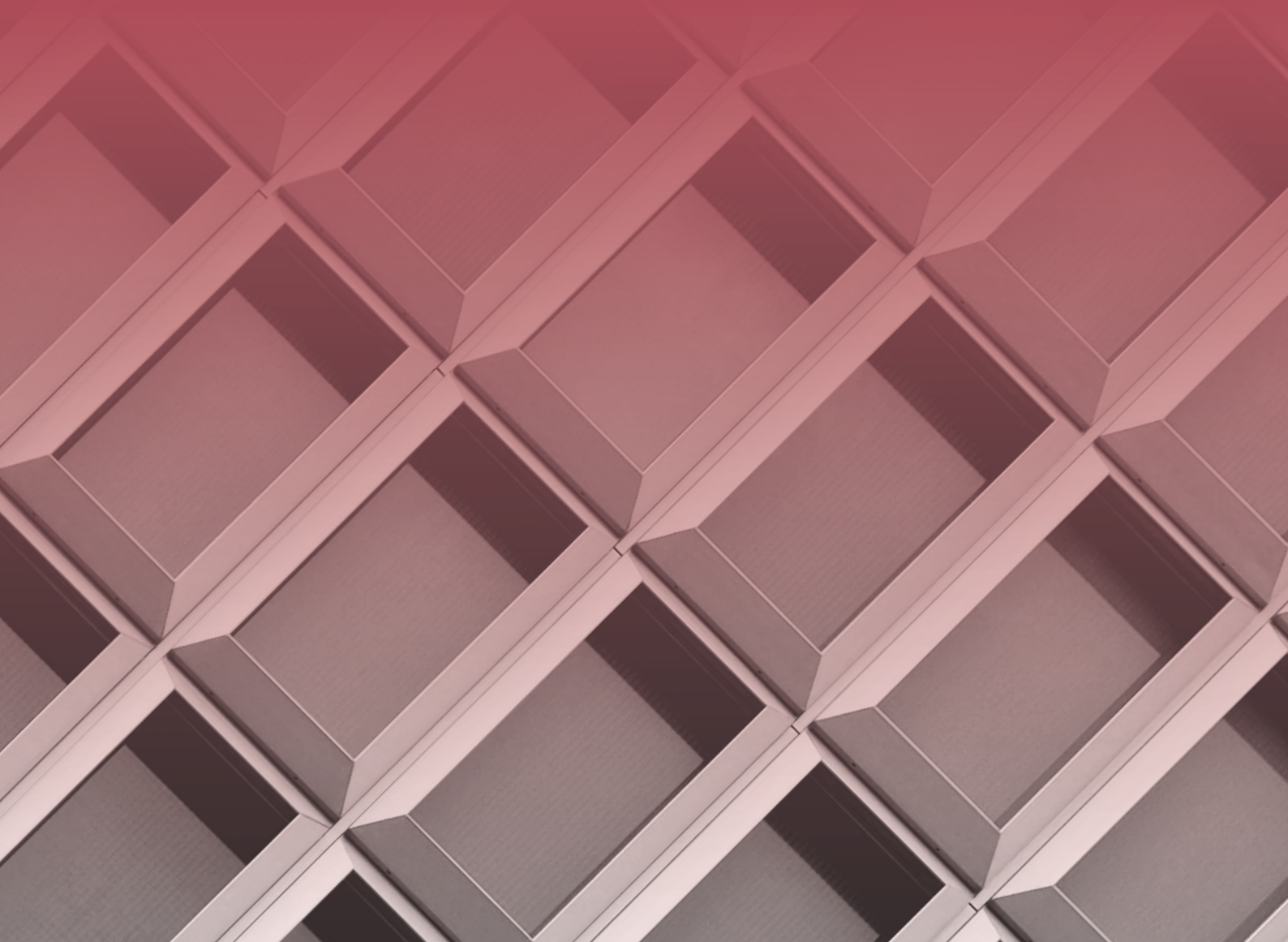
eflow

European trends in market abuse and trade surveillance 2025

How European regulatory enforcement stacks up against the rest of the world



Contents

Executive summary

Around 12 months ago, we published our first report exploring market abuse enforcement trends across Europe. As regulatory frameworks continue to grow in scope and complexity, the importance of understanding the trends that are driving enforcement action cannot be understated. For regulated firms, the need to understand shifts in regulators' strategies and how well they are placed to meet these evolving obligations is critical to the effectiveness of their future strategy.

Reflecting on the findings from our previous reports, one thing is abundantly clear: regulatory enforcement is speeding up. In Europe, 2024 saw a dramatic spike in terms of both the volume and value of enforcement action; the number of enforcement actions more than doubled, while the value of fines increased by 173% year-on-year. This trend was replicated across other global markets and jurisdictions.

So, what are the reasons behind these significant increases? While many factors have undoubtedly played a part, it will come as no surprise that the increasing prevalence of AI, algorithmic trading strategies, and other emerging technologies are playing a key role. As both regulators and regulated firms struggle to keep pace with these new and increasingly sophisticated technologies, enforcement actions are growing in both size and frequency.

As part of this technological evolution, we have also seen a shift in regulatory priority. From examining the enforcement data from 2019 to 2024, we can begin to see trends in the market abuse typologies most commonly being enforced against. Specifically, last year in Europe we saw a significant regulatory focus on enforcements related to trade surveillance systems and controls failures, with 89% of the total value of fines issued relating to this typology.

This marks a dramatic shift: in previous years, market manipulation was by far the most common enforcement category across Europe. On the basis of 2024's trends, the strength of a firm's underlying technology and processes should now form a critically important component of their regulatory strategy; simply stating that you have regulatory controls in place is not enough, you must be able to demonstrate how robust they are.

And now for the elephant in the room. Those of you who have read our previous reports will know that aggressive enforcement around eComms surveillance has defined

U.S. regulatory strategy in the past two years. In 2024 alone, U.S. regulators issued a staggering $740.7m in fines for failures related to eComms recordkeeping and monitoring failures. Conversely, European regulators did not issue a single fine for this typology during the same period.

While this disparity is startling, there is important context that needs to be raised at this point. European regulators have begun to place increased emphasis on the importance of implementing integrated surveillance solutions capable of monitoring both trade and communication data in a single system. While they may have been slower off the mark than their American counterparts, it seems highly likely that we will soon see eComms-related enforcement action occur across Europe.

With all of this complexity, it's almost impossible to predict what the next few years will hold with any degree of certainty. However, through a combination of global quantitative research and in-depth interviews with leading experts, we have been able to identify common themes that we expect to play an important role over the coming months and years. These include:

- Regulatory oversight is likely to evolve to incorporate a more collaborative approach, as regulators seek to work with firms to improve their governance processes and reward cooperation in investigations.
- An integrated approach to trade surveillance will become non-negotiable, with regulators expecting firms to have technology-led controls in place to deal with the increasingly sophisticated threat of market abuse.
- The role of AI in trade surveillance will accelerate significantly, with technological advances having the potential to support the automation of threshold calibration, the drafting of STORs, and potentially much more. However, it is just as important to note that there is very little to suggest we are at the point of AI fully replacing human expertise… yet.

In summary, while the ever-changing regulatory landscape may sometimes be challenging to navigate, there remain trends to be found once the data has been analysed. The increasing focus on new technologies - how firms can utilise them, as well as protect against their role in perpetrating market abuse – has underpinned much of the regulatory enforcement action of recent years. There is little to indicate that this will change in the foreseeable future.

The challenge for compliance teams remains being able to account for – and in some cases embrace – these new technologies to protect the industry and investors from the threat of market abuse.

Ben Parker

Chief Executive and Founder, eflow

Contributors

Ben Parker | eflow CEO & Founder

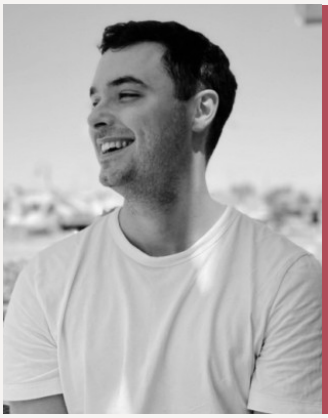
Ben Parker is CEO and Founder of eflow, one of the world's leading RegTech providers. Ben is an expert in financial services regulation and has a wide range of experience in tackling market abuse and developing the latest advances in trading surveillance. Having recognised the growing regulatory pressures 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.

The backdrop: unprecedented uncertainty

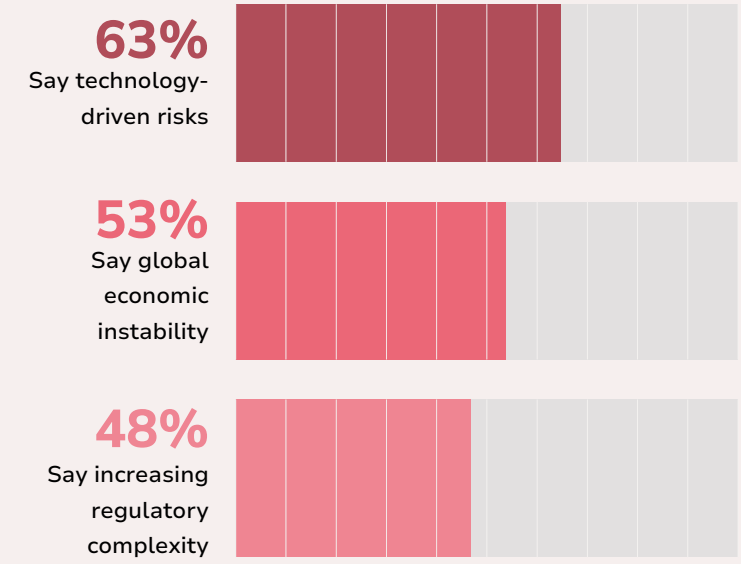
2024 was characterised by relentless uncertainty - both in Europe and further afield - driven by a confluence of factors that reshaped the global landscape. Political realignment heralded evolving regulatory philosophies, with implications for financial oversight and cryptocurrency governance. Meanwhile, geopolitical conflicts in Eastern Europe, Asia, and the Middle East exacerbated supply chain pressures and energy market volatility, intensifying the complexity of cross-border trading and surveillance.

Against this backdrop, regulatory evolution accelerated, with heightened scrutiny on trade surveillance systems in particular. Adding to this mix, persistent inflation tempered investor optimism, while technological advancements - particularly the rapid adoption of generative AI - ushered in both opportunities and novel risks in market operations.

Market participants face an intricate balancing act; retail and institutional investors seek opportunities amid volatility, and market intermediaries must drive profitability while safeguarding market integrity.

As the era of Covid-induced regulatory forbearance fades into memory, we're entering a new phase marked by intensified regulatory oversight. The compliance and risk management landscape has never been more unforgiving. Market abuse enforcements are trending upward in value and volume, and are quickly evolving in new directions. For firms, the stakes couldn't be higher.

Which market forces are most likely to cause compliance challenges in the year ahead?



This report captures our latest research - combining extensive primary and secondary data - analysing the past, present and future of market abuse and surveillance:

1. **Quantitative overview**: Presenting five years of market abuse enforcement data from 2019-2024.
2. **2024 Trends**: Taking a close look at the trends that defined market abuse in 2024.
3. **Predictions**: Revealing five predictions that our research points to.

Research methodology

This study builds on our 2024 research, combining the latest qualitative and quantitative, primary and secondary research to produce unique insights into the market abuse landscape. This year's research has been further enhanced by the inclusion of electronic communications enforcement actions, which are retrospectively analysed for the entire period in-scope (2019-2024).

300+

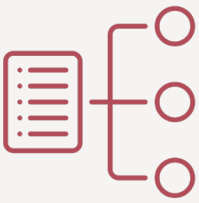
Financial services executives surveyed across five different industries

5 years

Of enforcement data collected and analysed from Q1 2019 - Q4 2024

8 jurisdictions

Analysed across three major financial markets: Europe, North America and APAC



5 typologies

To better understand the nature of abusive trading and process failures taking place

Detailed analysis

Of regulatory enforcement actions, consultation papers, policy speeches and more from all major financial regulators

10 expert interviews

With surveillance experts, traders, eflow's team and independent subject matter experts

5 predictions

Based on our research as to how the regulatory landscape will evolve

2024

A detailed analysis of all regulatory enforcements in the past calendar year

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.
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.
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 offer for your own benefit.

Quantitative overview

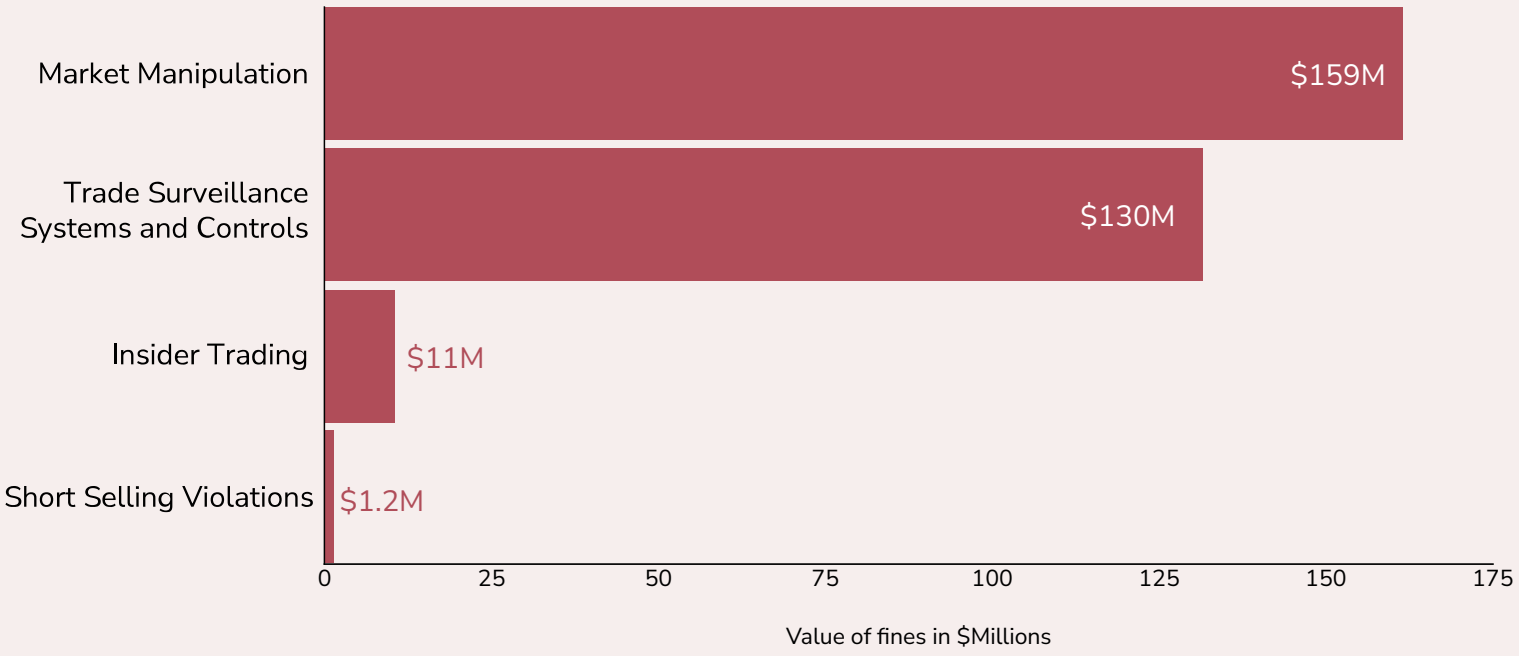
In the UK and EU from Q1 2019 to Q4 2024, there were:

80 fines
Issued for market abuse by selected regulators

$344 million
In total financial penalties issued

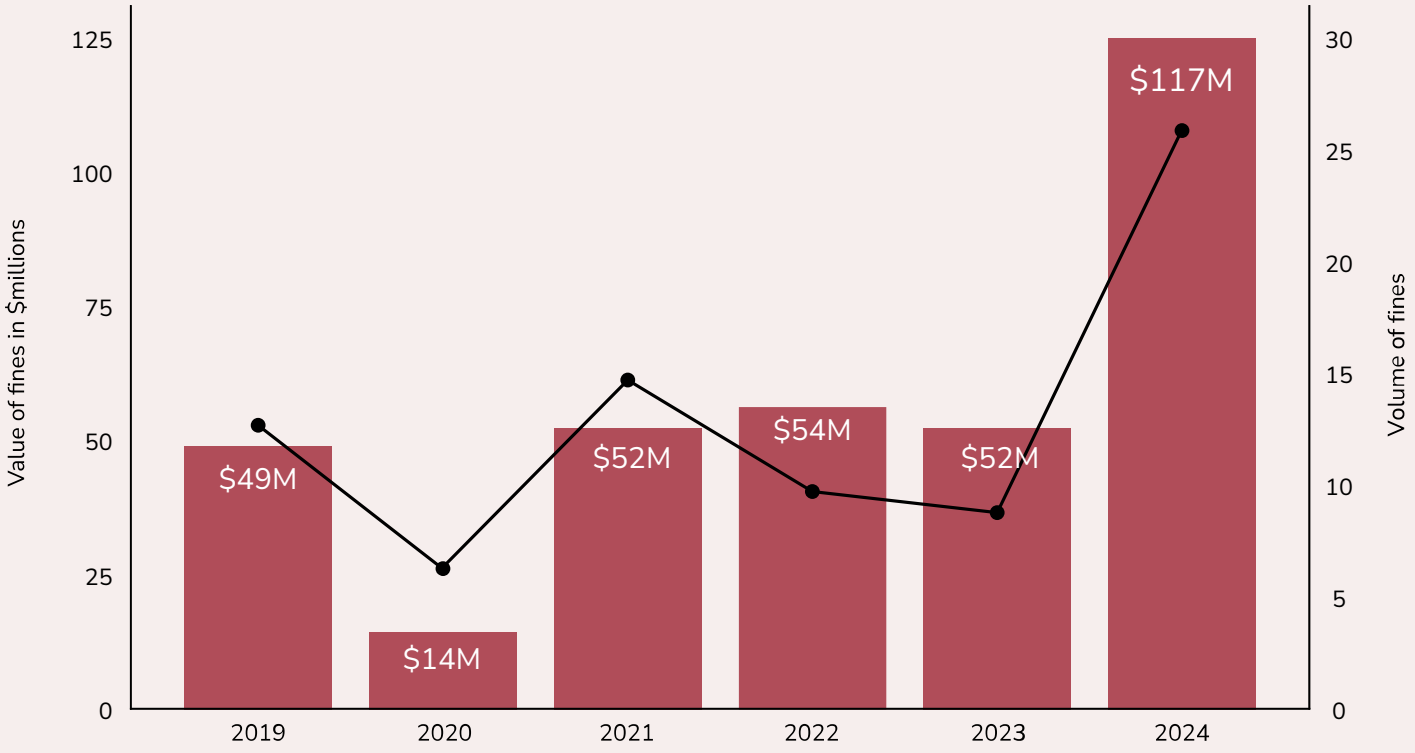
The scale of market abuse enforcement over the past five years is undeniable. Certain typologies, such as trade surveillance controls and market manipulation, have attracted the highest penalties, reflecting growing regulatory intolerance. Meanwhile, as later charts reveal, enforcement is expanding rapidly across other typologies as well. And if recent trends are any indication, this is only the beginning. The scale and trajectory of enforcement activity suggests that market participants should prepare for even greater scrutiny in the years ahead.

Breakdown of market abuse enforcements by typology



Annual enforcement trends

Value vs volume of enforcements



The data highlights a decisive shift in regulatory enforcement, culminating in a dramatic spike in 2024, increasing 125% year on year from 2023. 2024 reflects a sweeping crackdown, with regulators aggressively targeting firms of all sizes - small, medium, and large - resulting in both record-high volumes of enforcement action and substantial financial penalties. The post-COVID era of regulatory forbearance appears to be over, resulting in intensified scrutiny across the market.

What is (and isn't) driving this increase?

Our survey found that 62% of respondents feel at least somewhat confident in keeping up with regulatory changes. This aligns with the relative stability of core market abuse regulations and record-keeping requirements over the past decade. Yet, this confidence contrasts with rising enforcement actions, suggesting that the real challenge lies not in understanding the rules but in navigating an increasingly complex operating environment.

Take trade surveillance, for example. Expanding asset classes, sophisticated trading strategies, and cross-market manipulation make it harder to detect market abuse. Similarly, the proliferation of off-channel communication platforms increase the complexity of monitoring for insider trading and eComms record keeping-related infringements.

Without corresponding advancements in surveillance technology, firms risk falling behind - not due to a lack of regulatory knowledge, but an inability to implement compliance strategies effectively.

A note on eComms enforcement: The U.S. vs. Europe and the rest of the world

Perhaps the most striking contrast to be found in the enforcement data from 2019-2024 is the difference in fines related to eComms recordkeeping failures.

While $3.17bn in fines were issued for eComms recordkeeping-related failures, these were all issued by U.S. regulators, with no other regulator pursuing enforcement action for this typology during the examined period.

However, there is a nuance to this finding. While we're yet to see enforcement action from European regulators for eComms-related breaches, they have begun to place significant emphasis on the importance of implementing some form of integrated surveillance system, capable of monitoring both structured trade and unstructured communication data.

Case study: The FCA's 2025 review of off-channel recordkeeping

In August 2025, the FCA published their findings from a multi-firm review of off-channel recordkeeping. This review investigated the technology and processes implemented by regulated firms to monitor and archive communications while linking them to relevant trades over a 12 month period.

They found that, while most firms had taken steps to improve their eComms monitoring, 178 policy breaches were found during the 12 month period under investigation, with 41% involving individuals at director grade or above.

While enforcement actions have not been forthcoming, communication recordkeeping rules have been in place since the publication of MiFID II. Rule SYSC 10A states that "A firm must take all reasonable steps to record telephone conversations, and keep a copy of electronic communications, that relate to the activities in financial instruments".

The regulator's decision to instigate this review, as well as the findings it produced, signal that the FCA is gearing up to take a more proactive approach to the enforcement of this rule; firms would be well advised to ensure they have controls in place before it's too late.

2024 deep dive

In 2024 alone, there were:

22 fines

Issued for market abuse by selected regulators

$117 million

In total financial penalties issued

2024 has been defined by a surge in trade surveillance systems and controls enforcements. Out of the $117 million in fines issued by European regulators, $109 million related to trade surveillance failures - 89% of the total.

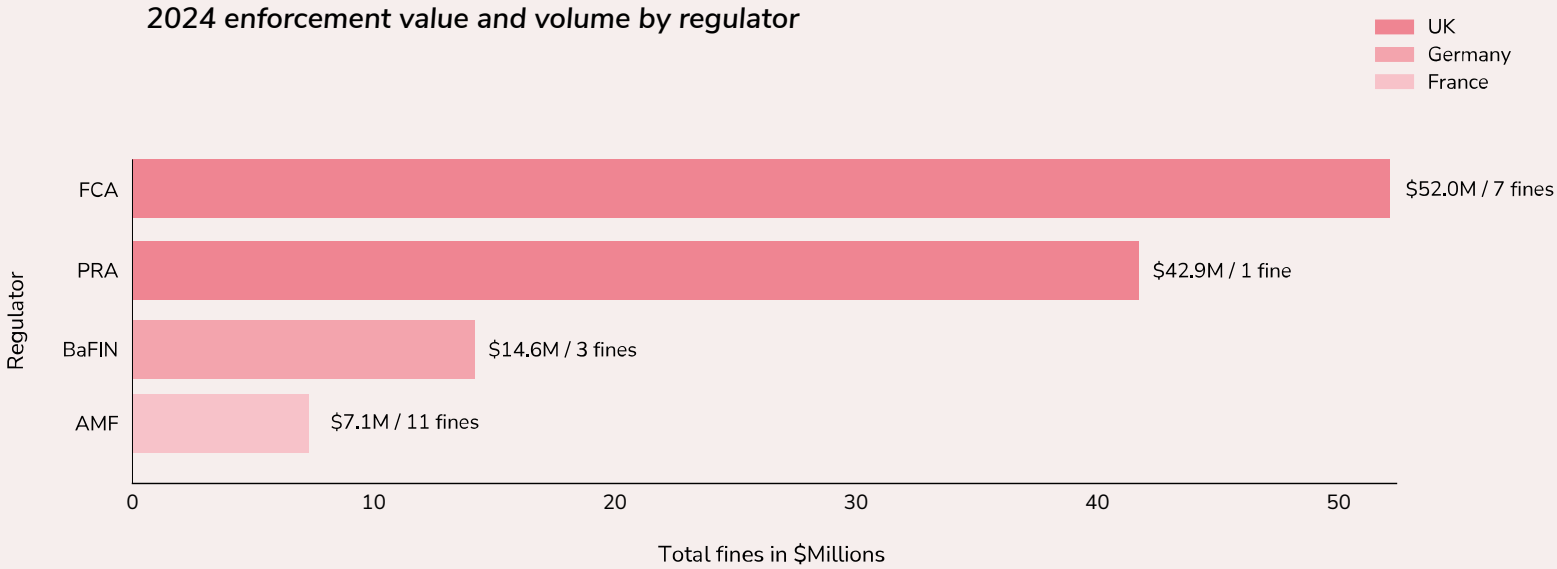
This focus aligns with our findings from last year's report. Increasing regulatory scrutiny on the data, systems, and controls firms use to monitor trading activities were beginning to be seen in 2023, and this trend seems to have continued. One head of surveillance previously warned that regulators now expect unprecedented detail and granularity in how firms configure alerts across venues, products, jurisdictions, and more.

Which regulators were most active in 2024?

The UK was by far the most active regulatory jurisdiction in Europe in 2024, enforcement actions from the FCA and PRA accounting for $94.9 million of the $117 million fines issued that year. The German BaFIN and French AMF were responsible for a number of fines each as well.

Notably, the AMF had the highest volume but lowest value of fines issued, with 11 fines being imposed for a total of just $7.1 million and an average fine value of $645,000. This indicates an increased focus on smaller and mid-market firms as opposed to just the larger tier one banks.

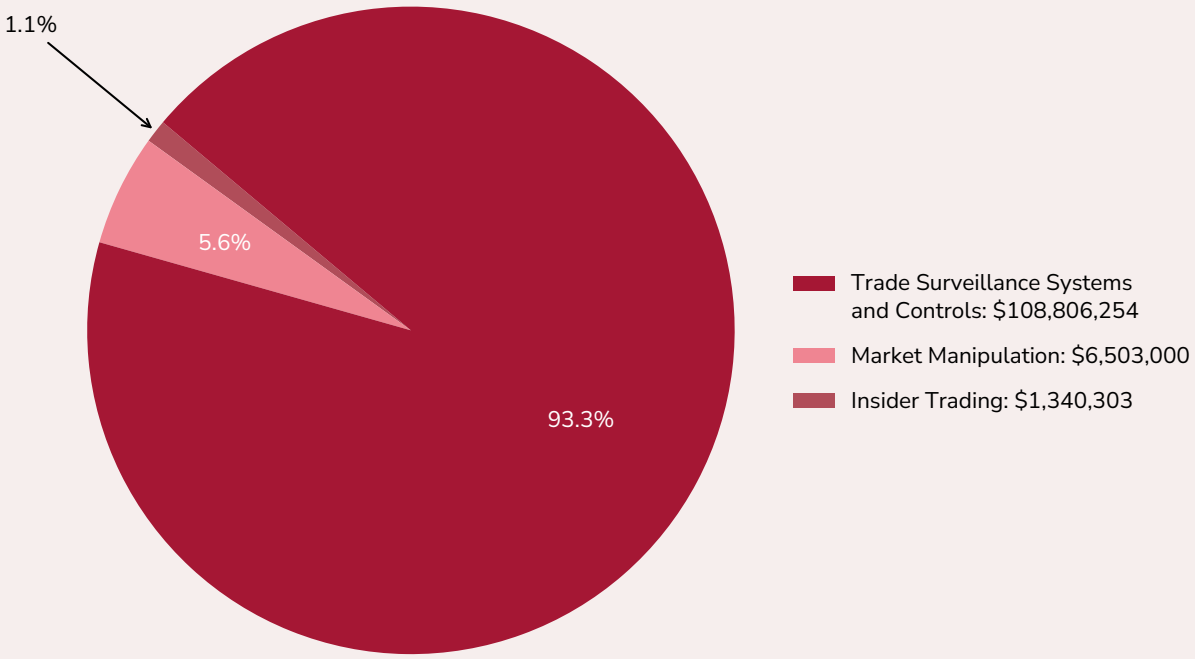
2024 enforcement value and volume by regulator



2024 enforcements by typology

In 2024, the major European enforcement efforts centred on trade surveillance systems and controls, highlighted by a significant case involving Citigroup Global Markets Limited (CGML). A trader's input error in May 2022 led to the unintended sale of $1.4 billion in equities, causing short-term market disruptions. This incident revealed critical deficiencies in CGML's trading systems and controls. Consequently, the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) imposed fines of £27.8 million and £33.9 million respectively, totaling £61.7 million. This case underscored the significance that European regulators continue to place on firms having robust trading controls in place.

Breakdown of European enforcement by typology



Trends in 2024

In 2024, market abuse continued to evolve in both sophistication and scope, presenting new challenges for regulators and firms alike. This section examines key market abuse trends across major financial centres, analysing significant enforcement actions and emerging typologies that shaped the year.

From the expansion of traditional manipulation schemes to the rise of cross-market abuse and social media-driven manipulation, we explore how regulatory responses and surveillance technologies are adapting to combat these evolving threats. Special attention is given to insider trading developments, data governance challenges, and the critical role of surveillance systems in maintaining market integrity. Through detailed case studies and expert insights, we provide a comprehensive view of the current market abuse landscape and essential strategies for prevention and detection.

The market abuse playbook is expanding

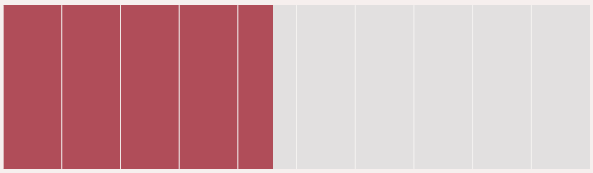
Market abuse continues to evolve, with an expanding array of manipulative practices presenting significant challenges for regulators and firms alike. This chart highlights some of the most prevalent forms of market manipulation identified this year, including pump-and-dump schemes, wash trading, spoofing, and more subtle behaviours such as cross-venue manipulation and marking the close.

While market manipulation cases in 2024 accounted for more than $63 million in fines globally across 28 enforcement actions, proving these offences remains extraordinarily complex, often requiring meticulous investigation and sophisticated surveillance systems. Regulators and firms deserve recognition for their progress in identifying these activities, but the diversity and scale of abuse underscores the ongoing struggle to maintain market integrity.

What trade surveillance struggles are compliance professionals facing in the year ahead?

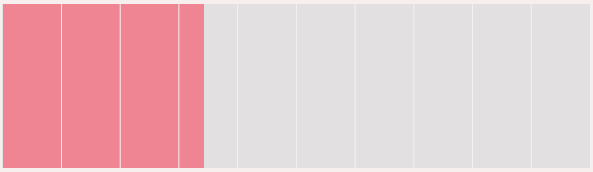
46%

Say accurately identifying market abuse keeps them up at night



33%

Are struggling to accurately configure their trade surveillance system to align with evolving risks.



Key typologies in two major European markets

United Kingdom

Flying and printing

The FCA's **Market Watch 76** reiterated concerns about firms publishing incorrect volume data, emphasising the market abuse risks posed by "flying" and "printing." These practices were first highlighted in **Market Watch 57** (November 2018).

- **Flying** involves a firm communicating to its clients, or other market participants, via screen, instant message, voice or other method, that it has bids or offers when they are not supported by, or sometimes not even derived from, an order or a trader's actual instruction.
- **Printing** involves communicating, by one of the above methods, that a trade has been executed at a specified price and/or size, when no such trade has taken place.

> *"We continue to see instances of possible flying and printing in several markets, including fixed income, commodities, and currencies in instruments such as bonds, swaps and options."*
>
> ***Financial Conduct Authority***

Both typologies distort supply-demand dynamics in quoted and OTC markets, influencing asset values and prompting trades based on false information. Despite previous warnings, the FCA continues to observe these practices, along with failures by firms to address them adequately, including:

- Failing to recognise the risks of flying and printing
- Failing to implement appropriate surveillance
- Failing to file Suspicious Transaction and Order Reports (STORs), or market observations, relating to flying or printing
- Taking a long time to investigate potential misconduct

Disruptive trading

Disruptive trading patterns don't always fall under traditional definitions of market abuse, but it can impact platform integrity. Expert interviews raised request for quote (RFQ) pinging: submitting a high volume of quote requests without genuine trading intent, probing for price discovery and liquidity information.

> *"One concern is around disruptive trading, which may not necessarily fall under market abuse but still poses challenges. For example, traders who engage in RFQ pinging can disrupt the market."*
>
> ***Head of Surveillance, Broker-Dealer***

Firms can take proactive measures to mitigate disruptive trading risk:

1. **Develop clear platform usage policies**
   Enforce well-defined guidelines that outline acceptable trading behaviours, particularly around high-frequency quote requests, establishing quantitative limits on the number of RFQs that clients may submit for a particular asset within a defined timeframe.

2. **Implement pre-trade risk controls**
   Deploy controls that monitor RFQ activity in real time to prevent excessive requests from overwhelming systems or degrading the trading experience for legitimate participants.

3. **Enhance monitoring and reporting**
   Adopt a data-driven approach to detect disruptive trading patterns. Metrics such as RFQ-to-trade ratios and response times can provide actionable insights

France

Dissemination of false information

On 11 December 2024, the **AMF fined multiple individuals and entities** €4.15 million for misleading investors and manipulating the share price of Auplata.

The case began when Auplata signed a financing agreement with the EHGO SF fund on 30 October 2017 but failed to disclose a key clause, misrepresenting the financing's true cost in a press release and its 2017 financial statements. The AMF held CEO Didier Tamagno responsible for these omissions and fined RSM Paris and its audit partner Stéphane Marie for failing to flag them.

Meanwhile, EHGO SF fund, despite commitments to hold its shares, sold a large volume, distorting market prices. The AMF deemed this price manipulation, holding Pierre Vannineuse and fund managers European High Growth Opportunities Manco SA and Alpha Blue Ocean Inc. accountable.

Cross-market manipulation

Cross-market manipulation - a form of market abuse where traders exploit the interconnections between financial instruments and trading venues - has received attention in 2024 as a typology which is especially sophisticated and immensely difficult to detect. At its core, this type of manipulation involves placing orders or executing trades in one financial instrument with the intent to illegitimately impact the price of related instruments, or the same instrument traded on different venues.

The sophistication of this approach offers two distinct advantages:

1. **Maximum impact**: Exploiting relationships between markets with varying liquidity profiles allows manipulators to minimise exposure while maximising impact. For instance, placing large spoof orders in liquid futures markets can influence less liquid cash markets, where price movements are more sensitive.

2. **Avoiding detection**: The sheer number of possible cross-asset and cross-market combinations creates significant surveillance challenges.

The FCA has been particularly vocal surrounding its desire to increase its ability to detect and pursue cross-asset class market abuse. The regulator's **2024/5 business plan** expressed the need to build on advanced analytics capabilities such as network analysis and cross-asset class visualisations. The FCA will develop improved market monitoring and intervention in Fixed Income and Commodities, covering both market abuse and market integrity.

Additionally, in their **Market Abuse Surveillance Tech Sprint** which began in May 2024 and ran for three months, the FCA explored how advanced solutions leveraging AI and ML could help detect more complex types of market abuse, like cross-market manipulation.

This technological evolution reflects a broader understanding of market realities:

> *I believe the FCA is positioning itself as the first line of defense against cross-venue manipulation. That doesn't eliminate the need for firms to monitor this themselves, but the FCA clearly understands the complexities involved and is addressing them with advanced solutions.*
>
> ***Head of Surveillance, Broker-Dealer***

Surveillance challenges

The complexity of detecting cross-market manipulation is particularly evident in modern markets. As one industry expert explains:

> *As a venue, detecting cross-venue manipulation is very challenging because we only see one side of the story. For example, if a competitor received a large RFQ sent to several dealers, and one of those dealers then used our platform to front-run it, we would only see the resulting trade on our platform. We have no visibility into the activity that occurred at the other venue.*
>
> ***Head of Surveillance, Broker-Dealer***

This challenge manifests across three key dimensions:

1. **Data fragmentation**: Trading venues operate in isolation, lacking visibility into related activities across platforms
2. **Pattern recognition**: The interconnected nature of instruments is nuanced, adding complexity to anomaly detection
3. **Jurisdictional complexity**: Cross-border activities require extensive regulatory cooperation

High risk markets

Three market segments have emerged as particularly vulnerable:

1. ***Commodities Markets**: The tight relationship between futures and cash markets creates natural opportunities for manipulation, with highly liquid futures markets often used to influence more sensitive cash markets.*

2. ***Over-the-Counter (OTC) Markets**: The virtually limitless combinations of related assets, coupled with market opacity, create significant surveillance challenges.*

3. ***Fixed Income Markets**: As one expert notes: "The FCA has reiterated that cross-market manipulation should be a focus in fixed income" - reflecting growing regulatory concern about fragmented trading venues in this space.*

Your role as a firm

The challenges of cross-market manipulation require a collaborative approach between regulators and market participants. Firms play an important role in addressing the three key dimensions identified earlier: data fragmentation, pattern recognition, and jurisdictional complexity.

Three approaches to cross-product surveillance

To detect cross-market manipulation patterns, firms need integrated surveillance systems that can simultaneously monitor positions and trading activity across related markets (like physical commodities and their linked derivatives). The system should track correlations between positions, identify uneconomic trading behaviour (like TOTSA consistently selling below market), and flag unusual patterns in volumes, pricing, or timing around key market events or benchmark windows.

1. **Hard-coded links**: Some assets are directly linked such as Corn Futures and Corn Spot prices, making them ideal candidates for hard-coded connections.

2. **Partially related instruments**: Some relationships are less direct but still meaningful. For instance, West Texas Intermediate (WTI) crude and Brent crude share a loose correlation based on their roles as global oil benchmarks, but price movements can differ due to regional or market-specific factors.

3. **AI-driven connections**: For the most covert connections, effective surveillance relies on AI and machine learning to identify subtle, non-obvious relationships between instruments, firms, or markets. These connections often go beyond simple product or industry ties, uncovering links that might not be immediately apparent.

> *It requires a lot of computational brainpower to sift through data and identify relationships that aren't obvious - such as connections between firms that don't share the same product line or industry but are still somehow related in their trading behaviour.*
>
> ***Head of Surveillance, Broker-Dealer***

Insider trading on the rise: new tactics and bigger fines

Concerns around insider trading were consistent throughout expert interviews. Not only did 2024 see a 137% increase in enforcement value compared to 2023, but the underlying tactics themselves have become more complex. In the U.S., it is **estimated** that the actual occurrence of insider trading could be up to four times higher than the number of cases prosecuted, and there is no reason to doubt similar disparity in European markets. Firms are losing ground, and more sophisticated detection mechanisms will be required to shift the balance in the years to come.

Several shifts in regulatory approach have fueled this increase, including:

1. Expansion of traditional insider trading concepts to include “shadow trading”
2. Focus on institutional control frameworks and systematic failures
3. Increased attention to organised crime involvement in market manipulation
4. Growing cooperation between international regulators
5. Emphasis on individual accountability alongside institutional responsibility

Regulatory initiatives

Regulators are increasingly focused on preventing insider trading in high-risk scenarios, particularly pre-trade information flows and market soundings:

IOSCO Pre-Hedging Consultation

IOSCO’s 2024 report examines pre-hedging, where dealers hedge trades before finalising them with clients. While it has legitimate uses, IOSCO flagged risks of conflicts of interest, insider trading, and market manipulation, noting that existing industry codes lack regulatory backing. Recommended safeguards include:

- Robust monitoring and surveillance of trading and communications
- Clear client complaint processes to address execution concerns
- Strong governance and oversight frameworks
- Mandatory training on pre-hedging policies

ESMA Pre-Close Calls

ESMA and National Competent Authorities (NCAs) have recently observed a number of high volatility episodes in EU share prices, some of which took place shortly after “pre-close calls” between issuers and selected analysts.

Essential controls for firms

Effective insider trading controls require a multi-layered approach, combining information management, surveillance, and governance frameworks. Regulators such as ASIC, SEC, and FCA emphasise the need for firms to establish robust policies to mitigate insider trading risks.

This section outlines key regulatory expectations and best practices for firms, covering:

- Information management – Preventing unauthorised access and improper handling of insider information
- Surveillance frameworks – Monitoring communications and trading activity to detect suspicious behaviour
- Governance and oversight – Ensuring compliance through strong policies, training, and reporting

These controls should be risk-based and proportionate to a firm's size and complexity while remaining sufficiently robust to meet regulatory expectations.

Information barrier controls

- Implement physical and technological segregation between different business units
- Establish formal wall-crossing procedures with documented approvals
- Maintain comprehensive insider lists with explicit notification and acknowledgment requirements
- Institute "need-to-know" principles for information dissemination

Deal documentation requirements

- Create and maintain real-time insider lists throughout deal lifecycles
- Document all deal-specific communication channels, including chat room participants
- Implement formal procedures for closing insider lists post-deal announcement
- Maintain records of insider notifications and acknowledgments

Communications monitoring

- Real-time surveillance of chat rooms and communication platforms
- Documentation and archiving of all deal-related electronic communications
- Regular review of communication patterns between insiders and external parties

Trade surveillance

- Enhanced monitoring of trading by identified insiders
- Surveillance of trading in related securities and derivatives
- Implementation of relational mapping to identify potential information flows
- Regular review and analysis of suspicious patterns

Compliance framework

- Dedicated oversight of insider information handling procedures
- Regular testing of information barriers and controls
- Periodic review and updating of policies and procedures
- Comprehensive training programme for all relevant staff

Reporting and documentation

- Enhanced suspicious activity reporting mechanisms
- Regular compliance reporting to senior management
- Maintenance of detailed documentation trails
- Periodic assessment of control effectiveness

Surveillance failures in the regulatory crosshairs

In 2024, regulators significantly intensified their scrutiny of firms' systems and controls, culminating in a 137% increase in enforcement value compared to the prior year. Supervisors took decisive action against those failing to detect and address suspicious activity, with the surge in enforcement activity highlighting structural weaknesses in trade surveillance frameworks, concerning everything from data governance to threshold calibration and escalation procedures.

The FCA's view

Following J.P. Morgan's historic $348 million **fine** in 2024, a number of global regulators made strengthened governance a point of emphasis. In May of that year, the FCA published **Market Watch 79**, emphasising data quality and governance as cornerstones of effective surveillance systems. The FCA's observations aligned with its North American peers, finding that:

Data governance was ranked among the top priorities for compliance decision makers, with more than one third of UK and EU-based respondents highlighting this challenge.

- Inadequate data governance often resulted in incomplete ingestion of trade and order data.
- Surveillance failures were frequently linked to fragmented or poorly tested systems.

One interviewee offered additional context for the FCA's position, with insights gleaned from a recent roundtable discussion held by the supervisor for broker-dealers:

> *The FCA made it clear that they understand firms will experience outages and gaps - those things happen. But there is zero tolerance for not knowing about a gap.*
>
> ***Head of Surveillance, Broker-Dealer***

The systemic fragmentation challenge

In general, firms respond to emerging risks by implementing discrete controls. Whilst this approach is targeted in addressing immediate compliance needs, it has led to a complex web of challenges:

Structural weaknesses

- Disparate data ingestion pipelines across asset classes create operational silos.
- Limited cross-departmental validation processes, unlike those present in trading or risk management functions.
- Incomplete data integration hampering comprehensive surveillance capabilities.

Operational impact

- **Detection gaps**: Fragmented systems and misaligned data flows increase the risk of missing suspicious activity.
- **Regulatory exposure**: Supervisory expectations clearly demand more sophisticated, integrated approaches.
- **Efficiency challenges**: Identifying and remediating issues within fragmented architectures requires significant resources.

Forward-looking implications

Proactivity is the name of the game, and the J.P. Morgan case should serve as a wake-up call for the industry.

Firms must strive to demonstrate:

- Comprehensive understanding of their data landscape
- Robust mechanisms for identifying and addressing surveillance gaps
- Clear remediation protocols for when issues arise
- Integrated approaches to system design and implementation

> *To the regulators, the key is having governance in place to identify gaps, understand their impact, and show a clear path to remediation. This is very different from the regulator discovering a gap the firm wasn't aware of.*
>
> ***Head of Surveillance, Broker-Dealer***

The impact of poorly calibrated surveillance

In 2024, scrutiny extended beyond data quality to how firms configure, calibrate, and monitor their surveillance frameworks. Firms must ensure their surveillance systems are not only built on high-quality data but also designed to adapt to evolving risks and regulatory expectations.

Regulatory expectations and market reality

In France, the AMF's 2023 **annual inspections** unearthed "poorly calibrated tools" among Investment Service Providers (ISPs) that result in alerts that are either "irrelevant to the ISP's business or are not acted upon". As a result, the AMF's 2024/5 action plan prioritises improving tool precision and alert quality.

Similar cases were also pursued in the UK, with the FCA **fining Macquarie Bank Limited (MBL)** £13 million on 26 November 2024 for serious control failures that allowed a trader to conceal over 400 fictitious trades. Between June 2020 and February 2022, a trader on MBL's London Metals and Bulks Trading Desk, recorded fictitious trades in an attempt to hide his trading losses. These trades went undetected due to significant weaknesses in MBL's systems and controls, which the bank had been previously warned about but failed to address in a timely manner.

> *MBL's ineffective systems and controls meant that one of its employees could, at least for a time, hide trading losses which cost the firm millions to unwind.*
>
> ***Financial Conduct Authority***

Threshold calibration: not all problems are made equal

The discrepancies in firms' trade surveillance confidence reflect the differing risk landscapes and operational demands of each business model. Firms with high-speed trading, complex products, or broad market access are naturally more concerned about configuring trade surveillance systems accurately.

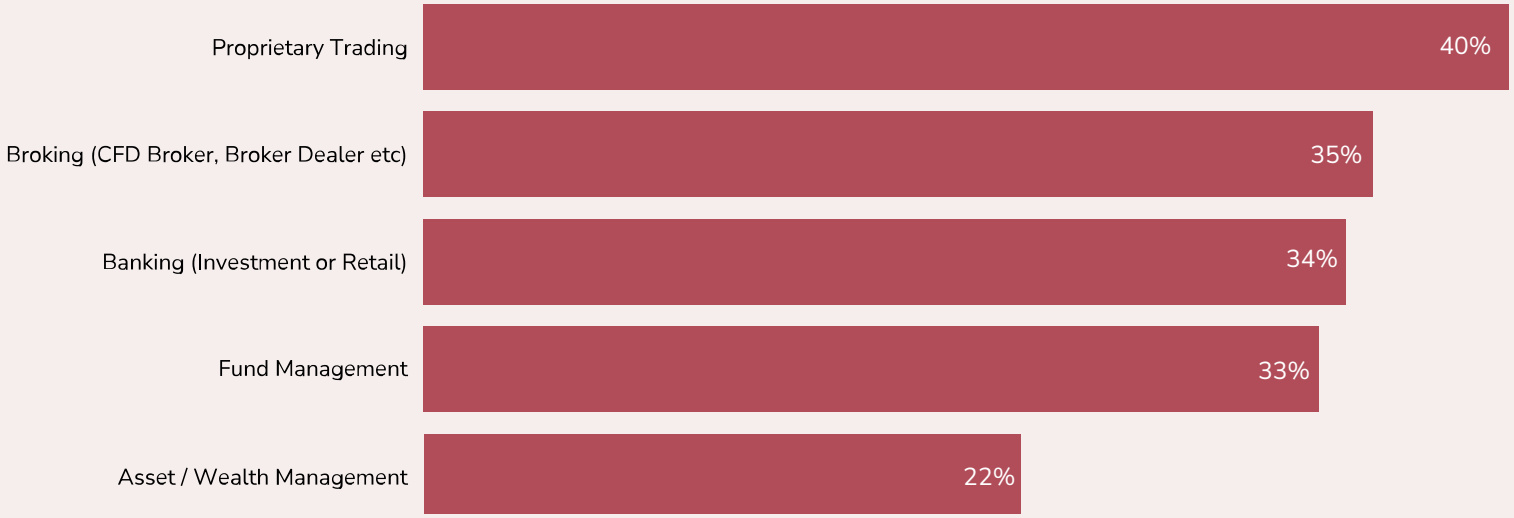
Proprietary trading firms report the highest levels of concern (40%) due to their direct market access and reliance on high-frequency, algorithmic trading strategies.

These firms operate in a high-risk, high-reward environment where performance is directly tied to profitability, requiring precise calibration of surveillance systems to detect market abuse in high-pressure environments. Their broad market access, diverse trading venues, and the dynamic nature of their strategies further complicate this process.

In contrast, asset and wealth management firms report significantly lower levels of concern (22%), which aligns with their simpler operations and long-term investment strategies. With lower transaction volumes and less complex products, these firms face fewer challenges in configuring trade surveillance systems.

Proprietary trading firms report the highest level of concern regarding technology-driven risks, with 70% of respondents identifying it as a key issue for 2025.

% of respondents reporting trade surveillance configuration as a top concern



Building a robust calibration framework

Antiquated trade surveillance approaches often fail due to their reliance on one-size-fits-all threshold calibration. Diverse trading characteristics across instruments - ranging from AIM-listed stocks to FTSE 100 companies, or government to corporate bonds - render uniform thresholds inherently problematic. For instance, a price movement that may indicate suspicious activity in one asset class could represent normal volatility in another.

To address this, firms must adopt dynamic controls that adjust to different market abuse typologies while accounting for the full spectrum of trading variables, including:

- Assets traded
- Actors involved
- Trading methods
- Venues accessed

Firms must also ensure that all orders and trades are monitored - this includes cancelled and amended ones. The surveillance of spoof orders can be critical in identifying certain forms of market manipulation, such as those that involve false or misleading signals to other market participants.

Modern solutions are already rising to meet these challenges, incorporating advanced features like conditional parameters that adjust to market volatility and liquidity. Additionally, sandbox environments for testing new configurations are empowering firms to refine their calibration frameworks in a controlled, low-risk setting. These innovations represent the next step in creating systems that are both robust and adaptable, addressing the complexities of modern markets.

Predictions

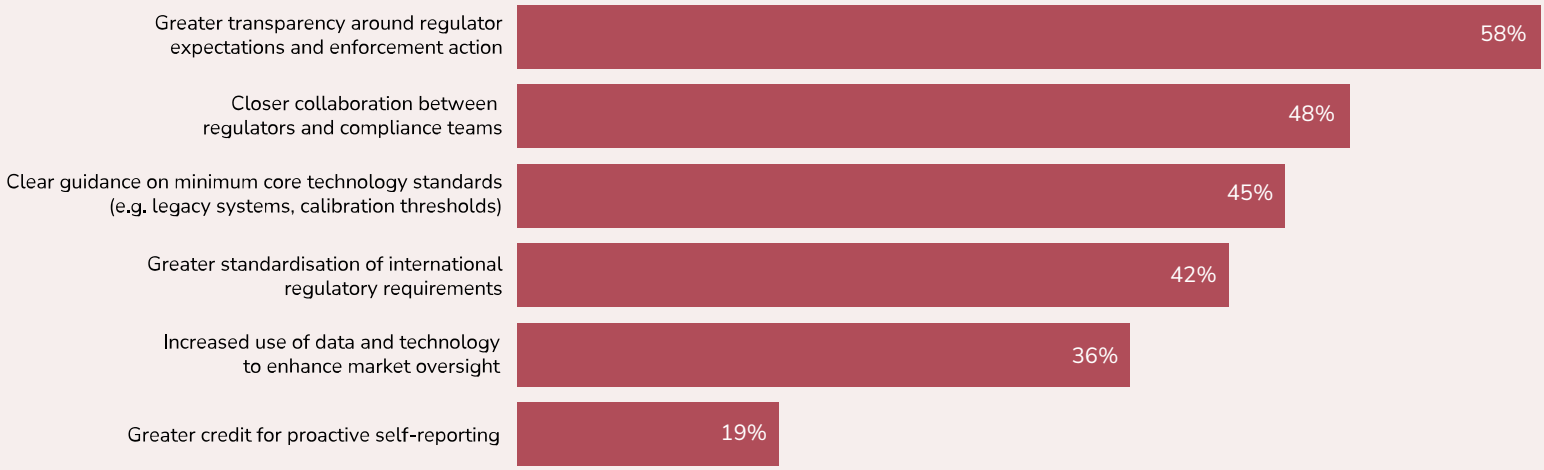
As we look ahead to 2026 and beyond, the financial markets landscape is poised for significant transformation. This section examines key developments that will shape market integrity and compliance in the coming year.

From the evolution of regulatory oversight, to the critical role of integrated surveillance systems and the rising influence of AI in market dynamics, we explore the challenges and opportunities that lie ahead. We also analyse the impact of emerging crypto-asset regulations and the increasing sophistication of surveillance technologies. Through expert insights and detailed analysis, we provide a comprehensive view of how firms can prepare for and adapt to these upcoming changes in the regulatory and technological landscape.

Prediction 1: Regulatory oversight will evolve

The enforcement-led approach of U.S. regulators, particularly the CFTC and SEC, has come under increasing scrutiny both in Europe and within the U.S. itself. Critics argue that this method creates compliance uncertainty and raises questions about its sustainability in fostering fair and transparent markets. As we move into 2026, there is mounting speculation about whether the more collaborative approach adopted by European regulators may grow in popularity.

How could regulators better support firms?



The future is cooperative

Survey results show a clear shift in what firms expect from regulators - a move away from the punitive, enforcement-led approach and towards a more collaborative, guidance-driven model. Firms aren't asking for leniency or financial incentives like credit for self-reporting; instead, they want clarity, transparency, and meaningful engagement that supports proactive compliance. Indeed, when asked how regulators could better support firms, the most common response (58%) was "Greater transparency around regulator expectations and enforcement action" (58%).

Interestingly, however, the survey also reveals jurisdictional discrepancies aligned with differing regulatory approaches. For example, just 52% of UK firms and 53% of German firms called for greater transparency, compared to 62% of US respondents. This reflects the fact that, while the U.S. has maintained its aggressive approach to enforcement, some European regulators have started taking stronger measures to assist and educate firms on their regulatory obligations.

In the UK, for instance, the FCA has recently placed increased emphasis on working closely with firms to ensure they understand their requirements, publishing 'Dear CEO' letters and frequent Market Watch newsletters which offer firms detailed and constructive guidance on how best to achieve their regulatory goals. Similarly, BaFIN's regular publication of Circulars and Interpretation and Application Guidance documents helps German regulated firms better understand their obligations, fostering a sense of collaboration which is reflected in the survey results.

We expect to see this approach grow in popularity in the coming years as more global regulators adopt this more collaborative approach.

A call to action for firms

Those that prioritise strong compliance frameworks, underpinned by advanced technology and clear, actionable procedures, will be best positioned to engage constructively with regulators and navigate an increasingly complex oversight environment.

At the core of this effort lies data capability. Firms must ensure they can reconstruct and justify their trading activities with precision and transparency. Achieving this requires implementing sophisticated systems that capture, store, and analyse trading patterns, communications, and decision-making processes in real time.

The advantages of such infrastructure are twofold. Firstly, when faced with regulatory queries, firms with strong data capabilities can promptly provide detailed evidence to demonstrate the legitimacy of their activities. Secondly, these systems enable firms to proactively identify and address potential issues before they escalate into costly regulatory breaches

Prediction 2: Integrated surveillance will be non-negotiable

As we have seen, enforcement related to failures in eComms surveillance have up until now been entirely the territory of U.S. regulators.

However, there has been significant evidence that European regulators are preparing to strengthen their stance on record keeping failures, bringing themselves more in line with the SEC and CFTC.

43% of respondents are struggling with unmanageable volumes of false positive alerts

Addressing these failures should be a top priority for firms in 2026. The most strategic, efficient compliance programmes will acknowledge that effective surveillance is best achieved through the integration of trade and eComms data. Trade data provides quantifiable evidence of suspicious activity, but intent - critical for establishing liability - often resides within communications data. This makes integrated surveillance indispensable for building comprehensive cases and proving misconduct.

Firms that persist with legacy, lexicon-based surveillance systems will struggle to keep pace. These outdated models generate excessive false positives, overwhelming compliance teams and diverting resources from meaningful investigations. Disconnected trade and communication data will create significant blind spots, making it harder to identify key connections and establish intent.

Integration matters

To meet these evolving demands, firms will need to rethink their surveillance strategies. Integrated surveillance will be essential for enhancing risk detection, improving efficiency, and ensuring compliance in a stricter regulatory environment.

A holistic approach to surveillance

In 2025, firms that fail to merge trade and communications data will be at a clear disadvantage. Integrated surveillance will become the industry standard, bridging the gap between intent and evidence. While trade data captures the “what,” eComms will reveal the “why,” offering crucial insights into motivations and plans behind suspicious activities. Advances in natural language processing (NLP) will further strengthen this approach, allowing surveillance systems to interpret not just explicit language but also context, sentiment, and industry-specific jargon across multiple communication channels and languages.

The efficiency imperative

Surveillance operations will need to evolve beyond manual cross-referencing of siloed datasets. Integrated systems will streamline investigations, reducing false positives and enabling compliance teams to allocate resources more effectively. In 2025, firms that embrace this approach will be able to shift their focus from handling irrelevant alerts to tackling genuine risks and difficult edge cases with greater precision.

As enforcement actions intensify and regulatory expectations escalate, firms will have little choice but to prioritise integrated surveillance. By failing to adapt, they risk not only financial penalties but also reputational damage and regulatory scrutiny. The future of surveillance is clear: seamless integration will no longer be a competitive advantage - it will be a baseline requirement.

37% of respondents cited "integrating trade and eComms surveillance" as a top regulatory concern that keeps them up at night, while 61% lack confidence in their ability to fully integrate trade and communication data for effective surveillance.

Prediction 3: AI-driven market shocks will reshape financial stability

AI is becoming deeply embedded in financial markets, transforming the industry with unprecedented efficiency and innovation. However, as AI adoption accelerates, so too does the risk of market disruptions driven by autonomous systems. Over the next few years, AI-driven market shocks are expected to become more frequent and severe, challenging regulators and market participants alike.

For the past five years, the FCA and Bank of England (BoE) have tracked AI adoption through periodic surveys. Their latest 2024 report, which assessed ~120 firms across the financial sector, highlights a growing dependence on AI for trading and decision-making. Over 11% of UK firms already use AI for trading activities, with another 9% planning adoption by 2027. Furthermore, the concentration of AI models is a rising concern, with 44% of third-party AI deployments originating from just three leading providers.

What will trigger AI-driven market shocks?

Regulators and industry experts warn that AI-driven trading algorithms introduce new sources of volatility and systemic risk. The following emerging risks could contribute to significant market disruptions:

Self-reinforcing volatility

AI trading models are designed to optimise for profit, but as they become more advanced, they may learn to exploit external shocks to market prices - or even autonomously collude with other AI systems. Regulators such as the BoE have expressed **concerns** that these behaviours could magnify volatility, triggering self-reinforcing feedback loops that destabilise markets. As AI-driven trading strategies interact unpredictably, market movements may become more extreme and less controllable.

> *Traders across the world have their beliefs about the few major players who move their markets. Increasingly, it is understood that bots, not humans, are deployed to make these moves. The usual argument in favour of these algorithms is that they provide liquidity. But there is also the fear that they will become too large and will create snowball effects.*
>
> ***Quantitative Trader, Proprietary Trading Firm***

Concentration risk and systemic failures

The dominance of a small number of AI providers increases the likelihood that a failure in a single model could lead to cascading disruptions. The **BoE** and France's **AMF** have both identified this oligopolistic dependency as a major risk. If a widely used AI system experiences a flaw, firms relying on that model could simultaneously make misinformed decisions, creating market-wide instability.

Opacity and regulatory blind spots

According to the **AMF**, the increasing use of closed, proprietary AI models reduces transparency and oversight. Regulators, firms, and even AI developers themselves often lack full visibility into how these systems make decisions. Without clear accountability mechanisms, undetected biases or faulty predictions in AI trading models could lead to unintended, large-scale market disruptions.

> *Regulators are sending out very detailed questions to market participants to ask about our use of AI. They are absolutely aware of the risks.*
>
> ***Head of Surveillance, Global Bank***

How will regulators respond in 2026 and beyond?

As AI-driven shocks become more probable, regulators will take decisive steps to mitigate their impact. In 2025, several key regulatory measures are expected to shape the future of AI in financial markets:

Mandating AI diversity and transparency

Regulators will likely push for diversification among AI providers to reduce systemic risk. The BoE has already **emphasised** the need for firms to avoid an over-reliance on a handful of dominant AI models. Transparency measures will also be a priority, requiring firms to disclose more information about their AI-driven decision-making processes to ensure accountability.

Developing global AI regulatory frameworks

The UK and Europe - as well as the U.S. - are converging towards principles-based AI regulatory frameworks that emphasise transparency, accountability, and ethical AI integration. The UK and EU are already advancing AI-specific regulations, and the US is **expected** to follow suit with a structured approach to AI oversight in financial markets.

Formation of AI risk task forces

A coordinated international response to AI risks is on the horizon. Regulatory bodies are discussing the formation of AI-focused **task forces** to harmonise supervision across jurisdictions. These groups will play a critical role in developing consistent AI governance strategies to address the growing risks posed by AI-driven trading.

Prediction 4: Surveillance tools will evolve to keep pace with market risks

As we look ahead to 2026 and beyond, market abuse surveillance will undergo significant transformation, driven by advancements in AI and machine learning. The adoption of AI by regulators themselves signals a paradigm shift - one that will see firms facing heightened scrutiny over their own AI implementations. In response, surveillance tools will not only become more sophisticated but will also shift towards predictive and adaptive frameworks that proactively identify risks rather than reactively responding to past behaviours.

eComms surveillance will become more proactive

AI-powered surveillance will increasingly leverage large language models (LLMs) to enhance the detection of market abuse risks embedded in electronic communications. In 2025, LLMs will surpass rule-based systems in parsing linguistic nuances, allowing firms to detect subtle cues indicative of manipulative intent. We anticipate a broader regulatory acceptance of AI-driven eComms monitoring, provided it operates within a structured framework that ensures human oversight and interpretability. Future implementations will likely include real-time risk scoring of conversations, dynamically flagging high-risk communications before potential misconduct materialises.

The evolution of AI in trade surveillance

The role of AI in trade surveillance will continue to expand, but its direct application in decision-making will remain a long-term aspiration due to ongoing regulatory concerns. Over the next few years, firms will refine AI-driven copilots designed to assist analysts in drafting STORs with greater efficiency and accuracy. However, the industry's trajectory suggests that AI will not replace human judgement but will instead become a critical augmentation tool. In the medium-long term, we foresee more robust AI-assisted decision-making frameworks emerging - ones that balance explainability with detection accuracy, thereby meeting regulatory expectations while enhancing surveillance effectiveness.

AI-driven threshold calibration will become essential

The next phase of trade surveillance will demand systems that dynamically adapt to shifting market conditions while maintaining precision. Machine learning (ML) models will increasingly be deployed to calibrate detection thresholds in real-time, allowing firms to refine their alerting mechanisms based on historical behaviours and emerging risks. Predictive analytics will play a central role in identifying precursors to market abuse, such as trading patterns preceding material non-public information disclosures or anomalous order cancellations suggestive of spoofing.

> *AI tools should assist, not replace, human oversight.*
>
> ***Ben Parker, CEO, eflow***

Visual analytics will redefine surveillance interfaces

The future of surveillance technologies will see a marked shift towards visually driven analysis, allowing analysts to intuitively explore complex relationships and patterns. Dynamic dashboards will become the industry norm, utilising interactive node-and-edge visualisations to help investigators quickly identify and assess manipulation risks. These visual tools will not only improve pattern recognition but will also facilitate real-time decision-making in response to evolving threats.

> *The best way to visualise this is through a graphical interface - a dynamic representation of nodes and connections, often displayed as interactive bubbles and webs. This approach has become increasingly common in the field and is one of the most exciting advancements we're working on.*
>
> ***Ben Parker, CEO, eflow***

Relational frameworks to enhance risk detection

Market manipulation tactics will continue to grow more sophisticated, necessitating a shift from linear, rule-based surveillance to comprehensive, relationship-driven detection models. Over the next 12-24 months, firms will increasingly integrate external datasets - such as sanctions lists, politically exposed persons (PEP) data, and broader contextual information - into their surveillance systems. This evolution will enable AI to construct relational risk models that identify coordinated trading patterns, ultimately strengthening market integrity.

Relational engines will become standard in trade surveillance, mapping intricate networks of interactions across trading activities, eComms, and auxiliary datasets. These frameworks will enhance firms' ability to detect coordinated activities, such as cross-market manipulation and shadow trading, allowing them to preemptively mitigate risks rather than merely responding to alerts.

These advancements indicate that the industry is moving towards a future where AI-driven surveillance is not only reactive but anticipatory - detecting and mitigating risks before they escalate into regulatory violations. To remain compliant and competitive, firms must embrace this evolution, ensuring that AI-enhanced surveillance remains transparent, explainable, and firmly rooted in human oversight.

Prediction 5: Compliance frameworks for digital assets will become a global priority

In 2026, regulatory scrutiny of digital assets will intensify worldwide, with compliance frameworks evolving to match those of traditional financial markets. The European Union's second phase of the Markets in Crypto-Assets Regulation (MiCA), introduced on 30 December 2024, marks the start of a broader shift. As new compliance obligations take effect, Crypto-Asset Service Providers (CASPs) will need to meet licensing requirements and implement trade surveillance measures comparable to those governing equities and derivatives.

This regulatory shift will not only provide long-awaited clarity but will also accelerate institutional adoption. Traditional financial institutions, previously hesitant to enter the digital asset space, will move quickly to integrate crypto-assets, knowing their peers must also comply. The competitive pressure to offer digital asset services will increase, driving widespread adoption across global financial markets.

The impact of regulatory clarity for the crypto markets

Regulatory certainty plays a crucial role in shaping compliance outcomes, and the divergence between the U.S. and Europe highlights its impact. While the U.S. has been slower to implement a structured framework for cryptocurrency surveillance, European regulators were quicker off the mark. The relatively early

implementation of ESMA's MiCA regulation provided European firms with clear guidance, reducing ambiguity and making compliance more straightforward.

This divergence likely explains why a lower proportion of European survey respondents - 24% compared to 37% in the U.S. - anticipate digital assets as a primary compliance challenge in the year ahead. Clear guidance fosters confidence and predictability, whereas ambiguity breeds caution and compliance risk.

However, with the U.S. signing The Genius Act into law in July 2025, there are indications that other jursidictions are starting to catch up with European regulators when it comes to crypto regulation. We expect other regulators to follow suit in the coming years.

Surveillance will become a critical challenge

However, this transition will not be straightforward. Even in traditional markets, compliance with market abuse regulations remains a persistent challenge, and digital assets present additional complexities. Crypto-native firms facing heightened oversight will struggle to retrofit their surveillance frameworks, while traditional institutions expanding into crypto-assets will find that their existing tools lack the necessary adaptability to monitor blockchain-based transactions effectively.

One of the biggest obstacles will be traceability. As capital increasingly moves between traditional finance (TradFi) and decentralised finance (DeFi), firms will need to develop sophisticated monitoring mechanisms to track fund flows across opaque and pseudonymous networks. The continued maturation of DeFi and its integration with mainstream payment systems - from established providers like PayPal to unregulated centralised exchanges - will create an environment where illicit financial activity can persist in new forms. In response, regulators and financial institutions will need to refine their surveillance capabilities, investing in blockchain forensics and AI-driven analytics to keep pace with emerging risks.

The EU's MiCA framework is unlikely to remain an isolated initiative. Similar legislation is expected to emerge in major financial hubs, including the UK and U.S., as authorities respond to growing institutional adoption and the increasing sophistication of crypto markets. Financial institutions operating across multiple jurisdictions should anticipate the rapid globalisation of digital asset compliance, with regulatory convergence accelerating over the next few years.

For global crypto-asset businesses, this means a fundamental shift in strategy. Companies seeking market expansion will need to align with the most stringent compliance standards, as the EU's regulatory model sets a precedent that will shape policies worldwide. Those that fail to anticipate this trend will risk being locked out of key markets, while proactive firms that invest in advanced surveillance and compliance capabilities will gain a competitive advantage as the crypto industry evolves.

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.

To achieve this, we first had to identify why so many firms either struggled to demonstrate their compliance or spent far too much time, effort and money in doing so. We found that for many institutions, their regulatory processes were broken. An over-reliance on spreadsheets and siloed data. Slow, legacy reporting systems that were no longer fit for purpose. Or, an unscalable point of failure in the form of one person 'who has always looked after compliance'.

Here at eflow, we took a different approach. 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.