eComms Surveillance
Benchmarking your approach

Benchmark Survey performed by JWG
Contents

1. Introduction....................... 5
2. Executive Summary........... 6
3. About the Survey............. 7
4. Summarized Findings........ 8
5. Detailed Results..............10
6. Conclusion.......................22
1. Introduction

Electronic Communications (eComms) Surveillance is an increasingly crucial element of trade surveillance for financial services firms. In the context of regulatory requirements from Dodd-Frank, MiFID II and MAR, firms are reliant upon being able to capture, analyse and index data from a wide range of electronic sources.

In August of 2018, JWG ran an eComms focused regulatory implementation survey which aimed to increase the understanding of existing compliance efforts within the financial services industry; how eComms Surveillance systems and procedures can be enhanced, and the application of new technologies to the process.

At JWG we have been working with firms, technologists and regulators since 2006 to help the industry as a whole understand and meet regulatory challenges. This paper details the anonymised survey results to help inform the industry of disconnects in existing approaches and identify gaps in the solution market place.
2. Executive Summary

The survey results affirm that it’s now time for financial services firms to prioritize investment in new technologies. The prevalence and levels of fines for non-compliance are increasing and firms appear to be poorly equipped to meet these rising regulatory standards. The results of the survey, which represent the input of representatives from a significant number of firms, supports this point in a number of ways.

Most firms are still not equipped to capture and monitor all forms of eComms. When firms were asked which channels presented the biggest challenge (in terms of detecting and preventing market abuse), ‘voice’ was the predominant answer, but respondents also noted various types of eComms as challenging as well.

For example, a third of respondents surveille fewer than 40% of all eComms and only 20% of respondents are not yet using holistic surveillance techniques.

Furthermore, over 15% of respondents were not able to meet the Dodd-Frank requirement for trade reconstruction, acknowledging that it took them on average over 72 hours to complete the trade reconstruction process.

In spite of all of these reported issues, the uptake of newer technologies such as Natural Language Processing and voice-to-text appears to be relatively slow. This suggest a worryingly reliance on manual surveillance methods. It’s clear that firms both want and need to have much better capabilities that are afforded by next generation surveillance solutions.

Key Finding Highlights

The prevalence and levels of fines for non-compliance are increasing and firms appear to be poorly equipped to meet these rising regulatory standards.

- 33% of the respondents surveille fewer than 40% of all eComms
- 15% of the respondents are not able to meet the Dodd-Frank requirement for trade reconstruction
- 60% of respondents are not yet using holistic surveillance techniques

For example, a third of respondents surveille fewer than 40% of all eComms and only 20% of respondents surveille between 81-100%. It’s clear from this that large volumes of data are falling through the cracks. Respondents also stated that false positives, the inability to link data and match eComms with other data, and the general lack of solutions were all equally problematic.

In spite of all of these reported issues, the uptake of newer technologies such as Natural Language Processing and voice-to-text appears to be relatively slow. This suggest a worryingly reliance on manual surveillance methods. It’s clear that firms both want and need to have much better capabilities that are afforded by next generation surveillance solutions.
The survey opened on August 19th, 2018 and ran for 4 weeks to September 7th. Our thanks go out to the individuals in senior technology, ops and compliance functions who provided us with responses.

In total, we received 42 responses from individuals at a minimum of 25 firms. It is impossible to say the precise number of firms as some responses were submitted anonymously, however the survey was only distributed to individuals with surveillance relevant roles at financial institutions globally, we are therefore confident in the integrity of these responses. We considered approaching our analysis by removing these responses, however, we found that the trends correlated with responses from non-anonymous respondents, therefore the data which you see in this paper includes these respondents.

All the respondents answered a majority of the questions, however, not all respondents answered all the questions, for this reason not all questions that are analysed in this paper have 42 responses.

Figure 1 breaks down the 25 firms mentioned above into sell and buy-side categories. Responses came from 17 sell side firms and 8 buy side firms, the results therefore represent a reasonable balance between the two perspectives, which from a regulatory point of view are very similar.

Over 90% are large firms who would be considered either tier 1 or tier 2.

Figure 2 categorizes the 25 firms in a word cloud by the country in which they are headquartered. The firms are headquartered in 9 different countries (all important financial hubs). It is fair to say that there is somewhat of a bias towards EU and North American headquartered firms.

All of the firms have a global footprint.
4. Summarized Findings

The survey results show several striking and clear trends:

1. Firms are currently lacking in surveillance capability and greater investment in surveillance capabilities is needed.

2. Firms are at risk of not meeting existing regulatory requirements and therefore at risk of substantial fines.

3. New technologies with the potential to improve compliance and achieve long term savings are largely being ignored.

The survey also paints a picture of a regulatory environment which is less tolerant of firms slow on the compliance uptake. A combination of factors including the LIBOR scandal and the significant delays to the implementation of the MiFID II framework has seen regulators, particularly across the EU (for now still including the UK) and North America, become more inclined to come down hard on firms that are not living up to regulatory standards.

It is reasonable to expect that this view will be applied sooner rather than later to firms’ surveillance functions given the prominence of market abuse in the wake of LIBOR. In fact many consider the case of Interactive Brokers being hit with an FCA fine of over £1m in 2018 (for failings in identifying and reporting suspicious transactions) a sign of what’s to come. Indeed other recent fines (such as a reported $1.27bn Soc Gen settlement with US authorities for a wide range of perceived failings) have strong links to surveillance functions.

Given all of these factors, why then are firms lacking in even the most basic surveillance capabilities?
Eighteen months ago it may have been fair to say that the lack of investment in new technologies was due to a lack of maturity and confidence in these technologies. But today, with a number of firms reporting at least partially successful implementations of technologies (ranging from voice-to-text to machine learning to natural language processing), this is not true today.

In this environment, firms that are still unwilling to invest risk being left behind.

Some will argue that given that surveillance is not a profit-making enterprise it makes sense to keep investment levels low. But these arguments do not take into account the cost and damage of regulatory enforcement actions, which are becoming more commonplace by the day.

Furthermore, firms (small and large, buy-side and sell-side) already invest significant time and resources into eComms surveillance, a consequence of their reliance on outdated technologies and manual methods.

These low-tech approaches are underpinned by a lack of strategic long-term thinking. With the right prioritization and technology investment firms have an opportunity to achieve both improved capabilities and long-term cost saving. Technologies in this space have matured sufficiently to the point where this prioritization exercise can be undertaken today (with a view to finalizing investment decisions in the next 12 months).

Another major factor that is driving implementation is the extent to which technologies are effective enough to spot suspicious activity, thereby preventing a firm from suffering significant losses in fines. As accuracy rates improve, budget holders will have even more justification to replace their outdated manual, legacy systems.

One thing is abundantly clear – existing surveillance approaches are failing and the consequences of not adapting and not investing in longer term, more strategic approaches could be very high indeed.
5. Detailed Results

Q1: Which of the following channels is the most difficult to monitor for the purpose of detecting and preventing market abuse?

Voice, as expected, is clearly perceived to be the biggest challenge in terms of surveillance. Surveilling voice communications has been a known issue for firms for several years now. As it is fundamentally different from most other forms of communications data it does not easily feed into established surveillance systems.

Both MiFID II and MAR have heightened surveillance requirements and made them more prescriptive. Requirements under MAR to detect intent to commit market abuse and monitor any sales recommendations given to clients, as well as MiFID II’s requirements relating to trading as Systematic Internalisers are particularly relevant in this respect.

The emergence of voice-to-text technologies are seen by some as a solution to these more prescriptive requirements, especially with respect to voice communications. In spite of this, the survey results show that there has not been a wide uptake in the adoption of these technologies, thus putting firms at risk.
The survey also shows the emergence of social media as a key focus of surveillance (which would have not been expected several years ago). Most firms appear to feel that they have more traditional eComms surveillance, such as email, under control. But this could also reflect a lack of investment as legacy systems are more suited to established forms of communication (such as email).

Overall there is a broad cross-section of responses and some variability, which indicates that some firms still consider the entire landscape to be a challenge (which could again be a symptom of inadequate investment in new surveillance technology).

Responses to ‘others’ focused on personal mobile devices as opposed to firm-issued devices. The difficulty in monitoring such devices is known to have led to some firms banning personal devices on trading floors. It appears that firms that have not taken this step continue to struggle with this issue.

**Q2**: What percentage of regulated users’ electronic communications (email, chat and text) do you currently perform surveillance on for threats?

- **29%** of respondents say that they are surveilling 81-100% of eComms
- **63%** say that they are surveilling over 40% of eComms
- **36%** of respondents are surveilling less than 40% of eComms
- **~10%** of firms say that they are surveilling 5% or less of total activity

These responses reinforce the previous results in the sense that firms are finding it difficult to capture eComms data across the full range of channels. It equally points to insufficient capabilities within firms and their existing approaches to these issues.
Q3: In relation to trade surveillance, what is your biggest challenge in terms of monitoring and detecting market abuse?

![Bar chart showing responses to Q3](Figure 4)

When it comes to monitoring and detecting market abuse, respondents clearly feel that there is a lack of adequate technology solutions. They view this as a more substantial challenge than high false positive rates or the ability to capture complete data, which we know from other questions are perceived as big challenges.

This could mean one of two things: 1) either they perceive that technological solutions to these problems do not exist in a viable form, or 2) their firms have simply not made the required investment in said technology. This is an important distinction since, as discussed previously, the general consensus among technologists is that the technology in this space has matured significantly, and is readily available to firms.

To better understand the responses to this question, we reached out to respondents to clarify. The broad consensus of respondents was that it was much more about a lack of investment than a lack of technology. Firms are being held back by a lack investment in new surveillance technology.

As with figure 3 we see here a broad range of responses showing that respondents, as expected, see challenges across the board. This puts into context the previous results, which showed that capturing all of the data is a big challenge, but only one part of the problem.
Q4: To what extent are eComms a priority for you in terms of your overall regulatory compliance strategy?

15% of respondents say it is top priority

85% of respondents say it is of high importance, not in the top

While there is a lack of investment in surveillance technology, it does not appear to result from a de-prioritisation of surveillance in favour of other compliance functions, as all of respondents firmly stated that surveillance is either a top or high priority for their firm.

Q5: As per the requirement under MAR, how confident are you that you are able to identify intent to commit market abuse?

Notably, not a single respondent answered that he or she was ‘completely confident’ in terms of his or her firm’s ability to identify intent to commit market abuse. This was one of the most heavily discussed new requirements under the EU’s Market Abuse Regulation (MAR). Nearly 20% of respondents are not confident at all that they are meeting the obligation.

This is quite an alarming statistic given that MAR was instituted in the EU in July 2016. Oftentimes when a new regulation is implemented, regulators provide a ‘grace’ period in which they will work with firms to get the implementation of new regulations right. During this time, it is typical to not see too many large fines for non-compliance. Given this grace period will soon come to a close, this level of confidence by respondents, of lack thereof, should concern senior managers, as it further underscores that existing surveillance capabilities are not up to the job.
Trade reconstruction under Dodd-Frank needs to be completed within 72 hours. Over 15% of firms are still outside of the Dodd-Frank requirements years after implementation. MiFID II mirrors Dodd-Frank by bringing in trade reconstruction rules in Europe. However, the rule is more vague, stating that trade reconstructions need to be completed ‘in good time.’ In spite of the vagueness of the language though, enforcement of ‘in good time’ in many cases has been stricter than the 72 hours mandated under Dodd-Frank.

To date, manual reconstruction has generally been sufficient because regulators requested only a small number of reconstructions. However, firms are experiencing an uptick in the number of requests for trade reconstructions and this is expected to continue. In light of this, firms are considering voice-to-text technologies as a means of helping to further automate the reconstruction process.

Q6: How quickly, on average, are you able to reconstruct a trade?

![Figure 6](image)

- Less than 12 hours: 15%
- 12 hours: 7%
- 24 hours: 26%
- 48 hours: 9%
- 72 hours: 23%
- One week: 16%
- Longer than 1 week: 4%
Q7: Which technologies are you currently utilising in your eComms Surveillance approach?

The answers to this question suggest a reliance on lexicon-based models and, most concerningly, manual techniques. The fact that these approaches heavily outweigh all of the others demonstrates a lack of investment in new approaches. Lexicon-based models and manual surveillance are traditional approaches to surveillance. There is a place for them, but near-ubiquitous reliance on them (given evolving forms of communication and more sophisticated trading techniques) is a worrying sign.

On the flip side, the adoption of newer technologies (such as Natural Language Processing and voice-to-text) appears to be relatively slow. Similarly, some firms have begun to utilise biometric analysis, but the uptake also appears to be slow.

Given the fact that (based on results discussed earlier) current approaches do not appear to be working and that, (based on results discussed below) firms feel that they require greater functionality from their surveillance systems one would expect broader adoption of new surveillance technologies.

Figure 7
In following up with firms on this question two things were clear:

- Firms that have begun implementing new technologies, while experiencing some teething problems, see value in new technologies delivering results now.
- Firms that have not implemented new surveillance technologies generally have not done so due to cost considerations.

This further clarifies the picture that the results through this survey are showing: **under-investment in technology is harming the ability of surveillance teams to fulfill their functions.**

**Q8:** Thinking of your ideal eComms Surveillance solution, how important are improving upon the following capabilities?

![Figure 8](image)

It is immediately clear that the lack of investment in new surveillance technology is not for lack of want for new capabilities. When asked specifically what capabilities they could benefit from most, while everything is seen as relatively important, both reduction of false positives and better accuracy top the list.

Still, there is not a single category of capabilities that respondents did not see as important, which should send a very clear message to senior managers.
Q9: Which, if any, of the following techniques are you utilizing to reduce the number of false positives being produced by your eComms Surveillance solutions?

The responses here correlate with earlier responses in suggesting a reliance on low-tech, traditional methods over using new technologies. The reduction of false positives via trial and error is inefficient and expensive due to the amount of manual resources required. In light of this, firms would be well advised to invest in new approaches for long-term savings.
The implementation of new technological solutions, particularly data heavy or enterprise-wide solutions is often far more feasible via the cloud. In contrast, ‘on site’ installations can be vastly more expensive and technically intensive. However, it is well known that many financial services firms have an aversion to cloud-based solutions, particularly with regard to sensitive data, such as trade or communications data.

The responses here suggest that this attitude continues to prevail. Fewer than 20% of respondents consider their firm ‘very willing’ to implement cloud-based solutions with only a further 24% ‘somewhat willing.’ It’s possible that this offers a partial explanation for the slow uptake of some solutions. Still, moving on to the cloud could also be important in transitioning toward holistic surveillance techniques.

**Q10:** How willing are you to consider using cloud-based eComms Surveillance solutions?

![Chart showing willingness levels]

- **Very willing:** 19%
- **Somewhat willing:** 40%
- **Not willing at all:** 29%
- **Unsure:** 29%
- **Not applicable:** 2%

**Figure 10**
**Q11:** To what extent are you implementing holistic surveillance techniques that monitor, collate and decipher data from numerous data stores (e.g. eComms, voice, trade data etc.)?

![Figure 11](image)

- Holistic is completely implemented: 44%
- To a great extent, but not for all aspects: 39%
- Using holistic methods on a limited basis: 15%
- Not using holistic methods at all: 0%
- Impossible to say: 0%

**Q12:** What, if any, are the biggest barriers to implementing a holistic approach to communications and trade surveillance?

![Figure 12](image)

- The resources needed: 39%
- The number of data sources: 35%
- Solutions are not yet developed enough: 20%
- Piece-meal is an adequate approach: 5%
- Other reasons: 15%
Regulations are putting pressure on investment firms to adopt a more proactive and preventative surveillance approach so they can identify risk before it occurs. To achieve this firms need to implement holistic trade surveillance controls that are capable of collating and deciphering information from separate data silos, including voice, eComms and trading data.

Firms often argue that, in terms of holistic solutions, no such ‘silver bullet’ yet exists, but the solutions available (and in use today) by leading financial services organizations refutes this. The reality is that some firms are just too risk-averse and others, too budget-constrained to take the leap forward. Nevertheless, to achieve full-compliance under the rule sets, investment firms (particularly the larger banks) will need to look to new technology to reinvent their business practices and bring together all of their data silos.

The responses to these two questions demonstrate that while no one has turned to a fully holistic approach, some progress has been made.

A lack of investment is clearly an important factor.
While here is no doubt that implementing a holistic solution is likely to be a costly endeavor given the large number of systems and data silos that will require reconciliation. Interestingly though, respondents hardly see it as the only barrier, the operational scope of the exercise in terms of data sources polls equally highly, as does the level of development of solutions.

Q13: To what extent is your approach to communications and trade surveillance a combination of using third-party surveillance solutions and developing solutions in-house?
Responses suggest a relatively high level of dependence on vendors and third-party surveillance. But there appears to be no one size fits all solution. Not a single firm developed everything in house and on the other side of the spectrum, fewer than 20% of respondents reported developing a majority of their surveillance capability in house.

Survey respondents named nine separate vendors that their firms use. The responses here would help to suggest that vendors bear some of the responsibility for transitioning the industry to higher tech approaches.

**Q14:** What are your motivations when determining whether to buy third-party solutions as opposed to developing in-house solutions?

![Survey responses showing motivations](image)

Respondents were clear that the most important aspect of a new solution is the cost. This jibes with the rest of the results which heavily suggest that budgetary pressure is a key limiting factor on surveillance capabilities.
6. Conclusion

The responses to the survey show a clear and worrying pattern.

Under-investment in surveillance solutions are causing large problems now and delays in fixing this problem put firms at risk.

There are a large number of challenges that surveillance teams are currently tackling including high false positive rates, monitoring voice communications, and data quality issues. These challenges can effect a firm’s ability to meet existing regulatory requirements under Dodd-Frank and MAR, and put firms at risk of enforcement actions and fines.

These challenges are only exacerbated by a general lack of investment in and utilisation of emerging technologies, such as machine learning, voice-to-text and biometrics.

Surveillance teams urgently require investment in better capabilities in order to get back on track in an environment ripe for big fines.
About JWG

JWG are operations and technology professionals, trusted by the global financial services industry as experts in regulatory change management. For the past decade, a team of independent analysts has helped the industry interpret large quantities of regulatory reform and action it in a smart and intelligent way.

www.jwg-it.eu

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com/compliance

Contact Us

Americas, Hoboken Office, NJ, Tel. +1 551 256 5000
EMEA, London office, Tel. +44 0 1489 771 200
APAC, Singapore Office, Tel. +65 6222 5123
compliance@niceactimize.com

The full list of NICE marks are the trademarks or registered trademarks of NICE Ltd. For the full list of NICE trademarks, visit www.nice.com/nice-trademarks. All other marks used are the property of their respective proprietors.

CONTENTS OF THIS DOCUMENT ARE COPYRIGHT ©2018