Communications Surveillance: Identifying and Preventing Misconduct in Digital Communications
Companies have sought to mitigate these risks and limit the possible consequences of these and other potentially damaging activities, as well as to comply with regulations requiring the surveillance and retention of all written communications. Surveillance of electronic and voice communications have been undertaken with mixed success. Measures currently in place are not always effective in identifying all possible instances of non-compliance. In addition, these methods often generate many false positives, creating major problems, diverting attention and distracting compliance officers and their teams with saturated alert queues.

Illegal and/or unethical actions are often perpetrated by individuals who have knowledge of existing surveillance measures and technology including potential gaps or weaknesses. These individuals may establish complex schemes to avoid detection and may change patterns frequently to camouflage their activities.

Adding to this complexity, companies are finding the need to access a large and growing number of internal and external data sources—from structured data such as trading records, market and securities master data, and from unstructured data such as voice and social media—to help detect rapidly evolving and fraudulent behavior. However, while there is some technology available to combat the problem, no holistic solution exists. Institutions also find they lack the skills needed to support the compliance, risk, legal, technology and other functions as they grapple with evolving threats.

To address the problem, financial institutions are encouraged to explore all forms of communication and consider ways to improve employee engagement and the adoption of company values.
Current State of Play

At the most basic level, financial services firms retain copies of all communications sent and received; this is required for compliance with Books and Records regulations.1 The email archive can be searched programmatically and/or periodically, using keywords such as names of individuals, sanctioned entities, securities on restricted lists, or even inappropriate language.

More sophisticated systems can scan all network traffic in real time for matches against an extensive list of rules or policies comprised of keywords and Boolean expressions (expressions resulting in true or false values). When traffic content encounters a rule, the systems trigger an “event” which may include flagging the communication for compliance review or, in the case of an outgoing message, using a “soft block” (warning the sender about a possible violation but allowing the message to be sent) or blocking its delivery altogether.

The proliferation of communications channels, and the exponential increase in the volume and variety of communications have in our view exhausted the capabilities of traditional lexicon-based surveillance. As well, it takes an enormous effort to maintain and update the lexicons for such surveillance to remain effective.

Many systems incorporate lexicon screening as part of their Data Loss Prevention (DLP) solution. These systems were put in place primarily to archive emails and, to a lesser extent, to prevent sensitive information from leaving the firm; allowing only rudimentary searches. Many firms have started to use feeds from other data sources, but the prevalent methodology is to flatten these conversations into a normalized email structure that can be viewed and searched by the company’s legacy systems. This approach—which generates a large volume of alerts typically reviewed inside organizational “silos” without sufficient context and knowledge—is both ineffective and cumbersome in our view. Compliance analysts do not always have the detailed knowledge of the business or its products to help spot potentially problematic issues.

New Regulatory Environment

New regulatory frameworks (including the Dodd-Frank Wall Street Reform and Consumer Protection Act in the US) require organizations to take a more proactive approach to surveillance, both in terms of technology and in terms of the methodology, skills and knowledge needed to establish adequate surveillance capabilities. Regulations change frequently and banks should be on constant alert. Regulatory bodies including the Securities and Exchange Commission, the Federal Trade Commission and the National Association of Insurance Commissioners, for example, have all become interested in understanding how financial institutions use social media communication channels.

In addition, new Financial Industry Regulatory Authority (FINRA) rules became effective in December 2014 and focus on, among other things, managing conflicts of interest in a firm’s supervisory system, performing risk-based review of correspondence and internal communications, monitoring for insider trading, and testing and verifying supervisory control procedures. FINRA has indicated that it wants a clear understanding of how firms are implementing these new requirements.2 Voice surveillance requirements are not entirely new to the financial services industry; such surveillance is required in other jurisdictions. New regulations (such as the Markets in Financial Instruments Directive or MiFID II regulations) are expected to address voice communications, with some deadlines anticipated as early as 2017.3 The new regulations are also detailed and prescriptive about how these records must be stored, and how accessible they must be. The technology needed for effective voice surveillance is still in its early stages and financial organizations, as well as technology firms, are struggling to keep up with these requirements.
The Challenge of Social Media

The rapid growth of social media and its use in the financial services industry creates another problem area for banks and capital markets firms. The Financial Conduct Authority (FCA) in fact, has gone so far as to propose guidance for review and discussion on what constitutes proper use of social media. As the FCA indicates, even in limited-character venues such as Twitter, messages of a promotional nature must be identified as such and must be “fair, clear and not misleading.”

In the US, FINRA has disseminated broad guidelines to help financial services firms use social media. For example, FINRA notes business records that appear on social media are subject to recordkeeping and supervision requirements, and that static content, such as a LinkedIn profile, needs to be reviewed, in advance, by a principal of the firm. Interactive content such as tweets may be reviewed after the fact. FINRA considers participation in social media a “public appearance” with the same requirements for supervision to be in place as for other public appearances, such as a speech or a televised interview.

According to the FCA’s final guidance on social media and customer communications, financial services institutions are expected to have a system in place to create a record of social media communications and retain this information for reference at a later time. Firms should not rely on digital media channels to maintain these records, as they will not have control over them.

Case Study: Monitoring Social Media at UBS
UBS, a leading global financial services provider, was looking for a comprehensive way to monitor and track social media. Working with Accenture, UBS designed a multi-layer operating model that defined process, structure and technology components, along with the resources needed to run the monitoring system.

Leveraging its Global Delivery Network, Accenture tracks and monitors comments in English, German, Spanish and Portuguese. Tracked content is monitored and analyzed by native speakers with an industry background to eliminate mundane postings, spot irony and understand context. Based on the tracking results and additional analysis, detailed reports are created for UBS and delivered on a regular basis.

UBS gets a comprehensive view on topics that might be starting to flare up and require a timely response. The service allows UBS to fulfill important communication and risk business objectives in the area of reputation management and customer trust as well as brand issues.


Figure 1. Example of a word cloud for real-time analysis of themes and trends
Some tools use data visualizations like a word cloud to help analysts understand themes or trends being discussed in real time.
A Rapidly Evolving Data Landscape

Emails and telephone calls are only two pieces of the surveillance puzzle. Structured data from transactions, positions, portfolio and performance history is proliferating rapidly, but firms are also generating more and more unstructured data, including emails on third party platforms such as Bloomberg and Reuters, internal chat and instant messages, news feeds, text messages, content from internal and external collaboration sites, and social media content from LinkedIn Corporation, Facebook Inc. among others.

Regulators require voice records and financial services firms are demanding greater quality and detail from vendors of voice communication surveillance solutions, such as identification of parties speaking, separation of multiple speakers, foreign languages, accents, slang, “trader talk” and conversion to text.

And, of course, new platforms are launched all the time, recent examples include WhatsApp Messenger and Snapchat. Uptake can be rapid (Snapchat may already have as many as 100 million daily active users), with each new platform generating its own stream of content and each posing new surveillance challenges. The evolving landscape is almost impossible to monitor, causing some firms to issue blanket bans on the use of outside devices for business purposes. These bans are difficult to enforce; a better approach is to create a solution that adds new sources of data and incorporates them into the surveillance engine, although this is easier said than done.

Within all this data are insights, sometimes into malicious behavior. The challenge for surveillance programs is to separate relevant, interpretable information from uninterpretable, irrelevant data, and then turn it into usable insights and effective action. At the same time, firms need to safeguard the privacy of client communications and data as per regulatory requirements.

The Human Capital Challenge

Complex surveillance mechanisms do not operate by themselves. Financial services firms face difficulties in identifying, developing and retaining enough people with the specific skills needed to establish and operate such systems. Companies should consider not only who is utilizing these technologies but where these people and teams should be located. Location strategy should be fit for purpose based on the scope and scale of the organization. Privacy laws must also be considered when designing an optimal location strategy. These laws vary greatly from jurisdiction to jurisdiction and present significant challenges to managing surveillance on a global basis.

The advanced compliance analyst is often not only proficient in regulations, policies, financial markets and products but also in areas such as contextual analysis, data mining and logical expressions. This individual—essentially a surveillance data scientist—should be able to analyze information from a variety of sources and grasp the full context of the communication in question. The reviewer or analyst should, as well, identify the reason or reasons for false positives and find ways to filter them out.

Ultimately, organizations could find themselves addressing the human capital challenge on two levels. Attracting highly-skilled people into surveillance and compliance, and on an enterprise-wide basis creating and promoting a stronger culture that incorporates ethical, self-correcting and self-policing behaviors that hold employees to a higher standard of compliance enterprise-wide.
Integrated Solutions for Surveillance of Electronic Communications

Next-generation electronic communications surveillance will not only enrich data by automatically cross-referencing multiple sources, it will also help support a proactive approach to reducing false positives while maintaining an acceptable degree of sensitivity to possible malicious behavior. Advanced filtering tools and artificial intelligence allow reviewers to prioritize high-risk alerts and work quickly through the queue of notifications. This frees up more time for thorough analysis, especially when done in conjunction with more investigative business and thematic surveillance reviews. Comprehensive “lookback” reviews—for example those conducted after major cases are settled—are also helpful in identifying vulnerabilities. These reviews also help create a culture of continuous improvement, one that utilizes lessons learned and integrates these back into processes and systems to help enhance controls.

For large firms, one of the key questions is how to find the right balance between detection and disposition; in other words, how to combine “push” methodologies for detection and issuance of high-risk alerts with “pull” methodologies for discovery of new threats and disposition of such threats. To reach this balance, firms should explore the concept of what has been called “integrated surveillance.” This approach relies upon the use of unified information access platforms to integrate large volumes of unstructured information as well as semi-structured (such as metadata) and structured information into a comprehensive environment.

Key elements of integrated surveillance include:

Enriching unstructured data from emails, chats, forums, social media and voice calls with structured information such as internal restricted lists, government maintained lists, transactions and activity logs.

This information can be automatically cross-referenced with other compliance systems such as Know Your Customer (KYC) systems, client/vendor lists, Office of Foreign Asset Control (OFAC) lists of restricted clients and securities, government watch lists, and organizations subject to sanctions, as well as repositories, control room lists and Anti-Money Laundering (AML) engines.

External resources such as feeds from brokers, regulators and other information sources should also be made accessible. User names, employee IDs, email addresses, phone numbers and chat room aliases are all automatically extracted and linked to group identities with associated pieces of information.

Integration of voice surveillance into the overall surveillance model.

While voice-to-text transcription technologies have improved drastically over the past few years, they still require extensive computational resources and human intervention to help maintain an adequate level of accuracy. Lexicons for transcribed voice conversations are inherently different from those used for other forms of text-based communications. Managing another set of lexicon rules specific to voice requires in our view an intimate understanding of behavioral linguistic characterizations for the desired target language. The effort required to review, or to listen to, voice conversations is substantially greater than that required for text.

Voice is still considered by many to be a safer and more secure media and is therefore riskier from a compliance perspective. People prefer to discuss sensitive matters over the phone, rather than leaving an electronic trail, so the need for more robust voice surveillance methodologies is more pressing than ever. Innovative companies working in voice surveillance are employing biometrics, advanced phonetics and other technologies to identify speakers and eliminate surveillance problems arising from background noise, different languages, dialects, speaking styles and voice to text transcription. This should help improve the quality of recordings and text translations and reduce false positives.

Verifying and centralizing data.

To help store, organize and access data from these and other sources, financial services firms are encouraged to establish new rules, execute ad-hoc queries and define comprehensive analytics against an extensive data repository. The first step is to confirm that both underlying source data and data from detection engines is timely, relatable, of high quality, and centralized. Another important step is creating an infrastructure that allows historical access (that is, greater than one year) to enterprise storage where all data sources can be accessed without cumbersome governance processes preventing access.
Providing speed and flexibility.
With data organized and centralized, teams should consider customized dashboards that enable them to revise rules autonomously, create an ad-hoc taxonomy and make other changes without going through layers of management or a prolonged Software Development Life Cycle (SDLC) with technology. Financial institutions are encouraged to complete the necessary audit trail regulators expect.

A near production-like User Acceptance Test (UAT) environment provides change management and surveillance personnel with an environment to pilot new ideas and thoroughly test changes prior to going to production thus minimizing adverse impacts and unmanageable volumes.

Adopting semantic technology.
In our view, analyzing unstructured data via lexicon character matching will no longer be sufficient, even if complex Boolean logic is applied. Advanced semantic technologies can automatically recognize concepts and topics, understand meaning, and categorize information. Semantic technology helps reduce false positives by recognizing low-risk activity, but also gives reviewers needed insight and context by immediately retrieving related information.

Using network analytics.
Semantic technology derives structured information from each communication, but additional insights can be gained by aggregating the metadata created by communications. The most advanced current level of electronic communications surveillance applies statistical methods to analyze networks and map relationships.

Showing interactions across groups of users exposes problematic connections and identifies breaches of established information barriers.
Clustering algorithms allow for filtering and grouping based on relationship strength and interactivity among users, who are ranked according to behavioral markers; for example, some are "influencers" while others are "listeners." Statistical models flag deviations in volume, concentration and sentiment of communications by utilizing pattern recognition and predictive analytics.

Incorporating visualization.
Visualization tools can also help facilitate discovery. As seen in Figure 2 below, dashboard monitoring activity supplement the classic alerts queue and allow easy viewing of actual communications.

Figure 2. Communication scoring dashboard
This type of dashboard can be created by applying advanced analytics to email traffic showing the risk profile of communications and highlighting outliers at any given time.

Source: Accenture prototype, August 2015
Moving Toward a Holistic Approach to Surveillance and Compliance

Detecting possible bad behavior among rogue employees—and non-compliant behavior in general—is an issue facing all financial services firms. A holistic approach to surveillance and compliance can help mitigate this issue, but can also enable firms to identify positive behavior along with the kind of business-building insights that generate sustainable profits and growth.

We believe that no single-solution approach can provide full insight into activity across all areas of the organization. Instead of relying on one or two solutions, firms should work toward implementing multiple, complementary surveillance capabilities some of which include lexicons, machine learning, semantic technology, network analytics and relationship mapping.

With a robust, integrated and centralized data model, visualization tools can help connect and support the various surveillance capabilities, while new case management tools facilitate tracking and centralize reporting of issues. Finally, companies need to keep in mind the importance of identifying, hiring, training and retaining talent with the right sets of skills for the complex, integrated new surveillance environment.

The proliferation of structured and unstructured data poses challenges to financial services firms as they seek to monitor, identify and prevent employee misconduct. Firms that take an integrated approach—treating data as an enterprise asset and using data and analytics to build and enhance their surveillance detection and prevention capabilities—will, we believe, be in the best position to prevent and or address regulatory concerns and avoid losses from ever-evolving threats on this front.

To find out more on how to enhance surveillance capabilities, please consult “Getting Surveillance Right: Protecting Banks’ Reputation and Profitability.”
References

Access at: https://www.finra.org/sites/default/files/industry/p006378_0.pdf

Access at: https://www.finra.org/industry/notices/14-10

Access at: https://www.fca.org.uk/firms/markets/international-markets/mifid-ii/mifid-review


About the Authors

Samantha Regan
Samantha Regan is a Managing Director in Accenture's Finance & Risk Services. She has 17 years of global experience working with C-suite executives and their businesses in compliance and regulatory initiatives. Samantha is the North America Lead for the Regulatory Remediation & Compliance Transformation group within Accenture's Finance & Risk Services practice.

Rory Craven
Rory Craven is a Senior Manager in Accenture's Finance & Risk Services. He has 10 years of business analysis experience in the financial services industry. Rory focuses on compliance and regulatory change initiatives challenging global banks. Rory is the Surveillance Lead for the Regulatory Remediation & Compliance Transformation group with Accenture’s Finance & Risk Services practice.

Weston Little
Weston Little is a Manager in Accenture's Finance & Risk Services. He has seven years of regulatory and compliance experience as a former regulator and corporate compliance officer. Weston works with businesses to evaluate, develop and transform their compliance functions to meet the demands of a rapidly evolving regulatory environment.

Daniel Krill
Daniel Krill is a Manager in Accenture's Technology Strategy practice, aligned to the Finance & Risk Services group. He has 12 years of global experience that spans several industries, including financial services, telecommunications, and business intelligence. Daniel specializes in helping clients develop and implement innovative technological solutions for pressing business imperatives, as well as establishing a strategic infrastructure that can accommodate a rapidly changing landscape.

Stay Connected

Accenture Finance & Risk Services

LinkedIn
www.linkedin.com/groups?gid=3753715

Join Us
www.facebook.com/accenture

Follow Us
www.twitter.com/accenture

Watch Us
www.youtube.com/accenture

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with more than 336,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$30.0 billion for the fiscal year ended Aug. 31, 2014. Its home page is www.accenture.com.

Disclaimer

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.