THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 53 No. 11 June 10, 2020

THE SEC AND FINRA'S USE OF BIG DATA IN INVESTIGATIONS . . . AND THE IMPLICATIONS FOR DEFENSE COUNSEL

In recent years, the SEC and FINRA have created a number of new units to increase their capacity to use data analytics in market surveillance and policy/rulemaking activities. In this article, the authors summarize these units, their objectives, and the types of investigations that most prominently use data analytics. They close with a discussion of the new challenges that defense lawyers face as regulators increasingly use big data in their enforcement actions.

By Robert A. Cohen and Angela W. Guo *

SEC Chairman Jay Clayton recently remarked that budgetary constraints make "data analytics work more important than ever."[1] Previously, former SEC Chair Mary Jo White described this new data-driven approach as "transformative."[2] Consistent with these observations, the SEC and FINRA have significantly expanded their use of big data over the last decade to identify promising leads, conduct investigations, and litigate cases. Both agencies aim to use big data to make more efficient use of resources, especially by focusing efforts on the leads they consider most promising and prioritizing potentially high-impact investigations. This regulatory use of big data has changed the landscape for companies and individuals subject to investigation and the law firms that represent them.

This article provides an overview of the SEC and FINRA's use of data analytics to perform trade surveillance and conduct investigations, including groups inside the SEC and FINRA that use big data, the data and analytical techniques they use, and the types of cases most influenced by data analytics. We also discuss

[1] Jay Clayton, SEC Chairman, Keynote Remarks at the Mid-Atlantic Regional Conference (June 4, 2019), https://www.sec.gov/news/speech/clayton-keynote-mid-atlantic-regional-conference-2019.

[2] Mary Jo White, Chair, SEC, Speech at the New York University School of Law Program on Corporate Compliance and Enforcement: A New Model for SEC Enforcement: Producing Bold and Unrelenting Results (Nov. 18, 2016), https://www.sec.gov/news/speech/chair-white-speech-new-york-university-111816.html.

* *ROBERT A. COHEN is a partner at Davis Polk & Wardwell LLP. ANGELA W. GUO is a law clerk at the same firm. Mr. Cohen formerly was Co-Chief of the Market Abuse Unit and Chief of the Cyber Unit at the SEC. While at the SEC, Mr. Cohen participated in some of the cases and other matters discussed in this article. This article includes only public information. Mr. Cohen is admitted in Maryland and New York, and is practicing in the District of Columbia under supervision of a partner of the firm. Their e-mail addresses are Robert.Cohen@davispolk.com and Angela.Guo@davispolk.com.*

RSCR Publications LLC Published 22 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $1,197 per year in U.S., Canada, and Mexico; $1,262 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call (937) 387-0473 or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 0884-2426.

the impact on defense counsel and their clients, including the need for defense counsel to anticipate and respond to novel challenges presented by regulators' increasing reliance on big data.

THE SEC'S IN-HOUSE DATA ANALYTICS

The SEC created several groups over the past decade to increase its use of big data:

- The SEC created the Division of Economic and Risk Analysis ("DERA") in 2009.[3] DERA employs economists, analysts, data scientists, computer engineers, and statisticians, in addition to attorneys, in its mission to "integrate financial economics and rigorous data analytics into the core mission of the SEC."[4] DERA supports other SEC divisions and offices, including the Enforcement Division, as well as the SEC's policy/rulemaking divisions.

- In 2010, the SEC created the Office of Market Intelligence within the Enforcement Division. "OMI" is responsible for the collection and analysis of tips, complaints and referrals, including referrals from self-regulatory organizations ("SROs"), such as FINRA, concerning possible trading violations.[5]

- The SEC created the Center for Risk and Quantitative Analysis in 2013. "CRQA" employs quantitative data analysis to profile high-risk behaviors and transactions in support of the Enforcement Division's investigations.[6]

- The SEC created the Retail Strategy Task Force in 2017 to, among other things, employ data analytics to target practices that may harm retail investors.[7]

- The SEC appointed its first Chief Data Officer in early 2020.[8] The SEC described the responsibilities of the new position as helping to "develop the SEC's data management strategy and priorities, enable data analytics to support enforcement, examinations, and policymaking, and ensure that the agency collects only the data it needs to fulfill its mission and can effectively secure."

The Market Abuse Unit

The SEC group whose use of data likely had the biggest impact on SEC enforcement is the Market Abuse Unit ("MAU"), which the SEC created in 2010 as one of the first five specialized units within the Division of Enforcement. MAU's mandate is to "focus on investigations involving large-scale market abuses and complex manipulation schemes by institutional traders, market professionals, and others."[9] These investigations include (1) insider trading cases, typically involving complex schemes with multiple traders; (2) high-volume market manipulation cases; and (3) market structure cases, including cases concerning order routing, dark pools, and stock exchanges. The front-line work by the SROs, especially the work by FINRA that is described below, has enabled the Market Abuse Unit to focus its efforts on potential trading schemes that are more complex and more difficult to detect.[10]

---

[3] *About the Division of Economic and Risk Analysis*, SEC, https://www.sec.gov/dera/about.

[4] *Id.*

[5] *SEC Names New Specialized Unit Chiefs and Head of New Office of Market Intelligence*, (Jan. 13, 2010), *available at* https://www.sec.gov/news/press/2010/2010-5.htm.

[6] *SEC Announces Enforcement Initiatives to Combat Financial Reporting and Microcap Fraud and Enhance Risk Analysis* (July 2, 2013), *available at* https://www.sec.gov/news/press-release/2013-2013-121htm.

[7] *SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors* (Sept. 25, 2107), *available at* https://www.sec.gov/news/press-release/2017-176.

[8] *Austin Gerig Named as SEC's Chief Data Officer* (Jan. 16, 2020), https://www.sec.gov/news/press-release/2020-11.

[9] *SEC Names New Specialized Unit Chiefs and Head of New Office of Market Intelligence* (Jan. 13, 2010), *available at* https://www.sec.gov/news/press/2010/2010-5.htm.

[10] Elizabeth P. Gray and Catherine E. Fata, *Increased Use of Big Data in SEC Enforcement* (June 21, 2017), *available at* https://www.willkie.com/-/media/files/publications/2017/06/increased_use_of_big_data_in_sec_enforcement.pdf.

In turn, MAU established its own Analysis and Detection Center ("A&D Center") in 2011. The A&D Center seeks to study insider trading like a "think tank," and leverage the expertise of industry specialists with quantitative skills in computer science and data analytics.[11] The creation of MAU gave the SEC an in-house platform to "study how information flows in the markets, how people communicate, and how traders use information to make trading decisions."[12]

The SEC's Data Sources

The primary data the SEC uses to identify possible insider trading is "bluesheet data." Broker-dealers are required to maintain this data and provide it to the SEC upon request.[13] Broker-dealers submit bluesheet data electronically, but the data is called "bluesheets" because, for many years, the Commission requested trading data by physically mailing questionnaire forms printed on blue-colored paper. Broker-dealers manually completed these forms with the requested information and mailed them back to the Commission.

The SEC has developed a specialized tool to analyze bluesheet data, called ARTEMIS, or the Advanced Relational Trading Enforcement Metric Investigation System. SEC staff created ARTEMIS, which combines trading data with other data sources to enable "longitudinal, multi-issuer, and multi-trader" data analyses.[14]

Trader-Based Lead Detection

Historically, the SEC often followed an "issuer-based" approach to develop leads for insider trading investigations. In an issuer-based approach, the SEC would identify a news report or receive a referral about suspicious trading in advance of a specific company's (the "issuer") M&A announcement, earnings release, or other material news event. The SEC would assess the lead and potentially begin its investigation by focusing on the trading in the securities of that company.[15] These issuer-based investigations sometimes led to a broader set of trades involving different companies.

After the establishment of the MAU and the A&D Center, the SEC increased and advanced its use of a different technique – a "trader-based" approach. The expansion of its own in-house data analytics unit created a platform for the Enforcement Division to detect potentially complex, more wide-spread patterns of suspicious trading. The SEC uses data analytics to search for patterns of potentially suspicious trades by individuals or groups of traders, across time, and across a variety of stocks. The lead detection and investigations begin with a focus on *traders*, not particular *companies*. The SEC's objective is to identify traders who might have a source of nonpublic information that is not limited to a single issuer; for example, a contact at an investment bank that advises on many deals, a public relations firm that helps a variety of corporate clients prepare public announcements, or someone selling hacked information about many different companies.

With an issuer-based approach, the SEC usually would begin an investigation with a single set of trades before a single event at one issuer, and then expand the inquiry to see if that trader had a suspicious history of other trades. With a trader-based approach, the SEC hopes to begin investigations after already identifying one or more traders who exhibit a suspicious pattern that cuts across a longer time period and across several issuers. With this data-driven approach, the SEC's goal is to focus immediately on potentially large-scale trading schemes. Because the SEC relies on FINRA to look at trades before individual stock price movements, the SEC can focus its resources on these deep-dive data analyses.

Types of Investigations That Use Big Data

The SEC has used big data analysis most prominently in insider trading and similar cases. One example is a 2015 hacking case in which the SEC charged six Ukrainians with hacking into the internal systems of several newswire services to access unreleased press

[11] Daniel M. Hawke and Laura D'Allaird, *The Trader-Based Approach To Insider Trading Enforcement* (Sept. 7, 2016), https://www.law360.com/articles/833488/the-trader-based-approach-to-insider-trading-enforcement.

[12] *Id.*

[13] Exchange Act Rules 17a-25 and 17a-4(j), 15 U.S.C. §§ 78q(a)(1), 78q(d)(1) – (2); *Electronic Submission of Securities Transaction Information by Exchange Member, Brokers, and Dealers*, Rel. No. 34-44494 (June 29, 2001), https://www.sec.gov/rules/final/34-44494.htm.

[14] Michael S. Piwowar, SEC Commissioner, Remarks at the 2018 RegTech Data Summit – *Old Fields, New Corn: Innovation in Technology and Law* (March 7, 2018), https://www.sec.gov/news/speech/piwowar-old-fields-new-corn-innovation-technology-law.

[15] Hawke and D'Allaird, *supra* note 11.

announcements.[16] The hackers were accused of sharing the stolen press releases with a wide variety of traders on the dark web, who allegedly paid the hackers based on a percentage of their illegal trading profits. Prosecutors filed related criminal charges in New York and New Jersey, which resulted in convictions,[17] and the SEC settled with some defendants.[18]

The government's allegations demonstrate the value of big data analysis. The SEC alleged that there was a "flurry of trading activity around a stolen press release just prior to its public release," and that the traders executed their trades in the sometimes brief timeframes between the time the hackers were alleged to have accessed the press releases and when the newswire services publicly disseminated the news.[19] The SEC said that the alleged scheme was uncovered through the SEC's "use of innovative analytical tools to find suspicious trading patterns."[20]

The SEC has used data analytics in other enforcements contexts, such as cherry-picking cases. Cherry-picking is the practice of an investment adviser allocating profitable trades to favored accounts, such as the adviser's own account, and non-profitable trades to other accounts. In 2017, the SEC brought charges against an investment adviser who also faced parallel criminal charges. When announcing the case, the SEC cited the MAU analysis of the adviser's trading, and an SEC official said, "Our probing analytical work will continue to root out investment advisers who subject their clients to cherry-picking."[21]

The results of data analysis, if compelling, can help the SEC confront a common challenge in complex trading cases – measures to evade detection. For example, one challenge is trading that originates overseas, where the SEC's investigative powers may be limited. In a recent insider trading trial, a witness testified that an "unbelievable" number of people committed insider trading abroad – almost as a "sport."[22]

Whether foreign or domestic, the SEC also has accused traders of creating false paper trails to cover-up alleged insider trading. In one of the most prominent insider trading cases in recent years, the government introduced evidence that Raj Rajaratnam was recorded discussing choreographed e-mails with fake reasons for a trade, and trading in and out of a stock, to evade government detection.[23] In another case, the SEC alleged that, after receiving a tip, a trader gathered research about the relevant stocks and sent e-mails to the middleman who conveyed the tips to create a paper trail of legitimate reasons to trade the stocks before placing the allegedly illicit trades.[24]

FINRA'S DATA-DRIVEN TRADE SURVEILLANCE

Although the SEC maintains principal responsibility for enforcement and other regulatory oversight of the securities industry, the Securities Exchange Act of 1934 also requires that SROs, such as stock exchanges and FINRA, monitor the activities of their members.[25] The

[16] *SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases* (Aug. 11, 2015) https://www.sec.gov/news/pressrelease/2015-163.html.

[17] *Former Hedge Fund Manager Sentenced to 60 Months' Imprisonment and Ordered to Pay $14.4 Million in Forfeiture for Role in International Securities Fraud and Computer Hacking Scheme* (March 21, 2019), https://www.justice.gov/usao-edny/pr/former-hedge-fund-manager-sentenced-60-months-imprisonment-and-ordered-pay-144-million.

[18] *SEC Obtains $30 Million From Traders Who Profited on Hacked News Releases* (Sept. 14, 2015), https://www.sec.gov/news/pressrelease/2015-191.html.

[19] *Hacker Sentenced to 30 Months in Prison for Role in Largest Known Computer Hacking and Securities Fraud Scheme* (May 22, 2017), https://www.justice.gov/usao-nj/pr/hacker-sentenced-30-months-prison-role-largest-known-computer-hacking-and-securities.

[20] *SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases* (August 11, 2015), https://www.sec.gov/news/pressrelease/2015-163.html.

[21] *SEC Uncovers Cherry-Picking Scheme, Charges Investment Adviser Behind It* (Jan. 25, 2017), https://www.sec.gov/news/pressrelease/2017-32.html.

[22] Rebecca Davis O'Brien, *Star Witness in Insider-Trading Case Describes Far-Reaching Scheme* (Jan. 10, 2020), The Wall Street Journal, https://www.wsj.com/articles/star-witness-in-insider-trading-case-describes-far-reaching-scheme-11578666631?mg=prod/com-wsj.

[23] Floyd Norris, *For Prosecutors, the Case That Got a Head Start on the Crime*, The New York Times (May 11, 2011), https://www.nytimes.com/2011/05/12/business/12norris.html.

[24] *SEC v. Eydelman, et al.*, Civ. Action No. 3:14-cv-01742-MAS-TJB (March 19, 2014), complaint at ¶ 62, https://www.sec.gov/litigation/complaints/2014/comp-pr2014-55.pdf.

[25] Robert W. Cook, FINRA President and CEO, *Equity Market Surveillance Today and the Path Ahead* (Sept. 20, 2017), https://www.finra.org/media-center/speeches-testimony/equity-market-surveillance-today-and-path-ahead; Exchange Act Section 19(g).

SEC relies heavily on FINRA to conduct frontline insider trading surveillance.[26]

FINRA's investigative authority and data capabilities differ from the SEC's in several ways. FINRA is a private organization; it does not have the law enforcement authority of a government agency. FINRA's authority also is limited to its member firms; FINRA cannot discipline or compel discovery from individuals or firms other than firms that are FINRA members and the licensed individuals associated with those firms. However, FINRA has broad responsibility under Regulatory Service Agreements in which FINRA agrees to conduct market surveillance on behalf of other SROs, such as stock exchanges.[27] Despite limited legal authority, FINRA's responsibility to conduct trade surveillance results in a broad surveillance mandate that is the securities market's equivalent of "guarding the waterfront."

FINRA has substantial resources dedicated to these surveillance activities. Although FINRA is responsible for only a portion of the securities industry, its operating revenue was $846.9 million in 2019.[28] FINRA relies on its Office of Fraud Detection and Market Intelligence ("OFDMI") to monitor "every transaction that takes place in both equities and options markets."[29] FINRA employs more than 50 professionals in OFDMI to monitor and investigate trading in stocks, bonds, and options. For reference, this group of insider trading surveillance experts is approximately the same size, and perhaps even larger than the SEC's Market Abuse Unit, which pursues not only insider trading cases, but also manipulation, market structure, and many other types of cases.

OFDMI deploys software called Securities Observation News Analysis and Regulation ("SONAR"). SONAR looks "for everything from suspiciously well-timed trades ahead of a corporate announcement to huge jumps in trading activity on penny stocks."[30] OFDMI uses SONAR to flag suspicious trading activity for further investigation. OFDMI determines whether the trading can be linked to news that resulted in a significant stock price move or, if not, a separate fraud surveillance group will analyze the possibility of non-insider trading schemes, such as market manipulation, issuer fraud, or "pump-and-dumps."

Because FINRA's authority is limited to policing its own members, OFDMI typically refers developed leads to the SEC's Enforcement Division for further fact-gathering and possible enforcement action.[31] During the early stages of an investigation, the SEC and FINRA are often in frequent contact. In more data-intensive and complicated matters in which FINRA may have already conducted a more extended inquiry, the relationship between the two institutions becomes even closer and more substantial.

FINRA recently announced a restructuring, including movement of departments formerly within OFDMI into a new group, the National Cause and Financial Crimes Detection Program.[32] Regardless of the internal structure, FINRA surely will continue to rely on the big data analysis tools developed in OFDMI.

FINRA's Data Sources

Like the SEC, FINRA relies on bluesheet data, and also uses electronic chronology information. When investigating timely trades placed before a material corporate news event, such as an announcement of a merger or acquisition, FINRA sends inquiry letters to firms involved in the event. FINRA requests chronologies of the facts surrounding the event, including dates and descriptions of all significant meetings, agreements, communications, events, and

[26] *Id.*

[27] *FINRA Signs Regulatory Services Agreement with CBOE and C2* (Dec. 22, 2014), https://www.finra.org/media-center/news-releases/2014/finra-signs-regulatory-services-agreement-cboe-and-c2.

[28] FINRA, *2019 Annual Budget Summary*, https://www.finra.org/sites/default/files/2019_annual_budget_summary.pdf. By comparison, the SEC's budget to oversee the entire industry for that same year was approximately $1.6 billion. *SEC Fiscal Year 2020 Congressional Budget Justification and Annual Performance Plan*, https://www.sec.gov/files/secfy20congbudgjust_0.pdf.

[29] FINRA, *Catching the Bad Guys: Inside FINRA's Office of Fraud Detection and Market Intelligence* (September 3, 2015), https://www.finra.org/investors/insights/catching-bad-guys-inside-finras-office-fraud-detection-and-market-intelligence.

[30] *Id.*

[31] *Actions Resulting from Referrals to Federal and State Authorities*, *available at* https://www.finra.org/media-center/actions-resulting-referrals-federal-and-state-authorities.

[32] *FINRA Appoints Greg Ruppert Executive Vice President of National Cause and Financial Crimes Detection Programs* (March 19, 2020), https://www.finra.org/media-center/newsreleases/2020/finra-appoints-greg-ruppert-executive-vice-president-national-cause.

developments leading up to the disclosure of the transaction.[33] FINRA requests the information in electronic format to make it easier to access the chronology data across investigations and to look for trends across a series of trades. FINRA also requests identification of all individuals, inside and outside of the company, who knew about the event before it became public.[34] FINRA uses this combination of information – trade data, a chronology of events, and a list of individuals aware of the nonpublic information – to investigate whether any of the potentially suspicious trades might have been based on a tip from someone who knew about the not-yet-disclosed event.

THE DEFENSE PERSPECTIVE: THE IMPACT OF BIG DATA WHEN DEFENDING AN INVESTIGATION

As the government expands its data analytics prowess, lawyers face new challenges in representing clients under investigation. SEC investigators and examiners increasingly request voluminous productions of trade data. Responding to these requests can consume substantial resources and risk exposing sensitive information, such as proprietary trading strategies. Defense counsel also can find themselves in the difficult position of turning over large datasets without knowing the metrics the SEC is running against the data.

Although the government usually is not very transparent about the issues it is investigating, a traditional document request and production generally gives defense counsel an idea of the issues in play. When reviewing documents before turning them over to the government, defense lawyers typically can identify e-mail communications and other documents that might attract the government's attention. With voluminous trade data, counsel and their clients might not know the trading practices the SEC is looking to find, and is unlikely to know the data analysis the SEC is using to review the data. The SEC might focus on a particular set of trades without defense counsel having an opportunity to explain why the government's metrics might have produced a false positive. As a result, it is important for defense counsel to be experienced in trading strategies and data analysis, and anticipate the types of analyses the SEC's data experts might use to hunt for potentially suspicious trades. In the not-too-distant future, with developments in artificial intelligence, the SEC and SROs might input historical trading patterns that resulted in enforcement charges and program computers to look for similar patterns in market-wide data.[35]

Finally, for both the government and defending firms, big data has potentially significant implications for litigation and trial. For the government, big data analysis is best used to generate what it deems to be promising investigative leads. In insider trading cases, by the time of litigation and trial, evidence of who said what to whom is more likely to control the outcome than any data analysis. But the government may attempt to use data analysis at trial, especially if presented through an expert witness. Big data analysis is more likely to be relevant at trial in other types of cases, such as market manipulation cases. For defense counsel, the many subjective decisions inherent in data analysis may present an opportunity to attack the government's case. The defense also might have an opportunity to present an alternative data analysis to show that the trades are not suspicious when viewed in their overall context.

Whether used to identify leads, conduct investigations, litigate cases or present them at trial, big data analysis is increasingly important to trading investigations. The SEC and FINRA both rely on home-grown tools, and it is important for defense counsel advising clients in these matters to be experienced in the techniques the government uses and prepared to counter them with both informed scrutiny and their own analysis. ■

****

This article is based on a panel discussion at the DC Bar Association, titled "SEC and FINRA Continue to Expand Use of Big Data – What Does this Mean for The Securities Bar?" on January 16, 2020.

[33] Joseph D. Edmonson Jr. et al., *Responding to FINRA's Insider Trading Inquiries*, Law 360 (April 13, 2012), https://www.law360.com/articles/328765/responding-to-finra-s-insider-trading-inquiries.

[34] *Id.*

[35] Scott W. Bauguess, *The Role of Big Data, Machine Learning, and AI in Assessing Risks: a Regulatory Perspective* (June 21, 2017), https://www.sec.gov/news/speech/bauguess-big-data-ai.