Speech

The SEC Enforcement Division's Initiatives Regarding Retail Investor Protection and Cybersecurity

Stephanie Avakian, Co-Director, Division of Enforcement

Washington, D.C.

Oct. 26, 2017

Introduction

Good afternoon and thank you for inviting me to speak today. Before I begin, let me give the required disclaimer that the views I express here today are my own and do not necessarily represent the views of the Commission or its staff.[1]

With that, I am very happy to be here and to talk about some of what we are doing in the Enforcement Division. This has been a year of transition for us. In May, we welcomed Jay Clayton as our new Chairman. And, in June, Steve Peikin and I were named Co-Directors of the Enforcement Division.

While new leadership certainly brings about all sorts of change, one thing that will not change is the mission of the Enforcement Division – to protect investors. But how we protect investors – specifically, what we identify as our priorities and how we allocate resources to meet those priorities – is subject to change. And so Steve and I have used this time to step back and take a fresh look at what we are doing and ask ourselves: What are our priorities? Are we allocating our resources in the best way possible to address those priorities? Is there something we should change?

So, what are our priorities?

As all of you know, Enforcement has a very broad mandate – we cover a lot of ground across the securities markets. One need only look at our various units, task forces, and working groups, as well as the cases we bring, to get a sense of our landscape. At a high level, our greatest priorities and where we allocate our limited resources do not really change over time, and nor should they. We are always going to be focused on retail investors. These are often the most vulnerable market participants who are most in need of our protection. We are also always going to be focused on cyber-related issues, which are only continuing to increase in number and impact. Finally, we are always going to be focused on issues raised by the conduct of investment advisers, broker-dealers, and other registrants, on financial fraud and disclosure issues involving public companies, and on insider trading.

And that leads to the next questions: Are we allocating our resources in the best possible way to address those priorities? Is there something we should change?

Here, we do think there is more we can do to align our resources with two of our key priorities – specifically, retail and cyber. To be sure, we have long focused resources in both of these areas, but we think that some structural

change and strategic focus will enable us to better fulfill our investor protection mission. And so the Commission recently announced the creation of a Retail Strategy Task Force and a Cyber Unit.[2]

The Retail Strategy Task Force

First, the Retail Strategy Task Force. Of course, protecting the retail investor has long been at the heart of what we do in Enforcement. So how will this effort be different from our other efforts in this space?

In short, this group will look at the many ways that retail investors intersect with the securities markets and look for widespread misconduct. It will draw from our experience in the retail space and elsewhere to identify strategies that have worked well for us across all kinds of cases, particularly those in which we used data analytics and technology. It will then apply those strategies and investigative techniques more broadly to look for incidents of widespread misconduct targeting retail investors.

We are increasingly able to identify threats to retail investors – everything from registrant-based threats to microcap-based threats – through the use of data analytics. We want 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. We are going to look to the Task Force to identify those uses of data analytics that can be scaled more broadly, and that can be used in targeted ways to identify misconduct.

The Task Force will work with others in Enforcement – like the Office of Market Intelligence and our Center for Risk and Quantitative Analytics – as well as with others in the Agency – like the Division of Economic and Risk Analysis (DERA) – to consider ways to apply new tools and technologies, like text analytics and machine learning, to the vast amounts of trade and other data that we have, including the more than 16,000 tips, complaints and referrals that the Commission receives every year – to cover the broad landscape of conduct that directly affects the retail investor, in the most strategic and efficient way possible.

The Task Force will also work closely with the Office of Compliance, Inspections and Examinations (OCIE) as well as investigative staff across the Enforcement Division. While the Task Force will have a dedicated staff, it will not generally be responsible for conducting investigations. The idea is for them to develop ideas and strategies, and then apply and analyze the results of those ideas to identify areas where there are problems. As they identify issues, they typically will refer further investigative work to staff across the Division.

One of the questions that I have been getting is, what do you mean when you talk about "retail"? When you say "retail", folks often think immediately of Ponzi schemes and microcap or offering fraud. And these sorts of schemes invariably will fall within the Task Force's ambit. But when we talk about "retail" in this context, we are also thinking about conduct that occurs at the intersection of investment professionals and retail investors.

The issues we see in this space are extensive and often involve widespread incidents of misconduct, such as charging inadequately disclosed fees, and recommending and trading in wholly unsuitable strategies and products. Some more specific examples of some of the problems we are continuing to see:

- Investment professionals steering customers to mutual fund share classes with higher fees, when lower-fee share classes of the same fund are available.[3]
- Abuses in wrap-fee accounts, including failing to disclose the additional costs of "trading away" or trading through unaffiliated brokers,[4] and purchasing alternative products that generate additional fees.[5]
- Investors buying and holding products like inverse exchange-traded funds (ETFs) for long-term investment. These can be highly volatile products that are generally intended as a hedge against exposure to downward moving markets, and that face a long-term high risk of losing their principal.[6] Yet, we are increasingly seeing retail investors holding these products long-term, including in retirement accounts.[7]

- Problems in the sale of structured products to retail investors, including a failure to fully and clearly disclose fees, mark-ups, and other factors that can negatively impact returns.[8]
- And, abusive practices like churning and excessive trading that generate large commissions at the expense of the investor.[9]

These are examples of just some of the problems we have seen. We have brought a number of cases addressing these issues – many of which were found using technology and data analytics – but, of course, there is more out there. OCIE examiners consistently continue to identify issues, and we in Enforcement also continue to find misconduct.

The Task Force is going to be strategic in looking for widespread abuses that affect retail investors, and in thinking about how we approach these investigations and potential cases. We will look to the Task Force to consider these issues broadly and look for opportunities to send effective messages in a way that maximizes our efficiency and preserves our resources.

But enforcement alone is not enough. A critical part of investor protection is education. And part of the Task Force's mandate will be to focus on investor outreach, converting what they learn about problematic conduct into direct messaging to investors. They will work together with folks in our regional offices and others across the Commission – like the Office of Investor Education and Advocacy – to identify areas where targeted education and outreach efforts are likely to benefit investors. An educated investor is an empowered investor, and our goal is to empower investors so that they are able to make informed investment decisions.

As I said at the outset, we know there is more out there. The goal of the Task Force will be to find those problems and think creatively about potential solutions.

Finally, I want to address one question that we have received a lot since announcing our retail focus; that is, whether our enhanced retail focus means that we are allocating fewer resources to financial fraud or policing Wall Street. The answer to that question is simple: No, we are not. The premise that there is trade-off between "Wall Street" and "Main Street" enforcement is a false one. Outside of the retail area, we have continued to address misconduct by financial and other institutions of all sizes, and the Task Force will focus on issues across the spectrum of the securities industry and markets.[10]

The Cyber Unit

So now let me turn to the Cyber Unit, which is the first new specialized unit since the units were created as part of the Division's reorganization in 2010. The need for the Cyber Unit arises in large part from the increasing frequency with which we are seeing cyber-related misconduct affecting the securities markets, and also the increasing complexity of these cases. These cybersecurity threats come from a wide range of sources, including foreign and domestic hackers, traders and others who traffic in stolen market-moving information, prospective market manipulators, state-sponsored actors, and others. The work of these actors in many instances has been facilitated by easy access to the dark web marketplace as well as the use of digital currency, both of which make it harder to track the flow of funds involved in cyber violations.

We see our potential enforcement interest in cyber-related issues as falling roughly into three separate types of cases. First, are cases where cyber-related misconduct is used to gain some sort of unlawful market advantage. Some examples include:

- Hacking to access material, nonpublic information in order to trade in advance of some announcement or event, or to manipulate the market for a particular security or group of securities;[11]
- Account intrusions in order to conduct manipulative trading using hacked brokerage accounts;[12] and
- Disseminating false information through electronic publication, such as SEC EDGAR filings[13] and social media,[14] in order to manipulate stock prices.

We have brought a number of significant cases in this space, including cases that fit each of the fact patterns I just described. The volume and complexity of investigations of these types of schemes only continues to increase.

The second area of enforcement interest includes cases involving failures by registered entities to take appropriate steps to safeguard information or ensure system integrity. The Commission has adopted rules – such as Regulations S-P, S-ID, SCI and others – that, broadly speaking, require registered entities to have reasonable safeguards in place to address cybersecurity threats. These rules are risk-based and flexible, and require firms to understand the risks they face and take reasonable steps to address those risks.

While we have brought several cases in this area, we also coordinate very closely with OCIE on these issues.[15] As potential investigations of these issues present themselves, we consult with OCIE at the outset to consider the approach that makes the most sense based on the specific facts. Among other things, we consider whether an enforcement investigation is warranted, or whether the circumstances suggest that it might be more appropriate for OCIE to conduct an examination in the first instance. Often, depending on the issue, OCIE may be better positioned to take the lead, and areas where improvement is needed may be addressed efficiently and effectively through the deficiency letter process. Other times, an Enforcement inquiry is the best approach.

The third area of potential enforcement interest includes cases where there may be a cyber-related disclosure failure by a public company. We have not yet brought a case in this space. The staff of the Division of Corporation Finance (Corp Fin) has frequently reminded registrants that material information regarding cyber risk may be required in connection with disclosures mandated by the Commission's rules regarding Management Discussion and Analysis, as well as other items, such as Risk Factor disclosures. In an era where nearly every company is dependent on computer systems to operate their business, it is frequently necessary to provide meaningful and timely disclosures regarding cyber risks and incidents. These disclosures are often material on their own or necessary in order to make other disclosures, in light of the circumstances under which they are made, not misleading.[16] The guidance issued by the Corp Fin staff in 2011 is principles based and remains an important indication of how issues related to cybersecurity should be disclosed in SEC filings.[17] We recognize this is a complex area subject to significant judgment, and we are not looking to second-guess reasonable, good faith disclosure decisions, though we can certainly envision a case where enforcement action would be appropriate.

So why a Cyber Unit?

This is an area where we already have a substantial amount of expertise in the Division. Until now, many of the cyber cases the Commission has brought have been investigated by our Market Abuse Unit. In large part, the Market Abuse Unit developed this expertise because there is a fair amount of overlap in the technology skills and investigative techniques we use in serial insider trading schemes and in many of these cyber schemes.

So, even though we are already doing this work in a somewhat focused way, we think it makes sense to aggregate that experience and focus in a single unit for a couple of reasons. First, the risk that the cyber threat poses is so serious that we think it is critical that we have a group of people specifically focused on dealing with it. And, second, how we as a Division approach and deal with the enforcement interest in this space warrants a consistent, well-informed, and oftentimes, measured, approach; having a dedicated unit consider and address these issues will help us achieve this goal.

For some of the same reasons, we are also including within the responsibility of the Cyber Unit our focus on the distributed ledger technology space, also known as blockchain technology. For reasons similar to those I just mentioned with regard to cyber, the emerging issues presented by blockchain technology warrant a consistent, thoughtful approach – and the best way to do that is to centralize the expertise and the focus in a single unit.

As folks likely know, the Commission recently issued a Report of Investigation cautioning that offers and sales of digital assets by "virtual" organizations – often referred to as "Initial Coin Offerings" or "Token Sales" – are subject to the requirements of the federal securities laws, which can include the registration of securities offerings.[18] Blockchain technology presents many interesting issues and can of course present legitimate opportunities for raising capital. But, like many legitimate ways of raising capital, the popular appeal of virtual currency and blockchain technology can be an attractive vehicle for fraudulent conduct. We think that creating a permanent

structure for the consideration of these issues within the Cyber Unit will ensure continued focus on protecting both investors and market integrity in this space.

Conclusion

So I hope that gives you some sense of how we are thinking about our overall priorities and, more specifically, how we are allocating resources to further address two of our more critical priorities – protecting retail investors and addressing the threat posed by cyber-related issues.

Thanks very much for having me here today.

---

[1] The Securities and Exchange Commission, as a matter of policy, disclaims responsibility for any private publication or statement by any of its employees. The views expressed herein are those of the author and do not necessarily reflect the views of the Commission or of the author's colleagues on the staff of the Commission.

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

[3] Press Release 2017-165, *SunTrust Charged With Improperly Recommending Higher-Fee Mutual Funds* (Sept. 14, 2017), available at https://www.sec.gov/news/press-release/2017-165; Press Release 2017-98, *Barclays to Pay $97 Million for Overcharging Clients* (May 10, 2017), available at https://www.sec.gov/news/press-release/2017-98 ("*Barclays*"); *Cadaret, Grant & Co., Inc.*, Exchange Act Release No. 81274 (Aug. 1, 2017), available at https://www.sec.gov/litigation/admin/2017/34-81274.pdf; *Credit Suisse Securities (USA) LLC*, Exchange Act Release No. 80373 (Apr. 4, 2017), available at https://www.sec.gov/litigation/admin/2017/34-80373.pdf.

[4] Press Release 2016-143, *SEC Charges Investment Adviser With Failing to Clearly Disclose Additional Costs to Investors* (July 14, 2016), available at https://www.sec.gov/news/pressrelease/2016-143.html.

[5] *WFG Advisors, L.P.*, Exchange Act Release No. 78189 (June 28, 2016), available at https://www.sec.gov/litigation/admin/2016/34-78189.pdf.

[6] U.S. Sec. & Exch. Comm'n, Office of Investor Education and Advocacy, *Leveraged and Inverse ETFs: Specialized Products with Extra Risks for Buy-and-Hold Investors* (Aug. 1, 2009), available at https://www.sec.gov/investor/pubs/leveragedetfs-alert.htm.

[7] Press Release 2017-46, *Morgan Stanley Settles Charges Related to ETF Investments* (Feb. 14, 2017), available at https://www.sec.gov/news/pressrelease/2017-46.html.

[8] Press Release 2016-197, *SEC Charges UBS With Supervisory Failures in Sale of Complex Products to Retail Investors* (Sept 28, 2016), available at https://www.sec.gov/news/pressrelease/2016-197.html; Press Release 2015-238, *UBS to Pay $19.5 Million Settlement Involving Notes Linked to Currency Index; Case Is Agency's First Against an Issuer of Retail Structured Notes* (Oct. 13, 2015), available at https://www.sec.gov/news/pressrelease/2015-238.html.

[9] Press Release 2017-180, *SEC Detects Brokers Defrauding Customers* (Sept. 28, 2017), available at https://www.sec.gov/news/press-release/2017-180; Press Release 2017-2, *SEC Charges Two Brokers With Defrauding Customers* (Jan. 9, 2017), available at https://www.sec.gov/news/pressrelease/2017-2.html.

[10] *See, e.g.*, Press Release 2017-196, *Rio Tinto, Former Top Executives Charged with Fraud; Worldwide Mining Company Alleged to Have Inflated Asset Values* (Oct. 17, 2017), available at https://www.sec.gov/news/press-release/2017-196; Press Release 2017-171, *Telecommunications Company Paying $965 Million for FCPA Violations* (Sept. 21, 2017), available at https://www.sec.gov/news/press-release/2017-171; Press Release 2017-120, *SEC Charges Oil and Gas Company and Top Finance Executives with Accounting Fraud* (June 28, 2017), available at https://www.sec.gov/news/press-release/2017-120; *Barclays*, *supra* note 3.

[11] Press Release 2016-280, *Chinese Traders Charged With Trading on Hacked Nonpublic Information Stolen From Two Law Firms; Marks First Time SEC Charges Hacking Into Law Firm Computer Networks* (Dec. 27, 2016), available at https://www.sec.gov/news/pressrelease/2016-280.html; Press Release 2016-256, *IT Specialist Settled Charges of Insider Trading on Hacked Nonpublic Information* (Dec. 5, 2016), available at https://www.sec.gov/news/pressrelease/2016-256.html; Press Release 2015-163, *SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases; Hackers, Traders Allegedly Reaped More Than $100 Million of Illegal Profits* (Aug. 11, 2015), available at https://www.sec.gov/news/pressrelease/2015-163.html.

[12] Press Release 2016-127, *SEC Sues UK-Based Trader for Account Intrusion Scheme* (June 22, 2016), available at https://www.sec.gov/news/pressrelease/2016-127.html.

[13] Press Release 2017-107, *SEC Charges Fake Filer With Manipulating Fitbit Stock*, (May 19, 2017), available at https://www.sec.gov/news/press-release/2017-107; Press Release 2015-110, *SEC Freezes Profits From Scheme to Manipulate Avon Stock*, (June 4, 2015), available at https://www.sec.gov/news/pressrelease/2015-110.html.

[14] Press Release 2015-254, *SEC Charges: False Tweets Sent Two Stocks Reeling in Market Manipulation; Criminal Charges Also Filed* (Nov. 5, 2015), available at https://www.sec.gov/news/pressrelease/2015-254.html.

[15] *See, e.g.*, Press Release 2016-112, *SEC: Morgan Stanley Failed to Safeguard Customer Data* (June 8, 2016), available at https://www.sec.gov/news/pressrelease/2016-112.html; Press Release 2015-202, *SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach* (Sept. 22, 2015), available at https://www.sec.gov/news/pressrelease/2015-202.html.

[16] U.S. Sec. & Exc. Comm'n, Div. of Corp. Fin., *CF Disclosure Guidance Topic No. 2: Cybersecurity* (Oct. 13, 2011), available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[17] *Id.*

[18] Press Release 2017-185, *SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities* (July 25, 2017), available at https://www.sec.gov/news/press-release/2017-131.