Sustainable Surveillance

Wednesday, 25 October 2017 | 8–9:30 a.m.
Breakfast, 8-8:30 a.m. | Program, 8:30–9:30 a.m.

Fordham Law School
Skadden Conference Center
150 West 62nd Street, New York City

CLE credits have been approved in accordance with the requirements of the New York State CLE Board for a maximum of one (1) nontransitional professional practice credit hour.

CLE COURSE MATERIALS & SPEAKER BIOS
Speaker Biographies

MODERATOR
Lisa Bloomberg
Principal Director, Regulatory and Compliance, Accenture
Lisa is a principal director within Accenture’s finance and risk practice of the North American Financial Services group. Over the course of her career, she has provided legal, regulatory, and compliance advice to asset managers, wealth managers, and investment banks involving registered U.S. and non-U.S. advisory products, including mutual funds, closed-end funds, alternative funds, and offshore funds. Lisa holds a J.D. from Tulane University Law School and a bachelor’s degree in economics and Spanish from Bucknell University.

SPEAKERS
Jacob Bukhsbaum
Senior Compliance Officer, Global Infrastructure Partners
Jacob is the senior compliance officer for Global Infrastructure Partners, a leading infrastructure investor. Prior to Global Infrastructure, he was vice president of compliance at Nomura Asset Management focusing on code of ethics surveillance and monitoring, marketing, and fund compliance matters. Prior to Nomura, Jacob was the chief compliance officer and associate general counsel at Winmill & Co., a family of registered investment companies, broker-dealers, and publically traded operating companies. Jacob holds a J.D. from Brooklyn Law School and a B.A. from Fordham University.

Mathew Epstein
Compliance Manager, Citadel LLC
Mathew is the head of electronic communication surveillance at Citadel LLC covering both the broker dealer and investment advisor. His team partners closely with the market surveillance team to design comprehensive monitoring coverage over a wide variety of regulations and misconduct scenarios. Prior to Citadel he worked at HSBC Securities for 2.5 years designing electronic communication surveillance for the broker dealer, bank, and asset manager. Before HSBC he ran the equities and municipal trading desks at Seaport Global, a boutique broker-dealer specializing in distressed and post-reorganization securities. He holds an M.B.A. from NYU’s Stern School of Business and B.A. from Brandeis University.

Joshua Kay
Compliance Manager, Royal Bank of Canada
Josh is a compliance manager at RBC managing electronic communication surveillance across U.S. capital markets. In this role, he develops surveillance strategies to mitigate regulatory, reputational, and legal risk at the firm. Prior to joining RBC, Josh worked at Proskauer and WilmerHale focusing on e-discovery. He holds a B.S. in engineering from Binghamton University and a J.D. from Villanova University School of Law.

Joseph W. Lodato
Managing Director, Global Head of Compliance Surveillance and Technology, Guggenheim Partners LLC
As a professional with more than two decades of experience in the financial services industry, Joe possesses a comprehensive understanding of the issues, trends, challenges, and solutions facing CCOs in today's dynamic and volatile financial services organizations. In chief compliance officer and chief operating roles, Joe led the successful integration of technology to ensure compliance and drive productivity across all levels of the organization and in a variety of settings, from startup organizations to large global services organizations, including Bank of America, Lehman Brothers, Barclays Capital, and AllianceBernstein. He holds a B.B.A. from Pace University’s Lubin School of Business.

Jonathan Turnbull
Senior Manager, Intelligence and Analytics, HSBC
Jonathan is a senior manager of intelligence and analytics within HSBC’s financial crime threat mitigation team. He has held a variety of policy, investigative, and analytical roles within HSBC’s financial crime risk organization, including designing, implementing, and running the enhanced due diligence program for correspondent banking. Before HSBC Jonathan was a consultant in Accenture’s financial services practice. He earned his undergraduate degree at the University of Oxford and an M.B.A. from the University of Chicago Booth School of Business.
TABLE OF CONTENTS

1. Presentation Slides

2. Communications Surveillance: Identifying and Preventing Misconduct in Digital Communications

3. Getting Surveillance Right: Protecting Banks’ Reputation and Profitability
AGENDA

- Moderator and Panelist Introductions
- Regulatory Drivers for Surveillance
- Challenges Persist, But the future is in Sight
- Critical Needs for Surveillance
- Q&A
MODERATOR AND PANELIST INTRODUCTIONS

Lisa Bloomberg
Accenture
Principal Director, Regulatory and Compliance

Lisa is a Principal Director in Accenture’s Financial Services group within Finance and Risk - North American Regulatory & Compliance practice. For over two decades, she has provided legal, regulatory and compliance advice to asset managers, wealth managers and investment banks involving registered U.S. and non-U.S. advisory products. Lisa has extensive experience counseling on regulations and industry best practices, creating an operational regulatory and best practice roadmap for adoption by the business. Lisa also has experience with mergers and acquisitions and other strategic arrangements involving asset managers.

Joseph W. Lodato
Guggenheim Partners LLC, Managing Director, Global Head of Compliance Surveillance and Technology

As a professional with more than two decades of experience in the Financial Services industry, Joe Lodato offers a comprehensive understanding of the issues, trends, challenges and solutions facing CCOs in today’s dynamic and volatile financial services organizations. In Chief Compliance Officer and Chief Operating roles, Joe led the successful integration of technology to ensure compliance and drive productivity across all levels of the organization, and in a variety of settings, from startup organizations to large global services organizations, including Bank of America, Lehman Brothers, Barclays Capital and AllianceBernstein.

Jacob Bukhsbaum
Global Infrastructure Partners
Senior Compliance Officer

Jacob Bukhsbaum is the Senior Compliance Officer for Global Infrastructure Partners, a leading infrastructure investor. Prior to Global Infrastructure, Jacob was Vice President, Compliance at Nomura Asset Management focusing on code of ethics surveillance and monitoring, marketing, and fund compliance matters. Prior to Nomura, Jacob was the Chief Compliance Officer and Associate General Counsel at Winmill & Co., a family of registered investment companies, broker-dealers and publically traded operating companies. Jacob holds a JD from Brooklyn Law School and a BA from Fordham University.

MODERATOR AND PANELIST INTRODUCTIONS (CONT.)

Jonathan Turnbull
HSBC
Senior Manager, Intelligence and Analytics

Jonathan is a Senior Manager, Intelligence and Analytics, within HSBC’s Financial Crime Threat Mitigation team. He has held a variety of policy, investigative and analytical roles within HSBC’s financial crime risk organization, including designing, implementing and running the enhanced due diligence program for correspondent banking. Before HSBC Jonathan was a consultant in Accenture’s financial services practice. He earned his undergraduate degree at the University of Oxford and an MBA from the University of Chicago Booth School of Business.

Mathew Epstein
Citadel LLC, Compliance Manager

Mathew Epstein is the Head of Electronic Communication Surveillance at Citadel LLC covering both the broker dealer and investment advisor. His team partners closely with the Market Surveillance team to design comprehensive monitoring coverage over a wide variety of regulations and misconduct scenarios. Prior to Citadel he worked at HSBC Securities for 2.5 years designing eComm Surveillance for the broker dealer, bank and asset manager. Before HSBC he ran the equities and municipal trading desks at Seaport Global, a boutique broker dealer specializing in distressed and post-reorg securities.

Joshua Kay
Royal Bank of Canada, Compliance Manager

Josh Kay is a Compliance Manager at RBC managing Electronic Communication surveillance across US Capital Markets. In his role, Josh develops surveillance strategies to mitigate regulatory, reputational, and legal risk at the Firm. Prior to joining RBC Josh worked at Proskauer and WilmerHale focusing on eDiscovery. Josh holds a BS in engineering from Binghamton University and a law degree from Villanova.
REGULATORY DRIVERS FOR SURVEILLANCE

Banks have spent vast amounts on initiatives related to regulatory compliance since 2008, but major fines continue to affect banks’ reputation and profitability. US regulators have sharpened their focus on practices and behaviors across the FSI, examining both how the FSI conducts business and how it addresses illegal behaviors.

- US regulators have issued both formal regulation and informal policy guidance about culture, ethics and conduct in banking.
- The New York Fed, OCC, FINRA, SEC and CFPB continue to focus on these topics in 2017 and beyond.
- US regulators are now looking for mechanisms to improve compliance with “spirit of the law” above and beyond strict adherence to “letter of the law.”
- MiFID II and CAT (Consolidated Audit Trail) bring additional requirements in 2018, notably the requirement to store and monitor voice communications.

Regulators are improving their own technology capabilities
- Surveillance technology efficiency is on the rise
- Regulatory and exchange reporting processes have enriched the volume and granularity of surveillance data
- Analytical tools are in use – Regulators are looking not only at behavior, but also at intent

Major fines have been levied in the US in 2016 and 2017 for breaches that include
- Unsound FX practices
- Volcker rule violations
- “Spoofing and Layering” charges
- Improper handling of ADRs
- Misleading clients about pricing trades
- Dark Pool violations

CHALLENGES PERSIST, BUT THE FUTURE IS IN SIGHT

Basic compliance is getting harder and more expensive as bad actors inside and outside the firm find new ways to avoid detection of illegal behavior. Surveillance modernization should be considered to bring best of “the new” and cost efficiency to Compliance organizations

Compliance budgets are built for BAU – not innovation

Compliance Budgets cannot fund the innovation needed to modernize surveillance capabilities

Scrubnty is Magnified

Regulators increased scrutiny of conduct controls and frameworks, and Regulators are bringing big data and analytics to their Surveillance toolkit

Current Toolsets cannot filter the noise

False Positives are still the top challenge, requiring significant bandwidth of Surveillance SMEs to find the illegal behavior “needle in the haystack”

A changing of the guard: RegTechs are leading Surveillance innovation

Surveillance RegTechs are proliferating — commercializing new, more efficient models (with Machine Learning), and data introspection services. At the same time, traditional products are getting closer to the end of life cycle.
CRITICAL NEEDS FOR SURVEILLANCE

A solution set of surveillance industry leading practices is emerging that applies not only to large, global firms, and also to mid size and smaller firms.

People
- Elastic Workforce - Trained surveillance resources that support SMA and BAU staff as needed
- Cost efficiencies with transformational Center of Excellence

Technology Platform
- Robust, Secure and scalable
- Rapid adoption of state-of-the-art RegTech solutions as they reach maturity

Data
- Data quality is high quality and data sets are fit for purpose.
- New Data sources can be quickly onboarded into an evolving analytical library

Models
- Models meet changing regulatory requirements.
- Model calibration is based on shared industry feedback

End to End Process
- Standalone and integrated surveillance analytics
- Machine Learning and Intelligent Automation are embedded in the Surveillance Process
- High Quality MI Dashboards and BI
- Integrated with Case Management

Detection
- Predictive Identification of illegal behaviors
- Quickly recognize suspicious patterns in large scale data sets

INTEGRATED SURVEILLANCE FRAMEWORK

Capabilities come to life through an understanding of how surveillance fits within the various business lines. The evolving surveillance landscape focuses on Ecomms, Voice, Trading, and the integration of the three.
Q&A

What questions do you have for our panelists?
The harmful actions of employees, clients, counterparties and others pose significant risks to financial services firms. While the monetary losses involved in activities such as unauthorized trading can be substantial, regulatory actions and reputational damage could have an even greater effect. Thanks in part to the growth of derivatives and leverage, these risks have experienced important growth. Banks should be on alert for indications of activities ranging from insider trading and money laundering to bribery, market rigging and violations of trading restrictions.

In addition to issuing strict regulations, authorities are cracking down on illicit activities with very large fines and other penalties. The headlines below indicate the range and complexity of issues related to electronic and digital surveillance, as well as areas on which regulators are focused.

“As U.S. Probes $12.7 Trillion Treasury Market, Trader Talk is a Good Place to Start” (Bloomberg)

“For Banks, 2014 was a Year of Big Penalties” (The Wall Street Journal)

“U.S. Charges British Trader with Helping Cause ‘Flash Crash’” (USA Today)

“The Biggest Banks have Paid $180 billion in Fines Since the Financial Crisis” (MarketWatch)

“U.S. Warns Banks it may Revoke Some Money-Laundering Settlements” (Reuters)

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 programatically 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.

<table>
<thead>
<tr>
<th>Mail from</th>
<th>Count: All network</th>
<th>Count</th>
<th>Risk category</th>
<th>Amber: 24,489</th>
<th>Green: 73,308</th>
<th>Red: 22</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td></td>
<td></td>
<td></td>
<td>22.66%</td>
<td>77.31%</td>
<td>0.03%</td>
</tr>
<tr>
<td>Risk category</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amber</td>
<td></td>
<td></td>
<td></td>
<td>22.66%</td>
<td>77.31%</td>
<td>0.03%</td>
</tr>
<tr>
<td>Green</td>
<td></td>
<td></td>
<td></td>
<td>77.31%</td>
<td>22.66%</td>
<td>0.03%</td>
</tr>
<tr>
<td>Red</td>
<td></td>
<td></td>
<td></td>
<td>0.03%</td>
<td>77.31%</td>
<td>22.66%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total number of emails received (blue) and sent (red)</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:richard.shapiro@bank.com">richard.shapiro@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:jeff.davolich@bank.com">jeff.davolich@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:tana.jonker@bank.com">tana.jonker@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:steven.kran@bank.com">steven.kran@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:sara.shakleton@bank.com">sara.shakleton@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:mark.taylor@bank.com">mark.taylor@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:louise.kitchell@bank.com">louise.kitchell@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:sally.beck@bank.com">sally.beck@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:john.lavorre@bank.com">john.lavorre@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:gerald.nemec@bank.com">gerald.nemec@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:sara.shakleton@bank.com">sara.shakleton@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:vincent.kaminski@bank.com">vincent.kaminski@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:barry.lycholz@bank.com">barry.lycholz@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:elizabeth.sager@bank.com">elizabeth.sager@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:kimberly.wattson@bank.com">kimberly.wattson@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:holden.salisbury@bank.com">holden.salisbury@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:daren.farmer@bank.com">daren.farmer@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:philip.jalleyn@bank.com">philip.jalleyn@bank.com</a></td>
</tr>
<tr>
<td><a href="mailto:jeff.davolich@bank.com">jeff.davolich@bank.com</a></td>
</tr>
</tbody>
</table>

**Red emails sent**
| sara.shakleton@bank.com |
| vincent.kaminski@bank.com |
| barry.lycholz@bank.com |
| elizabeth.sager@bank.com |
| kimberly.wattson@bank.com |
| holden.salisbury@bank.com |
| daren.farmer@bank.com |
| philip.jalleyn@bank.com |
| jeff.davolich@bank.com |

**Amber emails sent**
| kay.mann@bank.com |
| vincent.kaminski@bank.com |
| jeff.davolich@bank.com |
| chris.romney@bank.com |
| sara.shakleton@bank.com |
| sally.beck@bank.com |
| john.lavorre@bank.com |
| gerald.nemec@bank.com |

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 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.”

Figure 3. Communication traffic across network
The advanced visualization of network analytics, utilizing clustering, risk scoring and adaptive filtering help uncover hidden relationships and identify potential risks.
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
Connect With Us
www.linkedin.com/groups?gid=3753715

Facebook
Join Us
www.facebook.com/accenture

Twitter
Follow Us
www.twitter.com/accenture

YouTube
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.

Copyright © 2015 Accenture
All rights reserved.

Accenture, its logo, and High Performance Delivered are trademarks of Accenture.
Getting Surveillance Right: Protecting Banks’ Reputation and Profitability

High performance. Delivered.
Banks have spent vast amounts on initiatives related to regulatory compliance since 2008, but major events continue to affect banks’ reputation and profitability. Banks paid over $3.7 billion in fines in 2012 and 2013 for attempts to fix the London Interbank Offered Rates (LIBOR), and individual banks have paid multi-million and sometimes multi-billion dollar fines related to offenses ranging from insider dealing to benchmark rates fixing to rogue trading.

In most if not all cases, proper surveillance and early notification of improper and/or illegal activities could either have prevented the events from taking place or could have greatly limited their scope and the amount of damage inflicted. By not investing in surveillance capabilities – and by failing to coordinate and integrate such capabilities – banks risk severe regulatory and reputational damage. Capital expenditures that might otherwise be earmarked for growth and expansion of core businesses are diverted to cover legal costs, fines, operational fixes and reputational repairs.

There are other, more lasting costs related to poor surveillance. In our view, current and potential customers are far more likely to work with firms whose focus is on their own day-to-day business rather than those who have breached regulations and damaged their reputations.
The Future of Surveillance

New and more innovative approaches to surveillance will be dictated not so much by banks’ expenditures on people, process and technology as by their approach to the entire concept of surveillance. At present, surveillance is an activity that is driven primarily by regulation (although there is a competitive advantage derived from being best-in-class). The data generated by surveillance activities is typically confined within specific business units or trading desks, available only on a “need to know” basis.

Surveillance is often designed to identify specific actions taken by individuals within the organization. The thresholds for flagging such actions tend to be similar for all groups and business areas, based on an analysis of structured data using clearly defined algorithms.

As banks’ recent experience indicates, this overall approach leaves significant coverage gaps. Forward thinking banks are moving toward a surveillance model which is driven by organizational culture rather than specific regulations. In this model, data is available as needed, not kept in silos, supporting surveillance that takes place in real time and is proactive, rather than reactive. Having access to front to back data and relevant controls can help ensure that breaches are detected early or are completely avoided. Take an example of a wealth manager trading on behalf of a client. Data from pre-trade onboarding activities (Anti-Money Laundering/Know Your Client/Investment Profile) can be overlaid to completed trades to help identify potential suitability or market abuse patterns. Historic associations alongside current transactions can provide additional information to the bank which was previously not available.

Another characteristic of the future state of surveillance is the use of analytics to identify patterns of activities and behaviors, rather than specific events that cross predetermined thresholds. The thresholds used are flexible, based on profiles that reflect not just individual behavior but the normal activities of an entire trading desk or business unit. Finally, new model surveillance employs analytics using not just structured data – such as that generated by trading activity – but also unstructured data generated by emails, social media, and even telephone conversations. There is also the opportunity to overlay this data with HR and individual employee compliance data to look for patterns and potential triggers that could lead to a breach.
The Big Picture: Preventing Problems Before They Occur

Banks engage in a number of different types of surveillance, including trade surveillance and communications surveillance. Banks set trade limits and review breaches of such limits as they occur. In addition, profit and loss reviews and other control functions, as well as other compliance, back office and middle office reconciliation activities, help prevent abusive or illegal conduct.

Currently, however, these surveillance functions are rarely aggregated; in other words, surveillance is conducted desk by desk or business by business. Data gathered by one surveillance team is not shared with other teams, even though such sharing can provide both preventative and post-event investigative capabilities that can help mitigate risk. These separate surveillance functions include:

- **Financial Industry Regulatory Authority (FINRA)** – monitoring brokers for overcharging customers, making unsuitable investments and other infractions;
- **Social media** – tracking employees’ use of social media, both inside and, in some cases, outside the organization;
- **Market** – monitoring trading and trading functions to prevent illicit trading activities;
- **Employee** – monitoring employee email, personal trades and, in certain cases, phone calls;
- **Financial crime** – Anti-Money Laundering (AML), Anti-Bribery and Corruption and actions in contravention of sanctions.

As currently structured, surveillance is a reactive process using tools that look at past patterns to determine if a breach has occurred. For surveillance to realize its full potential, it should become more proactive. We believe that a planned, systematic approach to investing in surveillance capabilities could generate significant returns, not only in terms of preventing and minimizing adverse events, but in demonstrating banks’ commitment to being a stable, dependable business partner.

Firms should consider using advanced data analytics – harvesting information from new channels such as social media – to create predictive analytics. Through focused training and faster response, firms could help prevent breaches in areas identified as having a high potential for undesirable activity. Ideally, banks should be able to turn post-event investigative data and tools into preventative detection systems that utilize analytics and real-time reporting to spot deviations from behavioral norms as they occur. Using these methods, banks could also help create increasingly sophisticated risk profiles as they attempt to pre-empt breaches.

In our experience, the total cost of investing time and resources in comprehensive, preventive surveillance is often less than the cost of investing in disconnected, group-by-group efforts – and the results are better. The total amount invested can be spread over time, with priorities aimed at targeting gaps and weak points to provide immediate returns.

For the “Big Picture” approach to be effective, however, banks are encouraged to synchronize data across functions, allowing for pattern recognition and analysis from group to group. For example, a breach in value-at-risk (VAR) limits set by the market risk function – accompanied by increased trading activity and re-booked trades seen in the Profit and Loss (PnL) Explained – could be linked together by compliance functions following flagged counterparties. This, in turn, could lead both to preventive measures and to actions taken to address the unauthorized activities, rather than being used as investigative tools once the damage has been inflicted.

In addition to data synchronization, big picture surveillance requires advanced analytics and data technologies to run increasingly sophisticated queries across ever-larger data sets. Firms will need to invest in updating and maintaining their technical abilities.

As seen in Figure 1 below, the surveillance function encompasses banks’ entire risk framework and affects many areas of concern. Enhanced surveillance capabilities can improve banks’ overall operational, regulatory and reputational risk management programs.

---

**Figure 1. Impact of Surveillance Function on Risk Management**

Source: Accenture, January 2015
Bringing Business Units Together

To obtain a surveillance picture that is not only "big" but also comprehensive, different business units and functions need to create a pool of data that is regularly monitored and analyzed to identify patterns and anomalies. Traditionally, the business units that control and monitor activities within banks sit in different areas, with different objectives and reporting lines. Teams within compliance, risk, client onboarding, HR, product control and the operations have varied control functions and verify different aspects of trades and transactions. Identifying relevant data and sharing it within a cross-functional surveillance unit can help build patterns and identify both current and potential wrongdoers.

For proper execution, these teams and functions should provide input to a centralized location, with the compliance function serving as the overall surveillance owner.

Compliance
• Trade Surveillance (Looking at market abuse instances and patterns)
• Communication Surveillance (Looking at communications and behaviors)
• Control Room Surveillance (Surveillance of information abuse/conflicts of interests)
• Regulatory Risk Review (Review of desk trading behaviors, authorizations and regulatory gaps)
• Financial Crime (Assessing trade counterparty eligibility, frauds and crimes)

Risk
• Trading Desk – Market Risk Management (Looking at traders/desks market risk profiles to identify aberrations on granular and consolidated levels)

Product Control
• Profit and Loss Monitoring (Profit and Loss allocations, patterns and explanations)
• Trader Surveillance (Managing chinese walls, trader mandates, traded product assessments)

HR
• Leave Patterns/Block Leaves (Patterns of employees’ leave behaviors)
• Employee Onboarding (Understanding potential employee's background)

Client Onboarding
• AML (Understanding how and where the client money is allocated)
• Know Your Client (Understanding client’s business, history and associations)
• Business Objectives (Understanding client’s expectations concerning the bank)

Current Solutions
Most currently available surveillance solutions are unilateral offerings; focused on surveillance of one particular area. In many cases, the same vendor offers different solutions for different surveillance requirements.

While this works well at one level – when the product differentiation is clear – unilateral offerings do not provide optimal opportunities for collaboration, data sharing and pattern identification. In addition, unilateral offerings focus on specific types of information such as unstructured data, structured data, exchange activities, and unauthorized trading. Vendors are taking advantage of advances in big data, analytics and unstructured data analytics, but true cross-functional offerings are not yet available.

Implementing a Process-Driven Solution

We have identified three key elements that in our view are essential for a favorable transformation to a competent, proactive big picture surveillance function:

1. A commitment from top management expressed clearly as a set of working principles for team leaders and members;
2. Measured and focused investment in the right technology and tools;
3. The right culture, developed and fostered throughout the organization. This means that top management of each business unit and function should understand the benefits of actively sharing data.

The basic steps toward an effective, integrated surveillance framework include:

1. Creating an accountable risk governance structure for surveillance activities – with an executive committee representing members of involved business units – responsible for reviewing highest priority issues and supervising ongoing surveillance improvement.
2. Enhancing preventive risk identification methods.
3. Defining relevant data collection and data sharing requirements for different teams.
4. Integrating data across functions for a more comprehensive view and more effective, aggregated risk analysis.
5. Creating a centralized tracking and reporting center of excellence, using industry leading practices, technology, and coordination across functions.
6. Creating normal profiles of different trading businesses, trading desks and individual traders based on historical analysis.
7. Studying deviations, alerts and issues related to these normal profiles.
8. Reporting relevant findings to the appropriate stakeholders.
Maturity Model for Surveillance

It has been our experience that the adoption and implementation of big picture surveillance is a multi-tiered process. Acceptance and implementation will vary from bank to bank but typically takes place in three phases.

In Phase One, banks address their immediate needs, identify teams and define their requirements, with a focus on "at risk" areas and enhanced preventive capabilities. This phase usually includes a current state assessment of surveillance capabilities, followed by a budget and plan for execution based on the assessment’s findings and recommendations. Key tasks include aligning the management team, identifying stakeholders, defining the right data and how to share it. The risks to be mitigated and the criteria for success are agreed upon, as well. During this phase, banks also define an effective governance organization to help manage and implement the plan.

In Phase Two, the banks define what “normal” activity is and then begin to define requirements for the desired target state for surveillance. Teams review analytics and other technology solutions and define the process, needed resources and training to help reach this state. Data is integrated from source systems and core functions within a business area and may be re-aligned; for example, compliance control and surveillance teams may take responsibility for trade surveillance activities. Phase Two also includes the first steps in a phased implementation approach toward the target state, such as deployment of trader and client profiling technology, behavioral mapping and other innovations.

In Phase Three, big picture surveillance capabilities are in place and have begun to identify gaps and anomalies. The surveillance management structure is in place and the organization may have adapted a center of excellence model. External data from social media, newswires and elsewhere may be integrated into surveillance models. Training materials are developed and refined, and the entire process is updated as needed. Phase Three is marked by an emphasis on culture and human resources, as these are essential to the success of the ongoing program.

Benefits of Seeing the Big Picture

In our view, banks committed to improving surveillance through an integrated, big picture approach should see quantitative improvements in a number of key metrics:

- More breaches detected, with a reduced number of false positives;
- Lower costs associated with each incident;
- Faster detection leading to fewer incidents escalating;
- Over time, a reduction in breaches as employees, counterparties and others realize the extent of the bank's surveillance capabilities.

While effective surveillance requires investment in technology and human resources, the returns in terms of risk mitigation and enhanced reputation can be significant. Banks should look at their current "need to know" surveillance practices with these potential benefits in mind.
About the Authors

**Samantha Regan** is a managing director in Accenture's Finance & Risk Services. She has 17 years of global experience in banking and capital markets gained within industry and consulting. Samantha specializes in regulation and compliance and has been deeply involved in developing Accenture's regulatory and compliance management capabilities. She is the Global Regulatory & Compliance lead for Accenture’s Finance & Risk Services practice.

**Chris Beck** is a manager, Accenture Finance & Risk Services, based in Chicago. Specialized in strategy planning, operational risk management and compliance risk management, Chris brings his solid experience and skills in these areas to help financial institutions define and implement their governance and risk management structures.

**Amit Khare** is a manager, Accenture Finance & Risk Services. He is a CFA with over 9 years of global experience in capital markets working across multiple asset classes in sales, trading, risk and compliance functions. Amit specializes in the definition and implementation of surveillance and control functions, focused on complex products in the investment banking space.

Notes


About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with approximately 319,000 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.

Stay Connected

Accenture Finance & Risk Services:

LinkedIn
Connect With Us
https://www.linkedin.com/groups?gid=3753715

Facebook
Join Us
https://www.facebook.com/accenturestrategy
https://www.facebook.com/accenture

Twitter
Follow Us
http://twitter.com/accenture

YouTube
Watch Us
www.youtube.com/accenture