AN EFLOW EBOOK

MAR: Ten Years of Market Abuse Regulation

What it's achieved, what gaps remain, and how it will need to evolve in the face of new risks

Introduction

It has been ten years since the Market Abuse Regulation (MAR) came into force, and with it, a fundamental shift in how European markets identify, report, and prosecute market abuse. MAR raised the bar for firms, extended the regulatory perimeter to markets that had previously operated in the shadows, and built the surveillance infrastructure that modern capital markets now depend on.

But a decade is long enough to ask harder questions. Technology has transformed capital markets from fragmented trading floors into digitised global ecosystems, and catching market abuse in 2026 looks nothing like it did in 2016. Digital assets and artificial intelligence are set to stress-test the framework further still. The data suggests that, for all the progress, significant gaps remain.

This eBook takes stock of ten years of MAR: what it achieved, where firms are still struggling, and what the next decade is likely to demand.

A brief history of market abuse regulation

Before 2003, European market abuse regulation was fragmented. Each member state had its own definitions of what constituted market abuse, its own enforcement powers, and a varied appetite for exercising them.

The Market Abuse Directive (MAD I, or MAD 2003) was the EU's first attempt at harmonisation. It introduced common definitions for insider trading and market manipulation across member states and built the first common architecture for fighting market abuse across Europe. Many foundational elements of market abuse prevention were borne out of MAD I:

- It required each country to designate one National Competent Authority for overseeing market abuse.

- It introduced the first EU-wide suspicious transaction reporting (STR) obligation, requiring institutions to put procedures and controls in place to prevent and detect market abuse, and escalate any suspicious transactions to the NCA.

- It created a disclosure framework for inside information.

The Directive represented real progress, but implementation was a challenge. MAD I set the framework, but left each country to transpose it into national law. In practice, the final rules diverged across Member States, which largely undermined the harmonisation that MAD I set out to achieve.

MAD I also had a perimeter problem. It only covered instruments admitted to trading on regulated markets, so as trading activity migrated into OTC derivatives, spot FX and other instruments, the framework began to show its limits:

- **LIBOR rigging (exposed 2012)**: Coordinated manipulation of the benchmark underpinning trillions of dollars of contracts globally. Billions in fines, multiple major institutions implicated, and a direct demonstration that benchmark abuse sat outside existing market abuse rules.

- **FX rigging (2013–2015)**: Coordinated manipulation in spot FX markets. Largely outside MAD I's scope as an OTC product, and on a scale that implicated the world's largest banks.

These were systemic failures by major institutions, and they handed regulators the political mandate to act. The response was MAR.

Market Abuse Regulation (MAR)

MAR came into force on 3rd July 2016, replacing MAD I with a regulation that was directly applicable across all member states without national transposition. This was a structural choice to address the implementation problem that had limited MAD I's impact from the start. But the more substantive changes were in the details:

- **Expanded instrument scope**: OTC derivatives, spot commodity contracts, related financial instruments and benchmarks were all brought within scope.

- **STRs replaced by Suspicious Transaction and Order Reports**: The addition of orders was the key change. The surveillance duty now attaches at the point of intent, not just execution. That matters because the most common manipulation techniques (spoofing and layering) work by placing orders never intended to be filled.

- **Tighter insider list rules**: MAR tightened the obligations around who gets recorded as having access to inside information, and when. Insider lists became more prescriptive – firms had to maintain them in a specific format, update them promptly, and be ready to produce them to regulators on request.

- **Market soundings framework**: MAR sets out when a sounding is legitimate, what must be disclosed to the investor receiving it, and what records must be kept. It brought structure and accountability to a practice that had long operated in a legal grey area.

- **Stronger whistleblowing provisions**: MAR introduced a requirement for member states to establish effective channels through which potential or actual breaches could be reported to regulators and to ensure that those doing the reporting were protected from retaliation.

> *"MAR didn't just change the rules, it created an entire industry. A whole ecosystem of technology, expertise and process that simply didn't exist before."*

Ben Parker,
CEO of eflow

UK MAR and EU MAR: navigating regulatory divergence

When the UK left the EU, it onshored MAR directly into UK law, creating UK MAR as a near word-for-word copy. For several years, the two regimes remained aligned.

The EU Listing Act, passed in 2024, amended MAR and introduced a slight divergence between the two regimes for the first time. Key changes to EU MAR include:

- **Protracted processes:** Intermediate steps in complex transactions no longer require immediate disclosure. Only the final event must be disclosed. This applies from 5th June 2026.
- **Disclosure delay conditions:** The threshold for delaying disclosure has been lowered. Delayed information now must not contradict the issuer's latest public statement, replacing the previous 'mislead the public' test.
- **PDMR transaction threshold:** Managers' transaction reporting threshold raised from €5,000 to €20,000.

UK MAR is under review as part of the Edinburgh Reforms, but timing is unclear and no specific changes have been signalled.

Firms with securities listed in both the UK and EU now face two materially different sets of disclosure obligations for the same underlying information.

Core market abuse offences are defined uniformly in UK MAR and EU MAR. The surveillance obligations, STOR requirements, market soundings framework, and the fundamental prohibitions are all still substantively aligned.

ESMA's first in-depth review, published in 2020 after four years of implementation and extensive industry consultation, concluded that MAR had functioned well in practice and was fit for purpose. Respondents focused on specific amendments rather than a meaningful overhaul.

The FCA has also found no evidence of a deterioration in underlying market integrity over the decade. And beyond the statistics, MAR created a compliance infrastructure with sophisticated surveillance systems, eComms monitoring, STOR workflows and insider list management.

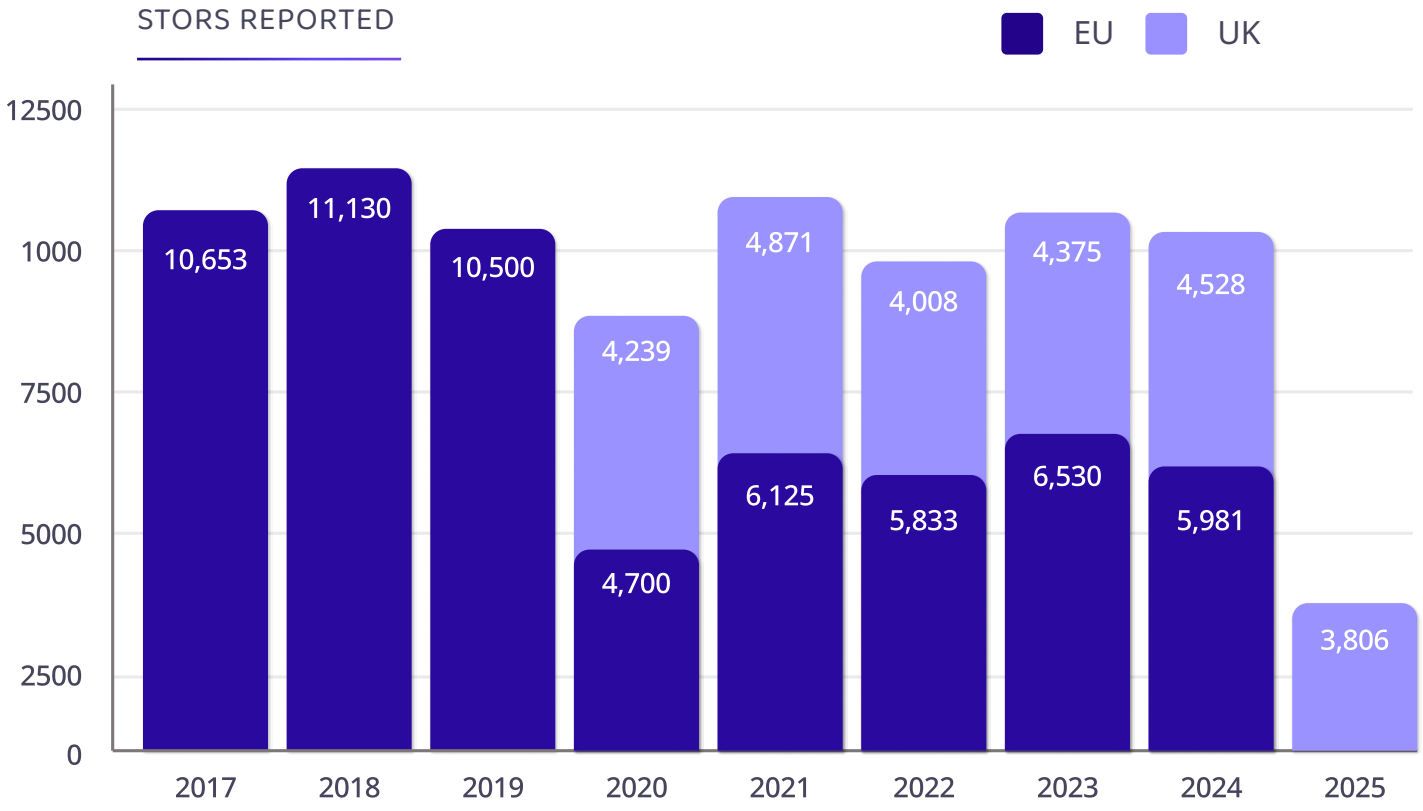
Taking stock: eflow's assessment

ESMA's 2020 review and the FCA's own market intelligence provide an important and broadly positive baseline assessment. But a lot has changed since 2020: crypto has moved from the margins to the mainstream, AI has entered both the trading floor and the compliance function, and the nature of market abuse itself has grown more complex.

To take a fuller measure of where things stand today, we have drawn on two sources. The first is our annual survey of 300 compliance decision-makers across the UK, France and Germany – three major MAR jurisdictions – covering everything from surveillance investment to the challenges keeping compliance teams awake at night. The second is eflow's own enforcement tracking database, monitoring outcomes across a core set of regulators over the past two years.

Suspicious transaction and order reports: The signals

STOR data provides insight into how the system is performing day-to-day. Combined, the UK and European reporting pipeline now handles around 10,000 to 11,000 STORs annually at its peak – a volume of market intelligence that simply didn't exist under MAD I. At face value, that pipeline represents exactly what MAR was designed to create: a steady flow of market intelligence giving NCAs and the FCA the raw material to detect, investigate and act.



Notes

- Data for 2017–2019 reflects combined UK and EU reporting before Brexit.
- 2019 should be treated as a transition year. Reporting patterns were disrupted as firms prepared for the UK's departure. ESMA provided a data range of 10,000 - 11,000 STORs; we have taken the middle value (10,500).
- From 2020, UK and EU figures are captured separately following the UK's exit from the EU; the apparent drop in overall volume from 2019 to 2020 largely reflects this split rather than a genuine reduction in reporting activity.
- 2025 UK data is from the FCA's annual STOR report; EU data for 2025 is not yet published by ESMA and will be available in due course.
- Data is aggregated from ESMA, which publishes annually, and the FCA.

Across both the FCA and ESMA datasets, the overwhelming majority of STORs (85-90%) concern equity trades. That reflects where surveillance infrastructure is most mature, not necessarily where most abuse occurs. Equities have transparent order books, standardised data and decades of developed surveillance tooling. Fixed income, FX, OTC derivatives and commodities remain under-reported.

Quality is a separate concern. ESMA's peer review found 13 NCAs partially compliant or non-compliant in their response to poor-quality or suspected non-reporting of STORs. The FCA has separately warned that delayed or vague reports point to deeper compliance failures, not just procedural missteps. The STOR regime is a genuine and important step forward. But filing a report and filing a useful one are not the same thing, and that gap remains live.

Our survey findings suggest that the gap is well understood on the ground.

- Aggregating data and providing full context for regulatory reporting, including STORs, is keeping 44% of European compliance leaders awake at night, against 37% globally. This challenge is cited by just 28% of UK-based institutions.
- The FCA has been explicit about STOR quality expectations. Its Market Watch bulletins have directly addressed what good and poor reporting looks like, giving UK firms clearer benchmarks to work against. This may contribute to the relative confidence in UK institutions.
- European firms face an arguably more complex landscape. Firms operating across multiple EU jurisdictions must navigate different NCA expectations, different reporting cultures, and, as ESMA's own peer review confirmed, significant variation in how NCAs supervise the obligation.

The FCA is direct about the benefit of STORs: “These reports are invaluable to our work, with over 70% of our current market abuse investigations originating from a STOR.” These reports are where the enforcement story begins, but converting that intelligence into proven cases is where complications arise.

Market abuse enforcement: The outcomes

Market abuse is notoriously difficult to prosecute. As ESMA has noted: “Insider dealing and market manipulation infringements imply extensive investigations and complex evidence gathering exercises. Sanctioning those infringements is likely to require more work and longer delays than administrative measures imposed for other infringements.”

Enforcement data, by its nature, shows only what regulators have been able to prove. eflow has been tracking enforcement outcomes across a set of core regulators for the past two years. Here’s what that data shows:

TOTALS BY JURISDICTION

Jurisdiction	2024	2025	Combined
United Kingdom	$95,402,748	$4,466,861	$99,869,609
France	$13,085,488	$17,294,432	$30,379,920
Germany	$14,558,679	$173,966	$14,732,645
UK & Europe Total	**$123,046,912**	**$21,935,259**	**$144,982,171**

BREAKDOWN BY TYPOLOGY

Typology	2024	2025	Combined	% of Total
Trade Surveillance Systems & Controls	$108,805,255 (5 fines)	$1,759,114 (3 fines)	$110,564,369 (8 fines)	76.5%
Market Manipulation	$12,455,196 (11 fines)	$14,100,770 (6 fines)	$26,555,966 (17 fines)	18.4%
Insider Trading	$1,340,304 (11 fines)	$6,075,375 (19 fines)	$7,415,679 (30 fines)	5.1%

Not all enforcement actions in this dataset constitute direct breaches of MAR. Fines for trade surveillance systems and controls failures can arise under MiFID II's organisational requirements or national equivalents such as the FCA's SYSC rules. However, given that Article 16 of MAR itself mandates that firms maintain surveillance systems capable of detecting suspicious activity, we treat these as part of the broader MAR compliance ecosystem. The same is true for criminal convictions of market manipulation or insider trading

Insider trading is a perpetual risk

Insider trading accounts for 30 of 55 fines across 2024 and 2025 – 54% of enforcement actions by volume, and the dominant category by a clear margin. That maps directly to what the STOR pipeline flags: insider trading represents ~55% of EU notifications and over 80% in the UK.

The reason insider trading appears modest by value, at just 5.1% of total penalties, is largely structural. These cases are predominantly brought against individuals rather than institutions, and many of the most significant 2025 outcomes were criminal convictions carrying custodial sentences rather than financial penalties.

With that said, enforcement still only represents a fraction of underlying misconduct. It is estimated that the actual occurrence of insider trading could be up to four times higher than the number of cases prosecuted. The FCA has been candid about why: "The challenges in prosecuting insider dealing are significant: sophisticated communications, international culprits, and outdated legislation."

The FCA is flagging that the Criminal Justice Act 1993, which governs criminal insider dealing in the UK, is over 30 years old and was not written for modern markets. It's a rare instance of the regulator explicitly naming legislative reform as a need.

STOR volumes and the enforcement mix point to a MAR framework that is generating intelligence, converting a meaningful share of it into action, and doing so in the areas where risk is most concentrated.

Trade surveillance systems are still a work in progress

Article 16 placed the surveillance obligation directly on institutions, requiring them to have systems and controls in place to detect and report suspicious activity. The entire STOR architecture depends on the effectiveness of these systems.

The dominant category across the two years by value is trade surveillance systems and controls deficiencies, accounting for 76.5% of total penalties. Firms are heavily penalised for failing to build and maintain the infrastructure to catch market abuse:

- **Surveillance coverage gaps and narrow alert logic**: Inconsistent coverage across asset classes, typologies and venues.
- **Calibration thresholds and alert overload**: Thresholds set too broadly generate noise; set too narrowly, they miss genuine risk.

- **Supervisory procedure design failures**: Written procedures that don't reflect how the business actually operates.

- **Data integrity and reporting system failures**: Inaccurate or incomplete trade data feeding surveillance and reporting systems.

On one level, this is evidence that MAR's standards are being rigorously enforced, but it also tells us that surveillance quality remains a systemic challenge ten years on. And the survey data shows the same signal.

- **44%** of institutions (UK and Europe) are concerned about accurately identifying insider trading and market manipulation

- **37%** are concerned about managing the volume of false positive alerts.

These statistics are both above the global averages.

> *"The calibration problem is easy to underestimate. We've seen firms take a surveillance framework that works well for their UK entity — properly tuned to FCA rules and UK trading behaviour — and apply it directly to operations in other jurisdictions.*
>
> *The controls weren't wrong; they just weren't tailored for the new region. Different instruments, different trading patterns, different regulatory expectations. The result was a programme that looked compliant on paper but wasn't calibrated to the risks that actually existed."*
>
> 
>
> *Ben Parker,*
> ***CEO of eflow***

Getting trade surveillance right is an ongoing challenge

For a trade surveillance framework – and the systems and controls within it – to be effective, it demands constant recalibration to align with the business structure and market abuse risk profile.

A firm with multiple business lines, asset classes and entities across jurisdictions needs to assess each individually. The instruments traded, the venues used, the regulatory environment and the manipulation typologies relevant to each desk can all differ materially. A framework calibrated for one entity is rarely transferable to another without significant adjustment.

Markets change, trading behaviour evolves, business lines grow and firms enter new markets. Surveillance frameworks have to keep pace with all of it, which means the work is never really finished.

What firms want from regulators

MAR placed firms at the centre of market abuse detection, and a decade on, they're not asking to be released from that obligation. However, they are asking for the collaboration, clarity and tools to meet those obligations more effectively. Given the surveillance deficiencies the enforcement data just exposed, that's telling.

You could reasonably have expected more pushback, more calls for simplification, more appetite for rollback, particularly in the current political climate where deregulation is on the agenda in several major markets. Instead, we see an industry that has internalised MAR's logic and understands the benefits of its infrastructure in promoting market integrity.

WHAT WOULD YOU LIKE TO SEE FROM REGULATORS?

Regulatory measure	UK & Europe
Closer collaboration between regulators and compliance teams	53%
Greater transparency around regulatory expectations and enforcement actions	49%
Avenues to safely test RegTech innovation (e.g. regulatory sandboxes)	45%
Clear guidance on minimum core technology standards	40%
Deregulation or simplification where burden is disproportionate to risk	34%
Increased use of AI/SupTech by regulators to enhance market oversight	34%

What does the future hold?

The partnership between regulators and institutions will be more important than ever before in the years ahead. The next decade will demand oversight of markets that are evolving faster still; more fragmented, more automated, and expanding into new asset classes.

Cross-product and cross-venue manipulation

Market fragmentation, algorithmic trading and the proliferation of linked financial instruments have created conditions for manipulation that can be engineered across markets, instruments and jurisdictions, exploiting their pricing relationships. The AMF has demonstrated that this can be detected and prosecuted, but doing so requires investigative capabilities – sequence-based pattern detection, cross-venue causality analysis – that go beyond what most firms' surveillance frameworks are designed to deliver.

31% of leaders say cross-product / cross-venue manipulation keeps them awake at night. The heightened enforcement focus in France may also explain regional sentiment. French respondents reported the highest level of concern around cross-product and cross-venue manipulation (35%).

> *"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 of eflow

Crypto and digital assets

When MAR came into force in 2016, crypto was a footnote. Today, 44% of UK and European compliance professionals cite digital assets as a top compliance challenge, up from 29% the previous year. MiCA, which replaced disparate national frameworks at the end of 2024, brings crypto market abuse explicitly within a regulatory perimeter for the first time and its market abuse provisions draw directly from MAR.

But crypto presents surveillance challenges that MAR was not designed to address. Markets operate 24 hours a day, across borders, on-chain and off-chain simultaneously. Manipulation vectors require monitoring capabilities that go beyond traditional order book surveillance. With MiCA's transitional period ending in June 2026, the practical implementation of those capabilities is an immediate challenge for firms providing assets to on-chain trading.

Future investment in artificial intelligence

The common thread across these changes is that trade surveillance has to evolve with them. The data suggests firms understand that and are investing accordingly.

AI maturity

16% of firms have fully deployed AI across all relevant surveillance functions, a further 31% are actively rolling out or piloting, and 24% are planning deployment within 12-24 months. Combined, 71% of firms are at some stage of the AI journey.

France has the lowest full deployment rate at just 8%, with Germany at 12%. These are the markets most troubled by false positive volumes: France at 42% and Germany at 40%, both above the global average of 33%. The data suggests the firms most overwhelmed by alert noise are the least advanced in deploying the technology best placed to reduce it.

The UK's full deployment rate sits at 20%, double France's and 67% higher than Germany's. Given that the UK's STOR quality gap with Europe is already narrower (28% of UK firms troubled by aggregating STOR data versus 44% in Europe) the AI maturity gap may be part of the explanation. Firms with better AI tooling are generating better intelligence.

What firms actually want AI to do

The application rankings tell the story of intent.

Enhancing detection of known abuse typologies tops the rankings across the UK (60%), France (67%) and Germany (67%). Firms want AI to make existing surveillance more accurate, not to replace the analyst's judgement in reviewing it. Risk scoring and anomaly detection follow. The lowest-ranked applications are the most autonomous ones: auto-closing alerts and copilot support for case investigation.

That's a deliberate "human in the loop" philosophy, and one that sits comfortably within what MAR implicitly demands. Accountability for surveillance decisions remains with the firm and its people. AI is the tool that surfaces the right cases; humans remain responsible for what happens next.

> *"Pulling together the full context for a STOR — trade data, communications, related activity — is exactly the kind of time-consuming, data-intensive work that AI can do well. Have the system do the aggregation, have a human review it, and submit something accurate and useful."*

Ben Parker,
CEO of eflow

Regulators are moving in the same direction

The FCA's 2025–2030 strategy demonstrates a clear focus on novel tools to improve surveillance efficacy.

The regulator states, "We will support firms in drawing on new, developing technology that not only improves anti-crime controls but reduces their costs," and frames its own role as "increasingly tech-positive."

Its innovation services have already helped over 200 firms test AI and machine learning in surveillance contexts.

Elsewhere in Europe, regulators have already deployed, or are committed to deploying, AI-powered tools to support more efficient detection of market abuse:

- BaFin deployed a machine learning algorithm within ALMA in May 2024, trained on over 1,500 confirmed cases of suspicious trading.
- ESMA's 2026 work programme commits to developing AI-powered tools specifically for anomaly detection and market abuse prevention, underpinned by its new data platform.

- The AMF has signalled its intention to develop a dedicated AI strategy and has stated explicitly that its 2025 inspections will assess “the use of artificial intelligence” in market abuse detection systems.

Regulators are building AI-enabled supervisory capability, and they expect firms to keep pace. The bar for what constitutes “adequate arrangements, systems and procedures” under Article 16 of MAR is quietly shifting, and AI is part of the answer.

Taking stock ten years on

MAR has done what it set out to do. It replaced a patchwork of national rules with a directly applicable framework and placed market abuse detection at the centre of what it means to be a regulated firm.

But the data tells a more complicated story. Surveillance quality remains uneven and a reporting pipeline generating thousands of suspicious activity reports a year should, in theory, be converting more of that intelligence into enforcement outcomes. The gap between the two suggests that a meaningful share of misconduct is still slipping through. And the challenges ahead – cross-venue manipulation, crypto markets, AI-enabled trading – are significant.

But this should not come as a surprise. Change is a feature of financial markets, not a bug. MAR provides a sound and durable framework. The question is whether everything around it – the technology firms deploy, the surveillance systems they maintain, and the partnership between industry and regulators – evolves fast enough to keep pace.

On that question, the survey data is quietly encouraging. Firms aren’t asking for less MAR. They’re asking for the tools, clarity and partnership to meet it more effectively. That’s a mature position. What it demands in practice, though, is sequencing. AI is genuinely promising. The survey data shows firms want to use it. Regulators are investing in it themselves. But AI deployed on weak foundations doesn’t fix a surveillance gap.

Getting the foundations right – data quality, coverage, calibration, escalation procedures – isn't a precursor to good surveillance. It is good surveillance. The next decade of MAR will reward firms that understand that.

About eflow

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

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

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

Explore our regulatory technology solutions at www.eflowglobal.com.