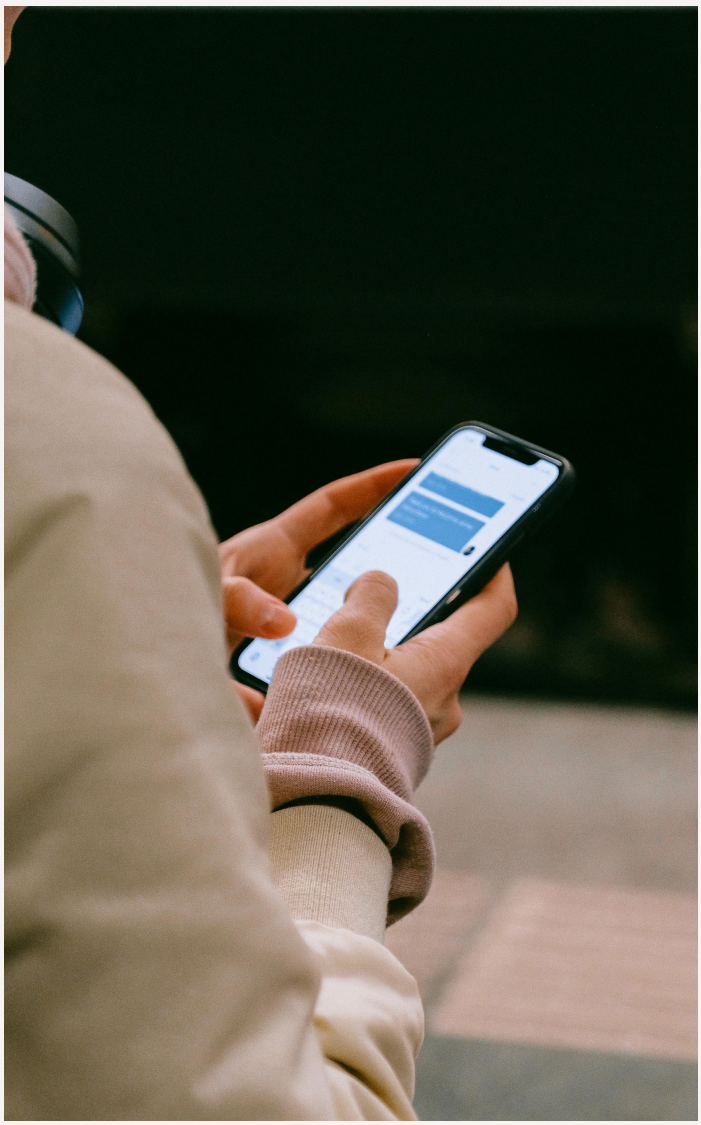
Integrating eComms and trade surveillance: Taking the next step

As the sophistication of market abuse accelerates, how do financial institutions evolve to a holistic surveillance strategy?

Integrating eComms and trade surveillance: taking the next step

Over the past few decades, the digital revolution has dramatically transformed communication across all sectors, including financial services. As a result, a huge variety of new channels, devices and applications have emerged, making communication more fluid and accessible. However, while the benefits of seamless connectivity are clear, it also presents unique challenges in trading environments, with bad actors able to exploit surveillance blindspots to gain an unfair advantage.

Global regulators have made it clear that as firms broaden their multi-channel communication strategies, there is an expectation that their surveillance capabilities must develop in tandem. Organisations need to have demonstrable, effective and up-to-date recording policies, procedures and management oversight arrangements with respect to business-related conversations, regardless of the communication channel.



In recent years, in the course of investigating market abuse, regulators have routinely found recordkeeping violations, ranging from inadequate systems and controls to entirely unmonitored “off-channel” applications. These findings have highlighted the need for a more holistic approach to electronic communications (eComms) surveillance, with supervisors making no exceptions to those who inadvertently restrict their ability to identify and mitigate market abuse.

This eBook explores the potential of holistic surveillance - performing eComms and trade surveillance in tandem - the challenges of building these tools in-house or implementing multiple, disparate technological systems, and the potential that lies within specialised, integrated technology solutions.

The regulators' stance

While both preventing and identifying market abuse is top of the agenda for all global financial regulators, it's the US regulators - specifically the SEC and CFTC - that have made headlines for their rigorous eComms enforcements. Since 2021, these agencies have handed out over $2.7bn in financial penalties to a number of firms ranging from Wall Street institutions to boutique investment houses.

Most recently, the SEC ordered 16 firms to pay more than $81 million combined to settle charges for widespread and pervasive recordkeeping failures. These firms generally had the necessary policies in place to restrict off-channel communications, but lacked sophisticated surveillance technologies to actually enforce them. These deficiencies expose systemic risks that are likely to be common across the financial sector due to lapses in governance and ineffective supervision of employees.

In the aforementioned case, firms also agreed to retain independent compliance consultants tasked with performing thorough evaluations of the firms' practices and procedures regarding the storage of electronic communications on personal devices, in addition to assessing their systems for managing employee non-adherence to these protocols. Regulators have made it clear that firms must implement adequate controls to achieve a depth of analysis that traditional methods simply cannot match.

The challenges of effective eComms surveillance

Capturing and matching structured and unstructured data

A fundamental challenge in eComms surveillance is the effective capture and integration of structured trade data with unstructured communication data sourced from a variety of platforms. This task begins with the ingestion of unstructured data - ranging from calls and emails to chat logs across trading terminals and social media platforms - which must be systematically structured for analysis. This structuring is crucial as it transforms disparate data into a unified format that can be compared and connected with structured trade logs.

The process involves sophisticated data engineering techniques to not only link references to specific transactions found within these communications but also to align them temporally. Communications might refer to future or past trades, and it is essential to establish a precise chronological relationship to accurately identify potential compliance issues. Ensuring the accuracy of these connections demands advanced natural language processing (NLP) tools that can parse and understand industry-specific slang, idioms and jargon, as well as entirely different languages, and correlate these elements with structured trade data.

All of this functionality must be streamlined and packaged so that it is both efficient and robust in the context of consistently high volumes of data. Furthermore, the data must be stored in a way that is clear and accessible for the purposes of investigations and audits.

Semantic analysis and alert precision

Once data is accurately connected and organised, the next challenge is the analysis of this data to identify genuinely suspicious behaviour. As well as identifying an association between trade and communications, the NLP capabilities within eComms surveillance tools must be powerful enough to interpret whether these informal, potentially coded communications contain an intent to perform market abuse. These systems must discern the subtleties of language - such as irony, context, and sentiment - to differentiate between innocuous and potentially malicious communications. It is crucial that these systems are refined enough to minimise false positives, thereby preventing compliance teams from being inundated with irrelevant alerts.

Data privacy regulations

In solving the challenges of data integration and analysis, firms must also take into account strict privacy regulations and data utilisation rules. Under regulations such as the GDPR, firms are required to notify employees about the monitoring processes they will be subject to, explaining the reasons, scope, and duration of the data surveillance. Moreover, the GDPR mandates that only the necessary data for a specific surveillance purpose is processed - a principle known as data minimisation. This is particularly pertinent when surveillance systems capture communications on personal devices or off-channel interactions. The UK's Information Commissioner's Office recommends using aggregated network data to identify unauthorised usage, with any further analysis carefully targeted and scoped to minimise the intrusion into personal communications.

MiFID II, MAR and other regulations concerning market abuse require that firms store business-related communications as part of record-keeping requirements. Paired with the aforementioned data privacy rules, it is clear that firms are tasked with a highly technical balancing act. Surveillance tools need to screen and categorise communications as personal or business-related in order to decide whether to discard them or store and process them in compliance with data protection standards and market abuse regulations.

The bottom line

Creating an effective eComms surveillance programme requires expert-level data and software engineering, data science, including machine learning and NLP, and an appreciation of underlying data privacy rules, all combined with subject matter expertise in market abuse typologies and regulations. It is an enormously complex task and, when laid out in full, it becomes unsurprising that many firms are falling short.

The case for an integrated eComms and trade surveillance strategy

What does it mean to have an integrated surveillance strategy?

An integrated eComms and trade surveillance strategy harnesses the power of both communications and trade data to maximise a firm's ability to detect suspicious activities and minimise the generation of false positive alerts.

Traditional surveillance solutions often analyse trade and eComms data in isolation, requiring many of the complex and cumbersome processes referenced earlier in this briefing note to be undertaken manually with a lack of unification of evidential channels (trade and eComms) where potential abuse is identified. Integrated solutions, however, seamlessly merge these structured and unstructured data sets. These sophisticated systems employ advanced algorithms that assess behaviours based on the intricate relationships between the two data types, significantly enhancing detection capabilities.

Context is king: the role of eComms data in market abuse investigations

In May 2023, the CFTC fined HSBC for widespread manipulative and deceptive trading practices related to interest rate swaps with bond issuers. During the course of the investigation, eComms records revealed that some supervisors and senior managers were aware of, and sometimes directed, these manipulative practices.

The surveillance data showed these employees using clear and direct language relating to manipulative tactics. For instance, the HSBC Head of North American Rates instructed a trader to aggressively influence market pricing before a transaction, telling them to "push the screen as much as we can before the pricing".

Not only did these records prove the involvement of senior management, they also confirmed the presence of a supervisor on the desk during the time that the manipulative trading activities took place, further evidenced by the timing of the direct instructions to manipulate market data.

So, while the trade data highlighted that manipulation took place, the eComms records told the true story of the malicious intent.

eflow's eComms surveillance solution, TZEC, can either be used as a standalone regulatory tool or integrated with its TZTS trade surveillance module as part of a holistic approach to identifying potential market abuse.

This approach enables firms to capture the full spectrum of electronic interactions taking place across their organisation, before linking them to relevant trade activity for further analysis.

The benefits of an integrated approach

Increased operational efficiency

In today's digital trading environment, the monitoring of both trade and eComms activity is fast becoming a core regulatory requirement. To achieve this, many firms use siloed systems that still require a significant amount of manual intervention and cross-referencing in order to 'join the dots'. eflow's TZEC system adopts a holistic approach that integrates both trade and eComms surveillance in a single technological solution. This eliminates the need for firms to develop complex data pipelines that link and analyse structured and unstructured data, resulting in more streamlined operations and reduced overheads.

Combining both eComms and trade surveillance into a single view allows for supporting evidence (eComms surveillance) for retrospective trade/order activity (Trade Surveillance) to seamlessly blend together in order to fulfill all regulatory requirements.

Enhanced decision making

Utilising machine learning-powered natural language processing (NLP), TZEC not only captures data but interprets it, connecting communications directly with related trades. This capability allows the system to construct a comprehensive narrative of each trade and uses sophisticated sentiment analysis to identify the intent and context behind actions, thereby providing deep insights into instances of potential market abuse.

Stronger governance

TZEC can undertake a deep-dive analysis of all types of communication channels in a matter of seconds. This means that firms can monitor and analyse vast quantities of data while streamlining surveillance operations and mitigating against the risk of non-compliance. The platform also maintains detailed logs of all relevant communication and actions taken, providing an essential component of regulatory record-keeping obligations.

Granular personalisation

With the capability to test system configurations in an independent sandbox environment, TZEC allows firms to fine-tune their surveillance parameters on an ongoing basis, tailoring the system to meet their specific operational needs at a granular level.

Why are firms turning to integrated surveillance now?

Growing sophistication of market abuse

Firms and regulators are constantly grappling with the intrinsic difficulty of proving market abuse, which entails extensive investigations and complex evidence gathering exercises. This challenge intensifies as bad actors employ more sophisticated strategies that span markets and products, while the proliferation of communication channels increases the potential for unmonitored blindspots. When combined, these dynamics are exposing firms to exponentially greater risk. Without a holistic approach to surveillance, it will become nearly impossible to piece together a complete narrative behind suspicious trades and, crucially, to prove liability in a legal setting.

Increasing regulatory scrutiny

Integrating trade data and eComms surveillance is quickly becoming a non-negotiable regulatory demand. With the quality of firms' recordkeeping in the spotlight, the frequency and severity of enforcement action that seen in the US is likely to spread across the world as regulatory bodies grow impatient with incomplete data acting as a roadblock for market abuse investigations. In the UK, for example, Ofgem levied a landmark £5.41 million fine against Morgan Stanley & Co in September 2023 for failing to record and retain electronic communications.

Firms must understand that collecting and storing communication data is merely the first step in the process. The true challenge lies in leveraging this data to detect and understand market abuse. Regulators rely on eComms data and expect firms to monitor their operations with equal rigour. Adopting a holistic approach to surveillance is essential for firms serious about safeguarding market integrity and maintaining their reputation.

Cost pressures

As firms have implemented increasingly complex surveillance technology over the past decades, they have discovered the operational burdens of generating high false positive rates with isolated lexicon-based, or rudimentary sample-based, surveillance. Integrated systems can significantly reduce the risk of false positives being reported, therefore reducing the amount of time that compliance teams need to spend reviewing them.

Furthermore, by consolidating analysis into a single platform, firms can lower their operational costs. This reduces the need for multiple surveillance tools and minimises the administrative overheads associated with maintaining separate systems for trade and eComms surveillance.

Key takeaways and future outlook

Integrating eComms with trade surveillance is a complicated endeavour that has often been hindered by data silos and disparate systems. This inherently complex approach has sometimes limited the perceived value that independent systems can offer to a firm's regulatory strategy.

However, the introduction of holistic surveillance tools offers a proactive and truly integrated solution to trade surveillance. It is no longer just a possibility, but a seamless option with an explainable approach combined with improved outcomes. With regulatory scrutiny of eComms surveillance set to intensify, firms are left with little choice but to take steps to get ahead of the curve with respect to technology adoption. Regulators are increasingly expecting firms to not only take proactive steps to prevent market abuse, but to protect their customers and mitigate systemic risk.

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.

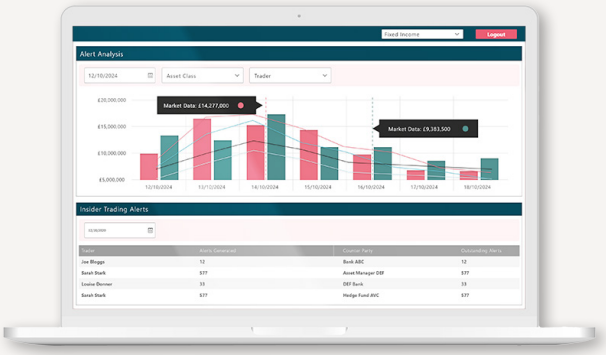
To achieve this, we first had to identify why so many firms either struggled to demonstrate their compliance or spent far too much time, effort and money in doing so. We found that for many institutions, their regulatory processes were broken. An over-reliance on spreadsheets and siloed data. Slow, legacy 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.

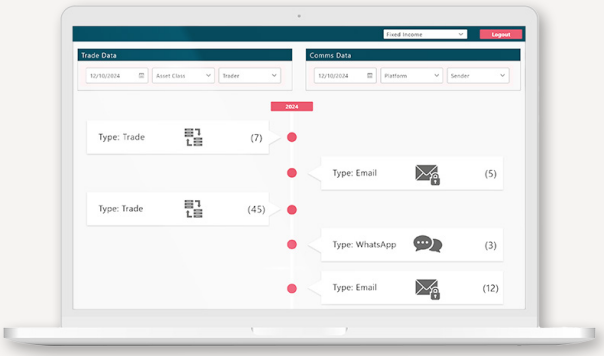
This means that as new regulatory challenges arise, as they inevitably will, you can rest assured that eflow's regulatory tools will already be one step ahead.

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

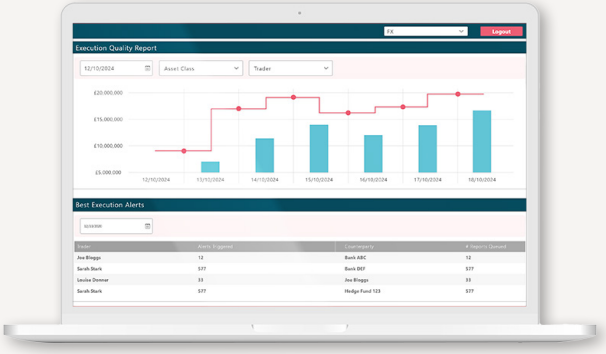
TZTS Trade Surveillance



TZEC eComms Surveillance



TZBE Best Execution



TZTR Transaction Reporting