Global trends in market abuse and trade surveillance

How Regulators have reacted and what changes are still to come

Contents

Executive summary

The regulatory pressures facing financial firms have never been greater or more diverse. As the financial services sector becomes increasingly globalised and diversified, regulators are demanding that institutions implement more robust regulatory controls to protect the interests of their clients and uphold market integrity.

When coupled with the perfect storm of multiple 'global shocks', the increasingly important (and sometimes troubling) role of new technologies, and the convergence of market activity, it is perhaps unsurprising to learn that 60% of compliance professionals told us that their firm struggles to keep up with evolving regulations.

As a result, firms are facing a multifaceted challenge: adapting their compliance strategies to meet changing regulatory obligations; doing so in an operationally efficient manner; and ensuring that these controls do not hinder commercial activity.

With all of these points in mind, eflow commissioned independent researchers that specialise in financial regulation to undertake qualitative and quantitative analysis of the global trends in market abuse and trade surveillance.

Firstly, they analysed regulatory enforcement across several of the world's leading financial markets to illustrate the similarities and nuances that exist between global regulators. This analysis highlighted several key takeaways:

- International regulators have taken different approaches to regulatory enforcement, with striking variations in the volume, financial severity and approach of penalising non-compliant firms.

- The impact of the COVID-19 pandemic saw the volume of penalties issued for non-compliance drop in recent years, although this trend is not expected to continue.

- The regulatory process is long and complex; the average enforcement time from start to finish is eight years. This suggests that we're unlikely to see the tangible impact of increased regulatory scrutiny for several years yet, but also highlights the time, money and resources that firms under investigation will need to deploy should they come under investigation.

While historic analysis is a useful marker of what's come before, it doesn't necessarily predict the future. In order to offer a dual perspective, this report also considers the emerging trends that are likely to shape the short to medium-term future of regulatory enforcement. Using both qualitative and quantitative methodologies, our research identified several emerging themes that compliance professionals need to consider:

- We are in the wake of several generationally significant global shocks, each of which have had (and continue to have) a seismic impact on market dynamics and regulatory strategy. These are likely to dominate the financial landscape for several years to come.

- The rapid acceleration in the use and sophistication of technology offers both risk and opportunities from a regulatory perspective. The emergence of digital assets and AI means that the potential for bad actors to perpetrate market abuse has possibly never been higher, but at the same time Regtech and Suptech offers compliance professionals and regulators more insight than ever before.

- The seemingly relentless globalisation of the world is creating new challenges for regulators. Financial markets are now increasingly borderless and information flow is quicker and more efficient than ever before; this creates new opportunities for market abuse that financial firms will have to be prepared for.

In summary, we are in the midst of a period that is both equally exciting and challenging. Regulatory pressure is increasing and the potential ways in which market abuse can be conducted are growing. However, the rapid acceleration of technology means that firms are potentially more prepared than ever before to manage and deal with their regulatory risks.

One thing is guaranteed - the role of compliance professionals in combating market abuse remains as vital as ever.

I hope you find the report an interesting read.

Ben Parker

Chief Executive and Founder, eflow

Contributors

Ben Parker is Chief Executive Officer and Founder of eflow Global, one of the world's leading RegTech providers. Ben is an expert in financial services regulation and has a wide range of experience in tackling market abuse and developing the latest advances in trading surveillance. Having recognised the growing regulatory pressures that compliance professionals are facing, Ben's mission at eflow is to create a new standard for digital infrastructure that can allow businesses to get one step ahead. Ben joined the company in 2004 as COO and most recently led eflow's Series A funding round of £7m.

Ben Parker

eflow CEO & Founder

Dr. Sian Lewin

Industry Expert

For the past five years, Sian was a Co-Founder of RegTech Associates, where she led research and client delivery activities. RegTech Associates was a research company founded in 2017 specialising in deep industry insights about Regtech and Risktech markets. As well as being a practitioner, Sian also has an academic background in regulation. In 2017, she was awarded a PhD from the London School of Economics. Her systematic research explored the challenges faced by banks in dealing with the volume and speed of regulatory change following the 2008 financial crisis.

With an extensive background in technology at a senior level, Jason's experience includes significant roles at Motorola, JP Morgan, and Credit Suisse. He possesses strategic acumen and has honed his skills in stakeholder management and aligning incentives, developed through lengthy tenures at these organisations. By 2017, he had established a research and advisory firm, focusing on the Risk and Regulatory Technology sectors. Additionally, Jason contributes as an investor and board advisor to earlystage startups and holds a position on the Financial Conduct Authority (FCA) Innovation Advisory Group.

Jason Boud

Industry Expert

Global enforcement trends around the world - a recent history

To generate a robust and data-led view of the global regulatory landscape, a quantitative analysis of regulatory enforcements and fines between Q1 2019 and Q3 2023 across was undertaken. This analysis covered all firm types, eight jurisdictions and 10 regulators, spanning Europe, Asia and North America. The research focused on five enforcement categories, defined as follows:

DISCLOSURE TO THE MARKET

Failure to provide accurate information to the markets by regulated entities. This includes disclosure requirements on corporate insiders - shareholders who own ~10% or more of the firm's stock, and the firm's officers and directors, who must disclose their trades in the firm's stock after the trades are made.

INSIDER TRADING

The possession and use of confidential, non-public information that provides an unfair advantage when trading financial instruments. This includes:

- 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;
- Takeover offers - using inside information from a proposed bid, knowing the implications on shares;
- Acting for an offer - using the knowledge gained as a result of acting on behalf of an offerer for your own benefit.

SHORT SELLING AND RELATED VIOLATIONS

Any transaction that breaches regulations regarding short selling. Short selling involves the practice of borrowing a security and selling it at current market value with the expectation that the price is going to fall. if the price does fall, they will buy the shares at a lower price and return them. Short selling is regulated under regulations such as SSR and MAS's Guidelines on the Regulation of Short Selling.

MARKET MANIPULATION

The deliberate attempt to alter the free and fair operation of a market to create false or misleading appearances with respect to the price of an asset. This includes:

- Selling or buying at the close of market with the purpose of misleading those who will act on closing prices;
- Wash trading - selling the same financial instrument to create a false impression of market activity;
- Spoofing - disguising the details of a communication channel to convince a target that they are interacting with a known, trusted source.
- 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.

TRADING

This enforcement category includes any regulatory breaches related to transaction or trading errors. These breaches are generally the result of failures and controls which enable illegitimate transactions. They can be easier to prove than other categories because they do not require judgements on the intentions behind the trade, simply the facts of whether a trade should have been executed or not.

Enforcement data highlights the impact of the COVID pandemic and differing jurisdictional approaches

A comprehensive analysis of the regulatory enforcement of market abuse between Q1 2019 and Q3 2023 illustrates a series of interesting trends and differences across global regulators. It is important to note that these statistics should be contextualised in terms of the Covid pandemic and the degree of forbearance shown by regulators during this period.

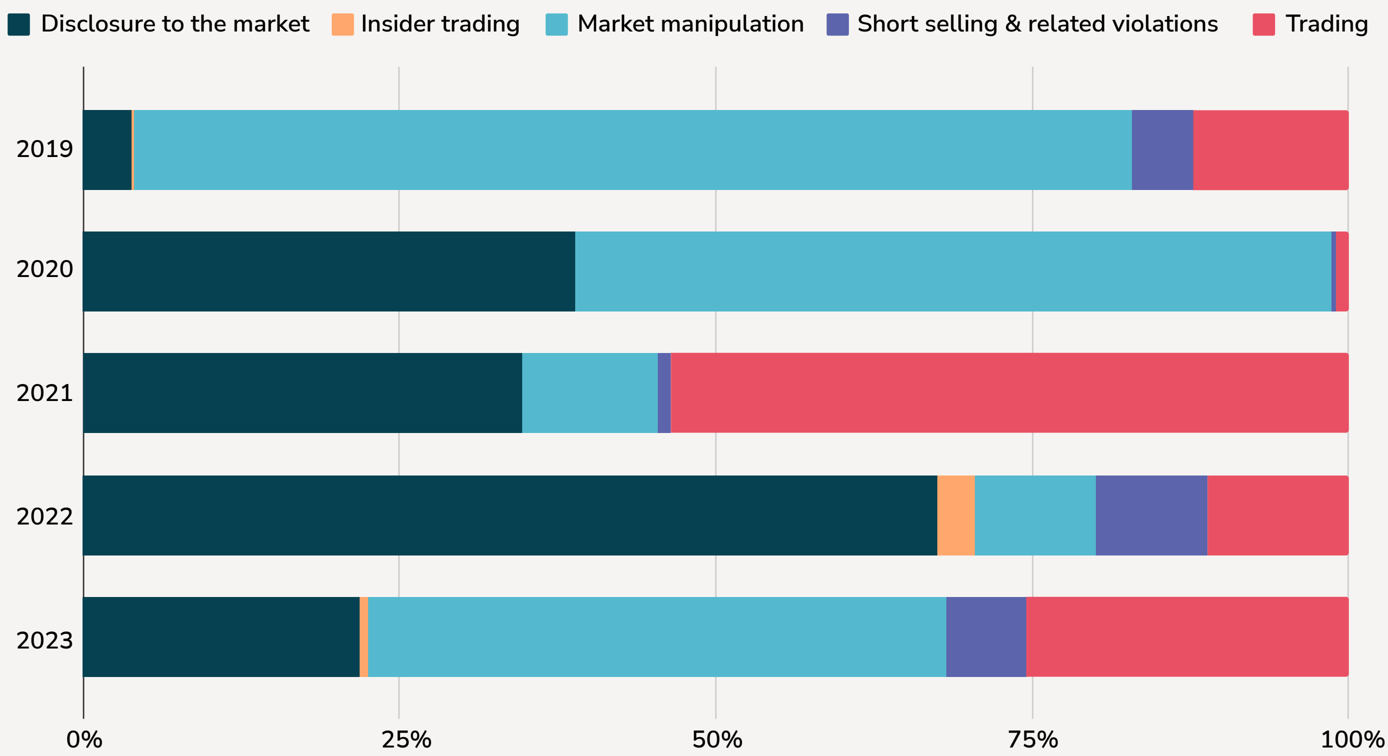
205
Fines issued for market abuse by selected regulators

$2.917bn
In total financial penalties handed out

$14.3m
Average value of fine issued by regulators

$920.2m
Largest fine handed out, to JP Morgan Chase and Co

Fines by enforcement category

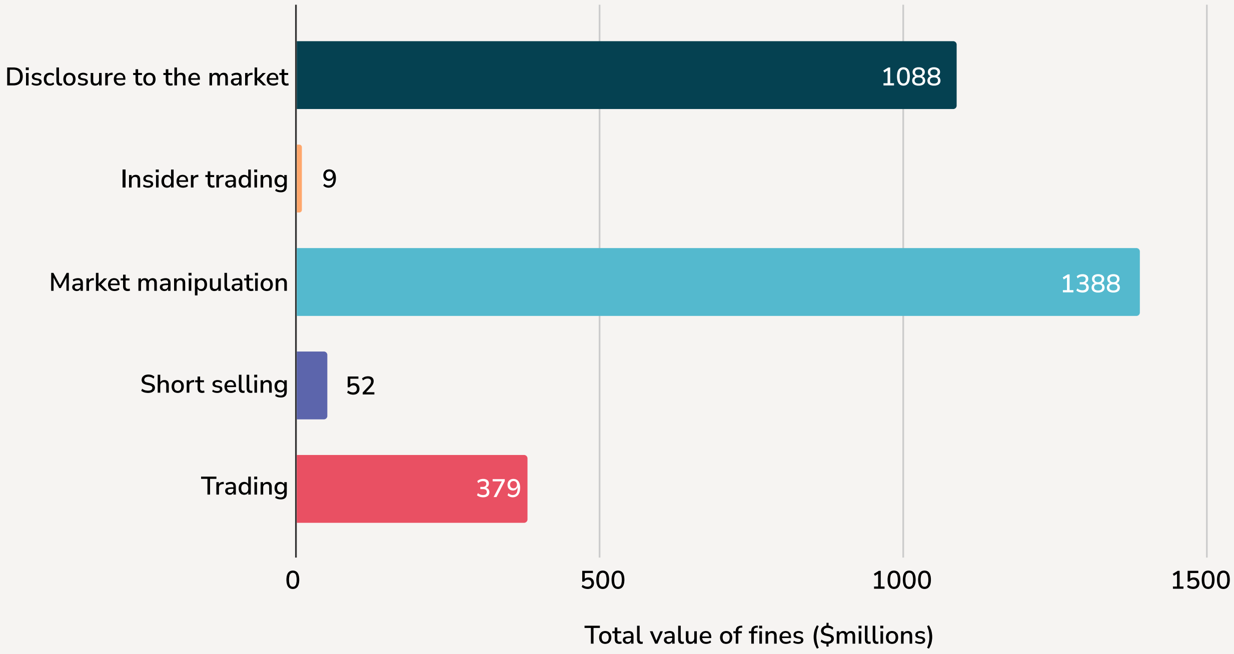


Of the 205 fines issued by regulators during the period in question, it is interesting to explore how penalties were distributed across the enforcement categories that were explored as part of the research.

Analysing the fines by volume, disclosure to the market (88 fines) was the most enforced category, followed by a close grouping of trading (42), market manipulation (39) and short selling and related violation (28). Insider trading saw just eight fines handed down over the same period.

It's when you explore the value of the fines issued by regulators that there is a much wider dispersion. Market manipulation leads the way with fines totalling $1388m, although it is important to note that this includes a single fine of $920m against JP Morgan Chase and Co, which was the single largest fine across the entire data set considered by our research. Disclosure to the market accumulated the second largest value of fines at $1088m, with trading ($379m) a distant third. At the other end of the scale, short selling and related violations racked up $52m of fines, with insider trading accounting for just $9m.

So, why are some enforcement categories seemingly being punished with greater frequency or severity? In the case of disclosure to market penalties, these are typically easier to prove than more complex market manipulation incidents, which goes some way to explaining why there are more than double the number of fines. The fines analysed as part of this research includes penalties for non-disclosures, late disclosures, and misleading or false disclosures. Many of these cases exhibit potential signs of insider trading, which the data suggests is much harder to prove in its own right, given the emergence of just eight cases across the same period.



Regulatory enforcement by jurisdiction

One of the most interesting aspects of the quantitative research is the wide variation in the volume and severity of penalties across the jurisdiction considered for this report.

Perhaps unsurprisingly, the US leads the way on both counts, and by some considerable margin. It was clearly the most active regulatory jurisdiction, with 133 fines totalling $2.67bn issued by regulators. While the overall value of penalties is buoyed by that single JP Morgan Chase and Co penalty, even when that individual case is taken out of the equation, the average fine issued in the US was still far higher than other jurisdictions at $13.2m.

The AMF in France led the European regulators in terms of activity. They issued 23 penalties worth $111m during this period, more than twice as many as the UK (10 fines totalling £87m) and Germany (9 fines totalling $15m). While the UK's Financial Conduct Authority (FCA) issued significantly fewer penalties overall, the fines associated with each case were significantly harsher, averaging $8.7m versus the AMF's $4.8m.

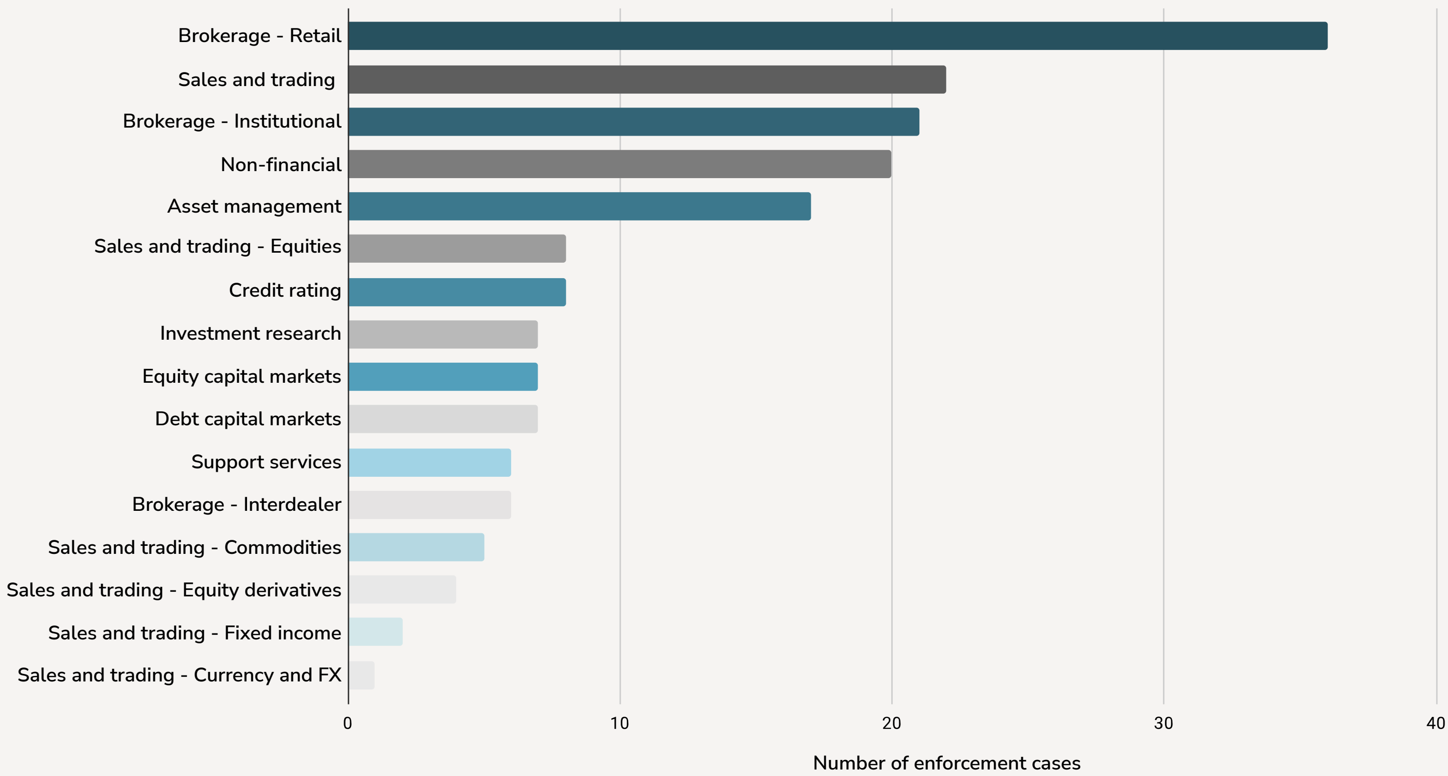
It's the approach of regulators in APAC that perhaps offers the greatest contrast when taking a global view of enforcement strategy. Hong Kong's SFC issued just one fine of $9M during this period, while Singapore's MAS did issue 21 fines but with a cumulative value of only $20.7m.

This is primarily due to the region's more reserved enforcement approach. Rather than using huge fines as a deterrent as in the case of the US or UK, these regulators tend to operate with discretion, reflecting cultural values that emphasise individual accountability and societal harmony over public reprimand. In this environment, fine values are relatively less important due to the higher cost of reputational damage.

Some other interesting trends emerge through analysis of the differing types of enforcement seen across the jurisdictions in question. For example, the UK has the highest proportion of fine value attributed to insider trading. This is consistent with findings from qualitative interviews, where UK-based participants consistently spoke of insider trading as a key typology in the region and also highlighted that this is reflected in the number of suspicious transaction and order reports (STORs).

In contrast, the APAC region has a significantly higher proportion of its total fine value occupied by short selling enforcements than other regions which should be considered against a backdrop of controversial short selling bans in various APAC countries.

Enforcement by service line

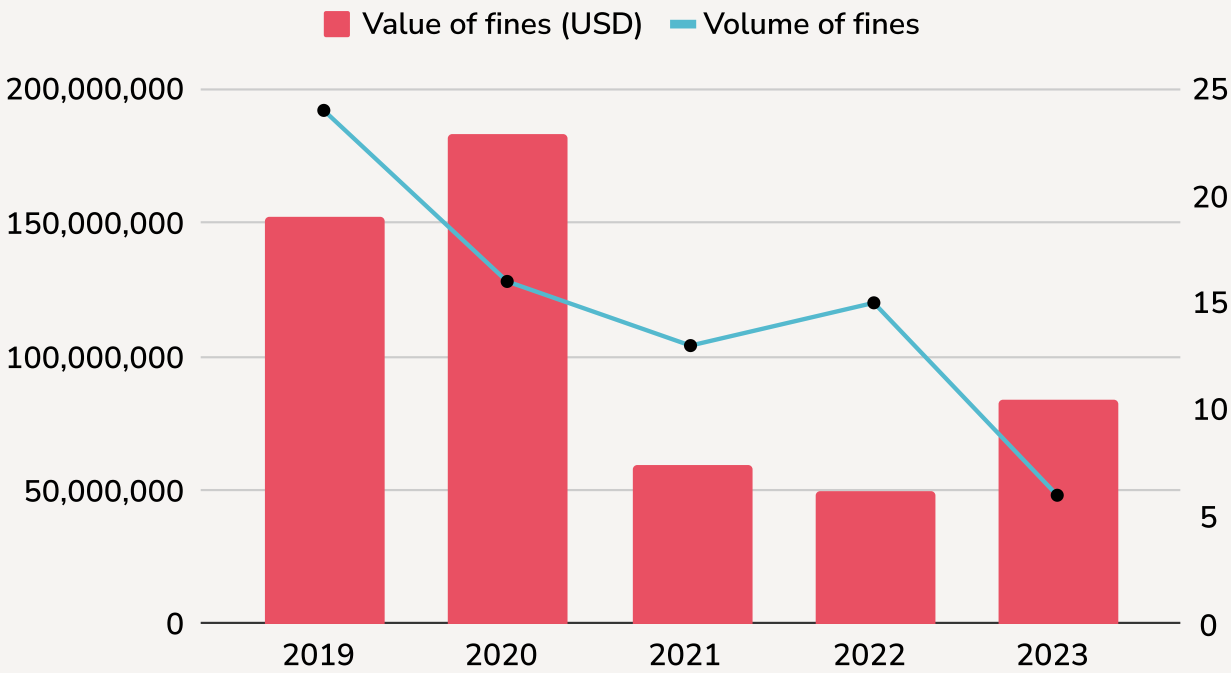


Taking a holistic view of the global data during this period, retail brokerage was by far the most targeted service line overall, raising questions over investor harm and retail investors as potential market abusers. Interviewees also noted flying prices as a key risk in the broker-dealer world.

Equities were the most commonly abused area within sales and trading, while fixed income and FX were among the lowest, which aligns the FCA's drive to increase STORs in these areas.

When considering non-financial lines, the majority of fines were linked to corporations that were punished for disseminating false information. All five cases of market manipulation in non-financial service lines were charged in France by the AMF, totalling almost $40m.

Annual enforcement trends



2020 fine of JP Morgan Chase and Co removed from statistics displayed above

When considering the annual trends in enforcement during this period, it's important to note several significant contributory factors. To look at the graph above, it would appear that both the volume and severity of penalties issued by global regulators is experiencing a steep decline since 2020. However, to jump to this conclusion would be overly simplistic for a number of reasons.

The impact of the COVID pandemic

The notable drop off in the value of fines in 2021 and 2022 may be due to a degree of general regulatory forbearance exercised during the peak of the COVID-19 pandemic and the subsequent period of economic recovery.

During this time, resources were devoted to more urgent regulatory objectives, and even regulators themselves were faced with unique operational challenges such as how their staff could investigate cases of non-compliance at a time when social mobility was greatly reduced in all jurisdictions. The impact of online court hearings and lengthy court backlogs were also features of the pandemic which would lead to delays in enforcement action being formally concluded.

Enforcement timelines - a long and complex process

Enforcement dates - those at which fines are issued - are often the culmination of a long investigatory and evidentiary process, so annual trends should be contextualised with this in mind.

In real terms, a representative sample of enforcement cases completed in 2023 illustrates that the average time from a breach start date to a formal enforcement date is eight years. So, while 81% of compliance professionals state that they feel under pressure from regulatory bodies to be transparent about their compliance processes, this increase in regulatory intervention is likely to only be reflected in actual enforcement penalties several years from now.

ESMA themselves have explained the approach that they take in such cases; "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." (Administrative and criminal sanctions and other administrative measures imposed under the Market Abuse Regulation in 2021, ESMA 2022)

A deep dive into enforcement action

Market manipulation

During the period analysed for this report, the CFTC was consistently issuing the highest fines for market manipulation, even when allowing for the enormous 2020 fine against JP Morgan Chase and Co mentioned earlier in this report.

In Europe, the AMF in France is also consistently bringing cases with higher values than similar European regulatory bodies in Germany and the Netherlands. The FCA did not enforce any market manipulation fines in 2021 or the first three quarters of 2023.

The AFM, MAS, BaFin and ESMA did not enforce any fines for market manipulation over the observed period, whilst the SFC were active only once, in 2020.

Key cases - Morgan Stanley and Lek Securities

Morgan Stanley were fined twice in 2019, once by the CFTC ($1.5m) on spoofing charges in the precious metals futures markets, and once by the AMF ($22m) on charges of price manipulation. The AMF found that the firm engaged in deceptive trading practices on June 16, 2015, by aggressively buying large quantities of French and German sovereign bond futures, then selling off 17 different French and eight Belgian bonds at inflated prices.

Lek Securities were also fined twice in 2019, once by FINRA ($900k) for failing to supervise and prevent manipulative trading practices, including layering and spoofing, by foreign traders using their platform, and once by the SEC ($1.5m) for being complicit in the layering and cross-market manipulation from 2014 to 2017, of a Ukraine-based firm, Avalon FA Ltd.

Insider trading

Though the FCA were inactive in all but one of the years considered as part of this research, a single large fine gives them the highest cumulative value at $5.8m. The AMF were most consistent over the period, with six insider trading enforcements totalling $2.4m.

BaFIN was the only regulator to enforce in the first three quarters of 2023, with a single fine worth $1.1m. All other regulators, including all US and APAC authorities, enforced no insider trading fines over the observed period.

Key case - GFI Group

GFI Group was fined by the FCA in 2022 for "failing to ensure they had appropriate systems and controls in place to effectively detect market abuse." From 2016-2018, GFI Group had manual, automatic and communications surveillance processes that were deficient, and which could not adequately control for market abuse through insider trading.

Short selling

FINRA was the only regulator to consistently enforce short selling fines in all observed periods, accumulating $21.6m across 15 fines. Over the same period, the SEC has accumulated $20.9m in short selling fines, despite enforcing only five penalties.

The SFC were active between 2019 and 2022, but did not record any penalties in the first three quarters of 2023. Their accumulated $7.8m in short selling fines represents 70% of their total core fines.

Other regulators were noticeably inactive in this area, with the FCA recording just one fine in 2020, whilst the CFTC, AFM, MAS, BaFin, ESMA and AFM all enforced no short selling fines during this period.

Key case - Bank of America

Bank of America faced three fines from FINRA for short selling violations over the observed period:

$150k in 2020 for multiple reporting and supervisory failures between May 2012 and September 2017. They incorrectly reported over 11,625 short sales without the necessary indicators and mismarked 32 sell orders as long sales, due to a persistent system issue.

$850k in 2021 for improperly netting trading activities of affiliated broker-dealer customers for close-out obligations and claiming undue pre-fail credit. The firm collectively calculated fail-to-deliver positions and pre-fail credits, allowing the use of purchases by one affiliate to reduce another's obligations. They also erroneously included foreign and non-broker-dealer affiliates' securities positions in calculating net positions of independent trading units.

$1.5m in 2021 for an inadequate supervisory system which led to failures in detecting, resolving and preventing the consequences of short positions in municipal securities.

Key takeaways

Unique regional approaches

The analysis of the quantitative data set highlights distinct enforcement trends across different regions, reflecting the varied expectations and approaches of regional regulators.

In summary, the UK, though imposing a relatively small number of fines (10), emphasises severe penalties, with the 40% above $10m, 60% above $5m, and 90% above $1m. The UK is unique in its active enforcement across all categories, maintaining fines over $1 million in each.

Across the Atlantic, US regulators lead the way in both volume and value of fines issued. The US stands out in market abuse enforcements, even when excluding a significant outlier fine of $920 million. Notably, these enforcements exclude insider trading cases but include recent substantial fines related to unmonitored communication channels.

The European Union's fines are weighted heavily towards market manipulation offences. One of the possible explanations for the prevalence of EU market manipulation fines is the clear and detailed definitions and behaviours set out in the Market Abuse Regime.

Despite taking a significantly different approach to enforcements, the Asia-Pacific region shows a notable over-representation in fines related to short selling.

Supervisory failures commonplace

Particular dynamics and correlations also emerge within and across service lines, enforcement categories and other enforcement details. Enforcements are most commonly observed in brokerage and sales and trading contexts.

Layering/spoofing and wash trades have been a key theme within market manipulation enforcements, while systems and controls and record keeping were most prominent in short selling cases. Supervisory failures were a feature of both.

Insider trading offences were rarely enforced over the period, but many closely related disclosure to the market cases were proven.

What's next?

Reviewing historical enforcement data sets the scene for market abuse and its regulatory trends, but it is not necessarily the best predictor of what the future holds and what actions regulators may take.

In the next section of the report, we draw on qualitative analysis and further quantitative research to identify the recent, current and upcoming factors driving market abuse behaviour and regulatory trends:

- ***Global shocks**: assessing the impact of recent global events on market abuse risks*
- ***Market evolution**: understanding the consequences of rapidly evolving technology and globalisation*
- ***Convergence**: identifying the technologies and partnerships touted to fight market abuse going forward*

Three key trends in market abuse perpetration and enforcement

It is no secret that regulatory enforcement is prohibitively complex. Opaque wording, jurisdictional variance and other such factors mean that market abuse enforcement is never as simple as “crime X leads to punishment Y”. As such, it is vitally important that we more closely analyse the global enforcement data put forward in the first half of this report in an attempt to establish key trends in market abuse perpetration and enforcement.

By establishing such trends, we are able to develop a deeper understanding of the enabling and motivating factors behind abusive trading, helping both regulators and regulated firms establish a more effective framework of protection and enforcement.

When analysed, the enforcement data reveals three distinct market abuse trends.

GLOBAL SHOCKS

We are in the wake of a series of global shocks - including the pandemic, supply chain crises, geopolitical conflicts, an inflation emergency, banking market upheavals, and events involving artificial intelligence (AI) and digital assets. These events have shifted the landscape of market abuse and its regulation, heightening economic and price volatility as well as changing the avenues and tools available to abusive traders. In particular, these global shocks have been felt in:

- Abusive commodities trading
- Abusive digital asset trading
- Abusive trading enabled by artificial intelligence

MARKET EVOLUTION

The modern financial landscape is becoming ever-more digitised and interconnected. Moving beyond traditional exchanges, digital trading platforms and ‘influencers’ operating on social media exert increasing influence over global markets. This has fundamentally transformed market dynamics, information flow, and the nature of market abuse. This intricate web demands a re-evaluation of how participants engage and combat misconduct. The effects of this market evolution can be seen in three key areas:

- Cross-market and cross-product manipulation
- Regulatory overlap
- Social media

MARKET CONVERGENCE

As the global landscape becomes increasingly interconnected, it opens new avenues for market abuse. This interconnectivity enables perpetrators to exploit regulatory gaps and unmonitored spaces, previously beyond the reach of traditional surveillance and regulations. To combat these evolving challenges, new initiatives are emerging which seek to align regulators and modernise institutions more broadly. These include:

- Collaborative regulation
- Developments in supervisory technology (Suptech)
- Developments in regulatory technology (Regtech)

Key Trend 1: Global shocks

In March 2023, Fabio Panetta, member of the European Central Bank's Executive Board, gave a speech titled "Everything everywhere all at once: responding to multiple global shocks". Panetta acknowledges that we are in the wake of a series of global shocks - including the pandemic, supply chain crises, geopolitical conflicts, an inflation emergency, and banking market upheavals - and which we can expand further, to events involving artificial intelligence (AI) and the proliferation of digital assets.

When surveyed, senior compliance professionals expressed similar concern about the impact of these global shocks on their ability to comply with global financial regulations. More than half of all firms surveyed believed that the accelerated use of AI and the instability of the global economy would cause compliance issues in 2024, with significant numbers also expressing worries about the impact of crypto assets and geopolitical unrest.

Which market forces are most likely to cause compliance issues in the next year?

1. The accelerated use of AI - 57%
2. Global economic instability - 56%
3. Digital assets and crypto markets - 40%
4. The geopolitical situation - 30%

These events have shifted the landscape of market abuse and its regulation, heightening economic and price volatility while providing criminals with new avenues and tools with which to conduct abusive trading. Panetta confirmed that regulators are grappling with the dual risks of under-reacting, which might exacerbate opportunism and criminality, and overreacting, which could lead to greater market instability.

The pandemic

The global COVID-19 pandemic brought about enormous economic impacts, instigating a period of significant price volatility. As well as - and perhaps because of - this fact, the global pandemic also brought about new market abuse risks.

The FCA emphasised the need for firms to adapt to home working, particularly with regards to trade surveillance and regulatory reporting. Regulators stressed the importance of implementing additional measures such as enhanced monitoring and the use of third-party surveillance systems in order to push back against these increased risks. Increased fund-raising activities during the pandemic also led to a surge in inside information within organisations, complicated further by new working arrangements and personal communication patterns.

Digital assets

The collapse of major digital assets projects, including Terra Luna and FTX, has placed a spotlight on the vulnerabilities of the largely unregulated crypto markets. These events underscore the potential for abuse within digital assets and ripple effects that these abusive behaviours can have on regulated markets.

Such instability not only exposes existing regulatory gaps, but also highlights the need for strong risk management. As a consequence of this, the entry barriers for traditional finance firms looking to venture into the digital asset space have been raised.

Geopolitics

Beyond the COVID-19 pandemic, a series of recent geopolitical upheavals - most notably the invasion of Ukraine and the Israeli-Palestinian conflict - have triggered substantial volatility in markets, notably affecting energy, fertilisers, and grains.

This volatility, compounded by trade disruptions and sanctions, has significantly impacted Russia and Ukraine as key exporters of these commodities. Such market instability heightens the potential for market abuse, as rapid price changes and supply chain disruptions create opportunities for manipulation and irregular trading activities.

Artificial intelligence

Recent breakthroughs in artificial intelligence, especially in natural language processing with large language models like GPT-3 and GPT-4, have ushered in a new era of optimism and widespread adoption of AI technologies.

However, despite the benefits and efficiencies that this adoption creates, the rapid and large-scale deployment of AI in trading strategies introduces unique risks. There's a growing concern about inadvertent or deliberate market abuse perpetrated as a result of algorithmic, AI-driven trading, leading to complex and potentially unpredictable market dynamics.

Economic instability

In many ways, the recent economic landscape has been defined by inflation crises and financial instability. Contributing events such as the collapses of SVB and Credit Suisse have generated uncertainty and price volatility, creating an environment conducive to market abuse. Fluctuating prices and uncertain financial conditions create fertile ground for manipulative practices, and bad actors have been quick to capitalise on these new-found opportunities.

Geopolitics and market infrastructure leave commodities susceptible to abuse

As we have already seen, price volatility caused by global shocks creates an environment where market abuse is more challenging to detect. Rapid and unpredictable price movements can camouflage manipulative activities, with bad actors taking advantage of increased market noise, reduced liquidity, and broader market uncertainty. Commodities are particularly vulnerable to abuse in the current landscape for two key reasons:

Price sensitivity

Finite supplies create bottlenecks or shortages. When the supply of a commodity is limited and demand remains constant or increases, any attempt to manipulate the supply can have a significant impact on prices. Commodities markets, especially specific niche areas, often have fewer participants compared to more established markets like stocks or bonds. This lower liquidity can make markets more susceptible to manipulation, as bad actors have more opportunity to influence asset prices with large trades.

Slower adoption of tech

Commodities are a less mature market from an electronic trading perspective - historically, much was open outcry exchanges and manually documented.

- *Information asymmetry: In less electronically advanced markets, access to timely and accurate information can be limited. Market players with better information or more sophisticated analysis tools can exploit this asymmetry to influence market prices.*
- *Manual documentation and processes: When trading and settlement processes are manual, they are slower and more prone to errors, misrepresentation and manipulation.*

Commodities enforcement

In the commodities market, single and cross-market spoofing, as well as insider trading, are the primary market abuse risk typologies. As such, these areas make up the majority of enforcement actions relating to commodities.

The CFTC further intensified its enforcement efforts in 2023, including a record number of enforcements against manipulation and spoofing actions. These cases demonstrate the CFTC's commitment to enforcing regulations against manipulative and deceptive practices in commodity markets, with a focus on holding individuals and entities accountable. The actions span a wide range of commodities and trading platforms.

Spoofing

September 26, 2022 - CFTC Orders California Trader and Prop Firm to Pay $750,000 for Spoofing in Treasury Futures

The order against Chen, who was a Tanius employee at the time, finds that he engaged in spoofing on over 1,000 separate occasions from October 1, 2020 to June 30, 2021 in 12 CME futures contracts — primarily Treasury futures contracts. The order against Tanius finds the firm vicariously liable for Chen's spoofing, which Chen engaged in while trading for Tanius.

August 24, 2022 - CFTC orders Chicago trader to pay $100,000 for spoofing in Natural Gas and RBOB futures

Insider trading

September 27, 2023 - Federal Court Orders Chinese National to Pay More than $350,000 for Fraudulent Scheme to Trade Against Employer

The order finds that, from approximately December 2021 to April 2022, Xie, a quantitative trader at a large, multinational corporation, misappropriated material, non-public information from his employer to fraudulently and deceptively enter into trades of feeder cattle futures and options for his personal benefit.

December 10, 2021 - CFTC Charges Puerto Rico Resident and His Firm for Misappropriation of Nonpublic Information and Fictitious Trading

How are regulators cracking down on commodities abuse?

ESMA and ACER: ESMA and ACER (The EU Agency for the Cooperation of Energy Regulators) have further enhanced their cooperative relationship by creating a new joint ACER-ESMA Task Force to improve information exchange and avoid potential market abuse in Europe's commodities spot and derivative markets.

FCA: As part of its Business Plan 2023/2024, the FCA aims to improve its capability to detect and prosecute fixed income and commodities market manipulation, through increased data capture, improved analytics, a dedicated non-equity manipulation team, and increased enforcement resources.

IOSCO: In its report "Principles for the Regulation and Supervision of Commodity Derivatives Markets", IOSCO outlines how market authorities should have a clear and robust framework for conducting market surveillance. Essential elements include monitoring the day-to-day, real-time and post-trade trading activity of the markets, monitoring the conduct of market intermediaries through examination of business operations and collecting and analysing trading information, typically analysed on a T+1 basis. IOSCO encourages "active and coordinated" detection and enforcement against manipulative schemes affecting trading on multiple venues as well as the underlying physical commodity markets.

Digital assets - same risks, same regulatory approach?

Regulators across the globe have been focused on the risks arising from increased digital asset adoption. We are seeing a growing number of fines, largely levied against individuals, for instances of market misconduct.

As an example, digital asset enforcements represented more than 20% of all CFTC actions filed during 2022. Whilst these are not all related to market manipulation, ESMA has highlighted some of the key risk typologies to bear in mind:

- Wash trading, in the case of crypto-assets, is facilitated by the pseudonymity attached to blockchains. Many crypto exchanges also inflate their traded volumes on purpose to attract new users and crypto-asset issuers - Cong et al (2019) identified wash trading on most unregulated crypto exchanges representing as much as 77.5% of the total trading volume on average.
- Pump and dump schemes tend to be conducted on less sizable crypto-assets as a smaller group of traders can have an impact on their price.
- Front-running (and extensions of it, namely 'back-running' and 'sandwich-attacks') risk is exacerbated with DEXs because of the publicity of transactions and the computational steps needed to confirm a transaction.

How are regulators responding to risks in digital assets?

Regulations are coming, but enforcements have already begun. Consensus on regulatory responses is yet to be reached, with approaches to cryptocurrencies varying across different regions, reflecting the complexity and novelty of the technology.

The UK and Europe have been notable for their efforts to establish clear regulatory frameworks aimed at protecting consumers and preventing market abuse. MiCA, in particular, will establish a number of rules specifically addressing market abuse in the crypto industry. The rules put forward in MiCA closely resemble the well-known Market Abuse Regulation in traditional finance. The existing regulatory fragmentation leaves room for regulatory arbitrage, something global standard setters such as ESMA and IOSCO are keen to prevent. While it's difficult to predict what 2024 and beyond holds for the digital asset industry, it is likely that increased uniformity across global regulators will lead to more trust and greater institutional adoption.

> *"Globally, regulators are enforcing fines against digital asset firms - for wash trading and insider trading in particular... MiCA will shape the regulatory landscape for digital assets.*
>
> ***ex-Head of Surveillance Technology, Global inter-dealer broker***

> *"Algorithmic trading is a risk. How would I be able to prove whether your ecommerce, electronic, FX or electronic fixed income desks have hired some specialist quants to devise some very clever code and strategies that can mask spoofing and layering in the market, which goes somewhat undetected? I couldn't tell you. So do we need better oversight capabilities for exploring what gets driven out of this space? Yes."*
>
> ***Head of UK Surveillance, Global Universal Bank***

There are four clear ways in which algorithmic trading and the use of AI presents additional risk with regards to market abuse.

Complexity and explainability:

More complex trading algorithms, particularly those powered by machine learning, can be hard to understand and explain. Their behaviour might change based on internal adjustments, making them unpredictable. Without a clear understanding of how these algorithms operate, it's difficult for regulators and market participants to discern between legitimate trading activity and potential market manipulation.

Susceptibility to market manipulation:

Machine learning models, by nature, optimise for their objectives. If market manipulation strategies offer a route to achieve these objectives, the models might inadvertently or explicitly adopt these strategies. Machine learning algorithms, especially those using reinforcement learning, can adapt and learn manipulative strategies if they see potential profits. Their objectives, like maximising profit, might inadvertently align with manipulative behaviours if they aren't properly supervised.

Misinformation and discrimination:

Algorithmic trading platforms might perpetrate or amplify misinformation. Moreover, the algorithms might show biases, leading to discriminatory trading practices. Biassed algorithms can lead to an unfair trading environment, and misinformation can mislead genuine market participants, leading to suboptimal trading decisions.

Accessibility and retail:

Interviewees confirmed that the most common risks and challenges of AI apply to their firm. They also raised a new concern, that the accessibility of highly dynamic and collaborative models such as GPT4 will aid individuals with little or no technical background and understanding in developing trading strategies. This raises the risk that retail investors will become perpetrators of abuse.

How are regulators responding to these risks?

ASIC - June 2023: ASIC encourages financial organisations to help lead through change. “As we realise the potential of tech, we have to do all we can to avoid negative disruption, learned market abuse, misinformation, discrimination, and bias – whether intended or unintended. I want to take this opportunity, as an aside, to emphasise that ASIC has AI as a high and important priority.”

AFM - February 2023: The AFM is particularly interested in potential risks to fair and transparent financial markets. Two risks are “directly related to what’s under the hood of these trading algorithms”:

- Explainability: In addition, the complexity of an algorithm, combined with the speed, the number messages a single algorithm sends and the fact that the model’s behaviour might change if the weights are adjusted requires strong risk-controls, appropriate testing, real-time monitoring and market abuse surveillance.
- Susceptibility to manipulation: more features and the effects of features on predictions being less obvious could increase the number of cases of market manipulation.

FINRA’s Regulatory Notice 15-09: Guidance on effective supervision and control practices for firms engaging in algorithmic trading strategies should be used to inform a firm’s surveillance program in areas such as general risk assessment and response; software/code development and implementation; software testing and system validation; trading systems; and compliance.

Key trend 2: market evolution

It is difficult to quantify just how drastically the financial landscape has changed in the past decade or so. Financial markets are more digitised and interconnected than ever; online trading platforms and social media influencers have fundamentally transformed market dynamics and information flow, resulting in a major change to the ways in which market abuse can be perpetrated.

This intricate web demands a re-evaluation of how participants engage with market abuse surveillance and how regulators govern it. Naturally, as financial markets continue to evolve, so too do the regulations governing them. As a result, regulated firms are often left playing catch up as regulations struggle to adapt to shifting market dynamics. When surveyed, 60% of compliance professionals claimed that their firms struggle to keep up with evolving regulations

In the case of market abuse, the increasing number of players in the ecosystem - markets, products, fintechs, crypto, social media platforms and regulatory domains - are a real challenge to effective surveillance efforts. In the following section, we will explore three areas in which market evolution is increasing risk by bringing important elements closer together:

- Cross-market/cross-product activity
- Regulatory overlap
- Social media

“Trading has changed, with more traders covering a wider range of assets and markets. This increases the complexity of their activity, and creates greater potential for market abuse: I think the way that the fixed income products operate and how the data can be captured is a good example of increased complexity. In the past, traders would basically trade singularly in equal measures. What I mean by that is you don’t get a trader who trades just cash anymore. You more often than not get traders who trade all three instruments (swaps, bonds and cash) and they can cross between them depending on which way they’re trying to hedge. And that’s what makes the cross product and cross market manipulation more topical and that’s why it’s an area of focus.”

Head of UK Surveillance, Global Universal Bank

Cross-market and cross-product abuse

As financial markets become increasingly borderless, so too must the surveillance tools we use to detect and combat market abuse. This is an opinion shared both by regulators and by regulated firms. When surveyed, 74% of compliance professionals saw cross-border regulatory challenges as an issue for their firms. On the regulatory side, IOSCO, the SEC and the CFTC have also all echoed this concern in one way or another.

However, addressing these concerns and implementing cross-market surveillance is easier said than done. Conducting trade surveillance across borders and addressing issues like cross-market spoofing presents two clear challenges:

Diverse regulatory frameworks

While financial markets are becoming ever more interconnected, the regulations governing these markets remain somewhat disconnected. In terms of market structure, trading practices, and surveillance mechanisms, there is still a good deal of global variance and, as such, traders can exploit regulatory arbitrage by moving their activities across jurisdictions with varying levels of oversight and enforcement.

Technological differences

Again, despite the growing interconnectedness of financial markets, different jurisdictions do use a variety of trading platforms and technologies. Such differences in infrastructure, trading protocols, and data formats can complicate the integration of surveillance systems to monitor activities seamlessly.

Social media and off-channel communications

In recent years, global regulators have made it clear that off-channel electronic communications such as private messaging applications are a regulatory challenge that will be taken extremely seriously.

Since 2019, $2.64bn of fines have been levelled against firms for issues relating to off-channel communications, with the average monetary penalty for such violations hovering around $50 million since 2020. As firms begin to remediate their record-keeping to better monitor off-channel communications, the conversation will inevitably shift up a level, with regulators questioning firms' ability to leverage unstructured data to enhance the detection of market manipulation and insider trading. As a result, firms are now exploring opportunities to combine trade and eComms data to give a more accurate picture of manipulative behaviour.

So, while posing obvious technical challenges, there is general consensus that eComms surveillance is a vital part of the trade surveillance process. However, this issue becomes even more complex when we add social media platforms into the mix. Slowly but surely, regulators are extending their remit to include provisions against the use of social media with relation to trading.

Regulators such as the SEC and the SFC are becoming increasingly vocal about the impacts of social media on investor protection. While these issues extend across all asset types, they're particularly pertinent amongst digital assets and "meme stocks". In addition to this, we are seeing a rise in gamification and social media-like features within trading platforms themselves, heightening the risk of manipulative and high-risk trading activities.

According to the SEC, there are three key areas in which fraudsters use social media to conduct schemes:

Pump and dump schemes

Pump and dump involves pumping up the share price of a company's stock by making false and misleading statements to create a buying frenzy, and then selling shares at the pumped up price.

Scalpling

Scalping involves recommending a stock to drive up the share price and then selling shares of the stock at inflated prices to generate profits.

Touting

Touting involves promoting a stock without properly disclosing compensation received for said promotion.

How are regulators responding?

SEC Investor Alert - August 2022: An SEC Investor Alert highlighted how retail investors increasingly rely on social media for information about investing and these platforms allow fraudsters to contact people quickly, cheaply and with minimal effort. The notice provides a host of scenarios in which fraudsters may impersonate brokers and investment advisers, SEC staff or celebrities in attempts to manipulate markets or defraud investors.

SFC Enforcement Reporter - September 2020: Elsewhere, Hong Kong's SFC has observed that an increasing number of retail investors have fallen victim to pump and dump scams conducted through popular social media platforms. Their 2020 SFC Enforcement Reporter illustrated that these scams account for about 20% of the market manipulation cases under investigation by the SFC.

Key trend 3: market convergence

As the global landscape becomes increasingly interconnected, it opens new avenues for market abuse. This interconnectivity enables perpetrators to exploit regulatory gaps and unmonitored spaces, previously beyond the reach of traditional surveillance and regulations.

The trajectory towards an increasingly connected state is irreversible, signalling a future where global interdependence only deepens. To combat these evolving challenges, new initiatives are emerging which seek to align regulators and modernise institutions more broadly. Three such initiatives are:

- Collaborative regulation: Cross-border alignment between financial regulators that seeks to minimise regulatory gaps
- Technological development by regulators: The increasing use of surveillance and supervision technology by regulatory bodies, with capabilities to identify market abuse
- Investment in Regtech by regulated firms: Regulated firms are now expected to harness third-party trade surveillance solutions to ensure compliance with market abuse regulations

Despite these developments, there is still a long way to go. While these initiatives do go some way towards addressing the increasing sophistication deployed by abusive traders, there remain organisational, technological and data silos which can limit progress.

For regulators, gaps don't only exist in their coverage of market abuse, but also in their understanding of what firms are doing about it. As well as proactive/public steps including events and initiatives, regulators' expectations are increasing in relation to how firms explain their controls.

Collaborative regulation

In an attempt to increase transparency around market abuse, regulators are engaging in collaborative relationships with national authorities, enforcement agencies and the private sector. Such partnerships are a pivotal tool in transitioning towards an intelligence-led approach to market integrity and capitalise on the overlap of objectives between regulators and the private sector.

There are countless real-world examples of such collaborations. The FCA has stressed the importance of these "partnerships" between themselves and market participants to understand the most direct risks to market integrity. IOSCO have also expressed their desire for greater cooperation and collaboration to minimise regulatory arbitrage, where possible.

In the US, regulators are taking a similar approach. To effectively protect markets, participants, and customers, the CFTC will continue its emphasis on coordination and parallel actions with criminal authorities and regulatory partners domestically and internationally. This is critical to deterring violators, punishing misconduct, preserving market integrity, and protecting market participants.

"The regulator expects firms to be able to explain how the controls work in detail. And there was a lot of back and forth around insider dealing to check exactly how our controls are designed. Firms use vendor products which are often not very well explained... how, for example, a vendor product deals with the idea of insider dealing, the benchmark period, the insider period, whether there's an overlap, what happens around those periods, what is the calculation, how exactly is the control working? Because we have instances where the regulator is catching some behaviour and the firm is not reporting it. And the regulators ask the firm 'why haven't you reported it?'"

Head of UK Surveillance, Global Universal Bank

Similarly, SEC commissioner Mark T. Uyeda recently stated that "if we are to work across borders, we need agreements and often assistance from foreign regulatory authorities and they need that same assistance from us". To this end, the SEC aims to:

- Provide cross-border clarity on regulatory scope
- Address conflicts of law (regulatory arbitrage) across jurisdictions
- Remove duplicative regulation
- Identify gaps in a foreign regulatory frameworks that the home jurisdiction believes are of key importance

Such collaborations are already taking effect. In December 2021, the HK SFC, the Hong Kong Police Force, Singapore MAS and the Singapore Police Force conducted a joint operation against an active and sophisticated syndicate suspected of operating ramp-and-dump manipulation schemes in Hong Kong and Singapore. The simultaneous joint operation involving securities regulators and law enforcement agencies is the first-of-its-kind in tackling cross border pump-and-dump scams. A total of ten people – including individuals believed to be the key members of the syndicates, their associates and some senior executives of Hong Kong listed companies – were arrested during searches of 33 premises in Hong Kong and Singapore by more than 190 officers of local police forces and regulatory bodies.

The Hong Kong-Singapore joint operation came after the SFC, which first discovered suspicious trading activities of the syndicate, referred the case to the MAS and the Hong Kong Police because of a cross-border element and the scale of suspected money laundering offences, in addition to specific market misconduct offences under the Securities and Futures Ordinance (SFO).

The joint operation was conducted under the arrangement of:

- the MoU signed between the SFC and the Hong Kong Police
- the IOSCO Enhanced Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information and Multilateral Memorandum of Understanding and the bilateral Memorandum of Understanding between the SFC and the MAS

The HK SFC's efforts are a good example of fostering effective regulatory and enforcement cooperation with fellow regulators in Hong Kong, mainland China and major overseas markets. Cooperation is often founded on MoUs which set out the agreed approaches to issues ranging from enforcement to market development. Over the years, the SFC has signed several bilateral or multilateral agreements with local, mainland and overseas regulatory bodies.

Technological developments by regulators

Regulators are turning to AI and Suptech (supervisory technology) to better monitor and combat market abuse. This strategic shift is fuelled by the recognition that surveillance methods of old are insufficient in the face of evolving market dynamics.

This marks a transformative step-change in the industry and sets a new standard for market oversight. As regulatory expectations evolve to include advanced technologies, the systems and controls put in place by regulated firms will be more closely scrutinised and they will be incentivised to adopt more sophisticated technology to align with compliance requirements.

What technologies are regulators implementing?

In May 2023, IOSCO published FR02/23 Principles for the Regulation and Supervision of Commodity Derivatives Markets. This report highlights the fact that modern algorithmic trading necessitates a need for changes in the way regulators monitor trading. Increasingly sophisticated algorithms that can monitor trading and detect patterns are a necessity in this high speed and complex trading environment in order to maintain market integrity and confidence.

In Singapore, MAS uses an advanced data science tool named Apollo to help enforcement officers detect misconduct in financial markets. Developed in-house by the MAS, Apollo analyses trading data and refers suspicious trades to human experts for further review. The augmented intelligence tool takes advantage of data science techniques such as machine learning to maximise efficiency, while modelling rogue trading behaviour using traits identified by subject matter experts.

Across regulator jurisdictions, there is also an increasing push towards the implementation of Sandbox testing environments. This was first brought about by the FCA who scrutinised exactly how firms are calibrating their systems - not only what their controls and parameters are, but how these configurations have been justified. As a result, sandbox environments are gaining popularity with firms keen to demonstrate the strength of their regulatory controls.

Accordingly, the FCA has also launched its own permanent Digital Sandbox, offering access to:

- High-quality datasets and APIs
- A collaborative ecosystem
- Regulatory observation

"Sandbox environments are being used to calibrate and test capability. Firms are testing alerts on synthetic data, to check whether they are really picking up all scenarios."

ex-Head of Surveillance Technology, Global inter-dealer broker

"The FCA explained at a recent AFME offsite that they are going to be deploying AI within their sandbox environment... typically, they will go first in trying something new, then there will be ramifications and expectations for financial institutions to follow if it works."

Head of Surveillance UK, Global Universal Bank

What challenges are there to the development of regulatory Suptech?

Clearly, the past few years have seen regulators invest heavily in improving their trade surveillance data analytics capabilities in an attempt to better identify market abuse. However, such technology is only as good as the data inputs feeding its analytics and firms' trade data and STOR reports are falling short of expectations. Constant administrative penalties for misreporting point to regulators' growing frustration with the quality of the data they receive from institutions.

Over the coming years, we are likely to see a push from regulators to overcome this data quality bottleneck. If successful, it would open the door for more effective trade surveillance supervision, boosting market integrity while facilitating more efficient and data led regulatory oversight. This will expose institutions to greater regulatory scrutiny, with supervisors shifting focus to firms' capabilities in identifying and preventing market abuse.

Investment in Regtech

The development of Suptech by financial regulators is mirrored by the implementation of Regtech by financial institutions. As regulators implement stronger and more robust technological solutions, their expectations for regulated firms will develop in a similar way. In recent years there has been a huge increase in the number of firms implementing third-party trade surveillance systems to manage their market abuse regulatory requirements.

When surveyed, an overwhelming 96% of compliance professionals stated that their firms were planning to invest in regulatory technology in 2024, with around half of these firms claiming that their investment would be "significant". This is not without its challenges, however.
Firms are constantly trying to sift through the "noise" of their existing surveillance systems - that is the inaccurate or irrelevant alerts (false positives) which can impede effective surveillance. Regtech solutions play a critical role in this pursuit.

By incorporating advanced technologies like artificial intelligence (AI) and machine learning (ML), they can enhance the precision of identifying and risk-scoring transactions. This involves the development of sophisticated algorithms capable of discerning nuanced patterns associated with potential market abuse. Additionally, we are seeing more firms attempting to integrate structured trade data with unstructured communications data. Although strides have been made, achieving optimal efficacy remains a work in progress.

> *"Although there is increased talk about AI, there is not yet any expectation that firms will replace traditional trade surveillance systems with AI - largely due to explainability issues - but there is a lot of interest in AI as a co-pilot."*
>
> ***ex-Head of Surveillance Technology, Global inter-dealer broker***

Artificial Intelligence and Regtech adoption

AI was the most talked about technological development among interviewees. While there was a cautious optimism among respondents, they were also clear on the current barriers to adoption.

The extent to which vendors are willing and able to explain their models is therefore an important factor in firms' procurement decisions.

However, for some, AI is clearly still a 'future state'. These contributors expressed a wider technological immaturity, which included an inability to explain AI models, but also pointed to more fundamental technological deficiencies.

> *"We use Rules based type scenarios, set parameters and thresholds. We don't even have any visualisation tools that we lay on top for trend analysis at the moment."*
>
> ***Global Head of Trade Surveillance, Global Investment Bank***

About eflow

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

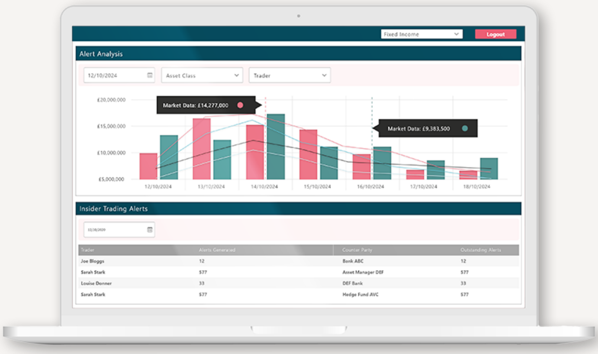
To achieve this, we first had to identify why so many firms either struggled to demonstrate their compliance or spent far too much time, effort and money in doing so. We found that for many institutions, their regulatory processes were broken. An over-reliance on spreadsheets and siloed data. Slow, legacy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

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

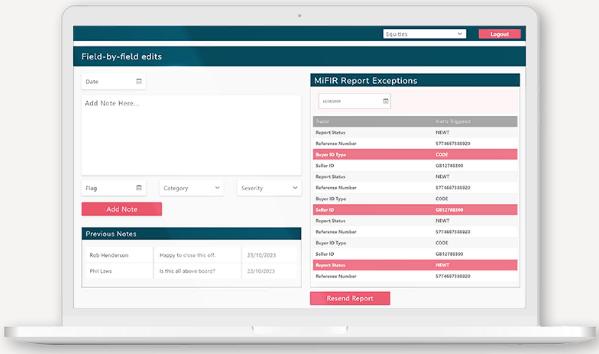
This means that as new regulatory challenges arise, as they inevitably will, you can rest assured that eflow's regulatory tools will already be one step ahead.

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

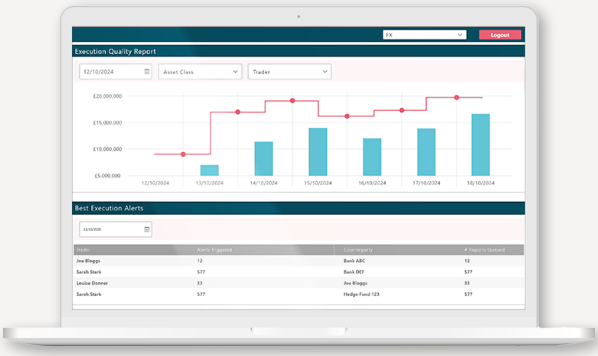
TZTS Trade Surveillance



TZTR Transaction Reporting



TZBE Best Execution



TZEC eComms Surveillance