U.S. trends in market abuse and trade surveillance 2025

How U.S. regulatory enforcement stacks up against the rest of the world

Contents

Executive summary

Welcome to eflow's second annual report on U.S. trends in market abuse and trade surveillance. Following the success of our inaugural report published last year, we have again delved deep into global enforcement data to understand the approach being taken by regulators and firms against the backdrop of an increasingly complex regulatory landscape.

At a headline level, U.S. regulators remain at the top of the global enforcement action league table, both in terms of volume of fines and their financial severity. During 2024, they collectively issued $1.67bn in fines for regulatory failures related to market abuse, which represents more than 90% of the total global value.

These figures not only highlight a notable year-on-year increase in the value of fines issued, but a staggering increase in the number of enforcement actions taken; the 119 penalties issued by U.S. regulators in 2024 is broadly comparable to the 133 they had issued in the previous four years (2019 to 2023) combined.

U.S. regulators widen the enforcement action cross-hairs

This massive increase in the volume of enforcement activity is perhaps the clearest indication of U.S. regulators showing their teeth when it comes to punishing firms for regulatory failures. However, it is also interesting to note that while the tier one giants continue to be penalised with nine-figure fines, 88 enforcement actions (74% of the U.S. total) carried fines of $5m or less. This particular insight shows a marked change in approach, with small and mid-market firms very much appearing in the regulatory cross-hairs. The days of smaller firms being able to 'fly under the radar' of U.S. regulators is long gone.

A deeper analysis of the enforcement action taken by U.S. regulators highlights their key areas of focus in 2024. Penalties relating to eComms recordkeeping, one of the most prominently targeted typologies of recent years, attracted the highest volume and value of fines at $740.7m. However, it was regulatory failures relating to trade surveillance systems and controls that was one of the biggest growth areas for enforcement activity; North American firms were fined $562.4m for these types of failures, as global penalties surged by 863% year on year.

An uncertain and unpredictable regulatory environment

In last year's report, I wrote about the stark difference in approach taken by U.S. regulators compared to the rest of the world. While the statistics mentioned above would appear to suggest that this 'enforcement first' strategy favoured in North America has only been increased, there are several factors in play that suggest there may be a change in approach on the horizon.

Firstly, the enforcement-led approach favoured by U.S. regulators, the CFTC and SEC in particular, has come under increasing scrutiny. There is a growing consensus of opinion that they will shift towards a more cooperative and guidance-oriented model that is widely used in Europe and APAC. This is certainly supported by our survey of U.S. regulatory professionals, 62% of whom called for greater transparency from regulators regarding the decision-making behind their enforcement action.

At the time of writing, President Trump's second term has so far been characterized by a flurry of executive orders, controversial decision-making, and significant economic volatility. It is proving difficult to predict what will happen next week, let alone months or years down the line. However, we do know that Trump's approach to public policy in his first term was defined by deregulation, and this stance appears to be even more aggressive in 2025.

While it's unlikely that the president's rhetoric will result in any significant changes to well-established regulations, it will be interesting to see how his administration's approach to digital asset regulation develops. The fragmented and uncertain regulatory environment surrounding digital assets in North America, particularly when compared to the structured framework of MiCA in Europe, is perhaps one of the reasons that 37% of U.S. regulatory professionals anticipate digital assets being a primary compliance challenge for their firm in the year ahead.

In conclusion...

The aggressive, enforcement-led strategy adopted by North American regulators has clearly remained in force during 2024, just as it has done for much of the last five years. However, the rapidly evolving economic and political landscape means that regulatory strategy could be set for a significant shake-up as we enter the second half of the decade.

The challenge of navigating this uncertainty means that the job of compliance professionals just got even harder. The ability of firms to deal with their short-term regulatory obligations, whilst also future-proofing against emerging risks, has never been more important.

I hope that this year's report offers some interesting insights that help to inform your firm's regulatory outlook.

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 recognized 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.

Jonathan Dixon | eflow Head of Surveillance

Jonathan joined eflow as Head of Surveillance in 2024 having fulfilled senior regulatory roles at Eventus, Kraken, Accenture and Barclays during his 15+ years in financial services. With significant experience in trade surveillance gained from both a vendor and client perspective, Jonathan helps to shape eflow's product offering in addition to working with clients to offer his unique insights regarding regulatory policy, strategy and system configuration.

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: a period of unprecedented uncertainty

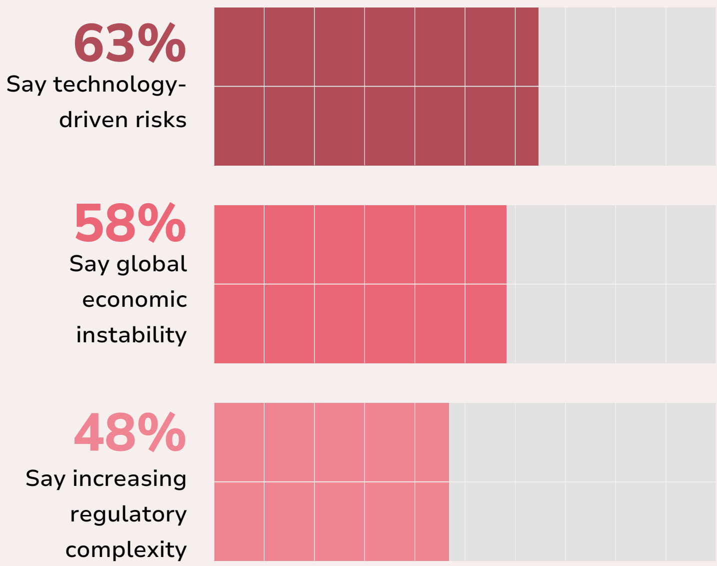
2024 was characterized by relentless uncertainty, driven by a confluence of factors that reshaped both the global and American regulatory landscapes. Political realignment, including the U.S. presidential election, heralded evolving regulatory philosophies, with implications for financial oversight and 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 and a hawkish pivot by the Federal Reserve 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 for U.S. firms in 2025?



This report captures our latest research - combining extensive primary and secondary data - analyzing 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 analyzed 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: North America, Europe 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 analyze 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 individual's 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 or for your own benefit.

The regulatory backdrop

From Q1 2019 to Q4 2024, U.S. enforcement figures far exceeded those by all other global regulators combined. During this period, there were:

252 fines
Issued for market abuse by **U.S. regulators**

$4.34 billion
In total financial penalties issued

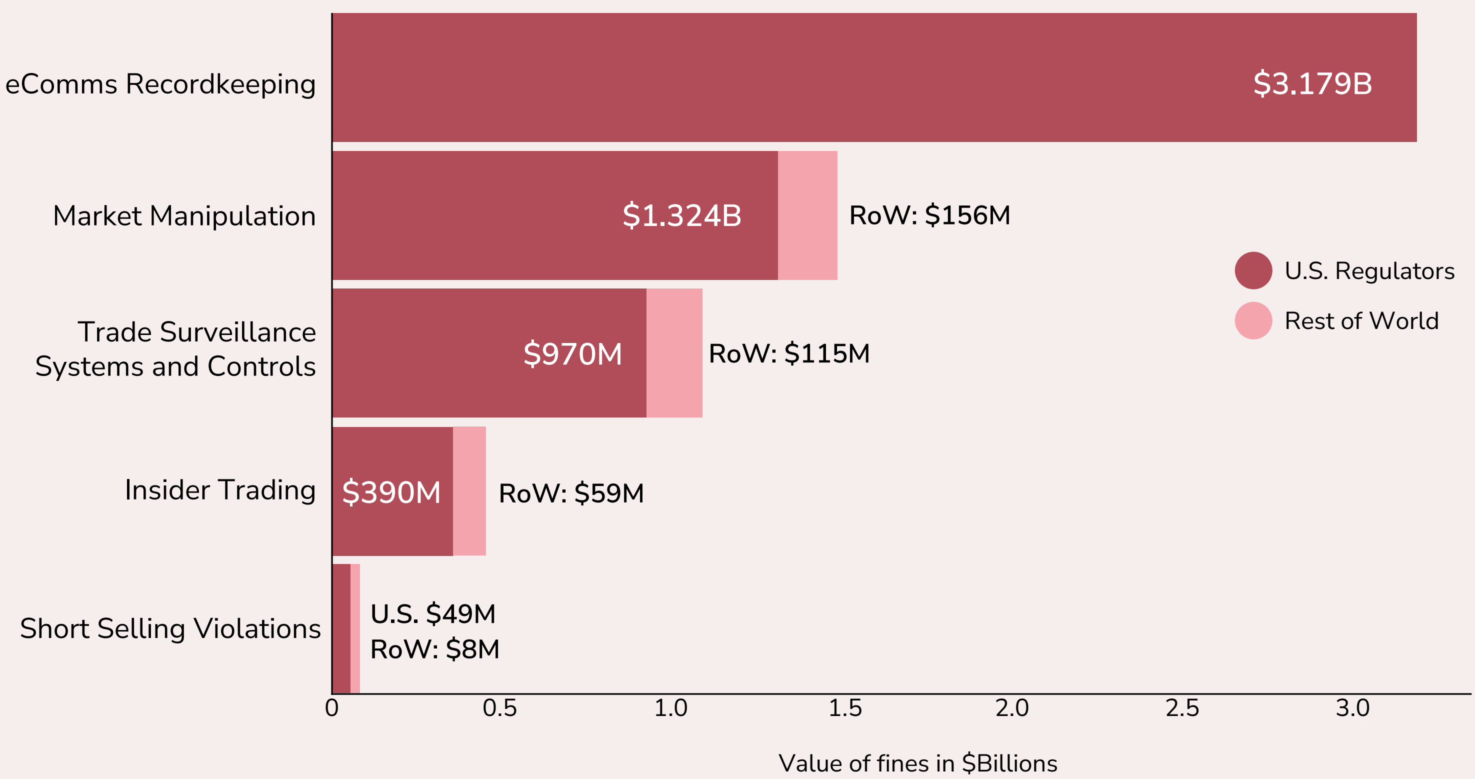
Compared to:

218 fines
Issued by **all other global regulators**

$1.96 billion
In total financial penalties issued

The scale of market abuse enforcement over the past five years, in particular by U.S. regulators, is undeniable. While U.S. regulators were more active across all typologies, eComms Recordkeeping in particular presents a striking gap; *100% of the $3.17bn in fines for eComms Recordkeeping-related failures were issued by U.S. regulators*, with no other regulator pursuing enforcement action for this typology during the examined period.

Breakdown of market abuse enforcements by typology

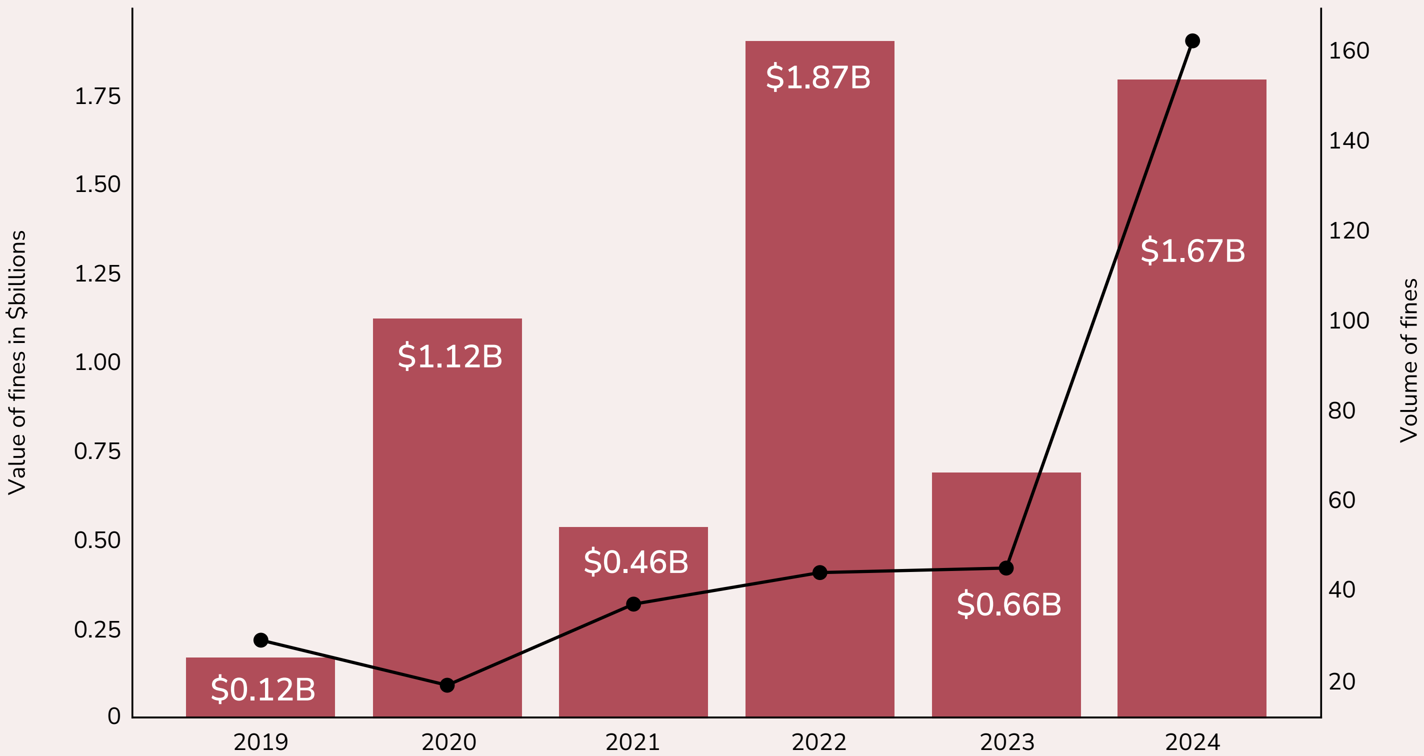


Beyond just eComms, these figures reflect a growing regulatory intolerance across all typologies. Enforcement is expanding rapidly across other typologies as well, and if recent trends are any indication, this is only the beginning. The scale and trajectory of enforcement activity suggests that market participants should prepare for even greater scrutiny in the years ahead.

Annual enforcement trends

The data highlights a decisive shift in regulatory enforcement, culminating in a dramatic spike in 2024. While 2022 saw a higher total value of fines, it was driven by a few major penalties. In contrast, 2024 reflects a sweeping crackdown, with regulators aggressively targeting firms of all sizes - small, medium, and large - resulting in both record-high volumes and substantial financial penalties. The post-COVID era of regulatory forbearance appears to be over, resulting in intensified scrutiny across the market.

Value vs volume of enforcements



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

Our survey found that 68% 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 eComms surveillance, for example. The widespread use of personal mobile devices and off-channel messaging apps like WhatsApp has undoubtedly added complexity to achieving compliance. The regulations haven't changed, but traditional surveillance methods struggle to keep pace with evolving communication habits. This regulatory friction - where compliance requirements remain static, but the tools available to market participants evolve rapidly - poses a growing challenge.

A similar issue arises in trade surveillance. Expanding asset classes, sophisticated trading strategies, and cross-market manipulation make it harder to detect market abuse. 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.

The mid-market crackdown

Prior to 2023, enforcement efforts focused heavily on major financial institutions, penalizing large banks for widespread use of unapproved messaging apps. This approach involved massive fines averaging $76 million each. However, by the end of 2022, regulators had **amended regulations** in a move to broaden their scope, increasingly targeting broker-dealers and investment managers of all sizes.

This shift in approach combined with the surge in eComms recordkeeping fines from 2021 onward reflects regulators' determination to tackle market abuse enablers, rather than just the most visible offences.

The latest data confirms that regulators have followed through on this broader enforcement strategy. In 2024, the average eComms recordkeeping fine dropped to $10 million, but enforcement volume surged, with 76 total actions, compared to just 24 in 2022. Notably, 64 of these fines were issued by the SEC, signaling an aggressive and sustained push to ensure compliance across the market.

> *It's no longer just tier one institutions that are being targeted for eComms; regulators are increasingly turning their attention to tier two firms and the mid-market space.*
>
> ***Jonathan Dixon, Head of Surveillance, eflow***

2024 deep dive

With this background context in place, we are able to better understand the regulatory activity that took place in 2024. In this year alone, there were:

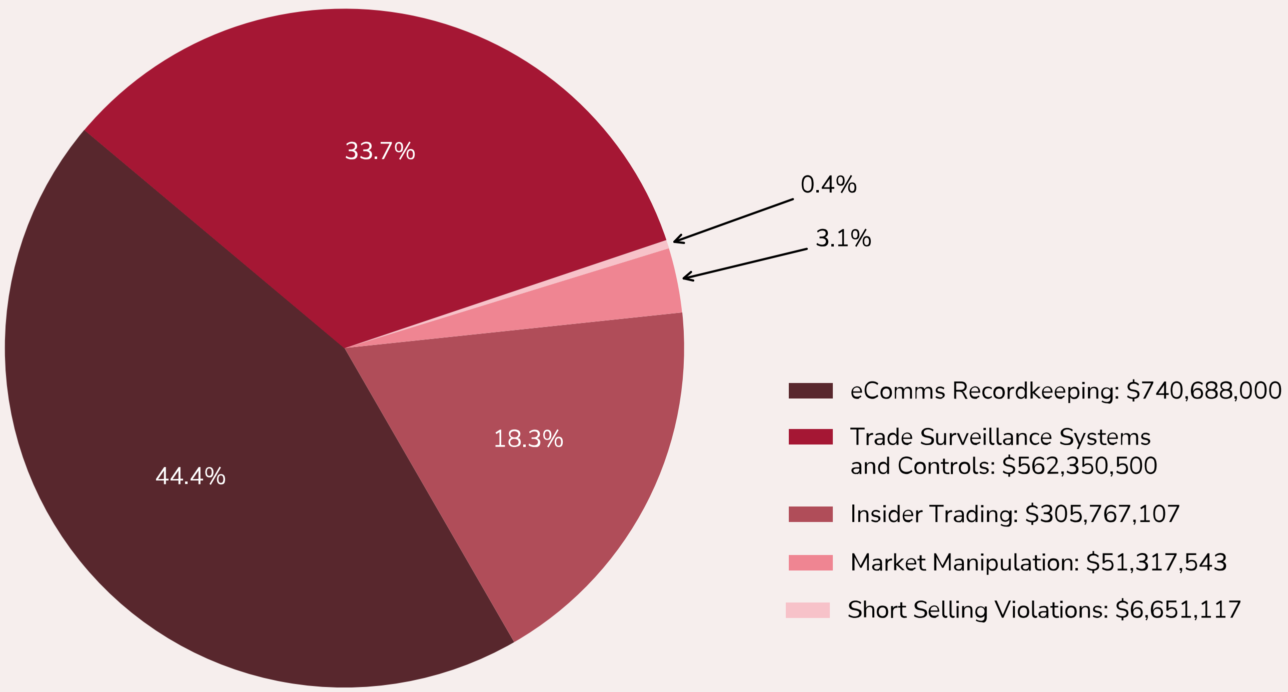
119 fines
Issued for market abuse by **U.S. regulators**

$1.67 billion
In total financial penalties issued

While eComms recordkeeping fines have risen significantly, 2024 has also been defined by a surge in insider trading and trade surveillance systems and controls enforcements. Last year's report highlighted the growing regulatory scrutiny on the data, systems, and controls firms use to monitor trading activities. 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.

The United States' enforcement breakdown stands out as the most balanced across typologies, with fines spread relatively evenly across eComms recordkeeping, trade surveillance systems and controls, and insider trading. This reflects the maturity of U.S. regulators' enforcement approach. Throughout the last five years, they have focused on identifying and punishing misconduct across multiple typologies, even leading the way on identifying new focus areas.

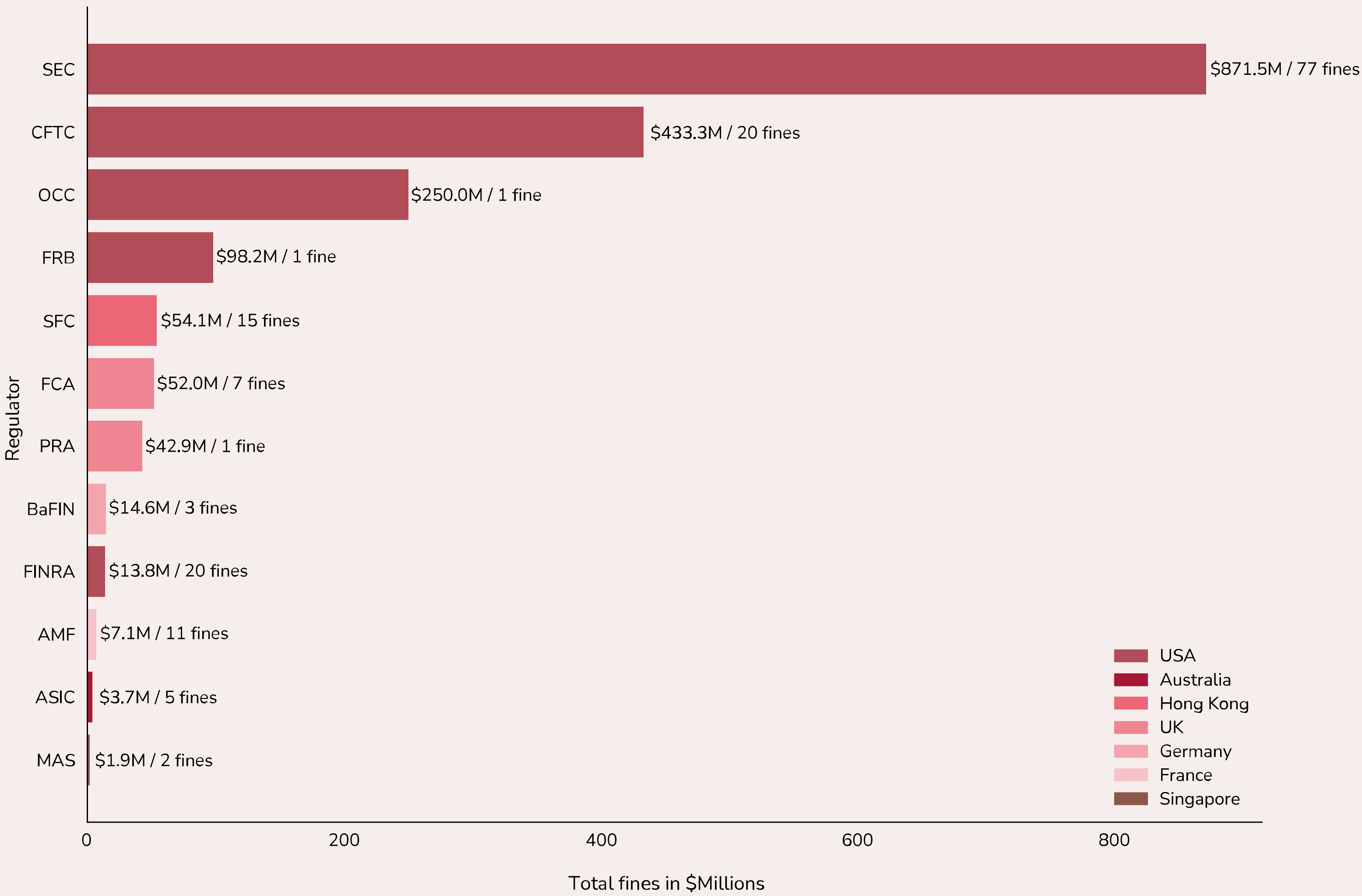
Breakdown of enforcement by typology



U.S. regulators compared to the rest of the world

Regulatory approaches vary significantly across jurisdictions, but 2024 has been another year of U.S.-led enforcement. The SEC and CFTC together account for over $1.3 billion in fines, reflecting the U.S.'s aggressive, enforcement-first stance. By contrast, UK regulators tend to take a more collaborative approach, engaging firms through 'Dear CEO' letters and guidance before resorting to penalties - which they will do where necessary. In Singapore and Hong Kong, regulatory frameworks remain pro-business, favoring guidelines over strict enforcement, with cases often pursued against individuals rather than firms.

2024 enforcement value and volume by regulator



In many of these cases, comparing them to the U.S. is comparing apples to oranges. Not only are the populations and economies of significantly different sizes, but their tradeable markets are too. In Australia, for instance, Macquarie Bank Limited were fined a record amount by ASIC's Market Disciplinary Panel for failing to detect and prevent suspicious orders. Naturally, much was made of this record breaking fine, which stood at just over $3 million. However, this is only a quarter of the U.S. average fine amount.

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 the U.S., analyzing 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

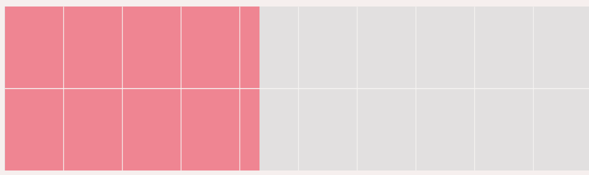
Market abuse continues to evolve, with an expanding array of manipulative practices presenting significant challenges for regulators and firms alike. This chart highlights some of the most prevalent forms of market manipulation identified this year, including pump-and-dump schemes, wash trading, spoofing,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

While market manipulation cases in 2024 accounted for more than $51 million in fines across seven 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 challenges are compliance professionals facing in 2025?

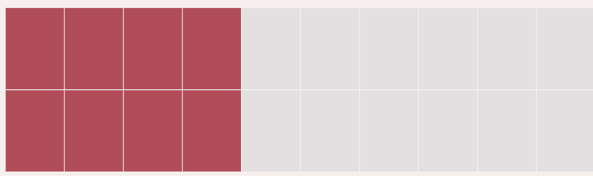
43%

Are struggling to keep abreast of ongoing regulatory changes



40%

Say accurately identifying market abuse keeps them up at night



Key market abuse typologies

The U.S. remains the chief enforcer of market abuse fines, with regulators addressing increasingly sophisticated schemes that exploit investor trust and market structures. Recent cases reveal a diverse array of risks, from deceptive trading practices to manipulative misinformation campaigns targeting retail investors.

Spoofing

In April 2024, a Nevada metals trader, Daniel Shak, was **sanctioned for spoofing** in gold and silver markets. Between 2015 and 2018, Shak placed numerous spoof orders in the gold and silver futures markets, creating false signals of supply or demand. He subsequently misled market participants, executing trades on the opposite side of the market at more favorable prices or larger quantities than he otherwise could have achieved.

The CFTC's enforcement response, including a $750,000 penalty and a permanent trading ban, underscores the regulatory emphasis on deterring such behavior, particularly among repeat offenders. This case was supported by the CME Group and the CFTC's Spoofing Task Force.

Short and distort

The SEC's **charges** against Andrew Left and Citron Capital LLC in July 2024 highlight a sophisticated "short and distort" scheme targeting retail investors. Left allegedly leveraged his Citron Research website and social media platforms to recommend positions in 23 companies while misrepresenting his own trading intentions. These recommendations typically triggered significant price movements, averaging 12%, which Left and Citron Capital exploited by taking contrary positions.

The scheme relied on trust built with followers, with Left allegedly making false promises, such as committing to hold a stock until it hit $65 while covertly selling at $28. Additionally, the SEC alleges that Citron misrepresented itself as an independent research entity, concealing compensation arrangements with hedge funds. These deceptive practices reportedly generated $20 million in profits.

Pump and dump

The SEC's **case** against two individuals orchestrating a microcap pump and dump scheme also demonstrates the use of digital channels to manipulate markets. According to the SEC's complaint, in the fall of 2019, one defendant secretly gained control of a large stock position in Minerco, a dormant penny stock company. The defendants allegedly then combined coordinated trading with false articles, social media campaigns, text messages and email distribution attributed to Minerco to give the impression of activity. The group created artificial demand before offloading their shares at a profit. The scheme manipulated prices in thinly traded stocks, where artificial demand can significantly distort prices, deceiving investors and resulting in significant losses.

Social media manipulation: Memes meet markets

Modern market manipulation is powered by smartphones and social media rather than trading terminals. Bad actors don't need complex trading algorithms or deep pockets - they just need followers, engagement, and a compelling story. Social media is enabling low-cost, coordinated retail investing that amplifies risks such as pump and dump schemes.

The numbers tell the story:
Finfluencers: 37% of U.S. Gen Z retail investors cite influencers as a major factor in their investment decisions (IOSCO).

Regulators are racing to adapt. FINRA's penalties, exemplified by the M1 Finance case, show growing scrutiny of influencer-led marketing campaigns.

IOSCO's ongoing consultation reflects the complex balance regulators must strike - acknowledging the potential benefits of social media for financial education while protecting markets from manipulation

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 minimize 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.

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: regulators have "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 behavior (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.

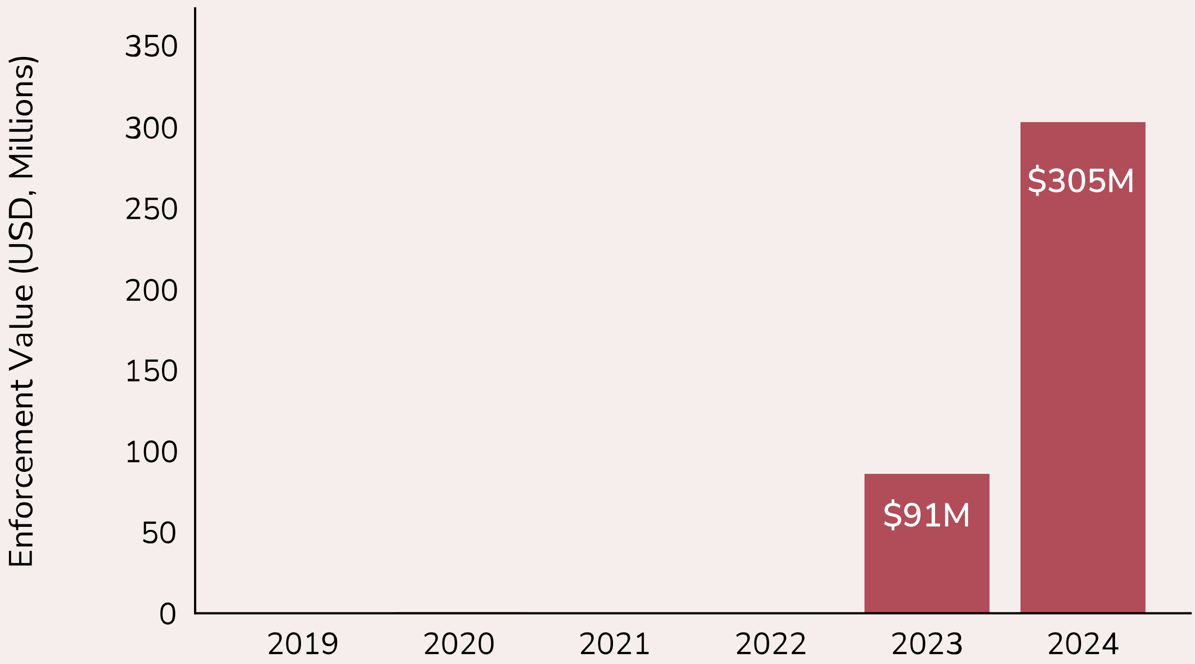
3. **AI-driven connections**: For the most covert connections, effective surveillance relies on AI and machine learning to identify subtle, non-obvious relationships between instruments, firms, or markets. These connections often go beyond simple product or industry ties, uncovering links that might 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 behavior.*
>
> ***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 235% increase in enforcement value compared to 2023, but the underlying tactics themselves have become more complex. It is **estimated** that the actual occurrence of insider trading could be up to four times higher than the number of cases prosecuted. Firms are losing ground, and more sophisticated detection mechanisms will be required to shift the balance in the years to come.

Insider trading enforcements



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 organized crime involvement in market manipulation
4. Growing cooperation between international regulators
5. Emphasis on individual accountability alongside institutional responsibility

Morgan Stanley block trading scandal

January 2024 saw the conclusion of the largest **insider trading enforcement** of the year, as Morgan Stanley was handed a $249 million combined penalty for systematic failures in its information barrier framework. The case centered on the firm's Syndicate Desk, where senior members leaked confidential information about impending block trades to buy-side investors. These investors then exploited the information by establishing short positions ahead of the trades.

The case highlighted several critical control failures:

- Breach of wall-crossing procedures between private and public-side employees
- Inadequate monitoring of trading alerts
- Delayed review of suspicious trading patterns
- Ineffective enforcement of written MNPI policies

Essential controls for firms

Effective insider trading controls require a multi-layered approach, combining information management, surveillance, and governance frameworks. Regulators emphasize 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 unauthorized access and improper handling of insider information
- Surveillance frameworks – Monitoring communications and trading activity to detect suspicious behavior
- 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 management

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

Surveillance framework

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 activity 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 transaction patterns

Governance and oversight

Compliance framework

- Dedicated oversight of insider information handling procedures
- Regular testing of information barriers and control effectiveness
- 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 an 825% increase globally 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.

Data governance as the foundation of effective surveillance

> *Everything comes back to data governance... that is at the top of the agenda.*
>
> ***Head of Surveillance, Global Bank***

Data governance took centre stage in 2024, catalyzed by J.P. Morgan's $348 million **fine** imposed by the FRB ($98.2 million) and OCC ($250 million) in March, followed by the CFTC ($200 million) in May, for failing to supervize its trade surveillance systems.

Despite prior commitments to improve oversight after a 2020 spoofing settlement, the bank discovered in 2021 that surveillance gaps had left billions of order messages across 30 global venues - including a major U.S. market - unmonitored for nearly a decade. These failures were rooted in misconfigured data feeds and an over-reliance on presumed "golden source" data without proper validation protocols.

In her **response** to the case, CFTC Commissioner Kristin N. Johnson said that J.P. Morgan should have "measured twice and cut once," highlighting that thorough preparation, careful assessment, and meticulous planning are essential to ensuring compliance initiatives succeed and deliver lasting improvements.

J.P. Morgan should have:

- **Double-checked their systems and processes** to ensure data completeness, accuracy, and proper configuration before deploying surveillance systems or relying on third-party providers.

- **Anticipated and mitigated risks** associated with data gaps or system incompatibilities, rather than assuming everything was functioning as intended.

> *Off the back of that [J.P. Morgan] fine, most tier one banks kicked off some sort of project to review their venue coverage and data governance.*
>
> ***Independent expert in Risk Assessments, Trade and Comms Surveillance***

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

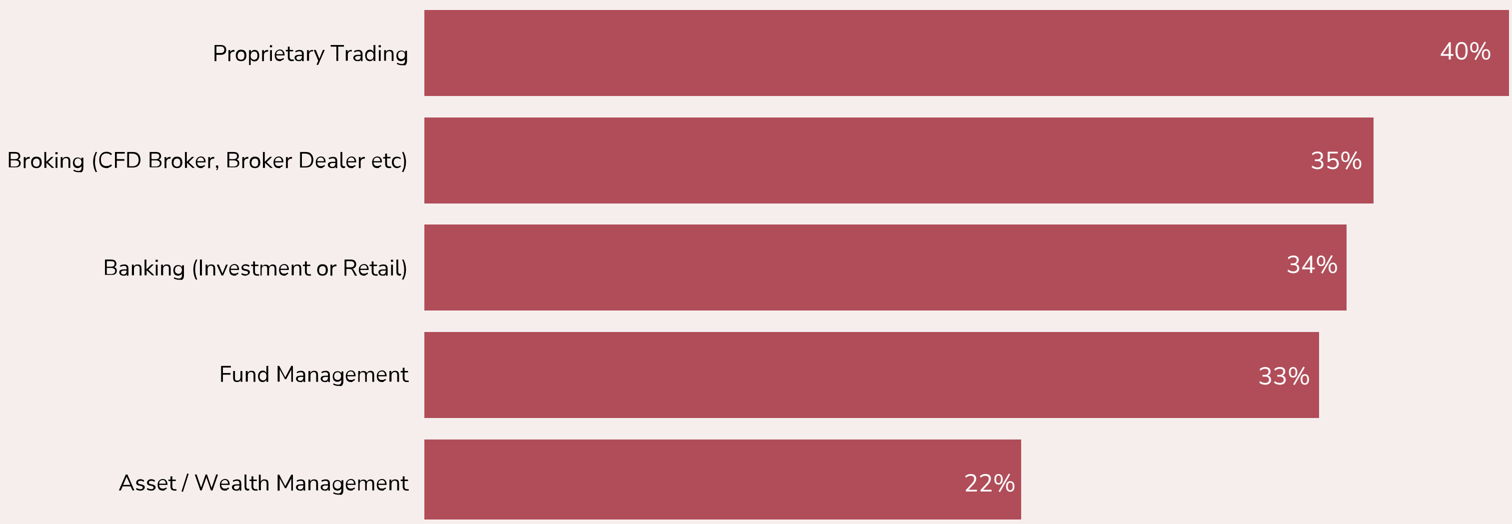
In 2024, scrutiny extended beyond data quality to how firms configure, calibrate, and monitor their surveillance frameworks. Firms must ensure their surveillance systems are not only built on high-quality data but also designed to adapt to evolving risks and regulatory expectations.

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.

% of respondents reporting trade surveillance configuration as a top concern



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.

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 analyze 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. Critics argue that this method creates compliance uncertainty and raises questions about its sustainability in fostering fair and transparent markets. As we move into 2025, there is mounting speculation about whether these agencies might shift towards a more cooperative and guidance-oriented regulatory model exemplified by international counterparts.

The importance of clear evidence

The Commodity Futures Trading Commission (CFTC) has come under intense scrutiny for perceived inconsistencies in its enforcement practices, sparking internal debates about the agency's approach to market oversight. At ISDA's Annual Legal Forum in October 2024, Commissioner Summer K. Mersinger delivered a pointed critique, emphasizing that enforcement should serve as a measure of last resort rather than the default response.

Her **comments** highlighted deep-seated concerns about ambiguous regulations, cautioning that overreach and novel interpretations could stifle smaller firms, ultimately diminishing competition and market diversity.

> *As I have said before, regulation through enforcement is the antithesis of regulatory clarity and transparency.*
>
> ***Summer K. Mersinger, Commissioner of CFTC***

Recent enforcement cases underscore the gravity of these concerns. In August 2023, the SEC fined Piper Sandler Hedging Services $14 million for recordkeeping violations related to off-channel communications. The following month, the CFTC imposed an additional $2 million penalty for similar breaches. This dual enforcement raised eyebrows, not least within the CFTC itself.

Commissioner Mersinger was particularly **critical** of the language employed in settlement orders, where terms like "business-related communications" and "firm business" were left undefined. The orders alluded to unapproved communication methods but failed to specify what records were absent or how their absence violated CFTC rules. According to Mersinger, this lack of clarity effectively suggests that any communication could qualify as a business record, eroding trust in regulatory processes. Such opacity burdens firms with heightened compliance costs as they overcorrect to mitigate the risk of punitive action.

Commissioner Caroline D. Pham **echoed** these criticisms, denouncing what she described as a lack of evidence underpinning the CFTC's claims. Addressing the Piper Sandler case, she stated "Once again, the CFTC has no evidence that a violation of CFTC recordkeeping rules for introducing brokers (IBs) actually occurred. This case also piggybacks off the SEC's investigation, veering into securities markets well outside the CFTC's jurisdiction."

These concerns are not isolated. In another **case**, Commissioner Pham's **dissent** alleged procedural shortcomings. The CFTC pursued enforcement relying on circumstantial evidence of market manipulation, despite internal compliance reviews and independent expert analyses confirming the legitimacy of the trading activity.

The implications of inconsistent enforcement are profound. Without clear, consistent evidence to guide actions, regulatory bodies risk undermining their credibility, fostering uncertainty, and inadvertently discouraging market participation.

The future is cooperative

There is a clear push from Commissioners like Mersinger and Pham for regulatory reform to make self-reporting more accessible and meaningful. Mersinger has highlighted the limitations of current practices, where credit for self-reporting is confined to disclosures made directly to the Division of Enforcement (DOE), excluding other oversight divisions. This narrow framework, she argued, discourages transparency by restricting companies' ability to receive recognition for proactive disclosure.

Mersinger also emphasized the need to better reward companies that invest significant resources in remediation and full cooperation. She contended that these firms, in effect, undertake much of the regulator's work at substantial expense and should be recognized with incentives that go beyond reduced civil monetary penalties. Such recognition would signal a shift towards a more constructive regulatory environment, rewarding accountability rather than simply penalizing missteps.

Commissioner Pham echoed these sentiments, commending the progress in cases like **Barclays** and **BNY Melon**, where cooperation was acknowledged. However, she pointed out that the current framework still falls short of fostering the kind of proactive compliance culture regulators aspire to achieve. For instance, while credit was given for cooperation, it was insufficient to significantly motivate firms to go above and beyond in ensuring compliance.

The SEC's approach to self-reporting in the case of **Atom Investors**, where prompt remedial actions and cooperation allowed the firm to avoid civil penalties altogether, has been praised as a model that could foster a more constructive relationship between firms and regulators.

How could regulators better support firms?

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.

The top-ranked response, "Greater transparency around regulator expectations and enforcement action" (62%), highlights the need to address criticisms such as those voiced by Commissioners Mersinger and Pham. Ambiguity in enforcement, as demonstrated in cases like Piper Sandler, has created a compliance environment where firms might overcorrect to avoid penalties, often at a significant cost to resources and trust.

Interestingly, the survey reveals jurisdictional discrepancies aligned with differing regulatory approaches. For example, 62% of U.S. respondents called for greater transparency, compared to 52% of UK firms. This difference reflects the contrasting strategies of regulators: the FCA's proactive approach, characterized by 'Dear CEO' letters and detailed guidance, stands in contrast to the SEC and CFTC's enforcement-first mindset.

Notably, "Greater credit for proactive self-reporting" received the least support (30%), suggesting that firms do not view the current mechanisms for rewarding self-reporting as meaningful or effective in fostering a proactive compliance culture. Instead, firms appear to prioritize action over reward - they are asking regulators to establish a transparent and predictable compliance framework rather than focus on after-the-fact financial benefits.

A call to action for firms

Those that prioritize 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 analyze 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

Market abuse enforcements have taken a steep upward turn, and this has largely been driven by surveillance; trade and eComms surveillance fines accounted for over 80% ($1.4 billion) of total enforcement penalties in 2024.

Addressing these failures should be a top priority for firms in 2025. 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.

30% of respondents are struggling with unmanageable volumes of false positive alerts

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.

> *eComms often serve as the 'smoking gun' for trade activities. They provide context, background, and insight into why something happened. Siloing communications from trade data makes it far easier for things to fall through the cracks. That's why we keep everything in one system*
>
> ***Head of Surveillance, Broker-Dealer***

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.

38% of respondents cited "integrating trade and eComms surveillance" as a top regulatory concern that keeps them up at night, while 52% lack confidence in their ability to fully integrate trade and communication data for effective surveillance.

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 prioritize 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.

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.

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 optimize 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 have expressed **concerns** that these behaviors could magnify volatility, triggering self-reinforcing feedback loops that destabilize 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 favor 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. 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

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.

How will regulators respond in 2025 and beyond?

> *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***

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. On the other side of the Atlantic, The Bank of England has already **emphasized** the need for firms to avoid an over-reliance on a handful of dominant AI models, and U.S. regulators are likely to follow suit. Transparency measures will also be a priority, requiring firms to disclose more information about their AI-driven decision-making processes to ensure accountability.

Stronger enforcement against AI misuse

Market abuse and AI-driven manipulation will face stricter penalties. Commissioner Kristin N. Johnson of the CFTC has **called** for tougher enforcement against firms that misuse AI for fraudulent activities. Her April 2024 speech at the Futures Industry Association's Law & Compliance Conference underscores an emerging regulatory focus on deterrence through harsher financial penalties and legal consequences.

Developing global AI regulatory frameworks

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

> *Data and AI were the two major topics in 2024, and I think those same two topics are going to continue into 2025.*
>
> ***Head of Surveillance, Global Bank***

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 harmonize 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 2025 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 emerging risks rather than reactively responding to past behaviors.

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 materializes.

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 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 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, utilizing interactive node-and-edge visualizations 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 visualize 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 priority

In 2025, regulatory scrutiny of digital assets will intensify, 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 which will undoubtedly be adopted by U.S. regulators. 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. MiCA provides a clear, structured framework, reducing ambiguity and making compliance more straightforward for European firms. In contrast, the U.S. has been navigating a fragmented and uncertain regulatory environment, intensified by an enforcement-led approach under Gary Gensler's SEC. His tenure left firms wary and reactive rather than proactive, contributing to a climate of regulatory unpredictability. Gensler's resignation at the end of 2024, coupled with a new presidential administration, has only added to regulatory uncertainty.

This uncertainty likely explains why a higher proportion of U.S.-based survey respondents - 37% compared to 24% in Europe - anticipate digital assets as a primary compliance challenge in 2025. Clear guidance fosters confidence and predictability, whereas ambiguity breeds caution and compliance risk.

The role of retail investors in digital asset markets

One key reason for the heightened regulatory focus on digital assets is the significant level of retail investor participation. Unlike traditional financial markets, where institutional investors dominate trading volumes, digital assets have been characterized by widespread retail involvement.

A JPMorgan Chase & Co. **study** found that as of mid-2022, nearly 15% of individuals had conducted transfers into crypto accounts. An EY-Parthenon **survey** from March 2024 revealed that 64% of retail investors plan to increase their crypto allocations, with 72% viewing digital assets as a core part of their overall wealth strategy. Finally, a Binance Research report found that 80% of Bitcoin in spot BTC ETFs is held by retail investors.

This retail-driven structure significantly influences regulatory priorities. When a market is composed primarily of institutional investors, regulators tend to adopt a more hands-off approach, focusing oversight on systemically important risks rather than individual investor protection. Conversely, retail-dominated markets invite stricter scrutiny due to the potential for consumer harm. The collapse of FTX, which left over one million creditors, the majority of whom were retail investors, underscored the consequences of regulatory gaps in digital asset markets.

This dynamic - regulatory intensity correlating with the risk of retail investor harm - was also evident in interviews, where contrasts can be seen in markets with little retail participation.

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 decentralized 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 centralized 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 the 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,. 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 standardized 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 customization 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.