SIFMA COMPLIANCE & LEGAL SOCIETY
CLE OUTLINE

21ST CENTURY SURVEILLANCE –
NEW TOOLS AND HEIGHTENED EXPECTATIONS

March 18, 2020
10:10 am – 11:25 am

Moderator

John O'Neill, Executive Vice President and Chief Compliance Officer, LPL Financial

Panelists

Lynn Konop, Vice President, Compliance, **Charles Schwab**
John Malitzis, Managing Director and Global Head of Surveillance, **Citigroup Global Markets, Inc.**
T. Peter R. Pound, Partner, **Morgan, Lewis & Bockius LLP**
Aleksandra Radakovic, Managing Director & Head of Surveillance, **J.P. Morgan Chase & Co.**
Kelly Zigaitis, Head of Oversight and Controls, Compliance, **Wells Fargo**

21ST CENTURY SURVEILLANCE – NEW TOOLS AND HEIGHTENED EXPECTATIONS
March 18, 2020

<div align="center">

OUTLINE SUMMARY

</div>

I.   **What Expectations Surround the Use of Data Analytics and How Are They New or Heightened?**

       A.   Changes in the Industry/Business Environment

              1.   Increased stakes in the cybersecurity and fraud arenas with new and emerging threats.

              2.   Costs of compliance with regulation and industry-wide pricing pressures drive increased need to become more efficient with resources.

              3.   Increased digitization and availability of firm, customer, and transactional data.

              4.   Technological developments (for example, in artificial intelligence (AI), and machine learning (ML)) and the rapid onset of RegTech

       B.   Changes in the Regulatory Environment

              1.   Continued increases in the complexity of the regulatory environment. New regulations, and overlapping requirements across regulators.

              2.   Increased availability to regulators of firm, customer, and transactional data.

              3.   Regulators' increasing expectations of firms' surveillance and compliance programs as RegTech options proliferate.

              4.   Regulators' own deployment of surveillance and their use of advanced data analytics, AI, and ML.

                    a.   Securities and Exchange Commission

                    b.   Office of Compliance Inspections and Examinations

                    c.   Financial Industry Regulatory Authority

              5.   Examples of FINRA and SEC Matters Relating to Alleged Technology Inadequacies

                    a.   Inadequate Supervision of Direct Market Access

                    b.   AML Program

   c.   Regulation SCI Compliance

   d.   AML Program Lapses

   e.   Email Supervision Lapses

   f.   Inadequate Supervision Infrastructure

II. **What Makes a Good Surveillance Program?**

  A. Regulatory Requirements

  B. Elements of an Effective Surveillance Program

   1. Infrastructure

   2. People

   3. Organizational structure

   4. Governance

  C. Challenges

   1. Supervising technology

   2. Outsourcing risks

   3. Privacy

   4. Cybersecurity and data-related risks

III. **Understanding the New Technologies of Artificial Intelligence, Machine Learning, and Other Data Analytics Tools, and Their Evolving Deployment in the Financial Services Industry**

  A. Knowing Our Data

   1. Structured data

   2. Unstructured data

   3. Semi-structured data

  B. Evolving Our Thinking: Novel Analytical Approaches and Novel Analytical Techniques

       1.   New analytical approaches

       2.   New analytical techniques

C.   What are AI and ML? How are they different?

D.   What are NLP and LDA?

E.   What is RPA?

F.   What are "Big Data Analytics"?

G.   What are "Biometrics"?

H.   How Can Firms Use These New Technologies?

       1.   Applications/Opportunities

          a.   Surveillance and Monitoring

          b.   Customer Identification and AML Compliance

          c.   Regulatory Intelligence

          d.   Reporting and Risk Management

          e.   Investor Risk Assessment

       2.   Firm size/maturity

       3.   Ways to get started and maximize investment

       4.   Longer term possibilities?

IV.   **The Regulatory Cost of Not Modernizing**

A.   Examples of Recent Enforcement Activity

B.   Regulatory Approach to Surveillance

C.   20/20 Hindsight Risk

D.   Need for Engagement and Advocacy with Regulators

V.   **Closing Thoughts**

OUTLINE

I.   **What Expectations Surround the Use of Data Analytics and How Are They New or Heightened?**

   A.   Changes in the Industry/Business Environment

      1.   Increased stakes in the cybersecurity and fraud arenas with new and emerging threats.

      2.   Costs of compliance with regulation and industry-wide pricing pressures drive increased need to become more efficient with resources.

      3.   Increased digitization and availability of firm, customer, and transactional data.

      4.   Technological developments (for example, in artificial intelligence (AI), and machine learning (ML)) and the rapid onset of RegTech.

         a.   The Institute of International Finance defines RegTech as "the use of new technologies to solve regulatory and compliance burdens more effectively and efficiently." *See* Institute of International Finance, https://www.iif.com/Innovation/Regtech (last visited Jan. 22, 2020).

         b.   Compliance and surveillance programs can use RegTech to create more effective, efficient, and risk-based programs. *See* FINRA, *Technology Based Innovations for Regulatory Compliance ("RegTech") in the Securities Industry*, 1 (Sept. 2018), https://www.finra.org/sites/default/files/2018_RegTech_Report.pdf [hereinafter *FINRA RegTech White Paper*].

         c.   "The emergence and mainstream adoption of innovative technologies in recent years has also played a role in the rise of RegTech. Compliance functions now have the potential to be streamlined using a variety of technologies, such as artificial intelligence (AI), natural language processing, big data and advanced analytics, cloud-based computing, robotics process automation, distributed ledger technology, application program interfaces (APIs), and biometrics. These technologies present great opportunities for firms to develop and use applications that may enhance existing compliance at reduced costs. Moreover, the utilization of these technologies may also offer unique

opportunities to enhance the integration of risk-management and compliance within the operations of an enterprise." *Id*., at 3.

B.   Changes in the Regulatory Environment

1.   Continued increases in the complexity of the regulatory environment. New regulations, and overlapping requirements across regulators.

2.   Increased availability to regulators of firm, customer, and transactional data.

   a.   The continued development of the Consolidated Audit Trail (CAT) provides the SEC with a vast pool of data to use for data analysis. "The Commission adopted Rule 613 to create a comprehensive consolidated audit trail that would allow regulators to efficiently and accurately track all activity throughout the U.S. markets in National Market System (NMS) securities. Among other things, the rule requires the self-regulatory organizations (SROs) to jointly submit a plan – called an NMS plan – to create, implement and maintain a consolidated audit trail. The rule specifies the type of data to be collected and when the data is to be reported to a central repository." *See* SEC Rule 613: Consolidated Audit Trail.

   b.   In late February 2019, it was announced that FINRA was taking over as the CAT plan processor, responsible for all aspects of the continued build out and ongoing maintenance of the CAT. The planned result is a huge universe of transactional data – approximately 58 billion records per day and approximately 100 million customer records. *See* Randy Snook, *Beware of Cat*, SIFMA (Nov. 30, 2017), https://www.sifma.org/resources/news/beware-of-cat.

   c.   There have been numerous delays in implementation timing, but the go live reporting commencement date for large broker-dealers for equities is April 2020, and May 2020 for options. *See* Consolidated Audit Trail, https://www.catnmsplan.com/timelines/ (last visited Jan. 22, 2020).

3.   Regulators' increasing expectations of firms' surveillance and compliance programs as RegTech options proliferate.

4.   Regulators' own deployment of surveillance and their use of advanced data analytics, AI, and ML.

Overview: Regulators in the U.S. and abroad are actively using data analytics to detect financial and market misconduct, identify high-risk firms and practices, and more efficiently allocate resources.

Question: Are the regulators ahead of the industry?

a.   Securities and Exchange Commission (SEC)

(i)   The third goal in the SEC's current strategic plan is to "elevate the SEC's performance by enhancing our analytical capabilities and human capital development," which includes, among other things, "expand[ing] the use of risk and data analytics to inform how we set regulatory priorities and focus staff resources, including developing a data management program that treats data as an SEC-wide resource with appropriate data protections, enabling rigorous analysis at reduced cost" and "enhance[ing] our analytics of market and industry data to prevent, detect, and prosecute improper behavior." *U.S. Securities and Exchange Commission Strategic Plan Fiscal Years 2018-2022*, SEC, 9 (Oct. 11, 2018), https://www.sec.gov/files/SEC_Strategic_Plan_FY18-FY22_FINAL_0.pdf.

(ii)   "To further our enforcement efforts on behalf of Main Street investors, in September 2017, the SEC announced the formation of a Retail Strategy Task Force (Task Force), which has two primary objectives: (1) to develop data-driven, analytical strategies for identifying practices in the securities markets that harm retail investors and generating enforcement matters in these areas; and (2) to collaborate within and beyond the SEC on retail investor advocacy and outreach. . . . We anticipate that new data-driven approaches will yield significant efficiencies in case generation and resource allocation by targeting enforcement efforts where the risks to Main Street investors are the most significant." SEC Chairman Jay Clayton, *Testimony before the Financial Services and General Government Subcommittee of the U.S. Senate Committee on Appropriations*, SEC (May 8, 2019), https://www.sec.gov/news/testimony/testimony-financial-services-and-general-government-subcommittee-us-senate-committee.

(iii)   "While data and data analytics can help the Commission prevent fraud, protect investors, and inform decision-making, it also helps inform intelligent and effective policy-making. I strongly believe in using facts to design good public policy. As such, analyzing and understanding data is critical to shaping future regulation. As the primary regulator of the financial markets, the Commission should employ a multi-disciplinary approach to analyzing and understanding market data. By deploying data scientists to work alongside the lawyers and accountants of the Commission, I believe the Commission will embark on a new model for enhancing both the efficiency and the effectiveness of its oversight." Former SEC Commissioner Kara M. Stein, *From the Data Rush to the Data Wars: A Data Revolution in Financial Markets*, SEC (Sept. 27, 2018), https://www.sec.gov/news/speech/speech-stein-092718.

(iv)   The SEC's Analysis and Detection Center of the Market Abuse Unit has been using big data for years in identifying potential insider traders. A 2018 SEC press release relating to an enforcement matter regarding a Silicon Valley Executive's insider trading stated that the SEC Market Abuse Unit's Analysis and Detection Center, "uses data analysis tools to detect suspicious patterns such as improbably successful trading in advance of earnings announcements over time. Enhanced detection capabilities enabled SEC enforcement staff to identify the unusual trading activity." *SEC Detects Silicon Valley Executive's Insider Trading*, SEC (Jul. 24, 2018) https://www.sec.gov/news/press-release/2018-142.

(v)   In a March 2018 speech, now former SEC Commissioner Michael Piwowar stated that the SEC uses a home-grown program called ARTEMIS (Advanced Relational Trading Enforcement Metric Investigation System) "which was designed by the Commission's staff to combine historical trading and account holder data with other data sources to enable longitudinal, multi-issuer, and multi-trader data analyses." Former SEC Commissioner Michael S. Piwowar, *Remarks at the 2018 RegTech Data Summit - Old Fields, New Corn: Innovation in Technology and Law*

(Mar. 7, 2018), https://www.sec.gov/news/speech/piwowar-old-fields-new-corn-innovation-technology-law.

(vi)   "At this point in our risk assessment programs, the power of machine learning is clearly evident. We have utilized both machine learning and big data technologies to extract actionable insights from our massive datasets. But computers are not yet conducting compliance examinations on their own. Not even close. Machine learning algorithms may help our examiners by pointing them in the right direction in their identification of possible fraud or misconduct, but machine learning algorithms can't then prepare a referral to enforcement. And algorithms certainly cannot bring an enforcement action. The likelihood of possible fraud or misconduct identified based on a machine learning predication cannot – and should not – be the sole basis of an enforcement action. Corroborative evidence in the form of witness testimony or documentary evidence, for example, is still needed. Put more simply, human interaction is required at all stages of our risk assessment programs." Scott W. Bauguess, Deputy Director, Division of Economic and Risk Analysis, *The Role of Big Data, Machine Learning, and AI in Assessing Risks: a Regulatory Perspective* (June 21, 2017) [hereinafter *Bauguess, Role of Big Data]*.

(vii)   Reuters has reported that "Divisions across the SEC are working on the effort to search huge volumes of data for potential violations, such as insider trading, pyramid schemes and 'pump and dump' attempts in penny stocks…." David Ingram & Emily Flitter, *U.S. Securities Regulator Expands Use of Powerful Software – Source*, Reuters (Sept. 30, 2015), https://www.reuters.com/article/usa-sec-enforcement/u-s-securities-regulator-expands-use-of-powerful-software-source-idUSL1N12039L20150930.

(viii) In 2013, the "the Commission introduced the Market Information Data Analytics System or 'MIDAS' system to analyze "big data" generated by our equity markets. Every day, MIDAS collects and processes about 4 billion records from the proprietary feeds of the national equity exchanges and the consolidated tape. MIDAS time-stamps every one

of the messages it tracks with microsecond granularity. This system allows our Division of Trading and Markets to monitor market behavior, understand market events, and test hypotheses about the equity markets with a high level of precision. In addition to the Commission's internal use of MIDAS, we have made a number of data series freely available to the public on an analytical platform that supports powerful research tools such as Python and Jupyter Notebook. Data scientists and economists can harvest MIDAS data particular to their area of interest and conduct their own analyses. The hope is that these empirical findings will be shared with the Commission, thereby increasing the bounty of insight we are able to reap about our equity markets." Former SEC Commissioner Michael S. Piwowar, *Remarks at the 2018 RegTech Data Summit - Old Fields, New Corn: Innovation in Technology and Law* (Mar. 7, 2018), https://www.sec.gov/news/speech/piwowar-old-fields-new-corn-innovation-technology-law.

b.   Office of Compliance Inspections and Examinations

(i)   In their 2020 Examination Priorities, OCIE noted that it "continues to make investments in human capital, technology and data analytics. . . . OCIE's technology tools and data analytics work also continue to mature and help drive many of its risk identification efforts, initiatives and examination processes. All of these resources help OCIE identify potential stresses on compliance programs and operations, conflicts of interest, and conduct issues that may ultimately harm investors." *2020 Examination Priorities Office of Compliance Inspections and Examinations*, SEC, 5, https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2020.pdf (last visited Jan. 22, 2020).

(ii)   In February 2019, the Director of OCIE discussed how OCIE uses data analytics to streamline the exam process and to identify high-risk firms and practices. Among other things, OCIE has or is in the process of developing tools that (i) ingest and analyze trading data and identify potential red flags; (ii) use textual analysis to review investment adviser registration forms (Forms ADV) to identify potential issues; and (iii) compare compliance

manuals of multiple firms to identify gaps. *See* Diana Novak Jones, *SEC Exams Chief Puts Focus on New Technology, New Firms*, Law360 (Feb. 5, 2019), https://www.law360.com/articles/1124963/sec-exams-chief-puts-focus-on-new-technology-new-firms.

c. Financial Industry Regulatory Authority

(i) In an effort to enhance its regulatory efforts through the use of RegTech, "FINRA has deployed cloud storage and computing, big data analytics, machine learning, and natural language processing to enhance its market surveillance and other regulatory functions." *FINRA RegTech White Paper*, at 2.

(ii) In January 2019, FINRA announced that FINRA saw an unprecedented amount of processing volume in 2018 – 66.7 billion electronic records per day, which was an 87.4% increase over the average daily volume in 2017. (FINRA has not yet announced its numbers for 2019). *Market Volatility Drives FINRA's Volume to New Record in 2018*, FINRA (Jan. 23, 2019) https://www.finra.org/media-center/news-releases/2019/market-volatility-drives-finras-volume-new-record-2018.

(iii) In late January 2019, FINRA had a RegTech conference in New York at which Jon Kroeper, the Executive VP of FINRA's Markets Group, responsible for surveillance and investigation in the equity and fixed income markets, shared that in 2018, FINRA took in nearly 67 billion events per day. At its peak, it took in 135 billion per day. Events – include orders, order routes, cancellations, quotes, trades. Emily Zulz, *AI Will Transform Surveillance Programs – Eventually*, ThinkAdvisor (Feb. 1, 2019) https://www.thinkadvisor.com/2019/02/01/ai-will-transform-surveillance-programs-eventually.

In terms of surveillance programs, Mr. Kroeper referenced "cross-market data models" deploying 172+ patterns. Equities, fixed income, options, and cross product patterns. Those 172 patterns focus on 308+ distinct threat scenarios. Scenarios are "potentially violative behavior." For example, in the wash sale scenario looking for wash sales,

prearranged trading, painting the tape, among other activity. *Id*.

(iv) "Advanced data analytics is a critical function within FINRA and an important component of our efforts to be a risk-based and data-driven organization. Given the importance of this function, as part of FINRA360, we reviewed our current structure and decided to enhance the communication between the business and technology elements engaged in this activity. Going forward, the teams engaged in advanced data analytics will form an integrated community to maximize the benefits of the investment FINRA has made, and continues to make, in this area. Governance for data analytics will be based on a 'hub and spoke' structure that will include business stakeholders, all advanced analytics groups and applicable technology support groups. The different groups will act in many respects as a single team, sharing information and collaborating across the underlying business units to leverage their expertise for the entire organization. We expect this new model will strengthen FINRA's advanced data analytics function by ensuring and promoting: increased coordination, communication and transparency across advanced data analytic groups; partnership for introducing newer technologies, tools and techniques and sharing best practices; better alignment of domain specific knowledge and business priorities across the advanced data analytic groups; consistent technology support for all advanced analytic groups; thought leadership empowerment through better coordination; and the ability for the 'spokes' and Technology to continue to produce cutting edge analytical tools and programs to enable FINRA to better protect investors and promote market integrity." *FINRA360 Progress Report, Data and Analytics*, FINRA (April 2018), https://www.finra.org/about/finra-360/progress-report/data-analytics.

(v) "Another technology core to our surveillance are the sophisticated computer programs—what we call 'patterns'—that we use to sift through this massive amount of data and to detect potential misconduct. FINRA today runs more than 175 independent patterns, which detect a wide variety of compliance issues and suspicious conduct

across markets. Pattern development takes time, requiring close coordination between surveillance analysts and data scientists to identify the right conduct and to set the appropriate parameters for the program to examine. A new pattern often requires months to develop and test, with a lengthy process to coax the signal from the noise and to minimize false positive results. Recently, we have been working to enhance and accelerate this process through the use of "machine learning," by which surveillance analysts identify specific instances of behavior of interest and allow algorithms to "train" themselves to identify additional instances in new data sets. We are using machine learning techniques to build new surveillance patterns, including some set to launch by the end of the year. And some elements of our operational surveillance patterns already rely on machine learning. To help us navigate the use of machine learning and other advanced data science techniques, FINRA created an external Market Surveillance Advisory Group, composed of leading cross-disciplinary experts from academia and the financial industry. We are grateful for their help and guidance as we look to ensure that our surveillance program continually evolves to take advantage of new technologies and meet emerging challenges." CEO of FINRA Robert Cook, *Equity Market Surveillance Today and the Path Ahead*, FINRA (Sept. 20, 2017), https://www.finra.org/media-center/speeches-testimony/equity-market-surveillance-today-and-path-ahead.

(vi)   One area in which FINRA relies heavily on data is the monitoring of high-risk brokers. FINRA has described running analytics on over 40 attributes collected on registered representatives. SIFMA Annual Seminar Comments from Thomas Nelli, Senior Vice President and Regional Director, FINRA (March 25, 2019).

(vii)   "On top of these initiatives, we are also advancing a number of operational improvements. We are working to strengthen our analytics and integrate additional data points into our risk model, such as the location of where a broker works or the degree to which his or her co-workers have committed misconduct, to inform our risk assessments. We are also seeking ways to leverage data to better understand

when new events may indicate broader issues or concerns, such as recidivist behavior. In addition, this year we are implementing improvements to our branch office risk model to include additional branch-level characteristics that may be indicative of future misconduct, such as the proportion of employees that are high-risk brokers." CEO of FINRA Robert Cook, *Equity Market Surveillance Today and the Path Ahead*, FINRA (Sept. 20, 2017), https://www.finra.org/media-center/speeches-testimony/equity-market-surveillance-today-and-path-ahead.

5.   Examples of FINRA and SEC Matters Relating to Alleged Technology Inadequacies

a.   **Inadequate Supervision of Direct Market Access Clients** – FINRA accepted a settlement with Credit Suisse for allegedly failing to supervise its direct market access ("DMA") clients. FINRA alleged that "[d]uring the review period, the firm executed over 300 billion shares on behalf of its DMA clients and generated over $300 million in revenue from its DMA business." FINRA found that "the firm did not implement reasonably designed surveillances and supervisory procedures to monitor for certain kinds of potentially manipulative activity by its DMA clients." FINRA said that Credit Suisse's clients generated over 50,000 alerts at FINRA and other exchanges for potential manipulative trading. FINRA alleged that Credit Suisse "did not begin to implement a supervisory system or procedures reasonably designed to review for potential spoofing, layering, wash sales or pre-arranged trading by its DMA clients" until years after it began expanding its DMA business. *Credit Suisse Securities (USA) LLC*, FINRA AWC No. 2012034734501 (Dec. 23, 2019), https://www.finra.org/sites/default/files/2019-12/credit-suisse-awc-122319.pdf.

b.   **AML Program Lapses** – FINRA accepted a settlement with BNP for its alleged failure to "develop and implement a written AML Program that could be reasonably expected to detect and cause the reporting of potentially suspicious activity." FINRA alleged that BNP accepted the deposit of nearly 31 billion shares of low-priced securities from at least 834 customer accounts associated with high-risk jurisdictions. According to FINRA, BNP's customers included companies known for depositing and reselling penny

stocks, which presented risks for money laundering, fraud, and lack of SEC registration. FINRA alleged that BNP's AML Program did not conduct any surveillance targeting transactions in penny stocks or include a review of wires in foreign currency. FINRA concluded that BNP's "AML Program was not reasonably designed to identify wire transfers (or a pattern of wire transfers) conducted in amounts that would avoid attention or review." *BNP Paribas Securities Corp. & BNP Paribas Prime Brokerage, Inc.*, FINRA AWC No. 2016051105201 (Oct. 23, 2019), https://www.finra.org/sites/default/files/2019-10/bnp-awc-102419.pdf.

c. **Regulation SCI Compliance Issues** – The Commission accepted an Offer of Settlement from Virtu Americas, LLC. (Virtu) for allegedly failing to comply with Regulation SCI. According to the Commission, Virtu allegedly utilized an automated system that monitored trading activity that was intended to keep its alternative trading system's trading volume below the compliance threshold for Regulation SCI. However, the system allegedly did not function as intended and Virtu exceeded the trading volume under Regulation SCI. According to the Order, Virtu violated Regulation SCI by failing to establish the policies and procedures required by Regulation SCI, file quarterly or annual reports, conduct an annual Regulation SCI compliance review, comply with business continuity and disaster recovery plans, and maintain books and records as required by Regulation SCI. *SEC Orders Virtu to Pay $1.5 Million Penalty for Violations of Regulation SCI*, SEC (Sept. 30, 2019) https://www.sec.gov/enforce/34-87155-s.

d. **AML Program Lapses** – FINRA accepted a settlement with Morgan Stanley for its alleged failure to develop and implement an AML Program "reasonably designed to achieve and monitor the Firm's compliance with the requirements of the Bank Secrecy Act." FINRA alleged that several of the firm's systems used to send and receive wire transfer information were flawed, undermining the system's surveillance of tens of billions of dollars of wire transfers. In addition, FINRA alleged that Morgan Stanley "failed to devote sufficient resources to review alerts generated by the Firm's automated AML systems, and as a result, the Firm's AML analysts often closed alerts" without sufficient investigation. *Morgan Stanley Smith Barney LLC*, FINRA AWC No. 2014041196601 (Dec. 26, 2018), https://www.finra.org/sites/default/files/Morgan_Stanley_AWC_122618.pdf.

e. **Email Supervision Lapses** – FINRA accepted a settlement with Raymond James for failing to have a supervisory system for reviewing email communication that was appropriate for the firm's business, size, structure, and customers. FINRA alleged that the lexicon used by the firm's email review system was not reasonably designed to identify potentially problematic conduct that the firm knew or should have anticipated would occur, given the firm's size, business model, and prior disciplinary history. FINRA also alleged that the firm failed to devote adequate personnel and resources to the team that reviewed emails as the number of emails to review increased over time. According to FINRA, the firm also failed to "periodically test the configuration and effectiveness of tis lexicon-based email surveillance system and lacked reasonable procedures for doing so." *FINRA Fines Raymond James Financial Services, Inc. $2 Million for Failing to Reasonably Supervise Email Communications*, FINRA (Dec. 21, 2017), https://www.finra.org/media-center/news-releases/2017/finra-fines-raymond-james-2-million-failing-supervise-email.

f. **Inadequate Supervision Infrastructure** – In a settlement with LPL, FINRA alleged that the firm increased the size of its broker-dealer subsidiary without a "concomitant dedication of sufficient resources to permit the Firm to meet its supervisory obligations." FINRA alleged that as a result, LPL failed to have adequate supervisory systems and procedures regarding certain aspects of its business. For example, FINRA alleged that the firm's surveillance system for reviewing trading activity failed to generate alerts for certain high risk activity due to technical flaws. In addition, FINRA alleged that the firm's automated system to review its trade blotter failed to display trading activity past due for supervisory review. *LPL Financial LLC*, FINRA AWC No. 2013035109701 (May 6, 2015), https://www.finra.org/sites/default/files/fda_documents/2013035109701_FDA_JMX1471%20%282019-1563047367963%29.pdf

II. What Makes a Good Surveillance Program?

A. Regulatory Requirements

1. FINRA firms are required to "establish and maintain a system to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules." FINRA Rule 3110.

2. FINRA Rule 3120 requires members to "designate and specifically identify to FINRA one or more principals who shall establish, maintain, and enforce a system of supervisory control policies and procedure that (1) test and verify that the member's supervisory procedures are reasonably designed with respect to the activities of the member and its associated persons, to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules; and (2) create additional or amend supervisory procedures where the need is identified by such testing and verification." FINRA Rule 3120.

   a. "A firm not only needs to maintain WSPs, but the firm also must have [supervisory control policies and procedures] to test and verify, at least annually, that its WSPs are reasonably designed with respect to the firm's and its associated persons' activities to achieve compliance with applicable securities laws and regulations and FINRA rules, and to create additional or amend WSPs as identified by such testing and verification. Risk-based methodologies and sampling may be used to determine the scope of testing. The testing ensures that a firm's supervisory procedures are reviewed and amended regularly in light of changing business and regulatory environments." *FINRA Rule 3110 (Supervision) Guidance*, FINRA https://www.finra.org/rules-guidance/key-topics/supervision (last visited Jan. 22, 2020).

3. According to FINRA, this supervisory requirement "includes having reasonable procedures and control systems in place for supervision and governance of RegTech tools, including supervision of AI-based tools and systems." *FINRA RegTech White Paper*, at 7.

4. SEC Regulation S-P requires investment advisers, brokers, dealers, and investment companies to adopt policies and procedures that address safeguards to protect customer information. *See also* NASD Notice to Members 05-49 (Safeguarding Confidential Customer Information) ("NASD members are required to maintain policies and procedures that address the protection of customer information and records. Among other things, these policies and procedures must be reasonably designed to protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.").

B. Elements of an Effective Surveillance Program

1. Infrastructure – data and tools

2. People – difficult resource allocation issues: compliance SMEs, testers, technology personnel with business expertise, data analytics/science teams with business expertise

3. Organizational structure – how situate people to facilitate maximum impact?

4. Governance – committees (including potentially new products and services, rules review, and parameter governance), and testing infrastructure (pre-deployment vs. post-deployment)

C. Challenges

1. <u>Supervising technology</u>: need for focus on governance, testing, and vendor management

   a. "Firms' increasing reliance on technology for many aspects of their customer-facing activities, trading, operations, back-office and compliance programs creates a variety of potential benefits, but also exposes firms to technology-related compliance and other risks. In particular, problems in firms' change- and problem-management practices, for example, can expose firms to operational failures that may compromise firms' ability to comply with a range of rules and regulations." 2020 Risk Monitoring and Examination Priorities Letter, FINRA (Jan. 9, 2020), https://www.finra.org/rules-guidance/communications-firms/2020-risk-monitoring-and-examination-priorities-letter.

   b. "Some of the RegTech applications … may use highly complex and sophisticated AI algorithms, which are designed to learn and evolve based on data patterns. Compliance and business professionals may not have the technical skills to understand in detail how these algorithms function." *FINRA RegTech White Paper*, at 7.

   c. "Auditing the methodology or logic used by an AI-algorithm to generate a specific output or decision can be challenging. Previously, FINRA has stated with respect to the use of technology-based trading tools: '[T]he use of algorithmic strategies has increased, the potential of such strategies to adversely impact market and firm stability has likewise grown. When assessing the risk the use of algorithmic strategies creates, firms should undertake a holistic review of their trading activity and consider

implementing a cross-disciplinary committee to assess and react to the evolving risks associated with algorithmic strategies.'" *Id.*

d. "[S]ome technologies are inherently challenging for the SEC to monitor. To mention just one example, consider artificially intelligent algorithmic trading (AI algo trading), which trade through time in non-predictable ways. Suppose an AI algo eventually starts spoofing without the knowledge of the algo creator. (Spoofing is a prohibited activity than involves creating and cancelling a large number of trades in an attempt to convey false information about market demand.) How should the SEC respond to that?" S. P. Kothari, SEC Chief Economist and Director, Division of Economic and Risk Analysis, *Policy Challenges and Research Opportunities in the Era of Big Data*, SEC (Jul. 13, 2019), https://www.sec.gov/news/speech/policy-challenges-research-opportunities-era-big-data.

e. FINRA has listed a series of considerations that broker-dealers may want to consider when adopting RegTech tools:

➢ Establishing a cross-functional technology governance structure.

➢ Simplified summary of the RegTech tools.

➢ Data quality risk-management.

➢ Process to identify and address errors or malfunctions.

➢ Training of personnel.

FINRA RegTech White Paper, at 8.

2. <u>Outsourcing risks</u>: "Firms are reminded that outsourcing an activity or function to a third-party does not relieve them of their ultimate responsibility for compliance with all applicable securities laws and regulations and FINRA rules associated with the outsourced activity or function. As such, firms may desire to adjust or update their written supervisory procedures to ensure that they appropriately address outsourcing arrangements (*see, e.g.*, Notice to Members 05-48 (Outsourcing))." *Id.*

Per FINRA, here are certain factors to assess when considering outsourcing:

> ➢ Whether an appropriate due-diligence analysis of the vendor was conducted including, where applicable, consideration of its technical, operational and financial soundness;

> ➢ Whether the vendor understands the regulatory requirements that it offers RegTech solutions for, and has a system in place to monitor for and incorporate any changes to such regulatory requirements;

> ➢ Whether the vendor's cybersecurity policies and procedures are appropriate, particularly when the outsourcing arrangement involves sharing of sensitive firm and customer data;

> ➢ Whether there is a need for a continuity and transition plan, in the event the vendor is unable to fulfill its obligations and the required functions need to be abruptly moved back in-house;

> ➢ To the extent the use of outsourced RegTech services leads to the creation of new records, firms may wish to consider working with vendors to develop appropriate processes to meet the firm's recordkeeping obligations such as those associated with Exchange Act Rules 17a-3 and 17a-4 and FINRA Rule 4511 (Books and Records: General Requirements).

Id. at 8-9.

3. Privacy: some RegTech tools involve the collection and analysis of customer-related data, and may involve sharing that data with a third party vendor. Firms have an obligation to protect the financial and personal customer information under SEC Regulation S-P (Privacy of Consumer Financial Information and Safeguarding of Personal Information).

4. Cybersecurity and data-related risks: potential for new vulnerabilities. "Security risk management should be an integral part of the evaluation and implementation of RegTech tools by firms. Specifically, firms should pay close attention to technology governance, system change management, risk assessments, technical controls, incident response, vendor management, data loss prevention, and staff training." *Id*. at 9.

III. **Understanding the New Technologies of Artificial Intelligence, Machine Learning, and Other Data Analytics Tools, and Their Evolving Deployment in the Financial Services Industry**

A. Knowing Our Data

1. <u>Structured data</u>: defined data types with characteristics and content that makes them easily searchable, such as data in rows and columns with elements that can be organized by fields. Examples: market data, customer portfolio data, transactional data.

2. <u>Unstructured data</u>: everything else: complex data that cannot be contained in row-column databases and does not fit an associated data model or relational database. Examples: text of emails, texts, or social media postings, content of voice recordings or call transcripts, photos, or websites.

3. <u>Semi-structured data</u>: data with unstructured content, but has some characteristics of structured data. Examples: email messages (content is unstructured, but other message content has structured data fields such as sender, recipient, time stamp, etc.) or digital photos (content is unstructured, but could have structured characteristics such as date and time taken, geospatial tagging, or technical information such as the camera device with which it was taken).

B. Evolving Our Thinking: Novel Analytical Approaches and Novel Analytical Techniques

1. <u>New analytical approaches</u> – evolving our thinking about how to analyze data. "RegTech tools generally aim to move beyond traditional rule-based systems to a predictive risk-based surveillance model that identifies and exploits patterns in data to inform decision-making. For example, computer programs trained with historical data may be used to look for suspicious patterns and trends in current data, or identify future patterns and trends. These programs also generally learn from periodically or continuously incorporating new data through a feedback process that seeks to refine future alerts." *Id*. at 4.

   a. <u>Rules-based</u>: traditional approach – developing tests and scenarios based on known rules/thresholds.

   b. <u>Supervised learning</u>: – a type of machine learning; basically, learning by example. A variety of known data inputs are provided and the logarithm identifies additional possible examples of the same conduct. Examples: classification (map inputs to output labels) or regression (map inputs to continuous outputs).

   c. <u>Unsupervised learning</u>: – a type of machine learning; the data itself defines or infers natural structures, relationships, or patterns within

the data. Example: clustering (grouping similar data together based on data points).

2. <u>New analytical techniques</u> – evolving the tools we use in our analyses. Some examples:

    a. <u>Text analytics</u>: unsupervised learning can identify hidden uses of words or phrases in text

    b. <u>Anomaly or outlier detection</u>: identify rare outcomes or events based on differences from the majority of the data reviewed.

    c. <u>Sentiment analysis</u>: extracting emotions of the speaker from voice or text data. In text, not just explanation marks (!!!) and ALL CAPs, but how negative and positive words are grouped together. For voice, tonality of conversations and acoustic characteristics are analyzed.

    d. <u>Network analytics</u>: identify relationships or links between similar events or entities.

    e. <u>Geospatial analytics</u>: overlay spatial (location) data to identify geographic similarities, differences, or patterns.

C. What are AI and ML? How are they different?

1. "Artificial intelligence generally refers to the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, pattern recognition, and decision-making." *Id*., at 12 n. 11.

2. "Artificial Intelligence is the broader concept of machines being able to carry out tasks in a way that we would consider 'smart'. And, Machine Learning is a current application of AI based around the idea that we should really just be able to give machines access to data and let them learn for themselves." Bernard Marr, *What Is the Difference Between Artificial Intelligence and Machine Learning?*, Forbes (Dec. 6, 2016), https://www.forbes.com/sites/bernardmarr/2016/12/06/what-is-the-difference-between-artificial-intelligence-and-machine-learning/#78176adf2742.

3. "Early AI attempts used computers to mimic human behavior through rules-based methods, which applied logic-based algorithms that tell a computer to 'do this if you observe that.' Today, logic-based machine learning is being replaced with a data-up approach. And by data-up, I

mean programming a computer to learn directly from the data it ingests. Using this approach, answers to problems are achieved through recognition of patterns and common associations in the data. And they don't rely on a programmer to understand why they exist. Inference, a prerequisite to a rule, is not required. Instead, tiny little voting machines, powered by neural networks, survey past quantifiable behaviors and compete on the best possible responses to new situations. If you want a tangible example of this, think no further than your most recent online shopping experience. Upon the purchase of party hats, your preferred retailer is likely to inform you that other shoppers also purchased birthday candles. Perhaps you need them too? Behind this recommendation is a computer algorithm that analyzes the historical purchasing patterns from you and other shoppers. From this, it then predicts future purchasing-pair decisions. The algorithm doesn't care why the associations exist. It doesn't matter if the predictions don't make intuitive sense. The algorithm just cares about the accuracy of the prediction. And the algorithm is continually updating the predictions as new data arrives and new associations emerge." *Bauguess, Role of Big Data*.

D. What are NLP and LDA?

1. "Natural language processing generally refers to the processing of a sample of human language (spoken or written) by computer programs in order to categorize and classify its contents." *FINRA RegTech White Paper*, at 12 n.12.

2. Natural language processing (NLP) is the application of topic modeling methods (including latent dirichlet allocation (LDA)) across text – measuring the probability of words within documents and across documents to define the unique topics thy represent. This is called "unsupervised learning" in the data scientist world. It allows computers with no content expertise to serve as a proxy for the initial identification of materials. "You don't have to know anything about the content of the documents. No subject matter expertise is needed. LDA extracts insights from the documents, themselves using the data-up approach to define common themes – these are the topics – and report on where, and to what extent, they appear in each document." *Bauguess, Role of Big Data*.

E. What is RPA?

1. "Robotics process automation (RPA) generally refers to software that can be easily programmed to do basic tasks across applications just as human workers do." *FINRA RegTech White Paper*, at 12 n.15.

2. Robotic process automation (RPA) is not considered AI, because RPA is strictly rule-driven. "For simplicity, you can think of RPA as a software robot that mimics human actions, whereas AI is concerned with the simulation of human intelligence by machines." *The Difference Between Robotic Process Automation and Artificial Intelligence*, Medium (Apr. 21, 2018) https://medium.com/@cfb_bots/the-difference-between-robotic-process-automation-and-artificial-intelligence-4a71b4834788.

F. What are "Big Data Analytics"?

1. "Big data analytics generally refers to a set of tools and processes required to work with large sets of diverse data that include different types such as structured/unstructured and streaming/ batch. Because of the very large volume of data, big data analytics often require new tools and processes that are different from traditional data management and processing systems." *FINRA RegTech White Paper*, at 12 n.13.

G. What are "Biometrics"?

1. "Biometrics generally refers to "[T]he measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity." *Id.*, at 12 n.18.

H. How Can Firms Use These New Technologies?

1. Applications/Opportunities

The FINRA RegTech White Paper outlined five specific areas where RegTech tools and new data analytics technology are and can be deployed:

a. **Surveillance and Monitoring**

(i) Applies to both "market surveillance and conduct monitoring, such as monitoring traders, registered representatives, employees, and customers for regulatory purposes." *Id.*, at 3.

(ii) The FINRA RegTech White Paper observed this is an area where RegTech is gaining "substantial traction" and that "[m]arket participants have indicated that they are investing significant resources in this area." *Id*.

(iii)   Potential to record, monitor, and analyze various of communications, incorporation, audio, video, and digital with text.

(iv)   Possibility to evolve from sampling-based approaches to comprehensive analysis of all relevant communications.

(v)   "[O]pportunity to potentially move beyond a traditional lexicon-based review focused on specific terms and instead move towards a more risk-based review utilizing processes such as natural language processing and machine learning to help identify patterns or anomalies." *Id*. at 4.

(vi)   Potential deployment of sentiment analysis, including "slang, tone, code language, and 'emotional words' denoting a strong reaction." *Id*.

(vii)   Possibility to link data sets that used to previously be siloed and reviewed in isolation. "For instance, the relationship between certain structured data (such as trade orders and cancels, market data, and customer portfolio) and unstructured data (such as emails, voice recordings, social media profiles and others communications) have historically been difficult to link together. However, RegTech tools are being developed that would help to integrate these disparate data forms and then identify and track related anomalies that merit attention." *Id*.

b.   **Customer Identification and AML Compliance**

(i)   FINRA Rule 2090 (Know Your Customer (KYC)) requires broker-dealers to "use reasonable diligence, in regard to the opening and maintenance of every account, to know (and retain) the essential facts concerning every customer and concerning the authority of each person acting on behalf of such customer."

(ii)   The Bank Secrecy Act of 1970 (BSA) requires all broker-dealers to, among other things, implement compliance programs to detect and prevent money laundering. In addition, FINRA Rule 3310 (Anti-Money Laundering Compliance Program) requires all broker-dealers to develop and maintain a written AML program to comply with the requirements of the BSA.

(iii)   FINRA's RegTech White Paper noted that "anecdotal statements by market participants suggest that traditional solutions and methods for customer identification and AML monitoring may, at times, have not been as effective as desired. The financial industry is exploring the use of RegTech tools as it looks for more effective solutions." *Id.*

(iv)   Solutions being offered include the use of biometrics, as well as the use of data analytics that combines various data sets from different sources, including data provided by clients, to provide "a more holistic view of the customer." *Id.*

(v)   The challenges posed by AML regulations has also promoted exploration of "central industry utilities as shared solutions for customer identification." *Id.*, at 5. While such tools would present data privacy challenges, collaborative platforms with pooled information could provide a more comprehensive view regarding transactional activity and, potentially, better compliance with regulatory goals.

c.   **Regulatory Intelligence**

(i)   "Regulatory intelligence programs refer to areas of compliance that focus on the identification and interpretation of changes to applicable rules and regulations, frequently across multiple jurisdictions, in order to update a firm's compliance operations." *Id.*

(ii)   RegTech tools is this area provide an indexed set of regulatory requirements that are not only kept up-to-date, but can be deployed in an automated manner in firms' supervision and compliance programs.

(iii)   "Some regulators are also exploring and adopting RegTech to facilitate dissemination of regulatory intelligence. For example, the UK Financial Conduct Authority (FCA) and the Bank of England (BoE) have launched an initiative to make their rulebooks "machine-readable," such that they can be easily processed and interpreted by machines and incorporated into firms' regulatory intelligence systems." *Id.*

(iv) Some RegTech offerings in this space are focused on delivering pre-clearance capabilities. "For example, in the context of derivatives trading, RegTech solutions are being offered to enable firms and their traders to ensure that their trades are compliant with applicable rules and regulations (such as those related to clearing and reporting) before they are executed." *Id.*

d. **Reporting and Risk Management**

(i) "Solutions in this space leverage technology to develop tools to facilitate or automate processes involved in risk-data aggregation, risk metrics creation and monitoring (for enterprise risk management as well as operational risk management), and regulatory reporting. For example, to assist with risk-data aggregation or regulatory reporting, a RegTech tool may be deployed to gather and analyze information on capital and liquidity for use in internal models or to report to regulators." *Id.*

e. **Investor Risk Assessment**

(i) FINRA rules require that firms collect adequate information from investors in order to be able to provide the investor with suitable investment advice.

(ii) Certain RegTech tools "seek to leverage technological innovations (such as data aggregation and machine learning) in combination with behavioral sciences to determine an investor's risk appetite and tolerance in a more scientific manner than existing tools. For example, some tools assess an investor's risk appetite and tolerance based on an investor's performance on "games" designed to provide insights into the investor's reactions to changes in market conditions and portfolio performance." *Id.*, at 6.

2. Firm size/maturity

a. What works for your firm?

b. Home grown vs. off-the-shelf?

c. Smaller firms – beware of specific risks of outsourcing.

d. For all: oversight responsibility.

3. Ways to get started and maximize investment

- Tracking emerging best practices. How?

- Use case testing.

  o Discussions with business, compliance, risk, technology.

    ▪ Where are the greatest needs in the firm?

    ▪ Which the presently-available technologies might most easily be integrated with the firm's current infrastructure?

  o Step-by-step: prove cases for business.

    ▪ Possibility of "running newer RegTech surveillance tools in parallel with their traditional tools and supplementing these automations with human reviews to validate their effectiveness."

- Do not try and "boil the ocean"!

4. Longer term possibilities?

- Integrated supervision and surveillance across various functions? Enterprise-wide monitoring?

- Shifting from rules-based, sample-driven, and retrospective monitoring to continuous / real-time monitoring?

IV.   The Regulatory Cost of Not Modernizing

A.   Examples of Recent Enforcement Activity

1. In December 2019, the SEC filed a lawsuit against an IT contractor and two tippees for violations of insider trading. The SEC alleged that the IT contractor stole confidential client information while working in the Singapore branch of an investment bank and provided the information to his wife and father. Kelly L. Gibson, Associate Director of Enforcement in the SEC's Philadelphia Regional Office said, "Our continued use of innovative analytical tools to find suspicious trading patterns and expose misconduct demonstrates our resolve to catch insider traders who seek to take illegal advantage of the U.S. markets for personal gain." *SEC Halts Alleged Insider Trading Ring Spanning Three Countries*, SEC (Dec. 6, 2018), https://www.sec.gov/news/press-release/2018-273.

2. In September 2018, the SEC filed a lawsuit against a New Jersey-based broker for alleged cherry-picking that was originally identified by the SEC's data analytics tools. *SEC Uses Data Analysis to Detect Cherry-Picking by Broker*, SEC (Sept. 12, 2018), https://www.sec.gov/news/press-release/2018-189.

3. In July 2018, the SEC settled a matter relating to a firm's failure to maintain and enforce policies and procedures aimed at preventing the misuse of material nonpublic information. Members of the SEC's Division of Economic and Risk Analysis were involved in the matter. *SEC Charges Mizuho Securities for Failure to Safeguard Customer Information*, SEC (July 23, 2018), https://www.sec.gov/news/press-release/2018-140.

4. In August 2017, the SEC filed a lawsuit against seven individuals for alleged insider trading that was discovered, in part, by the SEC's use of data analytics. SEC Uncovers Wide-Reaching Insider Trading Scheme, SEC (Aug. 16, 2017), https://www.sec.gov/news/press-release/2017-143.

B. Regulatory Approach to Surveillance

- Arms race risk?

- Just how much advanced data analytics is required for a "system to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules"?

C. 20/20 Hindsight Risk

- Compounding factor where you have possession of all your data

- Need for clarity regarding what you are doing, why, and why it is reasonable.

D. Need for Engagement and Advocacy with Regulators

- Engagement regarding evolving landscape

- Frank discussions about "yield" and associated challenges

V. Closing Thoughts