Recent Legal Updates from Dechert

March 2018

Dechert LLP

Table of Contents

FINRA Issues FAQs on Rules Relating to Financial Exploitation of Seniors and Other Vulnerable Adults ..... Tab 1

SEC Chairman Issues Major Statement on Cryptocurrency and ICOs ..... Tab 2

SEC Enforcement Division Priorities Pertaining to Retail Investors and Cybersecurity ..... Tab 3

Dechert LLP

ON**POINT** / A legal update from Dechert's Financial Services Group

January 2018

FINRA Issues FAQs on Rules Relating to Financial Exploitation of Seniors and Other Vulnerable Adults

The Financial Industry Regulatory Authority (FINRA) has published frequently asked questions (FAQs) for complying with new FINRA Rule 2165 (Financial Exploitation of Specified Adults) and amendments to FINRA Rule 4512 (Customer Account Information) (collectively, New Rules).[1] The New Rules become effective on February 5, 2018.[2]

The New Rules were developed to provide FINRA member firms (Firms) with a mechanism for quickly responding to situations where a broker-dealer has a reasonable basis to believe that financial exploitation of vulnerable adults has occurred or will be attempted. Rule 2165 allows Firms to "place a temporary hold on a disbursement of funds or securities from the Account of a Specified Adult" if the firm has a reasonable belief regarding financial exploitation of a customer, while Rule 4512 requires Firms to make reasonable efforts to implement a "trusted contact" system into their customer accounts.

As background, the New Rules were proposed for comment in October 2015, in an effort to combat a growing problem of the financial exploitation of adults over 65. Following the comment period, FINRA submitted the proposed New Rules to the U.S. Securities and Exchange Commission (SEC) in October 2016, and the SEC approved a final version of the New Rules in February 2017. For further information, please refer to *Dechert OnPoint*, SEC Publishes for Comment FINRA Proposal to Combat Financial Exploitation of Seniors and Other Specified Adults.

A further effort to combat the financial exploitation of adults over 65 is making its way through Congress. On January 29, 2018, the House passed the Senior Safe Act, which encourages Firms to disclose suspected financial exploitation of seniors to appropriate agencies, by granting immunity from any civil or administrative proceeding for the disclosure if it was made by certain trained employees in good faith and with reasonable care.[3]

The FAQs cover three main topics: temporary holds under Rule 2165, the trusted contact requirement under Rule 4512, and disclosure requirements under Rule 4512.

Temporary Holds under Rule 2165

Temporary Holds on Transactions in Securities Not Permitted (Q.1.1)

Rule 2165 permits a Firm to place a temporary hold on the disbursement of "funds or securities" from the account of a ''specified adult,''[4] if the Firm reasonably believes that financial exploitation may be occurring. The FAQs distinguish between securities transactions and the disbursement of assets, including securities, and clarify that Rule 2165 does not apply to a customer's order to purchase or sell securities. Rule 2165 does, however, permit a Firm to place a temporary hold on the proceeds from a securities transaction if the firm reasonably believes the customer is being financially exploited.

Permissible Degree of Temporary Holds on Disbursements from Customer Accounts (Q.1.2, Q.1.3)

A temporary hold on a disbursement is also permissible in the case of a disbursement between different accounts at the same Firm.

The FAQs clarify that when questionable disbursements involve less than all of the assets of a customer, a "blanket hold" cannot be placed on the customer's entire account, and that each disbursement request should be analyzed individually. Even when a questioned disbursement involves all the assets of the account in question, the Firm must permit the transaction unless it reasonably believes financial exploitation is involved. The FAQs provide, however, that it is permissible for a Firm to place a temporary hold on an entire account while still permitting legitimate disbursements, provided that the Firm has "procedures reasonably designed to permit legitimate disbursements."

Extension of Temporary Holds (Q.2.1)

Rule 2165 limits a temporary hold to 15 business days after first placed by the Firm, with a possible extension of an additional 10 business days upon a Firm's internal review that supports a reasonable suspicion of financial exploitation.

The FAQs confirm that the expiration date can be extended beyond the above-mentioned periods, if requested by a state agency or regulator investigating the matter. A request from a state agency or regulator need not be a formal order. The Firm does not have to report such a request to FINRA, but should keep a record of the request.

Trusted Contact under Rule 4512

Qualifications for the Trusted Contact (Q.3.1)

Rule 4512 requires a Firm to make reasonable efforts to obtain the name of and contact information for a trusted contact for its customer accounts, who must be a natural person at least 18 years old. Importantly, FINRA notes in the FAQs that asking a customer for the name and contact information of a trusted contact is sufficient to satisfy the reasonable efforts requirement of Rule 4512. The FAQs clarify that FINRA does not expect Firms to verify the age of the trusted contact.

Except for age, the FAQs note that FINRA does not impose any other qualifications on a trusted contact and does not preclude "joint accountholders, trustees, individuals with powers or attorney and other natural persons authorized to transact business on an account from being designated as trusted contacts."

Application of Trusted Contact Requirement to All Non-Institutional Accounts (Q.3.2, Q.3.3)

The trusted contact requirement does not apply to institutional accounts as defined in Rule 4512, but it does apply to the accounts of non-natural persons that do not meet the definition of "institutional account" in the rule. In response to Firm's questions, FINRA clarified that any authorized agent (*e.g.*, an officer, partner, or trustee) can satisfy the "trusted contact" requirement, so long as the Firm provides the disclosure required by Supplementary Material .06(a) to Rule 4512.

The FAQs note that Firm can use trusted contact information, if provided, beyond situations involving suspected financial exploitation, and indicate that "the trusted contact is intended to be a resource for [Firms]" (for example, to discuss with the trusted contact relevant issues in accordance with Supplementary Material .06(a) to Rule 4512, as discussed further below).

Trusted Contact Requirement for Accounts in Existence Prior to Effective Date (Q.3.4, Q.3.5)

The FAQs clarify that Firms are not required to immediately obtain trusted contact information for existing accounts upon the effectiveness of the amendments to Rule 4512, but may do so when Firms update their account information, "either in the course of the [Firm's] routine and customary business or as otherwise required by applicable laws or rules." The FAQs note that Firms should make reasonable efforts to collect trusted contact information the first time they update existing account information after the February 5, 2018 effective date.

After a Firm's initial effort to collect trusted contact information, Rule 4512 requires Firms to make reasonable efforts to obtain or update such information for accounts subject to the periodic update

requirements of Rule 17a-3 under the Securities Exchange Act of 1934. With respect to accounts that are not subject to Rule 17a-3, the FAQs suggest that Firms consider asking customers to provide or update, as applicable, their trusted contact information periodically or when there is reason to believe that the customer's situation has changed.

In cases where a customer has multiple accounts, a customer can choose to designate a single trusted contact, or different trusted contacts for different accounts.

Required Disclosure to Customers and Permissible Disclosure to Trusted Contacts (Q.4.1, Q.4.2)

Supplementary Material .06(a) to Rule 4512 requires Firms to disclose in writing to their customers "at the time of account opening … that the [Firm] or an associated person of the [Firm] is authorized to contact the trusted contact person and disclose information about the customer's account to address possible financial exploitation, to confirm the specifics of the customer's current contact information, health status, or the identity of any legal guardian, executor, trustee or holder of a power of attorney, or as otherwise permitted by Rule 2165."

The FAQs confirm that Rule 4512 does not mandate any specific form of written disclosure – for example, the disclosure could be in an account application or a separate document provided to the customer, and may be in an electronic format. The FAQs state, however, that the disclosure must include the information specified in Supplementary Material .06(a) to the rule. The SEC confirmed that disclosures to a trusted contact are because they are made with the customer's consent or authorization and to protect against fraud or unauthorized transactions, or to comply with legal requirements. Nevertheless, the FAQs remind Firms that their written disclosure should be drafted so that a customer clearly understands that s/he is consenting to the Firm providing identified categories of information to the identified trusted contact.

Footnotes

1) Frequently Asked Questions Regarding FINRA Rules Relating to Financial Exploitation of Seniors (January 3, 2018).

2) FINRA Regulatory Notice 17-11: SEC Approves Rules Relating to Financial Exploitation of Seniors (March 2017).

3) Senior Safe Act, H.R. 2255, 115 Cong. § 1 (2018).

4) A "specified adult" under Rule 2165(a) is (A) a natural person age 65 and older or (B) a natural person age 18 and older who the Firm reasonably believes has a mental or physical impairment that renders the individual unable to protect his or her own interests.

This update was authored by:

K. Susan Grafton
Partner
Washington, D.C. / New York
T: +1 202 261 3399 / +1 212 698 3611
susan.grafton@dechert.com

Elliott R. Curzon
Partner
Washington, D.C.
T: +1 202 261 3341
elliott.curzon@dechert.com

Albert Jung
Associate
Washington, D.C.
T: +1 202 261 3350
albert.jung@dechert.com

Dechert LLP

ON**POINT** / A legal update from Dechert

December 2017

SEC Chairman Issues Major Statement on Cryptocurrency and ICOs

- U.S. Securities and Exchange Commission (SEC) Chairman Jay Clayton weighed in on cryptocurrencies and initial coin offerings (ICOs) in a major statement.
- Chairman Clayton explained that, while not all tokens may be securities under the federal securities laws, simply calling a token something else does not bring an offering outside the SEC's purview.
- "Key hallmarks" of tokens being securities include, in the SEC's view, when an issuer:
  - emphasizes the possibility for tokens to appreciate in value or
  - encourages a secondary market for tokens.
- Chairman Clayton's statement, along with recent SEC efforts to stop certain ICOs, indicate that increased enforcement activity in this area is likely in 2018.

On December 11, 2017, SEC Chairman Clayton issued an important public statement outlining his views on cryptocurrencies and ICOs. In his statement, Chairman Clayton provided a clearer view of the SEC's stance and offered the industry much awaited guidance on what, in the SEC's view, constitutes a security in the context of rapidly evolving digital assets. Chairman Clayton's remarks put the cryptocurrency and ICO community on notice that there will likely be further SEC enforcement activity in this area.

The year 2017 has seen increased focus on cryptocurrencies and ICOs from the SEC.[1] On July 25, 2017, the SEC issued an investigative report (The DAO Report) concluding that a digital token, which was issued by The DAO as part of an ICO to raise capital for innovative projects, was a "security" within the

meaning of the Securities Act of 1933 (Securities Act) and the Securities Exchange Act of 1934 based on the application of existing securities law principles.[2] Most recently, the SEC shut down ICOs by each of PlexCorps and Munchee Inc. (Munchee). On December 1, 2017, the SEC filed a complaint seeking a temporary restraining order and preliminary injunction to halt PlexCorps' ICO, alleging that PlexCorps had promised purchasers "outlandish rewards" in connection with its offering of PlexCoin tokens.[3] On December 11, 2017, the SEC issued a cease-and-desist order (Order) against Munchee to halt its ICO, as discussed in more detail below.[4]

Statement of SEC Chairman Clayton Puts Cryptocurrency and ICO Community on Notice

In his statement, Chairman Clayton noted that "concerns have been raised regarding the cryptocurrency and ICO markets."[5] While he acknowledged ICOs' potential to be "effective ways for entrepreneurs and others to raise funding," he also urged ICO investors to "exercise extreme caution and be aware of the risk that [their] investment may be lost."[6] Chairman Clayton's remarks are consistent with the 2018 priorities outlined by the SEC's Division of Enforcement (Division), which include a focus by the Division's new Cyber Unit on the misuse of distributed ledger technology and ICOs.[7]

For "Main Street" investors, Chairman Clayton provided a list of questions that potential investors should ask before participating in an ICO. He cautioned investors that, "as they are currently operating, there is substantially less investor protection [in the cryptocurrency and ICO markets] than in our traditional securities markets, with correspondingly greater opportunities for fraud and manipulation." He also wanted investors to know that, to date, there have been no ICOs registered with the SEC, and that the SEC has not approved any exchange-traded products holding cryptocurrencies or other related assets. While his statement warned of fraud and manipulation in the ICO markets, Chairman Clayton did acknowledge the benefits that cryptocurrencies and ICOs can provide for improving efficiencies and funding entrepreneurial ventures.

As for "market professionals," Chairman Clayton indicated that securities lawyers, accountants and consultants need to take responsibility for analyzing whether a particular cryptocurrency or ICO token is a security. Simply calling a security something else does not in itself settle the question. Chairman Clayton focused on the importance of applying the SEC's guidance, particularly as set forth in The DAO Report, to conduct a careful analysis of whether a cryptocurrency is a security. He explained that the determination of whether an instrument is a security must be based on the relevant facts and circumstances. The primary analysis is the *Howey* test, as set forth in *SEC v. W.J. Howey Co.*[8] Throughout his remarks, Chairman Clayton referenced factors of the "*Howey* test," which the SEC applied in The DAO Report and in the Order against Munchee to determine whether a security existed. The *Howey* test considers four factors:

1. Whether there is an investment of money;
2. Whether there is a common enterprise;
3. Whether investors have a reasonable expectation of profit; and
4. Whether profits are derived from the managerial efforts of others.

Chairman Clayton stated that "key hallmarks" of a security and of a securities offering are whether "[p]rospective purchasers are being sold on the potential for tokens to increase in value – with the ability to lock in those increases by reselling the tokens on a secondary market – or to otherwise profit from the tokens based on the efforts of others." He cautioned issuers that simply changing the name of a cryptocurrency or the structure of an ICO would not bring an offering of securities outside the purview of the securities laws. His remarks emphasized that "calling something a 'currency' or a currency-based product does not mean that it is not a security" and, as in the Order against Munchee (discussed below), he made clear that "[m]erely calling a token a 'utility' token or structuring it to provide some utility does not prevent the token from being a security." Rather, the importance actually lies in the features of the cryptocurrency or ICO token and how it is presented to investors.

Although Chairman Clayton conceded that not all tokens are securities under the federal securities laws (referring to a hypothetical token for a participation interest in a "book-of-the-month club" as one such example), he observed: "By and large, the structures of initial coin offerings that I have seen promoted involve the offer and sale of securities and directly implicate the securities registration requirements and other investor protection provisions of our federal securities laws." Chairman Clayton indicated that

issuers and promoters of cryptocurrencies must either (1) be able to demonstrate that the instrument is not a security or (2) be prepared to comply with applicable securities laws regarding registration, disclosure and other requirements.

SEC Orders Munchee to Cease and Desist from its ICO

In issuing the Order against Munchee on December 11, 2017, the SEC gave effect to, and put an exclamation point on, the principles set forth in Chairman Clayton's statement. Munchee is a San Francisco-based company that operates an iPhone app where users can share reviews and photos of restaurants. According to the Order, Munchee sought to raise approximately $15 million by selling "MUN tokens" and, with this capital, Munchee intended to improve its app and to create an "ecosystem" in which MUN tokens would be used for, among other things, compensating diners for writing reviews and having restaurants pay for advertising on the app. The Order indicates that Munchee first issued MUN tokens on or about October 31, 2017, and shut down its ICO "within hours" of being contacted by the SEC staff.

In determining that MUN tokens were "investment contracts" and, therefore, securities pursuant to Section 2(a)(1) of the Securities Act, the SEC followed the *Howey* test, as applied in The DAO Report and as encouraged by Chairman Clayton in his remarks. According to the Order, Munchee stated in a whitepaper that the company also conducted a "*Howey* analysis" and had determined that "as currently designed, the sale of MUN utility tokens does not pose a significant risk of implicating federal securities laws." The SEC disagreed with Munchee's determination and found that Munchee had violated Sections 5(a) and 5(c) of the Securities Act by offering MUN tokens without an effective registration statement or a qualifying exemption from registration.[9]

Investment of Money

According to the Order, at the time of the Munchee ICO, 4,500 MUN tokens were equivalent to 1 Ether (approximately $300) or one-twentieth of a Bitcoin (approximately $325), and approximately 40 people participated in the ICO, paying 200 Ether (approximately $60,000) in the aggregate. For purposes of the *Howey* test, these amounts of cryptocurrency can be deemed to be an "investment of money."[10]

Common Enterprise

The concept of a common enterprise is subject to some debate and different commenters and courts champion different approaches. Although it remains a key component of the *Howey* test, the Order, as with The DAO Report, omits this leg of the test. This leaves open the possibility that a token or other digital asset could be structured in a way that is not a common enterprise.

Reasonable Expectation of Profit

The Order references an October 30, 2017 blog post by Munchee entitled "7 Reasons You Need To Join The Munchee Token Generation Event," reason 4 of which claimed that "[a]s more users get on the platform, the more valuable [users'] MUN tokens will become," and that token holders can "watch[] their value increase over time." The SEC also cited in the Order various statements made or endorsed by Munchee, which tout "gains" on MUN tokens after the ICO and the opportunity for a secondary market in which MUN tokens would be "available on a number of exchanges in varying jurisdictions." For these and other reasons, the SEC concluded that "[p]urchasers had a reasonable expectation that they would obtain a future profit from buying MUN tokens if Munchee were successful in its entrepreneurial and managerial efforts to develop its business." This analysis echoes Chairman Clayton's statement that selling purchasers on the potential for tokens to appreciate in value and to be traded on a secondary market is one of the "key hallmarks of a security and a securities offering."

Derived from the Managerial Efforts of Others

The SEC also concluded that investors would reasonably expect the efforts of Munchee and its agents to play an important role in increasing the value of MUN tokens. The Order indicates that Munchee described in a whitepaper how the $15 million would be used to develop and support the Munchee enterprise, namely by spending the offering proceeds on hiring, legal costs, app development and maintenance of the MUN token ecosystem. The Order also notes that "Munchee highlighted the credentials, abilities and management skills of its agents and employees" in Munchee's whitepaper and elsewhere. Similarly, Chairman Clayton's remarks confirmed that the SEC views issuers' claims that tokens will increase in value "based on the efforts of others" as another "key hallmark" of a security.

The SEC emphasized that the court in *Howey* stated that the *Howey* test is "capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits." In keeping with Chairman Clayton's statements, the SEC indicated in the Order that it would not be persuaded by an argument that virtual tokens carrying some sort of "utility" would not be deemed a security, stating that "[e]ven if MUN tokens had a practical use at the time of the offering, it would not preclude the token from being a security." The SEC cited *United Housing Foundation, Inc. v. Forman*[11] for this proposition, explaining that "whether a transaction involves a security does not turn on labelling – such as characterizing an ICO as involving a 'utility token.'"

Munchee agreed to the Order without admitting or denying the SEC's findings.

Conclusion

Cryptocurrencies and ICOs will be an important part of the SEC's agenda in 2018. Issuers can expect to see continued scrutiny of ICOs from regulators, and should therefore be mindful of whether their virtual currencies or tokens may constitute securities under the federal securities laws. While the SEC concedes that some utility tokens are potentially not securities, issuers of utility tokens should pay particular attention to whether, in structuring the tokens' features and offering, issuers (1) are emphasizing the possibility that the tokens will increase in value or (2) are encouraging a secondary market for the tokens. These key points, which Chairman Clayton emphasized in his statement and the SEC emphasized in its press release on the enforcement action against Munchee, represent a crystallizing of the SEC's position. It nevertheless remains important to monitor the SEC's enforcement actions and pronouncements as more light is shed on the ICO markets. It remains to be seen what direction the SEC will take, and whether its enforcement efforts will have a broader impact on the ICO markets. Chairman Clayton is clearly putting the cryptocurrency and ICO community on notice, and it is likely that there will be further enforcement activity in this area in 2018.

Footnotes

1) Other U.S. agencies have also demonstrated recent efforts to regulate the cryptocurrency markets. *See, e.g.*, *Dechert OnPoint*, *U.S. v. Coinbase*: Virtual Currency Holders Not Outside the IRS's Reach (discussing enforcement of an order from the Internal Revenue Service to produce records of cryptocurrency account holders); *Dechert OnPoint*, CFTC Staff Aligns with SEC Position on Initial Coin Offerings: Tokens May be Commodities.

2) Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81207 (July 25, 2017). For an earlier discussion of the SEC's focus on ICOs, and The DAO's tokens in particular, please refer to *Dechert OnPoint,* SEC Focuses on Initial Coin Offerings: Tokens May be Securities Under Federal Securities Laws.

3) Complaint, *SEC v. PlexCorps, et. al*. (E.D.N.Y. Dec. 1, 2017). The SEC's complaint alleged that PlexCorps had conducted an unregistered sale of securities by raising approximately $15 million from the issuance of PlexCoin tokens, which PlexCorps described as "a cryptocurrency ... that has a value based on the current market." According to the Complaint, purchasers of PlexCoin were promised "outlandish rewards of 1,354% in 29 days or less" – rewards that would result, in part, from the appreciation of PlexCoin's value "based on the managerial efforts of PlexCorps' team" and from the ability to trade PlexCoin on a secondary market. The District Court for the Eastern District of New York granted the SEC's request in an emergency action on December 4, 2017.

4) *In the Matter of Munchee, Inc.*, Securities Act Release No. 10445 (Dec. 11, 2017).

5) Statement on Cryptocurrencies and Initial Coin Offerings, Remarks of SEC Chairman Jay Clayton (Dec. 11, 2017).

6) Earlier this year, the SEC's Office of Investor Education and Advocacy released investor bulletins and alerts cautioning investors about the risks of participating in ICOs, particularly the risk that an issuer may be fraudulent in its offering. *See* Investor Bulletin: Initial Coin Offerings (July 25, 2017); Investor Alert: Public Companies Making ICO-Related Claims (Aug. 28, 2017).

7) *See Dechert OnPoint*, SEC Enforcement Division Releases 2017 Annual Report as Industry Looks Ahead to 2018, for a further discussion of the Division's 2018 priorities.

8) 328 U.S. 293, 301 (1946) (defining an "investment contract" as "an investment of money in a common enterprise with profits to come solely from the efforts of others"); *see also SEC v. Edwards*, 540 U.S. 389, 393 (2004).

9) The primary consequence of such a violation is liability for rescission of the purchase price of the security pursuant to Section 12(a)(2) of the Securities Act.

10) *See SEC v. Shavers*, No. 4:13-CV-416, 2014 WL 4652121 at *1 (E.D. Tex. Sept. 18, 2014) (holding that an investment of a virtual currency meets the "investment of money" component of the *Howey* test).

11) 421 U.S. 837 (holding that the purchase of stock solely for the purpose of obtaining housing would not be an "investment contract" because the purpose of the investment was not for profit).

This update was authored by:

Joseph A. Fazioli
Partner
Silicon Valley / San Francisco
T: +1 650 813 4836 / +1 415 262 4529
Send email

K. Susan Grafton
Partner
Washington, D.C. / New York
T: +1 202 261 3399 / +1 212 698 3611
Send email

Mark D. Perlow
Partner
San Francisco
T: +1 415 262 4530
Send email

Timothy Spangler
Partner
Orange County / Silicon Valley
T: +1 949 442 6044 / +1 650 813 4803
Send email

Chelsea M. Childs
Associate
San Francisco
T: +1 415 262 4566
Send email

dechert.com

Dechert LLP

ON**POINT** / A legal update from Dechert's Financial Services Group

November 2017

SEC Enforcement Division Priorities Pertaining to Retail Investors and Cybersecurity

In a keynote speech to the Securities Enforcement Forum on October 26, 2017, U.S. SEC Division of Enforcement (Division) Co-Director Stephanie Avakian emphasized the protection of retail investors and cybersecurity as Division priorities, as evidenced by the Division's newly created Retail Strategy Task Force (Task Force) and specialized unit dedicated to cybersecurity (Cyber Unit).

Retail Investor Protection

The mission of the Task Force, as described by Ms. Avakian, is to implement innovative strategies to root out misconduct by investment professionals in their dealings with retail investors. This approach reflects the ever-expanding use of technology and data analytics by the Division as well as by the SEC's Division of Economic and Risk Analysis (DERA) and the Office of Compliance Inspections and Examinations (OCIE) to detect patterns of suspicious activity.

The Task Force generally will not be responsible for conducting investigations. Rather, it will work with the Division's Office of Market Intelligence and Center for Risk and Quantitative Analytics, as well as DERA and OCIE, to develop ideas and strategies for identifying issues that may impact retail investors, and after analysis, refer issues to other Division staff for further investigation.

Ms. Avakian indicated that the Task Force will focus on incidents of widespread misconduct – as examples of such misconduct, she cited the charging of inadequately disclosed fees, and recommending and trading in wholly unsuitable strategies and products. In particular, she noted that the Task Force will focus on activities such as:

- The failure of investment professionals to ensure that retail investors are invested in the lowest fee mutual fund share class for which they are eligible (such as by the intentional sale of a more expensive share class for the purpose of generating higher commissions or the failure to notify retail customers that a less expensive share class is available);
- Misleading practices associated with wrap accounts (including the failure to adequately notify retail investors of fees associated with such accounts);
- The increasing number of retail investors holding highly volatile products (*e.g.*, inverse exchange-traded funds) as long-term holdings, including in retirement accounts;
- The failure of investment professionals to fully disclose fees, mark-ups and other factors that can negatively impact returns for structured products; and
- Practices designed to generate large commissions at the expense of retail investors (*e.g.*, churning and excessive trading).

The Task Force, together with other SEC offices including the Office of Investor Education and Advocacy, will also be responsible for conducting retail investor outreach to identify issues where targeted education and outreach efforts may benefit investors.

Cybersecurity

The Cyber Unit – the first new specialized unit created since the advent of these specialized groups within the Division in 2010 – was created to address the growing level of technology-driven misconduct in the securities markets. Ms. Avakian noted that the Cyber Unit will focus primarily on three types of cases. The first involves cyber activities used to gain an unlawful market advantage – for example, by hacking nonpublic information in order to trade or to manipulate the market; intruding into accounts and then manipulating trading; and "disseminating false information through electronic publication, such as SEC EDGAR filings and social media, in order to manipulate stock prices."

The second enforcement priority involves failures by registered entities to take appropriate steps to safeguard information or ensure systems integrity, including potentially violations of Regulations S-P, S-ID, SCI and other provisions. The third priority relates to failures by public companies to adequately disclose cyber-related issues. With respect to the latter, Ms. Avakian indicated that, although the Division has not yet brought an enforcement action on this basis, the staff of the Division of Corporate Finance has reminded registrants of their duties to disclose material information, including pertaining to cyber risks and incidents.

Ms. Avakian further indicated that, in order to have a consistent approach to enforcement regarding "emerging issues," the Cyber Unit will also be responsible for the Division's focus on distributed ledger (or "blockchain") technology.

Conclusion

The retail investor protection initiative signals the Division's expectation that investment professionals will be proactive in providing retail investors with adequate disclosure regarding the type and cost of investments. For example, financial advisors may want to implement systems to identify mutual fund customers who are eligible for less expensive shares and take steps to move those customers to that share class. Additionally, financial advisors may want to review disclosure documents to make sure that all fees are appropriately disclosed.

Financial advisors also may want take steps to: secure private information; implement plans and procedures to prevent cybersecurity breaches in the first instance; and disclose material information regarding the occurrence of any cyber issues. In light of the creation of a specialized Cyber Unit, there likely will be an uptick in cyber-related enforcement due to a more focused approach to these issues and a team dedicated to bringing such cases. Accordingly, the industry should closely follow SEC action in this area to understand the level of care and measures that the SEC expects of the industry on various aspects of cybersecurity.

This update was authored by:

K. Susan Grafton
Partner
Washington, D.C. / New York
T: +1 202 261 3399 / +1 212 698 3611
Send email

Catherine Botticelli
Partner
Washington, D.C.
T: +1 202 261 3368
Send email

Mark D. Perlow
Partner
San Francisco
T: +1 415 262 4530
Send email

Colleen M. Evans
Associate
Boston
T: +1 617 728 7164
Send email

The authors would like to thank Eric Auslander for his contributions to this *OnPoint*.

Thank You

For further information,
visit our website at dechert.com

Dechert lawyers acted on the matters listed in this presentation either at Dechert or prior to joining the firm.

Dechert
LLP