the knowledge gained as a result of acting on behalf of an offeror for your own benefit.

- Trade Surveillance Systems and Controls: Deficiencies in data, systems and controls required to monitor trading activities and ensure compliance with regulatory requirements, including data governance. It involves the use of technology and processes to detect and investigate potential breaches, such as market manipulation, insider trading, and other forms of misconduct.

- Short Selling Violations: Any transaction that breaches regulations regarding short selling, such as SSR and MAS' Guidelines on the Regulation of Short Selling, which cover issues including naked short selling (the sale of securities that are not owned/borrowed) or settlement failures.

Note: Quantitative analysis focuses exclusively on traditional financial asset enforcement actions. While digital assets are addressed in the qualitative assessment, they remain outside the scope of the quantitative metrics to maintain data consistency and comparability with last year's research.

# Sources

## Primary

**Expert interviews**

The study incorporates interview insights with subject matter experts, including:

- Surveillance executives at global organisations
- Traders
- eflow's technical experts
- Independent subject matter experts

**Market survey**

A quantitative survey of 300 compliance decision-makers, evenly split across five major jurisdictions:

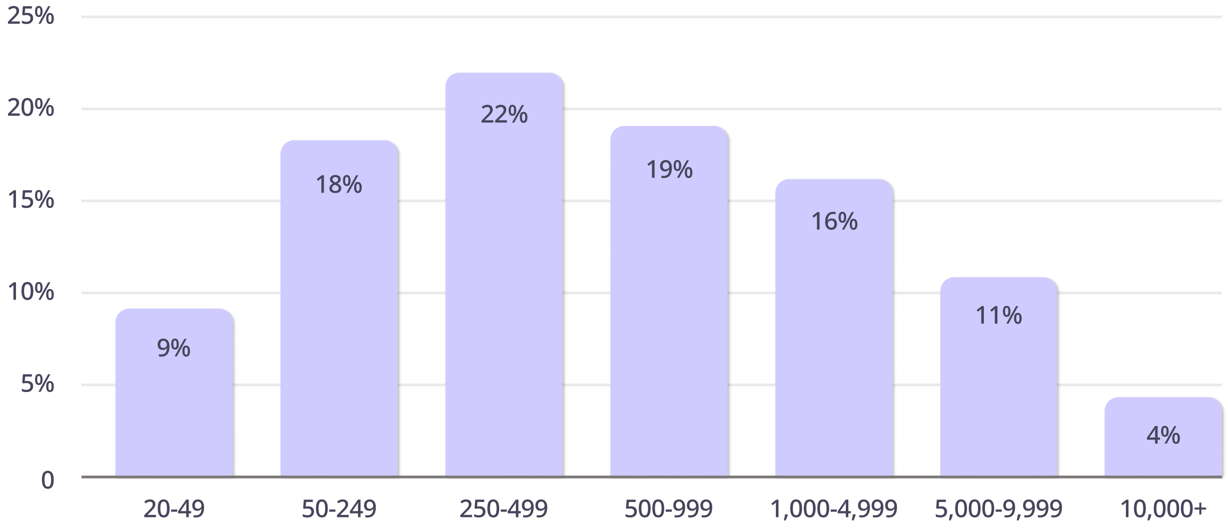
- France
- Australia
- North America
- United Kingdom
- Germany

With coverage of five types of organisation:

- Asset/wealth management: 23%
- Fund management: 22%
- Broking (CFD Broker, Broker Dealer, etc.): 17%

- Banking (investment or retail): 20%
- Proprietary trading: 18%

Including companies that range from boutique firms to tier one enterprises:



## Secondary

The study also draws on a range of authoritative, directly sourced regulatory documents:

- Regulatory enforcement actions
- Policy speeches and public statements
- Consultation papers
- Supporting documentation for enforcement cases
- Forward-looking regulatory guidance

These sources offer direct insight into enforcement priorities, regulatory reasoning, and anticipated policy shifts for 2026.