Intelligence Design: An Analysis of the SEC's New Office of Market Intelligence and Its Goal of Using Big Data to Improve Securities Enforcement

Geoffrey Christopher Rapp

Follow this and additional works at: https://scholarship.law.uc.edu/uclr

Recommended Citation
Available at: https://scholarship.law.uc.edu/uclr/vol82/iss2/2

This Article is brought to you for free and open access by University of Cincinnati College of Law Scholarship and Publications. It has been accepted for inclusion in University of Cincinnati Law Review by an authorized editor of University of Cincinnati College of Law Scholarship and Publications. For more information, please contact ronald.jones@uc.edu.
INTELLIGENCE DESIGN: AN ANALYSIS OF THE SEC'S NEW OFFICE OF MARKET INTELLIGENCE AND ITS GOAL OF USING BIG DATA TO IMPROVE SECURITIES ENFORCEMENT

Geoffrey Christopher Rapp*

I. INTRODUCTION

On January 13, 2010, the Securities and Exchange Commission (SEC) announced an internal reorganization. Among the changes was the creation of a new Office of Market Intelligence (OMI or Office) within the Division of Enforcement. To a large degree, OMI’s creation addressed the persistent and troubling failures on the part of the SEC to process and respond to numerous tips concerning the massive Ponzi scheme perpetrated by Bernard Madoff. Analyzing the SEC’s failings in the Madoff case, Donald Langevoort argued in 2009 that “the SEC needs to turn itself into a ‘Financial Intelligence Agency’ that uses more effective ‘on the ground’ surveillance tools to understand and monitor emerging risks to investors in the financial markets and securities industry.” While the SEC did not entirely shift its approach, OMI represents its answer to Professor Langevoort’s challenge.

This Article describes the motivation for the formation of the new Office, the SEC’s understanding of OMI’s mission, the Office’s initial structure and evolution, and offers a prognosis for its future. The Article explores how the Office aligns with two templates—“market intelligence” as a business tool and the more traditional intelligence functions pursued by the federal government: its national defense,

---

* Harold A. Anderson Professor of Law and Values, University of Toledo College of Law. I would like to thank Professor Black and the University of Cincinnati for the opportunity to participate in a wonderful symposium and contribute this work to the published Law Review volume.


security, and increasingly, law enforcement roles.

In particular, OMI challenges two aspects of the broader federal experience with intelligence. First, the key conceptual framework for most intelligence activities involves a "cycle," with intelligence tools being deployed according to prioritized needs and intelligence results or products feeding back in to the identification of new intelligence missions. At first glance, at least, OMI appears to be driven more by capabilities than by requirements, and it is unclear whether the SEC has fully embraced a cyclical approach to its nascent intelligence function. Second, particularly as America has turned its attention to combatting violent extremism abroad, most federal intelligence activities have pursued a unification of intelligence functions with operational functions; arguably, by carving out intelligence separately within its operational/enforcement apparatus, the SEC has bucked this trend.3

Will the new OMI make a difference? The null hypothesis, which must be our starting point in reflecting upon any internal structural change pursued by an agency in response to perceived failings in the past, is that the new structure will make no difference in the agency’s performance in the future.

Consider, for instance, the regular reorganization of national defense intelligence activities. After failing to predict the collapse of the Soviet bloc4 or the Iraqi invasion of Kuwait in the early 1990s,5 America reorganized its intelligence community (IC), creating joint intelligence centers,6 unifying different military intelligence units, and the like. But the IC missed 9/11.7 Post-9/11, there were again major shifts in intelligence administration, including the creation of a new Director of National Intelligence (DNI) position8 and the augmentation of a National Counterterrorism Center9, but the IC failed to predict the so-

---

3. On the other hand, it might be argued that OMI does not represent a carve-out of intelligence, but the creation, for the first time, of an intelligence function.


5. Franklin Foer & Spencer Ackerman, The Radical: What Dick Cheney Really Believes, THE NEW REPUBLIC, Nov. 20, 2003, http://www.newrepublic.com/article/the-radical (stating that "[w]hen Saddam first began amassing troops on the Kuwaiti border in mid-1990, conventional wisdom in the U.S. intelligence community held that he was attempting to gain leverage in OPEC talks and, at the most, might seize a Kuwaiti oil field").


7. Friedman, supra note 4.

8. The DNI was created "to lead the intelligence community and to serve as the President’s primary intelligence advisor for national security, functions previously performed by the Director of the Central Intelligence Agency (CIA)." Anne Joseph O’Connell, The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World, 94 CAL. L. REV. 1655, 1657 (2006).

9. McKay M. Smith, The Nuclear Terrorism Readiness and Alert Center: Transforming the
The failure of the intelligence community’s reorganization rounds to produce different outcomes is by no means unique. Perhaps two thirds of organizational change efforts fail to achieve their goals. Any reorganization spurred by “a panicked desire to quickly offset negative public reaction” will face an uphill battle when it comes to producing real-world benefits.

II. ORIGINS OF THE OMI

Like most great origin stories, OMI’s roots are found in a “sad and important story.” In spite of numerous, high-quality tips, the SEC failed to act in a timely fashion to address the Madoff financial fraud. The Commission’s jarring lack of a response, in spite of receiving high-quality tips from Harry Markopolos and others, stimulated both internal soul-searching and external criticism. As one author put it, “The SEC’s investigation of Madoff was a failure of colossal proportions.”

Although the SEC’s 2009 Inspector General Report on the Commission’s role in the Madoff scandal is “more recitation than analysis,” from it one can identify two critical failures on the part of the agency—the first was cultural in nature, the second process-oriented. OMI represents an attempt to break both traditions to align the SEC of the future for more effective and timely intervention.

---


12. Id. at 628.


15. Langevoort, supra note 2, at 914.


17. Langevoort, supra note 2, at 901.
A. Cultural Failings at the SEC

The SEC has a terrible track record in regards to its attitude toward whistleblowers and tipsters. Whistleblowers, of course, are a thorny bunch. They are, as Fred Alford, a Maryland sociologist, has observed, generally not the kind of people with whom you want to have a beer.\(^{18}\) Understandably but unforgivably, the SEC has repeatedly shown disdain if not outright hostility when confronted with tips about fraudulent schemes within its regulatory purview when those tips come from individuals rather than highly respected Self-Regulatory Organizations.

Just as corporations have individual cultures which influence the actions of their agents,\(^{19}\) so to do administrative agencies. In the SEC’s case, its traditional culture has proved an impediment to receiving and processing information from outside sources.

In the Madoff scandal, the SEC simply did not take whistleblower allegations seriously. The IG’s Report indicates that SEC personnel, in a variety of offices and over a period of years, thought that a complaint from someone other than a Madoff client simply was not worth pursuing. Staff members “quickly made the judgment that [whistleblower Harry Markopolos] was obnoxious and self-absorbed, deep into his own personal crusade against Bernie Madoff,” which led to less “attention” being paid “to the underlying argument” the whistleblower had advanced.\(^{20}\) Cultural roadblocks meant that the SEC staff failed to discern how truly different the complaints raised by Madoff Whistleblowers were from other tips that the Commission received.

The Madoff scandal is not the only instance in which the SEC has demonstrated a poor culture for responding to whistleblowers. For the decade between the passage of Sarbanes–Oxley and the roll-out of rules under Dodd–Frank, the first federal avenue for whistleblower complaints was the Occupational Safety and Health Administration (OSHA). Even though dozens, if not hundreds of tips regarding financial fraud were being generated by Sarbanes–Oxley (SOX) discrimination complaints, the SEC abdicated responsibility for follow-up investigation. Its officials indicated that they wanted to leave the issue of whistleblower complaints to OSHA.\(^{21}\)

---

whistleblower’s identity to counsel for the company for which the whistleblower worked.22

Clearly, the SEC’s cultural failings have led the agency to miss multiple opportunities to leverage an increase in information about financial fraud into more effective regulatory oversight.

B. Process-Oriented Failings

The second set of failings on the part of the SEC regarding the Madoff scandal had to do with bad process. There was a tremendous lack of coordination in the SEC’s responsiveness and follow-up to Madoff-related tips. Two different SEC offices were investigating Madoff at one point, and learned of their parallel inquiries from the subject of the investigation.23 The SEC’s processes failed to recognize that repeat complaints involving the same essential entities and accused wrongdoers were a sign of something worthy of a follow-up. Responses to tips were delayed, at times without explanation.24

SEC personnel assumed resources would not be available to conduct follow-up investigations, without conducting even basic triage of tips and complaints to decide which ones could be investigated at a reasonable or feasible cost. They also narrowly confined the scope of their inquiry of Madoff to align with the specialty of the investigators (looking only at the possibility of front-running).25 SEC Regional Office investigators gave no consideration to joining forces with examiners from other offices, in spite of their suspicions regarding “Madoff’s performance and returns.”26

C. Yet Another Piece of Evidence that the SEC is “Captured” by Wall Street?

Reinforcing both its cultural and process-oriented failings in the Madoff affair is the likelihood that the SEC has been the victim of “regulatory capture.” It has long been criticized for being too cozy with the industry it regulates and relying excessively on information provided by that industry in its enforcement investigation.

The modern American investment market, perversely, does a poor job of allocating capital to businesses—instead, profits are generated

23. MADOFF OIG, supra note 1, at 34.
24. Id. at 29.
25. Id. at 30.
26. Id. at 32.
primarily through the secondary market.27 These profits, however, are massive. As the regulator of an incredibly wealthy sector, the SEC is particularly vulnerable to influence by the firms over which it exercises oversight.

The SEC’s cozy relationship with the industry it regulates has been enhanced, some argue, by the Commission’s strong push to receive cooperation from the targets of its investigation. Through a “darker lens,” this “can imply a quiet agreement between a firm and its regulator, in which the firm acquires leniency in exchange for assisting Enforcement staff . . .”28

Moreover, SEC attorneys know that their best employment prospects after government service include working for the very firms that represent the targets of governmental investigations: “[T]hese attorneys know that the legendary knights of so many crusades are now the elites of the securities enforcement defense bar, which may incline ambitious SEC lawyers to follow the same path.”29

Critics argue that “the problem” at the SEC is not “simply with the particular staff members involved in the fiasco,” but rather a broader and more “insidious form of corruption inherent in the SEC’s culture, whereby what happens inside the agency is largely driven by the desire of top officials to cultivate lucrative job opportunities on Wall Street when they leave.”30

III. TEMPLATES

A. The Federal Approach to Intelligence

In addition to considering OMI’s creation in light of the SEC’s historical approach to handling tips, it is worthwhile to situate OMI against the broader background of federal intelligence activities. Federal intelligence activities have long been bedeviled by expectations that are too high or too low31 and by a failure to grasp the importance of educating the public, not just the government’s top decision makers,

30. Langevoort, supra note 2, at 900; but see generally David Zaring, Against Being Against the Revolving Door, 2013 U. ILL. L. REV. 507 (2013) (arguing that the explanatory value of the revolving door indictment is overstated).
about the role and limits of intelligence activities.32

1. The Intelligence Cycle

The cornerstone of intelligence is the concept of an intelligence cycle: the “process by which information is acquired, converted into finished intelligence, and made available to policymakers.”33 Different sources would list different steps in the cycle, but five are typically identified: (1) planning and direction, (2) collection, (3) processing, (4) analysis and production, and (5) dissemination.34 Here, collection means the “purposeful acquisition of any information that might be desired by an analyst, consumer, or operator.”35 Analysis “involves the integration of collected information—that is, raw intelligence from all sources—into finished intelligence” products.36 A simpler, four-stage formulation would involve the generation of intelligence requirements, collection, analysis, and dissemination.37 The feedback mechanism following dissemination and prior to the adjustment of the next round of requirements is critical to the success of intelligence and requires regular “customer assessment of intelligence value.”38

The intelligence cycle provides a formal structure and discipline for intelligence activities.39 Without a cyclical and formal approach to intelligence, there is the danger that intelligence functions can become “disjointed,” representing no more than a “series of discrete events” as opposed to a “reinforcing cycle between intelligence collector, analyst, and consumer.”40 The cycle provides insurance of an “integrated and holistic system,” with parties responsible for “each stage of the cycle . . . accountable to the others in a non-linear fashion.”41 The cycle makes intelligence a process, rather than an event.42

Figure One depicts visually an example of the intelligence cycle, in this case from the FBI.
2. The Shift to Bayesian Techniques

Traditionally, federal intelligence activities made "little use of either machines or formal methods." Things have changed. As one former Soviet intelligence analyst observed, "We're all Bayesians now." Bayesian analysis is a term used to "describe both an inclination and a process to update subjective probabilities in light of new evidence."

What does this mean in the setting of intelligence? First, one would ask the question of interest—for instance, how likely is a terrorist attack? Analysts would then identify the many paths that could unfold to lead to an attack, focusing on "indicators that rank higher in 'uniqueness'"—that is, those indicators that could only be explained by reference to the outcome event—and considering the "visibility" of different indicators, meaning whether particular indicators could be measured by intelligence capabilities.

The Bayesian approach to an intelligence problem "becomes an assessment of conditional probabilities"—the baseline assessment of a

---

44. GREGORY TREVERTON, INTELLIGENCE FOR AN AGE OF TERROR 11 (2009).
45. Id.
46. Id.
47. Id. at 41.
48. Id. at 42.
49. Id. at 43.
group’s potential to launch a terrorist attack is tracked with “each available indicator increas[ing] or diminish[ing] that baseline assessment.”

3. The Unification of Intelligence and Adaptive Operations

Among the major changes initiated after the horrific attacks of 9/11 were centralization (including the creation of a National Intelligence Director and steps aimed to reduce overlap and duplication in intelligence activities) and the creation of a National Counterterrorism Center (NCTC).

These changes continued a pre-9/11 merger of intelligence and operations. The CIA created its Counterterrorism Center (CTC) in 1986 to serve as a “nexus of intelligence and covert action.” Operators and analysts were “merged ... under the same command,” and “work[ed] together to identify, track, and defeat the terrorist entity.”

The 9/11 Commission recommended enhanced unification of “intelligence and operational planning.” This is part of a broad trend to integrate intelligence capabilities into operational functions, recognizing the “symbiotic” relationship between the two.

B. Market Intelligence in the Business World

A second template for the OMI is the use of market intelligence in business circles—typically something one hears about from management consultants. Market intelligence “helps organizations understand their business environment, compete successfully in it, and grow as a result.” A market intelligence unit “collects information about market players and strategically relevant topics and processes it into insights that support decision-making.” It builds on traditional concepts of “business intelligence” and “competitive intelligence.”

50. Id.
51. Id. at 82–83.
52. CRUMPTON, supra note 31, at 121.
53. Id. at 122.
57. Id.
58. Business intelligence has sometimes “earned ... a shady reputation” and been “narrowly perceived as keeping an eye on the competition.” Id. (internal quotations marks omitted).
Broadly defined, market intelligence activities were pursued by 76% of companies in one survey of 989 firms, and of those firms surveyed without such a function, 1/3 planned to launch one within the next year.59 A typical market intelligence unit would consist of thirteen staffers.60

Market intelligence has a variety of uses for business firms, including strategic planning, marketing, sales and account management, innovation and product management, and supply chain management.61 Market intelligence functions can provide early warning by identifying "weak signals" of business shifts, whereas management might typically focus only on strong signals.62

The keys to a successful market intelligence activity include a small number of organizational layers between the market intelligence function and the firm’s CEO, the regular production of “deliverables” by the MI unit, and centralized and larger MI activities.63

1. The Market Intelligence Cycle

As in the military and defense settings, the concept of a “cycle” distinguishes market intelligence from simple competitive espionage.64 One description involved six stages: (1) needs analysis, (2) covering secondary information sources, (3) primary research, (4) analysis, (5) delivery, and (6) utilization and feedback.65 Among the most important of these steps is the first—needs analysis. It is wrong-headed to assume “that the management of a company knows what information the company will need.”66

Just as military and security intelligence exploits new technologies, tools, and advanced statistical techniques, market intelligence does the same. For instance, the content of web sites can be “mined” using algorithms to generate useful intelligence.67

59. Id. at 22.
60. Id. at 28.
61. Id. at 20.
62. Id. at 138.
63. Id. at 31–32.
64. Id. at 10 (“Processing business information into actionable insights that help organizations understand, compete and grow in their market is a cyclical process.”).
65. Id. at 63, fig. 5.1.
66. Id. at 66.
67. See, e.g., Danxiang Ai et al., Web Content Mining for Market Intelligence Acquiring from B2C Websites, 4256 LECTURE NOTES IN COMPUTER SCIENCE 159 (2006).
C. Market Intelligence in the SROs

Perhaps the most direct parallel to OMI’s new portfolio is FINRA’s “Office of Fraud Detection and Market Intelligence” (OFDMI), formed as the result of the combination of the NYSE and FINRA insider trading programs. OFDMI was created in 2009 to investigate and refer potential fraudulent matters, with a focus on insider trading and Ponzi schemes, to the SEC or federal law enforcement agencies. By the end of its first year, OFDMI had 130 staff members. Its three teams—the Central Review Group, Office of the Whistleblower, and Insider Trading and Fraud Surveillance—are responsible for the centralized intake and evaluation of regulatory filings and investor complaints.

In 2010, FINRA’s OFDMI referred more than 550 matters to the SEC, including 244 insider trading cases. OFDMI’s work is supported by “specialized computer software,” known as the Securities Observation News Analysis and Regulation or SONAR system. OFDMI is a “high-tech, specialized unit that uses artificial intelligence and dozens of analysts to comb through SEC filings, trading records, press releases and its own database of prior investigations to look for suspicious trading.”

---


72. Scott, supra note 69, at 4.


74. Montagno, supra note 70, at 595.


IV. OMI

A. Mission

OMI’s responsibility, according to Enforcement Chief Robert Khuzami, would be the “analysis, risk-weighing, triage, referral and monitoring of the extraordinary number of tips, complaints and referrals that the SEC receives each year.” OMI would exploit the “information tapestry” available to the SEC. It would be a “different sort of specialized unit.”

B. Capabilities & Activities of the OMI

1. Role of the OMI

OMI’s first role is as the initial entry point for whistleblower tips. OMI uses a variety of tools to “blend the public complaint information that formerly came in through our Enforcement Complaint Center with the complex market data provided by the self-regulatory organizations.” OMI would serve as the principle entity to conduct “triage and develop tips and leads to get that information to the right people within the Division [of Enforcement] in real time.”

All tips received by the SEC’s Division of Enforcement are now channeled to OMI, which reviews those complaints and when triage suggests further investigation is warranted, assigns the complaint to a Regional Office or specialized unit within the Division of Enforcement. A complaint that does not merit investigation would be designated NFA (no further action), though NFAs would be reviewed a second time and might be referred to “an external government agency or other agency for action.” The SEC’s Office of the Whistleblower (OWB) could also trigger expedited triage of a particularly credible tip


79. Khuzami, supra note 77.

80. Id.

81. Id.


83. Id.
2. OMI's Technology

In addition to its triage and referral role, OMI would "proactively identify market practices and activities that pose risks to investors and assess how to best address those practices and activities." OMI generates a daily intelligence report distributed within the SEC.

Technologically, OMI's activities would be facilitated through the construction of a "state-of-the-art data collection, surveillance, and analytics room." The room includes Bloomberg terminals and real-time stock pricing monitors. All of the "plumbing" was brought into one place.

OMI's new systems would come to replace the previous SEC "Enforcement Complaint Center," which has been described as a "fancy name for an e-mail box at the SEC where the public could send tips." This existing e-mail box would be retired in favor of a web-based form that tipsters could fill out on-line, with data feeding into systems allowing OMI to "audit the workflow on an ongoing basis" and "generate red flags if matters deemed significant later 'die on the vine.'" Importantly, the database would be accessible to all 2,300 SEC employees, who could access tips and obtain updates on the progress of investigations launched in response. The new system cost the SEC some $21 million.

The new system for receiving complaints is certainly an

84. Id.
85. Sporkin, supra note 78.
91. Id.
92. Lynch & Goldstein, supra note 89.
93. Id.
improvement. The SEC’s former “Complaint Center,” depicted in Figure Two, contained a link to an e-mail address, enforcement@sec.gov, which was immediately followed by the admonishment, “Please do not use this email box for general comments or questions.” If the goal of a site is to recruit tipsters, this somewhat unwelcoming tone runs contrary to that objective. The improved version in Figure Three, is a much more modern system. After logging in, a tipster checks various boxes and provides free-form responses to various questions. Importantly, this helps channel a tip into a usable format. Whistleblowers, left only with an e-mail address to contact, may often do themselves a disservice by failing to provide sufficient detail or by selecting e-mail “handles” that undermine their standing in the eyes of SEC attorneys—like one whistleblower, who used the e-mail address bountyman@aol.com and described the subject of his email “Application for Award of Bounty” (at a time when bounties were not available in his case). The new system also allows the tipster to upload supporting documentation to their complaint.

Figure Two: Old SEC “Complaint Center”

---


95. Rapp, supra note 22, at 127.

3. Staffing

OMI staff initially consisted of around thirty\textsuperscript{97} personnel—the results of cannibalizing the staff of the Office of Market Surveillance and the Office of Internet Enforcement.\textsuperscript{98} It would grow to include forty former traders, exchange experts, accountants, and lawyers,\textsuperscript{99} and eventually, apparently, to a staff of sixty-five.\textsuperscript{100} Public documents reveal that the Office's staff included a Bank Secrecy Act specialist,\textsuperscript{101} a dedicated FCPA liaison\textsuperscript{102} to the FCPA unit,\textsuperscript{103} and an embedded FBI Supervisory Special Agent.\textsuperscript{104}

\footnotesize
\begin{itemize}
  \item \textsuperscript{97} Carton, supra note 88.
  \item \textsuperscript{98} Id.
  \item \textsuperscript{99} Protess & Ahmed, supra note 86.
  \item \textsuperscript{100} Lori Walsh, LINKEDIN, http://www.linkedin.com/pub/lori-walsh/a/26b/218?trk=pub-pbmap (last visited Feb. 8, 2014).
  \item \textsuperscript{103} The SEC created its Foreign Corrupt Practices Unit in 2010 as part of a "big" and "bold" effort to enforce anticorruption laws in the financial setting. See Eric C. Chaffee, The Role of the Foreign Corrupt Practices Act and Other Transnational Anti-Corruption Laws in Preventing or Lessening Future Financial Crises, 73 OHIO ST. L. J. 1283, 1316 (2012).
  \item \textsuperscript{104} Dep't of Justice, Financial Crimes Report to the Public, FBI.GOV, http://www.fbi.gov/stats-
The Office added five FTE positions in 2011 to “strengthen” its “intelligence analysis function,” including its role in “risk assessment” and “strategic planning” to maximize the Commission’s “strategic, swift, smart and successful” investigations. The Office added twenty-eight staff members in the 2012 Fiscal Year budget request. The Commission’s FY2014 budget request sought twenty-six new positions to “strengthen the intelligence analysis function,” including staffing TCR points-of-contact in the SEC’s eleven regional offices. These technological responses and increased staffing are essential in light of the rapid increase in tips expected in the aftermath of the adoption of bounty rewards in the Dodd–Frank Act. Bounties have caused a spike in tips from twenty a day, to more than 200 a day, and OMI itself has generated seven quality tips a day.

4. Future Plans

Initial technology would be supplemented as time progressed through the support of MITRE, a quasi-governmental advanced technology operation. MITRE is assisting the SEC in developing its OMI technological platforms, and is planning an “artificial intelligence upgrade to help connect tips and complaints that might not appear related.” These systems will support the use of statistics to “trace connections” between tips, syncing with the intelligence community’s increased interest in Bayesian techniques.

While the exact details of MITRE’s contribution remain undisclosed, some hint is provided by the research projects in the area conducted by MITRE. For instance, it published a study entitled Evidence-Based

services/publications/financial-crimes-report-2010-2011. The first agent assigned to OMI, Jeffrey Horner, is an “accountant who worked for audit giant PriceWaterhouseCoopers before joining the [FBI] in 2004.” Lynch & Goldstein, supra note 89.


109. Carton, supra note 90.


111. Carton, supra note 90.

112. Protess & Ahmed, supra note 86.
Analysis for Financial Data which aimed to "conduct time series analyses of known transactions of interest to law enforcement personnel, regulators, and intelligence analysts in order to identify non-accounting evidence that can be correlated with those transactions." By "non-accounting evidence" MITRE means "corporate filings, public statements, and press coverage from 24 months prior to the transaction to 36 months after." The study would seek to identify "indicators...that correlate to offenses" and use "data visualization tools and other techniques" to facilitate use of that intelligence in enforcement activities.

MITRE's contribution suggests that OMI is embracing the Bayesian approach pursued by federal intelligence activities in the defense and security contexts. The Bayesian intelligence approach in the financial fraud context would look at the timing of various activities and focus both on unique indicators (those that are only associated with financial fraud) and on visible indicators (those that can be measured). This approach will likely draw on recent research suggesting that a variety of data mining techniques—such as "logistic models, neural networks, the Bayesian belief network, [and] decision trees"—can provide effective tools for fraud detection.

D. Leadership

The Office's first leader, Thomas Sporkin, was a "rising star" and the son of "perhaps the most famous SEC enforcement director," Stanley Sporkin. The Washington Post quoted one securities lawyer as observing, the "Sporkin family is to SEC enforcement what the Manning family is to NFL football."
An intelligence activity should be led by someone with strong communication skills and the ability to "lead up" the chain of command. Intelligence activities should be directed not just by someone with the usual leadership skills, but also a persuasive style that can market the intelligence function "both towards top executives and to interest groups across the organization." Leadership itself is more important than hands-on experience in the day-to-day intelligence work.

Sporkin's experience as the SEC's Deputy Chief of the Office of Internet Enforcement was particularly relevant given OMI's emphasis on exploiting advanced technological tools to conduct its oversight activities.

In 2013, Vincente Martinez took over the leadership of OMI. A former SEC Staff Attorney and Senior Counsel, he had left the SEC to become director of the Commodities and Futures Trading Commission whistleblower office.

IV. PROGNOSIS AND INITIAL SUCCESSES

A. Reasons for Caution

OMI's launch has not been without hiccups. An Inspector General Report in January 2013 criticized the office for lacking a "written policy" to cover the number of days a tip remained in "manual triage." Although OMI's responses were found to be timely, the Office lacked a standard "for determin[ing] whether the response is prompt or not." Most critically, the IG found that OMI had "not established any performance metrics." The IG expressed concern that the absence of performance metrics could impede performance and lead to "unnecessarily long response times."

In the time since, OMI has addressed these concerns. Two more significant—and related—questions surround any effort to predict the efficacy of OMI in the coming years.

First, intelligence activities in the national security and business sense have both embraced the notion of a cycle, in which finished products help feed into the identification of new intelligence priorities, the

120. HEDIN ET AL., supra note 56, at 102.
121. Carton, supra note 90.
123. SEC OIG, WHISTLEBLOWER REPORT, supra note 82, at 17.
124. Id.
125. Id. at 20.
126. Id. at 17.
allocation of collection resources, and future intelligence activities. OMI was stood up in response to past failings but perhaps with less than clear direction on what the SEC’s intelligence priorities were or should be. The initial fanfare paid to OMI concentrated on its tools, rather than its missions. One wonders whether intelligence requirements, as opposed to technological capabilities, are driving the development of the Office. As other federal agencies have developed intelligence functions, such as the FBI after 9/11, those agencies have also struggled to overcome “structural and cultural” obstacles to the development of an integrated intelligence cycle. At the SEC, there are no doubt similar obstacles, but the larger area of concern is that OMI has not yet articulated a self-identity based on the feedback cycle essential to effective intelligence.

What would a meaningful intelligence cycle look like for OMI? First, some entity or actor within the SEC must be given tasking authority—the institutional power to formulate intelligence priorities. While OMI appears to have inferred its priorities from past SEC failures and current enforcement activities, focusing, as discussed in the next Part, on high-concern areas like insider trading and microcap fraud, it is not yet clear where the Office’s tasking authority resides. Alternatively, to the extent that OMI has been structured primarily as a processing activity for tips, the danger is that it will lack focus—concentrating only on reactive processing rather than engaging in disciplined requirements-driven analysis that marshals all available information to generate actionable intelligence deliverables.

To some extent, OMI operates in an environment for which the most apt exemplar is not military intelligence or the all-source activities of the Central Intelligence Agency, but rather the National Security Agency, responsible for analysis related to the intercept of communications or “signals intelligence.” The NSA deals with an “enormous” “flow of data,” and the “key to success” is the careful “tailor[ing]” of its activities according to “targeting priorities” identified by its intelligence community customers. Similarly, the volume of data surrounding

---

127. CUMMING & MASSEY, supra note 37, at 27.
128. It is possible such a concept has been generated internally, but the author was unable to find any public reference to a cycle of analysis applicable to the OMI, including in the SEC’s various statements on the Office, the Commission’s strategic plan, http://www.sec.gov/about/secstratplan1015.pdf, and its Enforcement Manual. SEC Div. of Enforcement, Enforcement Manual (2012), available at http://www.sec.gov/divisions/enforce/enforcementmanual.pdf. A search of SEC documents available on the Commission’s web site for “intelligence cycle” generated no hits.
129. CUMMINGS & MASSEY, supra note 37, at 39.
131. John Cary Sims, What NSA is Doing . . . and Why It’s Illegal, 33 HASTINGS CONST. L. Q.
financial market activity under the SEC’s authority is massive.\(^{132}\) Without a mission tailored around enforcement “targeting priorities,” OMI’s effectiveness will be undercut.

On a related note, the decision to carve an intelligence apparatus out of the Division of Enforcement creates a potential danger that intelligence will become disconnected from the enforcement operational activities it is meant to serve. In the national security setting, recent changes have shifted intelligence into operational activities, rather than carving it out. Will OMI be evaluated based on how well it generates products which appear to reflect “intelligence analysis”? Or, as would be proper, on the degree to which its activities facilitate enforcement success? While the full staffing of OMI is not publically available, the fact that OMI contains liaisons to various other units (and that regional offices will be hiring or appointing liaisons to OMI) may mitigate this concern. These regional liaisons may help to ensure that OMI’s products remain connected to the SEC’s operational-level enforcement activities.

Moving forward, OMI’s strategic direction, first and foremost, should embrace the notion of an intelligence cycle and that cycle should specify the various entities responsible for each step in the intelligence process. Figure Four represents a suggested vision for OMI. Metrics are essential—but OMI should go beyond metrics surrounding how quickly it processes information and develop metrics based on the impact of its intelligence activities.

---


OMI should also consider adding to its activities techniques and tools employed by other intelligence analytical operations. For instance, OMI could create a "red cell." A team could be assigned to "think unconventionally about the full range of relevant analytical issues," taking an "‘out-of-the-box’ approach" and producing deliverables "intended to provoke thought rather than to provide authoritative assessment."

133. The Director of National Intelligence was required by law to "establish a process and assign an individual or entity the responsibility for ensuring that, as appropriate, elements of the intelligence community conduct alternative analysis (commonly referred to as ‘red team analysis’) of the information and conclusions in intelligence products." Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, § 1017 (2004). For a useful discussion of red team analysis, see Mark Mateski, Red Teaming: A Short Introduction, REDTEAMJOURNAL.COM (June 2009), http://redteamjournal.com/papers/A%20Short%20Introduction%20to%20Red%20Teaming%20(1dot0).pdf.

conceive and design a Ponzi scheme or an insider trading arrangement designed to avoid detection.

B. Success Stories

Initial stories have emerged describing some of OMI’s successes. OMI participated in an insider trading probe netting a trader named Garrett Bauer and his tipster, attorney Matthew Kluger, who had worked at New York law firms including Cravath, Swaine and Moore, LLP, and Skadden, Arps, Slate, Meagher and Flom, LLP, but ceased providing tips at some point out of a fear of detection. The scheme resumed after Kluger moved to the Washington, D.C. office of the Silicon Valley firm Wilson, Sonsini, Goodrich and Rosati, LLP. Between 2006 and 2011, the two men invested $109 million and made over $32 million in profits, avoiding detection through a variety of techniques including the use of pay phones and throwaway cellular telephones. OMI examined the trades of Mr. Bauer and identified a correlation with mergers on which Kluger’s firm, Wilson Sonsini, had provided counsel.

A second publicized success story involved OMI’s use of “enhanced techniques” to scrutinize microcap stocks and identify dormant shell companies employed as part of pump-and-dump schemes. This led to a trading suspension order affecting 379 companies, the largest such order in SEC history.

The details of OMI’s contributions to these investigations are not available, but the fact that the Office has been credited in some of the more high profile enforcement actions of the last two years is a positive sign.

C. A New Hope?

These success stories may hint to the potential positive effects of the OMI. At least two important positive consequences may flow from the new Office’s activities.

First, the Office may help to break the traditional culture of resistance...
to outside information. OMI (and the related Office of the Whistleblower) staffers will be evaluated on how effectively they handle outside tips, at least in part. It is entirely understandable that, in the past, an SEC enforcement attorney would choose to pursue a “high value” tip generated by a respected SRO, rather than a tip received from a whistleblower with possibly questionable motives. Given resource limitations, an SRO tip would strike an attorney as much more of a sure thing. OMI, however, will be judged not just according to how it responds to the obviously valuable tip, but based on how it responds to tips from less traditional sources. This should provide hope that the SEC of the future will do a better job in identifying fraud in spite of tips coming in from unusual (and sometimes difficult) individual whistleblowers.

Second, the Office may help to build a new willingness on the part of the SEC to think about its regulatory portfolio along a longer time horizon. Donald Langevoort has suggested that the SEC may, due to resource limitations, have preferred to “fight the fires surrounding it” rather than “invest in a deeper knowledge base with, at best, long-term payoffs.” He fears that the SEC’s “internal culture” includes a “disinclination to know too much in ways that would destabilize beliefs that are adaptive in maintaining organizational coherence.”

The very absence of an “intelligence cycle” driving OMI’s mission may mean that OMI pursues open-ended questions that present unexpected answers which can help shape the future activities of the SEC. The SEC’s operations in the past have arguably been guided by simplistic performance metrics, such as the “need to have year-by-year increases in the number of cases opened, brought and settled,” which leads the Commission to avoid “the daunting and the costly.” As a result of the stand-up of OMI, we may come to see “far greater financial sophistication” introduced to the “agency’s thinking and training.”

V. CONCLUSION

How significant a shift OMI represents in the SEC’s internal organization remains open to question. Time will tell whether the creation of OMI and other new offices helps improve the SEC’s actual—and perceived—effectiveness.

139. Langevoort, supra note 29, at 1615.
140. Id.
141. Langevoort, supra note 2, at 906.
142. Id. at 910.