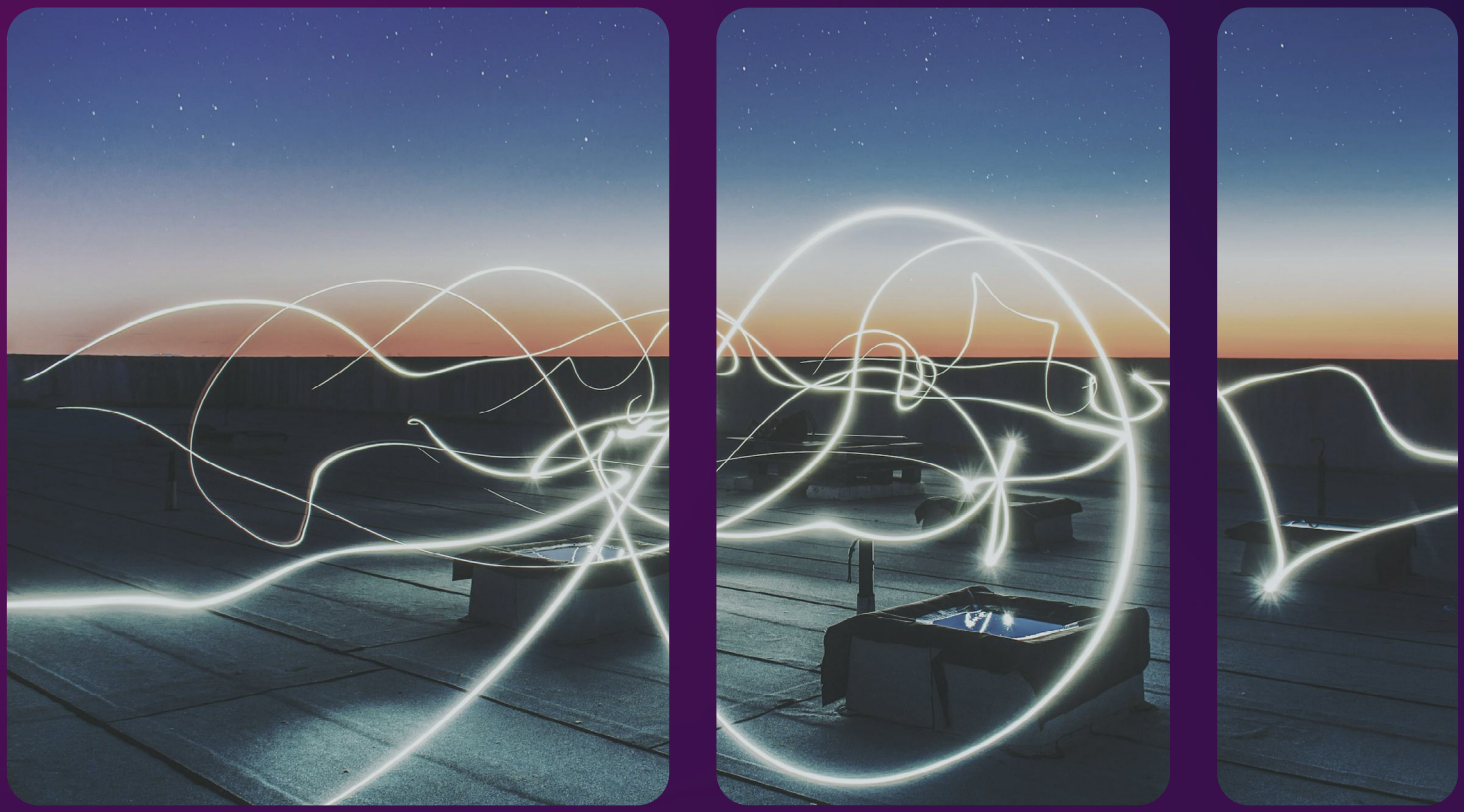


AN EFLOW EBOOK

Trade surveillance has a signal problem

The surveillance leader's agenda for 2027 and beyond

Contents

01 Introduction 3

02 The signal-to-noise ratio is breaking down 4

03 Why is surveillance generating so much noise? 5

Weak data foundations 6

Poorly configured surveillance logic 9

Limited testing infrastructure 12

04 The problem is intensifying as the surveillance perimeter expands 13

05 Regulatory expectations are rising in tandem 19

06 Where surveillance leaders go from here 21

About eflow 23

01

Understanding compliance teams' biggest trade surveillance challenges

Throughout 2026, eflow has engaged with more than 300 compliance and trade surveillance professionals across the UK, U.S., Europe and Australia. These conversations span investment banks, asset and wealth managers, hedge funds, brokers and proprietary trading firms, from smaller specialist institutions to large multinational organisations. Drawing on perspectives from Chief Compliance Officers, Heads of Surveillance and other regulatory practitioners, this paper examines the recurring challenges and emerging priorities shaping trade surveillance across global markets.

The central findings from 2026

False positives are symptomatic of deeper weaknesses in how surveillance systems process, interpret and assess trading activity. Firms are generating excessive alerts on legitimate trading activity, overwhelming analysts with unnecessary reviews, while potentially failing to detect genuine misconduct. Excessive noise is a significant operational problem, but missed signals represent serious compliance risks with even greater consequences.

These weaknesses are becoming more consequential as surveillance expands across products, venues, asset classes and trading hours. At the same time, regulators are looking beyond the existence of surveillance controls and increasingly scrutinising how firms design, calibrate and demonstrate their effectiveness.

01

Too much noise

Excessive alerts on legitimate trading overwhelm analysts with unnecessary reviews.

02

Missed signals

Genuine misconduct may go undetected – the risk with even greater consequences.

03

Rising scrutiny

Regulators want to see how controls are designed, calibrated and proven effective.

02

The signal-to-noise ratio is breaking down

False positives have been the Achilles' heel of trade surveillance since electronic compliance systems first went online. But the sheer volume of transactions in modern financial markets has scaled this noise to the point that it now actively undermines the effectiveness of surveillance programmes.

Throughout 2026, practitioners have described situations in which alert volumes have become operationally unsustainable:

> "We're drowning in false positives and our team can't keep up with the review process."
>
> **Chief Compliance Officer, North American Broker-Dealer**

33% of surveillance leaders say "**managing the volume of false positive alerts**" is among their **top three challenges**.

Source: 2026 Global trends in market abuse and trade surveillance

Surveillance leaders naturally focus on building controls that detect the broadest possible range of potential misconduct. But greater sensitivity, whether through lower thresholds, wider parameters or broader trigger conditions, is only useful if the system can still distinguish suspicious activity from legitimate trading. Otherwise, expanding detection coverage simply generates more work without necessarily improving effectiveness.

A 2025 enforcement action against Velocity Clearing illustrates the consequences of getting this wrong. Its surveillance system generated alert volumes that overwhelmed review capacity, with more than 15 million alerts left unreviewed or closed without substantive analysis. Nominal coverage remained in place, but once alert volumes exceed the firm's ability to investigate properly, **having surveillance in place becomes almost meaningless.**

03

Why is surveillance generating so much noise?

Across our conversations with surveillance practitioners in 2026, three recurring weaknesses emerged that help explain why systems struggle to distinguish legitimate trading from potentially suspicious activity.

01 **Weak data foundations**

Problems with the quality, completeness and connectivity of surveillance data.

02 **Poorly configured surveillance logic**

Rules that lack sufficient context, are inadequately tailored to trading activity or generate multiple alerts for the same event.

03 **Limited testing infrastructure**

Insufficient ability to test, refine and validate surveillance controls before changes go live.

Weak data foundations

Surveillance systems depend on the data feeding them. Incomplete, inaccurate or disconnected data can undermine even well-designed detection rules, either generating false alerts or failing to identify suspicious activity.

Data governance has been a regulatory focal point for several years, and took centre stage in 2024 with J.P. Morgan's $348.2 million fine imposed by the Federal Reserve ($98.2 million) and the OCC ($250 million) in March, followed by a further $200 million penalty from the CFTC in May.

30% of surveillance leaders rank "**data governance, including end-to-end data lineage**" in their **top three challenges.**

Source: 2026 Global trends in market abuse and trade surveillance

Across our 2026 conversations, many of the same fundamental problems persist. Three weaknesses emerged repeatedly, each affecting the quality of surveillance differently:

- Data mapping errors generating excess noise.
- Insufficient data granularity causing firms to miss abuse signals.
- Fragmented data losing the context needed to distinguish between the two.

Data mapping errors

Not every false positive originates in the surveillance rule. Some are created upstream, when trading data is incorrectly mapped or translated into the surveillance environment. One individual described problems with how their firm's trade files were interpreted:

> "One of the biggest issues from our perspective is the mapping of our trade files... buys and sells around the wrong way or the right way depending on which way you want to translate the trade."
>
> **Director of Operations, UK-based Investment Bank**

In this instance, incorrect mapping caused legitimate trading activity to be flagged as potential wash trading:

> "There'll be a trade there of a buy of 10,000. There'll be a sell of 10,000. And then it generates a wash trade order when we know full well that it isn't. It's another instance of another false positive."
>
> **Director of Operations, UK-based Investment Bank**

Firms can spend considerable time adjusting surveillance thresholds to reduce false positives when the underlying problem sits in the data itself. **Calibration cannot compensate for inaccurate inputs.**

Insufficient granularity

While inaccurate data creates false signals, insufficient data can prevent genuine signals from appearing at all.

A scenario can run every day and still generate alerts, yet be unable to identify the behaviour it was designed to catch. This is because the data that would reveal it never reaches the system.

One asset manager highlighted the limitations of relying on aggregated order data rather than individual execution records:

> "For a lot of the market manipulation use, you would need more granular fill-level data. And we haven't really got there... some of the market manipulation tests are not really going to work on your top-level order data."
>
> **Head of Compliance, Global Asset Management Firm**

A surveillance question cannot be more sophisticated than the data beneath it. Certain manipulation patterns – such as wash trading or marking the close – depend on the sequence, timing and characteristics of individual executions. When that level of detail is unavailable, surveillance controls may lack the information necessary to identify them.

Data fragmentation

When relevant trading information is distributed across separate systems, surveillance can lose the context needed to identify genuine misconduct or recognise legitimate activity.

> "We have data scattered across five different systems and no way to get a unified view for surveillance purposes."
>
> **SVP of Compliance, Global Investment Bank**

Context is not just useful for investigating an alert. The relationship between activities can itself be the signal. When the relevant data sits in separate silos, manipulation that spans instruments, venues or accounts becomes much harder to identify, especially when individual trades look benign in isolation.

CASE STUDY

$7.1m

Settlement between Credit Suisse Securities, FINRA and U.S. exchanges

Credit Suisse Securities was found to have routed hundreds of millions of trade, order and position records into an "orphan file" rather than its surveillance systems between 2012 and 2020. Until June 2018, nobody reviewed it for surveillance purposes. Surveillance ran against an incomplete picture, leaving potential insider dealing and manipulation undetected.

Most data gaps are less obvious. The underlying risk, however, is the same: surveillance can appear comprehensive while leaving material activity outside its effective coverage.

Poorly configured surveillance logic

Even with accurate and complete data, surveillance systems can fail. Rules must be granular and sensitive enough to detect signals of misconduct, but appropriately weighted to distinguish them from legitimate trading activity.

Across our practitioner conversations, three recurring configuration weaknesses emerged:

01

Omitting key context, even when the data exists

02

Insufficient tailoring to different trading activities

03

Failing to consolidate alerts relating to the same event

Missing context

Surveillance rules can identify behaviour without sufficient context to judge its significance.

Many traditional surveillance systems rely on static thresholds, such as flagging orders cancelled within a specified number of seconds. These rules may not adequately account for the counterparty, client type, instrument, market conditions or relationship to other trading activity.

Analysts often compensate for this missing context themselves. One asset manager described recognising recurring alerts as benign almost immediately:

> "Sometimes when you come to this screen... you can easily decide that these alerts are all going to be for the same reason... it happens to be a bank that you're dealing with."
>
> **Head of Compliance, European Asset Management Firm**

The analyst understands why the activity is legitimate, but the system repeatedly flags it. The same alerts are investigated and dismissed, **without that accumulated knowledge informing future detection.**

Blanket exclusions are not necessarily the answer

Suppressing alerts for particular counterparties may reduce noise, but it can also create blind spots. The objective is to incorporate more relevant context into how activity is assessed, while maintaining appropriate coverage and testing what is being filtered out.

One size fits none

Surveillance logic also needs to reflect differences between business models, trading strategies and asset classes. Yet practitioners described systems that apply the same tests across activities with very different trading characteristics.

> "You might have a long/short fund versus a macro fund or strategy... they all go through the same tests. But the problem is, they trigger a huge amount of false positives."
>
> **North American-based Compliance Consultant**

A long/short equity fund and a macro fund trade different instruments, at different frequencies, in different sizes. A threshold that suits one will misread the other's ordinary activity as anomalous. The test is not wrong; it is applied to the wrong baseline, and that is what undermines its effectiveness.

Calibration should account for meaningful differences in trading behaviour. However, excessive customisation brings its own maintenance and validation burden. The objective should be **proportionate tailoring**, rather than a separate set of rules for every desk or strategy.

FURTHER VIEWING

Our market abuse risk webinar series explores why risk assessments should inform surveillance control design, calibration and effectiveness testing.

Watch the series →

When one event generates hundreds of alerts

Even when rules flag the right things, configuration choices can multiply alerts and bury analysts. This can arise when individual executions are assessed separately, scenarios overlap, look-back windows repeatedly flag the same activity, or duplicate feeds generate additional alerts.

One commodities firm described an incident in which two traders accidentally traded against each other. Its incumbent surveillance system generated more than 200 alerts from the same event:

> "Two members of the team accidentally traded against each other, 35 lots in one-lot clips. We were getting six alerts for every lot, so it created over 200 alerts on the London Metal Exchange alone. I was literally selecting 200 alerts and writing the same three lines for each."
>
> **Compliance Analyst, UK-based Commodities Firm**

The underlying activity warranted investigation, but more than 200 individual alerts added little investigative value. One event effectively became hundreds of separate review tasks.

This highlights the importance of recognising related activity as a single investigative episode. Alert consolidation can significantly reduce duplication, provided distinct suspicious behaviours remain identifiable and the underlying alerts are retained for audit.

Stress-test your surveillance framework

Context
Does the system have sufficient information to assess the significance of an alert?

Tailoring
Are rules calibrated to the characteristics and risks of different trading activities?

Consolidation
Can the system recognise when multiple alerts relate to the same underlying event?

Limited testing infrastructure

A recurring frustration among practitioners is the lack of testing tools, configuration flexibility and resources needed to refine surveillance controls effectively.

The most fundamental limitation is the inability to test changes before deployment. Without a dedicated test environment, firms may only discover a configuration change's impact once it starts generating live alerts.

> "You don't really know what you're configuring until you get the results after the fact. There's no testing available."
>
> **Compliance Manager, UK-based Asset Management Firm**

Calibration then becomes a process of trial and error in production:

Change parameter → **Generate alerts** → **Review output** → **Adjust it again**

Each cycle consumes operational capacity and runs on live surveillance.

Limited configuration flexibility compounds the problem. One compliance professional at an investment platform described the constraints of their existing system:

> "It's limited in the way you can configure the [alert] tests within the system. It's not particularly dynamic."
>
> **Senior Surveillance Analyst, North American-based Investment Platform**

Even where improvements are technically possible, teams may lack the capacity to implement them. As one asset manager explained: **"We're wearing many hats and it's all about efficiencies."**

Together, these constraints make it difficult to move beyond reactive calibration. Without the ability to test changes, assess their impact and refine controls systematically, firms risk perpetuating the same surveillance weaknesses that have cost billions of dollars in fines.

04

The problem is intensifying as the surveillance perimeter expands

The weaknesses outlined above are becoming more consequential as financial markets evolve. Surveillance teams are being asked to detect misconduct across a wider range of trading activity, often using systems and controls designed for a narrower operating environment. This expansion is taking several forms:

Across products and venues	Manipulation may span correlated instruments, multiple venues, or an equity and its derivative.
Across time	Extended trading hours introduce different liquidity, volatility and behavioural conditions.
Across asset classes	Crypto, tokenised assets and prediction markets are entering frameworks built for traditional markets.

> "The scope of surveillance is widening across asset classes. Crypto, tokenised assets and prediction markets are all becoming much more significant, while changes such as 23/5 trading in U.S. equities will create a different set of surveillance challenges."
>
> **Ben Parker, CEO, eflow**

Each development places additional demands on data coverage, detection logic and calibration, potentially amplifying the weaknesses already affecting surveillance effectiveness.

Cross-product surveillance

Cross-product manipulation is particularly difficult to detect because suspicious activity may only become apparent when transactions across different instruments or venues are assessed together. It exploits structural gaps between venues, instruments and pricing mechanisms. Detecting it means linking activity that most surveillance systems assess in isolation, and doing so without overwhelming analysts:

> "We're looking for manipulation between correlated products... equity to derivative or whatever it may be. I think it's very hard to do without flooding yourself with false positives."
>
> **Surveillance Lead, Global Investment Bank**

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

The challenge is therefore not simply to monitor more instruments or venues, but to establish which relationships are relevant to potential misconduct, and calibrate detection accordingly. Widening the lens multiplies alert volumes, and firms must still justify their approach:



> "The challenge for firms is how to surveil across markets in a way that's technically credible, proportionate, and defensible to regulators."
>
> **Ben Parker, CEO, eflow**

Extended trading hours: the move to 23/5

U.S. equities are moving to near-continuous trading. The SEC approved Nasdaq's 23/5 framework in April 2026, with launch targeted for 6 December 2026, subject to Securities Information Processor (SIP) readiness and remaining SEC approvals.

Extended trading hours broaden international participation and change the conditions under which trading takes place. Overnight sessions may have thinner liquidity, different volatility patterns and fewer market participants. Activity that appears anomalous during regular trading hours may be entirely normal overnight, and vice versa.

> "[23-hour trading is] another realm of difficulty to tame the alerts for."
>
> **Surveillance Lead, Global Investment Bank**

Thresholds calibrated against regular trading conditions may therefore generate excessive alerts during extended sessions or fail to detect genuinely suspicious activity. This introduces a further testing burden. Surveillance teams will need to assess how their controls perform under different liquidity and volatility conditions, and recalibrate them as trading patterns evolve. For firms already constrained by limited testing infrastructure, this creates another challenge for maintaining effective detection.

MORE DETAIL ON OUR BLOG

What does 23/5 trading mean for my surveillance framework?

Read more →

> "Extending U.S. trading hours naturally opens those markets further to the rest of the world. That increases the burden on regulators to understand foreign participation, licensing structures and intermediaries, and I expect a regulatory rebalance once they see how the market changes in practice."
>
> **Ben Parker, CEO, eflow**

Prediction markets

Prediction markets are introducing new forms of market abuse risk, particularly around the misuse of non-public information.

In our previous Global Trends in Market Abuse and Trade Surveillance report, we identified prediction markets as an emerging regulatory priority for 2026. Subsequent enforcement activity has reinforced those concerns, including cases involving the alleged misuse of confidential corporate information and classified government intelligence to trade event contracts.

Q1 2026

The first two cases emerge. Both were on Kalshi and both were actioned by the exchange. We predicted direct regulatory enforcement would follow.

Q2 2026

The CFTC brought its first insider trading actions on prediction market event contracts: one against a U.S. Army service member, one against a Google engineer.

~$1.6m

Combined alleged profits, from classified intelligence about a military operation and confidential search data.

The underlying surveillance challenge is different from conventional insider dealing. In traditional securities markets, inside information often relates to an identifiable issuer, transaction or corporate event. Prediction markets allow participants to trade on outcomes spanning politics, geopolitics, corporate developments and other events. The potential sources of informational advantage are therefore much broader, and the individuals possessing that information may have no connection to financial markets.

> "Material non-public information used to be something you could track quite easily if it was leaked. But now you've got people putting [positions] on political or geopolitical events where they almost definitely have inside information, but you can't actually track that back to the source."
>
> **Ben Parker, CEO, eflow**

For surveillance teams, this creates difficult questions about what constitutes suspicious trading, which information sources are relevant and how potential misuse can be identified.

Regulatory approaches to prediction markets also differ between jurisdictions, introducing further complexity for firms operating internationally.

> "In the U.S. it comes under the CFTC, and they're very adamant that it needs to be treated in the same way as other markets. The UK takes a very different view. The FCA has banned binary options, and these are very similar – akin to gambling. I think the FCA will continue to ban it for retail customers."
>
> **Ben Parker, CEO, eflow**

Digital assets

Interest in digital asset markets is growing, and greater regulatory clarity is giving firms more confidence about what participation requires. But adapting controls for markets that operate very differently from traditional securities is not straightforward.

30 Dec 2024
EU: MiCA's market abuse provisions apply

1 Jul 2026
EU: maximum transitional period for existing cryptoasset service providers ends

30 Sep 2026 – 28 Feb 2027
UK: authorisation window open

25 Oct 2027
UK: new cryptoasset regulatory regime commences

In the U.S., the regulatory framework remains less settled, although the SEC and CFTC have taken steps to clarify their respective oversight of cryptoassets as broader market structure legislation develops.

> "The UK regime brings crypto in line with traditional registration and licensing under the FCA, and probably more in line with what we're seeing in Europe as well. Those intending to be market participants have to have the systems and controls of the traditional finance market."
>
> **Ben Parker, CEO, eflow**

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

The practical requirements are becoming more specific

MiCA's regulatory technical standards on market abuse require ongoing monitoring of orders and transactions both on-chain and off-chain, including order-book activity and aspects of distributed ledger technology that could indicate market abuse.

OFF-CHAIN
Orders, transactions and order-book activity

ON-CHAIN
Ledger activity that could indicate market abuse

01 **Start with the foundations**
Firms are mapping trading activity across platforms and blockchain networks to ensure their surveillance systems capture the necessary data.

02 **Adapt and test detection rules**
The next challenge is adapting and testing detection rules against the characteristics of crypto trading.

03 **Calibrate for how crypto actually trades**
Many abuse patterns are familiar, but crypto markets operate continuously, often across fragmented venues and with different liquidity conditions. Firms need to calibrate their controls accordingly, rather than assuming rules developed for traditional securities will perform as intended.

05

Regulatory expectations are rising in tandem

As surveillance becomes more complex, regulatory expectations are also becoming more demanding. A recurring theme is the shift from demonstrating that surveillance controls exist to explaining why they are appropriate and providing evidence that they work.

For surveillance leaders, that means being able to answer some fundamental questions:

Q1
Why does this threshold exist?

Q2
Why is it calibrated this way?

Q3
Is it proportionate to the risk?

Q4
Can you demonstrate it works?

Calibration is under scrutiny

Practitioners describe supervisors taking a closer interest in how surveillance systems are configured. One compliance leader at an investment platform told us an FCA supervisory visit examined "the calibration of the system", alongside resources, escalations and STOR decisions. As another practitioner explained:

> "It's not so much 'do you have a system in place?' anymore. It's 'how effective is that solution?' They really are looking at the amount of false positives being generated. And then they ask: what's the rationale? Why do you have the system configured the way you do?"
>
> **Surveillance Specialist, European-based Wealth Management Firm**

FCA MARKET WATCH 86, OCTOBER 2026

UK retail brokers visited by the FCA

The FCA's own public findings corroborate this. All seven firms had automated surveillance systems and written procedures, yet the FCA identified material weaknesses in how controls were designed and operated:

- Some firms applied flat price-movement thresholds without accounting for differences in stock volatility.
- Others set minimum trade-value parameters so high that significant amounts of client activity were excluded from monitoring.
- In some cases, those responsible for surveillance could not adequately explain how their systems worked, appearing to rely on default vendor settings.

The FCA's findings closely reflect the challenges raised in our practitioner conversations and throughout this paper. Surveillance effectiveness cannot be judged by alert volumes alone. Firms need to test whether their controls are detecting the risks they are designed to identify, and where potential blind spots remain.

Surveillance decisions must trace back to risk

Firms must be capable of demonstrating that surveillance controls reflect the market abuse risks identified in their business.

> "A lot of firms have got surveillance systems in place, but where they're seeing the downfall is the risk assessments and having that link back."
>
> **Senior Market Surveillance Specialist, UK-based Investment Platform**

MARA - The market abuse risk assessment - should provide the starting point for surveillance design, informing which behaviours need monitoring, how controls are configured and how their effectiveness is evaluated.

FURTHER VIEWING

Our market abuse risk governance webinar series explores the connection between risk assessment, surveillance design, calibration and effectiveness testing.

Watch the series →

Greater scrutiny is not confined to the largest institutions:

> "We've seen scrutiny across our customer base on mid-sized firms, like investment managers. There's a lot more around justification and proof. It's a full top-down approach: the big institutions, as well as mid-size and smaller firms."
>
> **Ben Parker, CEO, eflow**

This raises the bar for surveillance teams of all sizes. It's no longer enough to rely on standard vendor configurations or point to the existence of detection rules. Firms need to justify why particular risks are monitored, why thresholds have been set where they are, and how they've established that those decisions provide adequate coverage. Just as importantly, they need to understand what their controls may be missing.

06

Where surveillance leaders go from here

If your surveillance team is struggling with false positives, take a forensic approach to diagnosing the root causes. Our conversations this year have highlighted several recurring weaknesses, but the potential causes extend well beyond those covered in this paper.

01

Start with the data

02

Examine rules and calibration

03

Scrutinise the technology

The key is to investigate systematically rather than simply adjusting thresholds to reduce alert volumes. Start with the data, then examine how surveillance rules are configured and calibrated against the risks and trading characteristics of your business. At the same time, scrutinise the technology itself. **Does your system give you the flexibility to refine controls and test changes properly, or is it part of what's holding you back?**

LOOKING AHEAD TO 2027

There's a real competitive advantage to getting this right. Firms with effective, adaptable surveillance will be better placed to enter new markets, expand their product offerings and pursue new lines of business, confident that their controls can keep pace. And they'll be able to do so without overwhelming compliance teams, continually adding headcount or allowing surveillance costs to spiral.

THE BOTTOM LINE

The measure of effective surveillance is not how many alerts a system generates, or even how many it eliminates.

It's whether the right risks are being detected, investigated and addressed, and whether you can demonstrate that your controls are working.

Talk to our team →

About eflow

Twenty years ago, we realised that many firms' regulatory processes were broken. Too time-consuming, too expensive, too reliant on legacy technology that was no longer fit for purpose.

So, we built the PATH platform; a constantly evolving digital infrastructure tailored to each of our client's individual compliance needs. Today, it is trusted by over 140 financial institutions around the globe, ranging from top-tier investment firms to multinational brokers, innovative trading platforms, and a lot more in between.

In 2025 we launched PATH AI to incorporate the very best of this emerging technology. This evolution of the PATH platform ensures that every eflow product keeps our clients fully in control of their compliance and that they stay one step ahead of any regulatory changes.

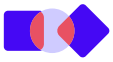
Trade Surveillance



Noise-cancelling market abuse and insider dealing monitoring.

Explore Trade Surveillance

eComms Surveillance



Multi-channel communications monitoring and archiving.

Explore eComms Surveillance

Best Execution & TCA



Regulator-ready Best Ex and transaction cost analysis.

Explore Best Execution

Transaction Reporting



Automated MiFIR reporting with audit trails.

Explore Transaction Reporting

Noise-cancelling surveillance

Explore our regulatory technology solutions at www.eflowglobal.com

Book a demo →