Aité PARTNER. ADVISOR. CATALYST.

From Lexicon to Language: Overcoming the Challenges of E-Communications Surveillance

DECEMBER 2018

Prepared for:

NICE ACTIMIZE

© 2018 Company Name. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

TABLE OF CONTENTS

INTRODUCTION 3
METHODOLOGY 3
COMMUNICATIONS AND SURVEILLANCE TECHNOLOGY: A DEVELOPMENTAL OVERVIEW 4
COMMUNICATIONS TECHNOLOGY AND REGULATORY EVOLUTION 4
REGULATORY COVERAGE 5
SURVEILLANCE TECHNOLOGY EVOLUTION 6
E-COMMS MONITORING TRENDS AND CHALLENGES 11
DEMAND DRIVERS 11
E-COMMS SURVEILLANCE CHALLENGES 11
ACHIEVING INTEGRATION AND ACCURACY IN E-COMMS MONITORING 12
ACCURACY AND INTEGRATION: TOP PRIORITIES 12
BEST PRACTICES FOR EFFECTIVE E-COMMS SURVEILLANCE 13
CONCLUSION 15
ABOUT AITE GROUP 16
AUTHOR INFORMATION 16
CONTACT 16

LIST OF FIGURES

FIGURE 1: EVOLUTION OF E-COMMS AND REGULATION IN CAPITAL MARKETS 5
FIGURE 2: IMPORTANCE OF SURVEILLANCE FUNCTIONALITY IMPROVEMENTS 8
FIGURE 3: APPROACHES TO E-COMMS MONITORING 9

LIST OF TABLES

TABLE A: GLOBAL COMMUNICATIONS REGULATORY SUMMARY 6

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.

INTRODUCTION

The importance of communications to investment operations is clear, and investment personnel have benefited greatly from the advent of ever-expanding communications technology. The evolution of electronic communications (e-comms) has provided capital markets participants with the ability to communicate efficiently and instantaneously, among other advantages. Moreover, being able to leverage the growing collection of investment-specific apps and platforms available on smartphones and tablets has increased both the accessibility of investment data and the immediacy of its application to investment strategies.

The benefits of e-comms technology to the investment industry are indisputable, but they do not come without increased compliance risks. Thus, firms' monitoring policies must keep pace with communications technology, but this can be difficult to achieve for many reasons—not the least of which is the formidable task of implementing the regtech solution best designed to fit the firm's monitoring needs. However, deploying the most appropriate surveillance solution is only part of the battle; firms must also rise to the challenges of data source integration and incorporate advanced analytics into alert generation.

This white paper highlights the changing dynamics of e-comms in the financial world and the integral role that mobile communications will play in the evolution of the surveillance and compliance technology.

METHODOLOGY

This white paper has been commissioned by Nice Actimize and is based on proprietary Aite Group research as well as publicly available information provided by global regulatory entities. The primary research that serves as the basis for the analysis presented in this paper was conducted via quantitative surveys in 2016, 2017, and 2018, in addition to qualitative in-depth interviews with industry participants during the third quarter of 2018. Industry participant interviews included representatives from the buy-side, sell-side, and U.S. regulatory bodies. Also referenced in this work are results from a survey of 42 representatives from at least 25 different sell-side and buy-side firms, which was conducted by JWG[1] in August of 2018 on behalf of Nice Actimize.

1. JWG is a London-based financial services firm that provides regulatory change management solutions and regulatory analysis support to global capital markets firms. The data collected by JWG that has been referenced in this report is the intellectual property of Nice Actimize and is licensed for its exclusive distribution.

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.

COMMUNICATIONS AND SURVEILLANCE TECHNOLOGY: A DEVELOPMENTAL OVERVIEW

Communications are an integral part of investment firm operations, and in today's technology-based culture, most written communications are conducted via electronic methods. From email to chat messaging and social media platforms, financial firm employees rely on e-comms to facilitate both external and internal communications. In this white paper, which focuses on surveillance and monitoring of e-comms for compliance purposes, voice communications and video calls conducted via both cellphones and landlines are included in the category of e-comms. This first chapter of the report provides a review of technology development in the e-comms realm, juxtaposed with the related regulatory coverage; subsequent sections will cover important aspects and challenges of e-comms compliance monitoring, guidance for navigating e-comms surveillance challenges, and analysis of the future direction of the space.

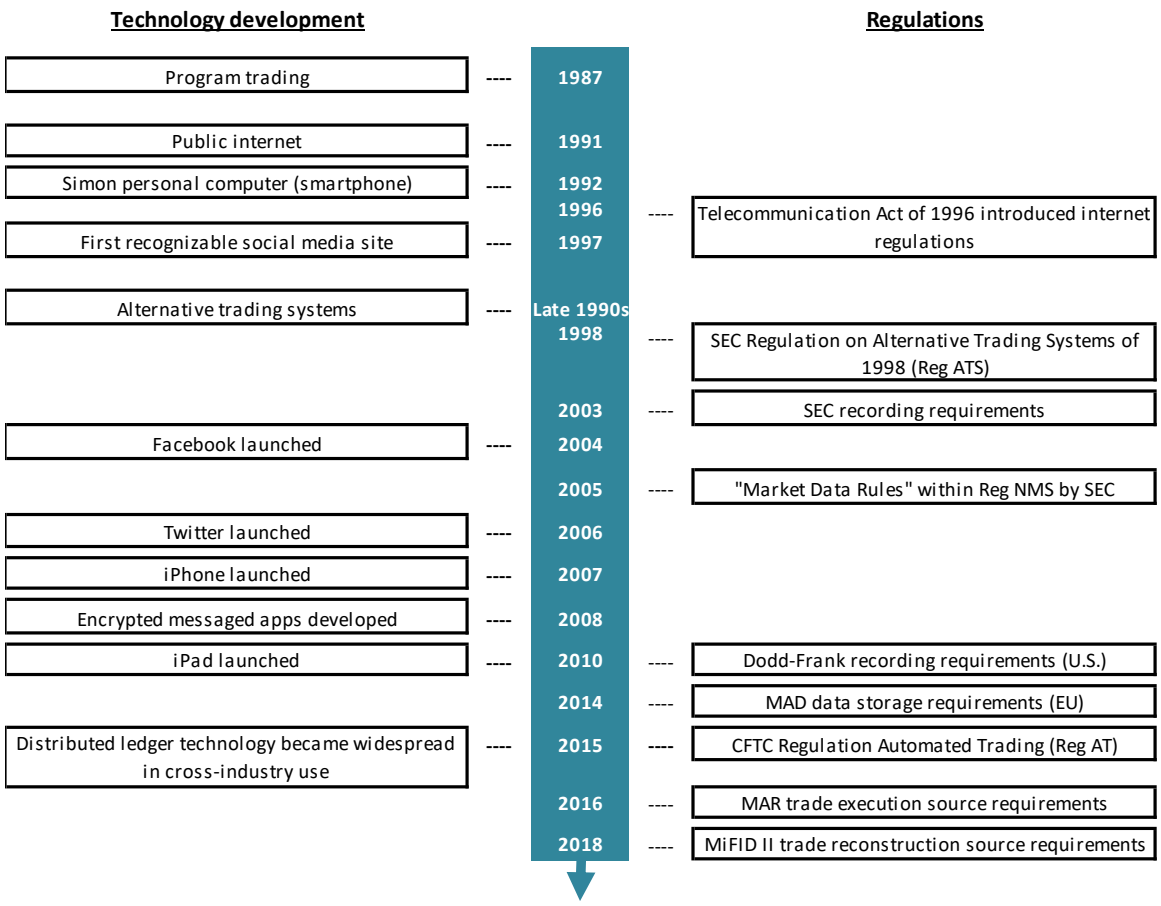
COMMUNICATIONS TECHNOLOGY AND REGULATORY EVOLUTION

While the argument can be made that the history of e-comms reaches back to the invention of the telegram, we can consider the modern e-comms age to truly begin with the launch of email systems in 1972, although email did not enter widespread use until the early 1990s. Facsimile machines (faxes) were also one of the first key e-comms developments, becoming commonplace by the mid- to late-1980s; although the technology is now considered relatively antiquated, most financial firms still use faxes for certain key operations—particularly those requiring signatures. In this internet age in which cybersecurity breaches are a tangible and imminent threat, dialing back on internet-based technology is sometimes preferred when firms are handling sensitive information. Since the late 1990s, communications technology growth has become exponential, as the years have seen the introduction and proliferation of messaging and chat platforms as well as social media and easily available encrypted messaging.

In the case of most communications technology developments, there are significant lags between the entrance of the technology into popular use and the implementation of relevant regulations. Figure 1 provides a brief overview of this historical evolution, as well as a summary of the eventual regulatory responses.

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.

Figure 1: Evolution of E-Comms and Regulation in Capital Markets



Source: Aite Group

REGULATORY COVERAGE

Most regulations focus on recording and storage, and they have only recently focused on specific data sources to be included. They do not, however, detail the manner in which firms are expected to accomplish communications monitoring, thus leaving the surveillance roadmap up to the firms to decide and develop. This substantial gray area has resulted in inconsistencies in compliance requirements across the industry, increased regulatory risk for firms, and significant underdevelopment of firms' overall e-comms monitoring infrastructure.

As regtech focuses on loss prevention rather than profit generation, making a case for compliance technology investment is no easy task, even when the regulatory mandate is clear—and it is certainly not made easier when the actionability of regulatory requirements is left open to interpretation. Moreover, achieving effective communications monitoring is further complicated by the inherent difficulty of unstructured data analysis, as well as the unreliability of the original data inputs. If unclear regulation and inescapable structural challenges weren't challenging enough, the e-comms monitoring space has also been plagued by occasional adoption of solutions that were not quite ready for deployment. All of these factors, in addition

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.

to the difficulty of integrating e-comms monitoring into a holistic trade surveillance infrastructure, have resulted in the reality of many firms remaining significantly below par in their e-comms surveillance evolutionary development.

Regimes in the U.S. and Europe have attempted to address the issue, but details regarding how to accomplish effective coverage are sorely lacking and thus are largely left to individual firms to determine. The points from global regulations detailed in Table A have been selected as the most relevant to the e-comms surveillance challenge.

Table A: Global Communications Regulatory Summary

Year	Regulation	Relevant requirements	Sources covered
2003	MAD	Anti-insider trading and market abuse directive	Not specified
2003	SEC	Requires firms to record and maintain communications for three years	All platforms—covers cellular by default
2010	DFA	Recording, record-keeping, technology audits	Email, instant message, voice
2014	MAD	Updated to include recording and storage of trade-related communications	Phones, computers, devices
2016	MAR	Recording and storage of communications related to trade execution	Phones, faxes, e-comms, meetings, websites, blogs, social media
2018	MiFID II	Recording and storage of communications, use in trade reconstruction	Phones, e-comms, internal and external communications
Ongoing	CFA	Recording and storage	All

Source: Global regulatory regimes, CFA Institute, and Aite Group analysis

SURVEILLANCE TECHNOLOGY EVOLUTION

To satisfy regulatory mandates, surveillance technology designed for e-comms monitoring has necessarily evolved as well. Especially during the last two to three years, e-comms monitoring solutions have benefited from vendor development; functionalities and scope have been heavily fortified and expanded in several ways. Key drivers of e-comms surveillance technology include the following:

- **Analytical functionality:** As the method of reviewing source data and generating alerts based on that information, the method of analysis employed is particularly important to the success of any e-comms monitoring system. Analytics in e-comms surveillance have evolved from the basic lexicon-based keyword review to natural language processing (NLP) techniques.
- **Holistic alert integration:** Once analysis of e-comms data is conducted, any alerts generated are dramatically increased in effectiveness if they can be automatically

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.

integrated into the main case management system and correlated with alerts from the firm's main surveillance platform. Further, the ability to integrate voice data with trading alerts is a key component of the holistic approach.

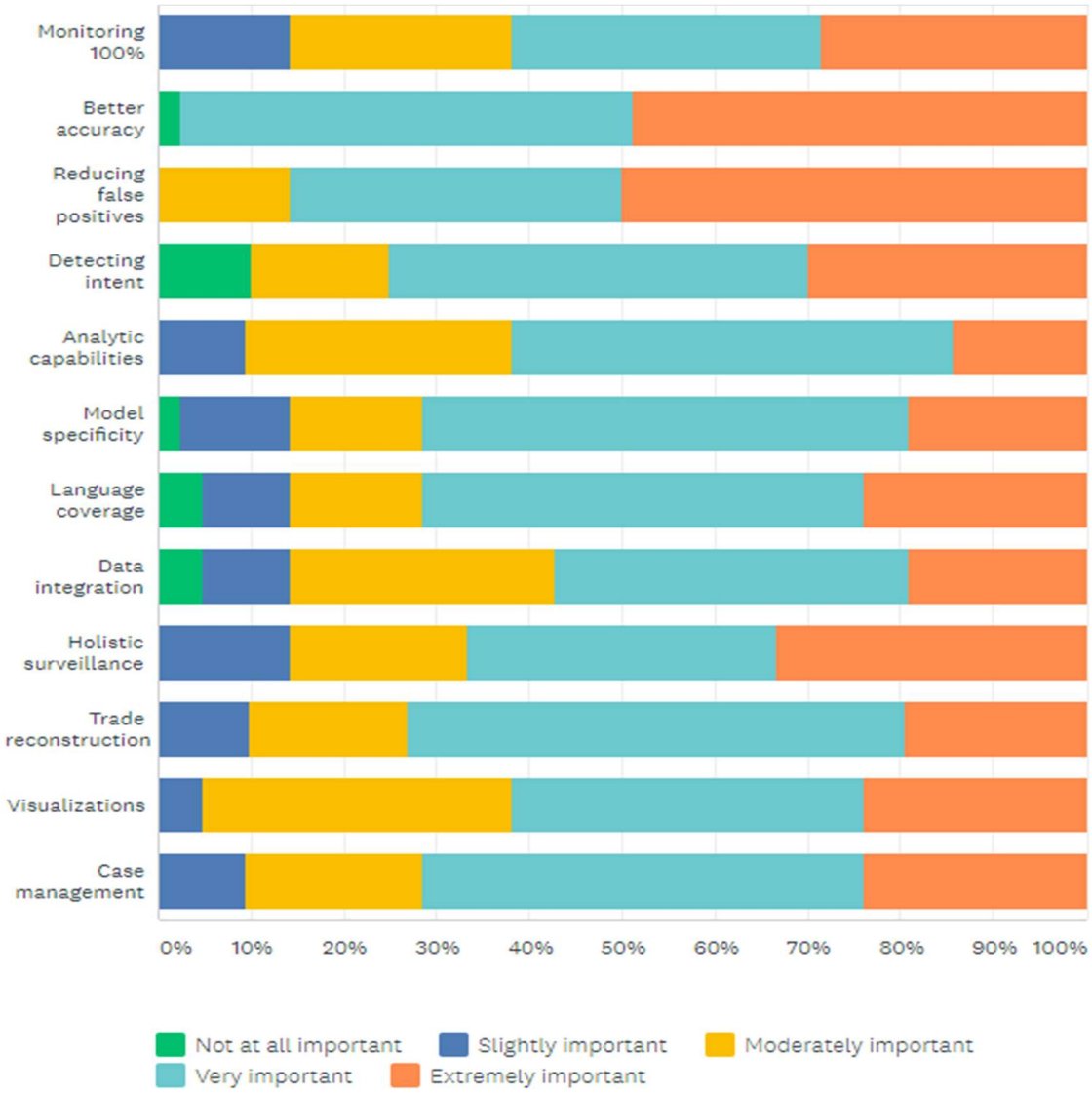
- **Storage integration:** Record-keeping practices and data storage requirements are heavily featured in existing regulations, so e-comms technology benefits from easy integration with the firm's data storage component.

The integration components have been through several common iterations, but the highest level of integration on the market involves holistic single-vendor platforms. However, over half of firms that employ systematic e-comms monitoring are still using stand-alone systems, which basically leaves alert integration to manual or rudimentary methodologies.

Likewise, e-comms analytics have progressed quite a bit since the first-generation lexicon-based approach, which was the standard methodology until the recent introduction of more advanced solutions. When the lexicon-based approach was the only feasible solution available, many firms were discouraged from attempting to review and process the resulting alerts, as false positive incidences were unmanageably high—making the alerts nearly as ineffective as no alerts at all. Furthermore, many systems produced alerts based only on a random sample (2% to 5% of total communications), which further decreased true effectiveness. Improving accuracy and reducing false positive remain by far the most important priorities for compliance and surveillance personnel (Figure 2).

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.

Figure 2: Importance of Surveillance Functionality Improvements



Source: JWG

TWEAKING THE RECIPE: A PINCH OF LEXICON AND A DASH OF NLP

The second-generation of analytics includes NLP. Although NLP-based analytics are more accurate than lexicon-based ones, they must be carefully programmed to understand financial industry language to be able to deliver on their promise. Some technology providers have recently achieved this by tuning their models using financial markets dictionaries they created. These models can effectively process the labyrinth of trader language, and users are reporting improvements in false positive attacks.

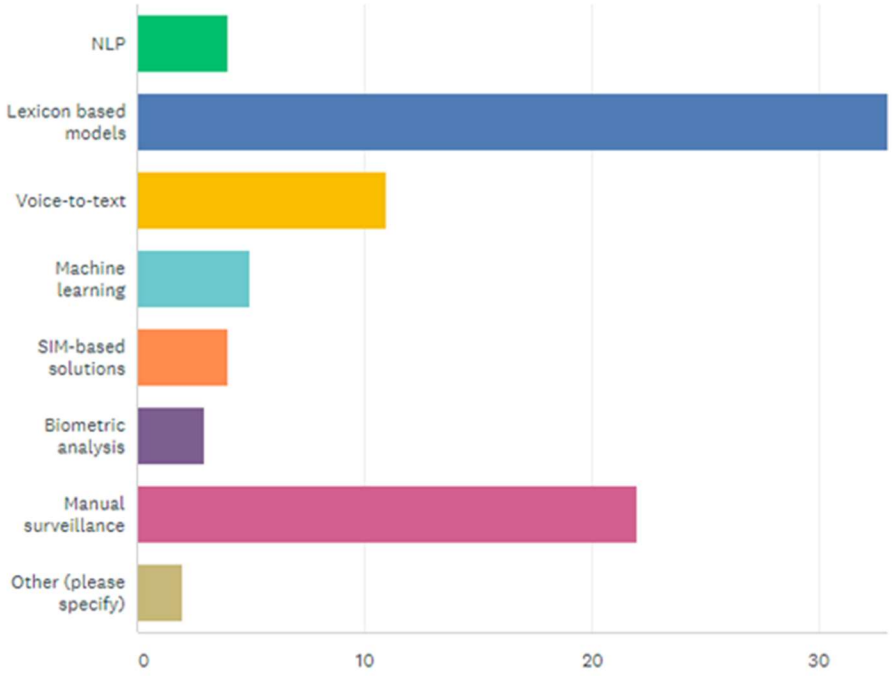
Since NLP models require time and effort to tune and adapt to the needs of each organization, few firms have fully transitioned their e-comms infrastructure to solely rely on NLP. Most firms use lexicon-based solutions, which can be easily implemented and adjusted to adapt to changing regulations and surveillance needs, along with NLP-based analytics. The lexicon-based models

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.

serve as a first line of defense while NLP solutions serve as an additional filter to produce more accurate alerts and reduce false positives

Resulting from this transitional period, lexicon-based approaches are still the most commonly used e-comms monitoring model—either alone or in conjunction with NLP or other surveillance support technologies. There is arguably a strong correlation between the persistence of lexicon-based alerts as seen in Figure 3, the unreadiness of many NLP-based alerts, and the emphasis on the importance of accuracy improvement and false positive reduction as seen in Figure 2.

Figure 3: Approaches to E-Comms Monitoring



Source: JWG, Nice Actimize

Despite the lack of adoption thus far, and stemming from the reasons discussed above, NLP techniques fit well in the toolbox of communications analytics due to the technology's ability to understand the context of communications including ambiguity, emotions, or sentiment. For example, one of the improvements made to NLP technology has been the ability to tune the model inputs based on financial markets dictionaries. Even further, vendors that devote the resources to maintaining updated databases of industry jargon—and that support this in multiple languages—can provide recent examples of successful NLP deployment. If properly done, combining both structured and communications data should enrich the depth of the alerts, reducing the number of false positives and giving further insight to a potential case of criminal behaviors.

Other key technologies that support e-comms surveillance alert generation include the following:

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.

- **Voice-to-text analytics:** This functionality involves the recognition of spoken language and its transcription to text. Multiple techniques are essential to ensure accuracy, including language identification and domain-specific training of the language models.
- **Entity extraction:** This refers to the process of identifying subjects in the corpus of a text. Subjects can include people as well as legal entities, such as companies. Entity extraction can be done via statistical prediction as well as pattern matching.
- **Sentiment analysis:** This refers to the process of programmatically identifying the tone, attitude, or opinion of a particular text. Typically, these range from negative to neutral to positive. Sentiment can be associated with a document or voice file as a whole or be specific to topics or entities in said communications.
- **Machine learning:** This broad term refers to a group of techniques—including entity extraction and sentiment analysis—that attempt to extract meaning from written text. These techniques include adding context to the text based on its grammatical structure, as well as identifying elements of the text using rules or statistical significance.
    - **Supervised machine learning:** This machine-learning technique utilizes algorithms that can be trained from a dataset of known outcomes. It's called supervised because the machine is instructed on what the predicted result should be, and the model adjusts the input parameters to be able to predict the outcome based on the data provided.
    - **Unsupervised machine learning:** This machine-learning technique uses algorithms to identify commonalities in the data without explicitly being told of labels or categories. This is the most useful way to identify commonalities in the data that may be previously unknown.

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.

E-COMMS MONITORING TRENDS AND CHALLENGES

DEMAND DRIVERS

E-comms monitoring is a crucial component of detecting market abuse activities, including insider trading. Regardless of how well prospective market manipulators attempt to cloak their intent, indicators of planned illicit activities can usually be found with the help of advanced analytics. Under MiFID II, firms are required to record communications throughout the entire trade life cycle, regardless of the execution method and status for client orders. While the regulation does not specify how a firm should display intent, correlating communications data with trading alerts is a main strategy—but not every firm has the resources to do this effectively, as it involves the always-challenging task of marrying structured and unstructured data. The purpose is not only to identify engagement in criminal activities but also to establish the intention of doing so. In the United States as well as in Europe, enforcement of market abuse, insider trading, and corruption cases can hinge on the ability to show intent of wrongdoing as opposed to an innocent mistake.

E-COMMS SURVEILLANCE CHALLENGES

Several of the top surveillance challenges among firms depend heavily on the firm integrating effective e-comms surveillance with its overall trade monitoring systems. Because of the number of aspects involved in achieving successful e-comms monitoring, effective results can be difficult to achieve. Many firms report an overall dearth of solutions, but alert integration, data capture, and false positives are all crucial roadblocks to firms' surveillance efforts. This boils down to an issue of technology strategy quality—firms who have invested heavily in holistic regtech and who have selected vendors based on quality instead of simply searching for the cheapest possible way to achieve compliance are generally in much better shape in terms of integration and efficacy.

Since depth of coverage is one of the components of effective e-comms surveillance, a firm's consideration of the line between surveillance and privacy plays a key role in the outcome of e-comms monitoring efforts. Because of the extensive gray areas in legislation, the extent of mobile communications coverage is largely decided by firm executive committees. The more aggressive the firm in terms of coverage, the more data the firm will have for e-comms surveillance integration. While firms have generally improved in the percentage of communications selected for monitoring, most firms are still not reviewing 100% of e-comms data.

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.

ACHIEVING INTEGRATION AND ACCURACY IN E-COMMS MONITORING

ACCURACY AND INTEGRATION: TOP PRIORITIES

ACCURACY REMAINS KEY CONCERN

Alerts are indeed the lifeblood of employee monitoring; their accuracy is key, and they are essential to the success or failure of any surveillance system. Inaccurate alerts generally translate into an excess of false positives, which pose a time management challenge for the surveillance employee who needs to review them and likewise places cost pressures on the staffing budget. Reducing false positives is no easy task, especially considering that the increased amount of data utilized for monitoring is often still not being properly handled. Lexicon-based alerts provide only so much insight into potential cases, which combined with an exponential growth of data can result in an explosion in the number of false positives. Moving from a lexicon centric review process of e-comms to an NLP centric one would indeed refine the data results and allow firms to more seamlessly integrate e-comms flags within the overall surveillance infrastructure. Financial institutions are still struggling with prioritizing and contextualizing each case, and with automating the process itself (dismissing irrelevant alerts).

Oftentimes, the nature of the data source itself is the root cause of the degree of challenge. Because of the comprehension difficulties and the sheer number of high-end technologies involved in producing alerts with minimal false positives, voice data is considered by far to be the most challenging data source to monitor.

CHALLENGE OF INTEGRATING DATA SOURCES TO BE TACKLED

Integration of data sources remains a challenge for financial institutions, with almost two-thirds of firms interviewed in 2017 finding it very or extremely challenging. This is particularly related to the need to not only review flagged trading patterns but to also enrich the view by adding other sources, such as e-comms data, so that a more accurate picture might be revealed. Communications surveillance is so important for regulators that the wording in new regulations includes references to the relevance of records in criminal prosecution cases. The lack of change can be read as an opportunity for future improvement; as of 2017, just over 40% of firms are still processing e-comms alerts independently from their trade surveillance platforms.

Moreover, only a quarter of respondents are set up to integrate e-comms reviews and related alerts with their master trade surveillance platform and review process. This dependence on legacy surveillance ecosystems results in a significant shortfall from the level of holistic integration required for efficient and proactive compliance. Even more disturbing, over one-third of respondent firms use neither a stand-alone model nor an integrated review. In consideration of the high levels of automation reportedly used in firms' overall trade surveillance processes, these generally low levels of e-comms surveillance technology development reveal a significant weak spot—one that should be addressed sooner rather than later.

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.

Ironically, the e-comms technology weak link holds particularly true among buy-side respondents, in which over half of firms studied persist in employing a stand-alone e-comms review model. A top fear of buy-side compliance officers has always been the danger of insider trading—a violation that can shut down even a top asset manager if the infraction is severe enough. As communications surveillance is one of the—if not *the*—most important tool in detecting insider trading intentions, many buy-side firms are in dire need of an overhaul in the e-comms surveillance department. In the near future, it is likely that many buy-side firms will be replacing their outdated e-comms review systems with an updated and (hopefully) integrated approach.

BEST PRACTICES FOR EFFECTIVE E-COMMS SURVEILLANCE

Ultimately, no matter how much a firm focuses on technology investment, management must also institute compliance policies to support the firm's technology efforts. Through quantitative studies and qualitative interviews with industry participants, Aite Group has identified several common best practices among financial firms and market centers:

- Policies should be unambiguous and uniformly applied to all employees. Large firms tend to have more detailed and clearer directives than do smaller firms; this seems to be a natural effect of resource allocation.
- Policies should clearly define which communication devices should be used for various purposes. Many—but notably not all—financial firms maintain written policies requiring employees to conduct business calls and e-comms solely on company-provided devices. Company-provided devices are usually fully monitored, and the employee is informed and required to give consent, but personal devices tend to fall outside the monitoring realm and should thus be avoided.
- Firms that allow employees to use personal devices for business communications require some form of consent to monitoring; however, this is sometimes limited to company email, which neglects voice calls and texting applications, and the very presence of e-comms devices in the workplace.
- Employees are usually discouraged or outright prohibited from using mobile devices for talking or texting within the office workspace—this appears to be a universal expectation across firm segments, but it is most strict in sell-side firms.
- Regular reminders regarding device usage should be disseminated, and policies should be updated periodically.

Selecting an e-comms surveillance platform that uses the most effective technology available to help firms achieve the most effective monitoring—while keeping false positive incidences to a minimum—is certainly a challenging endeavor. Some key functionality to look for when evaluating e-comms surveillance tools include the following:

- Automatic collection and review of 100% of communications

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.

- Use of NLP-driven analytics and models tuned for financial markets to pinpoint suspicious communications and reduce false positives
- Analysis of voice and e-comms together, enabling analysts to execute complete investigations
- Correlation of e-comms with trade surveillance alerts
- Case manager that saves time and money by automating workflows, requests for information, and tasks using robotic process automation

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.

CONCLUSION

- **The regulation and risk interchange:** Most regulations focus on recording and storage, and they have only recently focused on specific data sources to be included. They do not, however, detail the manner in which firms are expected to accomplish communications monitoring, thus leaving the surveillance roadmap up to the firms to decide and develop. This substantial gray area has resulted in inconsistencies in compliance requirements across the industry—and persistent regulatory risk for firms, unless they adopt technology strategies to help mitigate this risk. Especially during the last two to three years, e-comms monitoring solutions have benefited from vendor development; functionalities and scope have been heavily fortified and have expanded in several ways.

- **Changing with the times:** The second-generation of analytics includes NLP. Although NLP-based analytics are more accurate than lexicon-based ones they must to understand financial industry language to deliver on this promise. Some technology providers have recently achieved this by tuning their models using financial markets dictionaries they created. These models can effectively process the labyrinth of trader language, and users are reporting improvements in false positive attacks.

- **Choice or chance:** E-comms monitoring is a crucial component of detecting market abuse activities, including insider trading, and indicators of planned illicit activities are more likely to be detected with the help of advanced analytics. Under MiFID II, firms are required to record communications throughout the entire trade life cycle, regardless of the execution method and status for client orders. While the regulation does not specify how a firm should display intent, correlating communications data with trading alerts is a main strategy—but firms need to invest in the resources to do this effectively.

- A**lerts are the lifeblood of employee monitoring:** Their accuracy is key, and they are essential to the success or failure of any surveillance system. Inaccurate alerts generally translate into an excess of false positives, which pose a time management challenge for the surveillance employee who needs to review them, and likewise increase cost pressures. Lexicon-based alerts provide only so much insight into potential cases, which, combined with unstructured data challenges, can result in an explosion in the number of false positives; thus, the addition of next-generation monitoring solutions is a crucial component in effective monitoring.

- **The best practices for effective e-comms surveillance:** Ultimately, no matter how much a firm focuses on technology investment, management must also institute compliance policies to support the firm's technology efforts. Policies should be unambiguous and consistently applied, particularly surrounding communications practices. Most importantly, electing an e-comms surveillance platform that uses the best available technology is well worth the investment.

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Danielle Tierney
+1.617.261.2409
dtierney@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

© 2018 Nice Actimize. All rights reserved. Reproduction of this report by any means is strictly prohibited.