SEC Enforcement: Past, Present And Future
By Brian Rubin and Gregory Amoroso
December 4, 2017, 1:07 PM EST

In Dan Brown’s latest best-seller, “Origin,”[1] he explores the questions: (1) Where do we come from (meaning, how did life get formed)? and (2) Where are we going (or, how will we evolve)? While the U.S. Securities and Exchange Commission Division of Enforcement’s “Annual Report, A Look Back at 2017”[2] is no “Origin,” "The Da Vinci Code" or even "Inferno," and co-directors of enforcement Steven Peikin and Stephanie Avakian are no Robert Langdon or Ambra Vidal (as far as we know), the SEC has raised "Origin"-like questions and answers, focusing on its “broad range of the significant enforcement actions, penalties and money returned to investors”[3] during fiscal year 2017 (where do we come from?) and its priorities for the coming year: “Our goal is to continue to protect investors, deter misconduct, punish wrongdoers and keep our markets the safest and strongest in the world”[4] (or, where are we going?). Without the chase scenes, conspiracy theories and symbolism of a Dan Brown book (and without a pile of murdered bodies), this article focuses on certain past priorities of the SEC and current (and possibly future) enforcement actions.

Main Street Investors

Those who buy Dan Brown books are Main Street investors (and some Wall Street traders), and those investors have become the focus of the SEC. As Chairman Jay Clayton stated, one of his core guiding principles is that “Our analysis starts and ends with the long-term interests of the Main Street investor.”[5] As part of that focus, on Sept. 25, 2017, the SEC announced the creation of the Retail Strategy Task Force.[6] In its announcement, the SEC said the task force was designed to “develop proactive, targeted initiatives to identify misconduct impacting retail investors.” In defining “retail,” Avakian indicated that it’s not just related to addressing Ponzi schemes and microcap or offering fraud, but “we are also thinking about conduct that occurs at the intersection of investment professionals and retail investors.”[7] Avakian went on to provide some specific examples of problems the SEC is seeing related to retail investors:

- Steering customers to mutual fund share classes with higher fees when lower-fee share classes are available;
- Abuses in wrap-fee accounts, such as failing to disclose the additional costs of “trading away” and purchasing alternative products that generate additional fees;
• Investors buying and holding short-term products such as inverse exchange-traded funds;
• Problems in the sale of structured products, including failing to fully and clearly disclose fees, markups and other factors negatively impacting returns; and
• Abusive sales practices like churning and excessive trading.[8]

Peikin explained the importance of protecting the retail investor when he said, “By dedicating additional resources and expertise to developing strategies to address misconduct that victimizes retail investors, the division will better protect our most vulnerable market participants.”[9]

True to this message (which does not need to be deciphered using a Ph.D. in symbology), the SEC has brought several enforcement actions during the past year that attempt to remedy “wrongs” allegedly perpetrated against retail investors. Specifically, some of these SEC enforcement actions include the following:

• Thirteen individuals were charged with a cold-calling scheme that purportedly bilked more than 100 victims out of more than $10 million through high-pressure sales tactics.[10]

• Twenty-seven individuals and entities were charged with various alleged stock promotion schemes that left investors with the impression they were reading independent, unbiased analyses on investing websites while writers were being secretly compensated for touting company stocks.[11]

• A firm settled an action that it improperly charged advisory fees for services it wasn’t performing, recommended more expensive share classes when less expensive share classes were available, and charged excess fees due to miscalculations and billing errors by the firm. The firm agreed to pay more than $97 million in disgorgement and penalties to settle the commission’s claims.[12]

• A firm settled an action that it improperly made unsuitable recommendations to its advisory clients related to investments in single inverse ETFs. The firm agreed to pay an $8 million penalty and admit wrongdoing to settle the charges.[13]

• Two registered representatives were charged with being engaged in a fraudulent “in-and-out” trading strategy that was unsuitable for customers in order to generate hefty commissions for themselves.[14]

While the SEC does not have Robert Langdon’s code-breaking skills to protect Main Street investors and to identify potentially problematic activity, it does have data analytics. As Avakian has stated, the SEC wants “to think strategically, at a high level, about what to look for, how to do it, and how to efficiently pursue it. There are all sorts of ways to use technology to slice and dice data and apply analytics to look for all kinds of problems — by product, by investor type, by location, by sales or trading practice, by fee, you name it. There are also other tools and techniques that can be used across data sets to identify suspicious activity, make connections, and aggregate and analyze information.”[15]

**Takeaways:** Given that the protection of Main Street investors appears to be one of the SEC’s core areas of focus, firms may want to replicate or clone the SEC’s activities (and that is not an "Origin" spoiler alert) (or is it?).[16] For example, firms may want to identify their “Main Street investors.” Firms may
then consider using analytics similar to what Avakian discussed to review these investors’ types of investments, the fee structures used in obtaining and maintaining these investments, and the potential risks that could arise from these types of investments.

**Cybersecurity**

In addition to Robert Langdon and Ambra Vidal, one of the other stars of "Origin" is a supercomputer named Winston (and the book even pays homage to the computer in “2001: A Space Odyssey,” which was named HAL because, as every nerd knows, each letter occurred alphabetically one letter ahead of IBM). While the SEC does not have its own Winston (as far as we know) (and as far as the SEC staff know), the SEC did announce the creation of a cyber unit in September.[17] The cyber unit is tasked with ferreting out cyber-related misconduct falling into one of three categories:[18]

1. Misconduct used to gain unlawful market advantage such as hacking nonpublic information to trade in advance of some announcement or account intrusions to conduct manipulative trading using hacked brokerage accounts;

2. Failures by registered entities to take appropriate steps to safeguard information or ensure system integrity in implementing related rules, such as Regulations S-P, S-ID and SCI. These rules require that firms have adequate procedures in place to address cyberthreats and that firms understand the risks and take reasonable steps to address those risks; and

3. Failure by public companies to make cyber-related disclosures, such as cyberrisks and incidents. These disclosures could be mandated by rules regarding management discussion and analysis as well as risk factor disclosures.

Although the cyber unit is relatively new, the SEC has been bringing cyber-related enforcement actions for some time, including a settled action a year ago against a dually registered firm for failing to adopt policies and procedures reasonably designed to protect customer data.[19] In that matter, a representative transferred data regarding 730,000 accounts to his personal server, which was ultimately hacked by third parties. Although the firm prohibited representatives from downloading or transferring data, the firm was sanctioned for failing to have reasonable systems in place that restricted access to customer data based on each employee’s legitimate business need. In addition, the firm failed to audit or test the portals allowing access to customer data, nor did it monitor or analyze employees’ access to those portals. The firm agreed to pay a $1 million penalty to settle charges related to its failure to protect customer information.

The SEC also brought two high-profile hacking cases where it alleged that individuals hacked into brokerage accounts of unwitting victims and made unauthorized trades.[20] The perpetrators then conducted trades in the same securities in their own accounts and profited from the artificial price rise. To put the case in perspective, Avakian said that, “Account takeovers are an increasingly significant threat to retail investors and it is exactly the type of fraud our new Cyber Unit is focusing on.”[21]

While the SEC has brought only a few cybersecurity enforcement actions thus far, in examinations it has been finding a number of deficiencies. In a recent speech, Peter Driscoll, then-acting director of the Office of Compliance Inspections and Examinations, cited some of the most common cyber-related deficiencies:[22]
• Policies and procedures that do not appear to be adequate. Specifically, the policies and procedures were not reasonably tailored because they:
  • provided employees with only general guidance;
  • identified limited examples of safeguards for employees to consider;
  • were very narrowly scoped; or
  • were vague and did not articulate procedures for implementing the policies.

• Regulation S-P-related issues where firms did not appear to adequately conduct system maintenance, such as installing software patches to address security vulnerabilities and other operational safeguards to protect customer records and information. Examples include:
  • stale risk assessments;
  • use of outdated operating systems that are no longer supported by security patches; and
  • lack of remediation efforts from penetration tests or vulnerability scans.

**Takeaways:** Given the SEC’s emphasis on these issues as well as the focus on this issue by hackers (not to mention Dan Brown’s instructions on how to break into a dead person’s smartphone), firms may want to consider taking the following steps:

• Establish and implement written, proactive cybersecurity policies that are regularly updated to account for the latest hacker tactics and techniques;
• Monitor the dark web for stolen firm information that could impact their business or their clients;
• Assess the scope of its data and adopt procedures to prevent intrusions and how to react to an intrusion if one takes place.[23]

**Who Done It (Or Who Should Be Held Liable for Doing It)?**

In "Origin," as in all of Dan Brown’s books, there are good guys (Robert Langdon and whoever his sidekick de jour is) and there are bad guys (and good guys who are really bad) (and vice versa), such as [REDACTED] in "Origin" (redacted to avoid possible spoiler). Similarly, at the SEC, the term “individual accountability” has been a buzzword that the SEC has been using for years in discussing its plans to bring tougher enforcement actions. With the appointment of Jay Clayton as the chairman, the SEC appears to be recommitted to holding individuals accountable. During his confirmation hearing, Clayton said that “individual accountability drives behavior more than corporate accountability.”[24]

The SEC appears willing to take on individuals, despite the fact that individuals who are charged may have to litigate against the SEC to try to protect their professional lives. In its 2017 annual report, the SEC said that “with more to lose, individuals are more likely to litigate with the Commission. But that price is worth paying.”[25] (Dan Brown couldn’t have written it better himself.)

**Takeaways:** Consequently, all persons in the securities business, from registered representatives and investment adviser representatives all the way up to board members, may need to be thinking about how they conduct themselves professionally. Individuals may want to focus on:

• What do they believe their jobs to be?
• What do the firm’s procedures say about their jobs?
• Whom do they supervise, if anyone, and how?
• Who supervises them, and how?
• How do they document their job performance?
• What do they do if they encounter red flags?

* * *

The prior administration focused on “broken windows” (which could be a good Dan Brown book title). The SEC under Clayton, however, has made it clear that the SEC is pulling back from that prosecutorial approach.[26] Instead, Clayton has said that he plans to focus on protecting “Mr. and Mrs. 401(k)” and vigorously monitoring cybersecurity issues.[27] Therefore, firms and individuals may want to proactively focus on these issues before the SEC shows up on their doorsteps. Or, as Dan Brown put it in "Inferno," “The decisions of our past are the architects of our present.”[28]

Brian L. Rubin is the Washington office leader of the Eversheds Sutherland litigation group and the head of the firm’s SEC, Financial Industry Regulatory Authority and state securities enforcement practice. He is a former deputy chief counsel of enforcement for NASD (now FINRA) and a former senior enforcement counsel at the SEC.

Gregory S. Amoroso is a securities litigation consultant in Eversheds Sutherland’s Atlanta office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.


[4] Id.


[16] It’s not.


[21] Id.


