Investment Management Regulatory Update

September 30, 2020

COVID-19 Update

Please refer to Davis Polk's "**Coronavirus Updates**" webpage for content related to the outbreak.

Rules and Regulations

SEC Expands Access to Private Offerings

On August 26, 2020, the Securities and Exchange Commission ("**SEC**") expanded the definitions of "accredited investor" in Regulation D and of "qualified institutional buyer" in Rule 144A under the Securities Act of 1933 ("**Securities Act**"), thereby allowing a larger pool of investors to have access to private investments, including in hedge funds, private equity funds and venture capital funds. While the previous definition of "accredited investor" relied on an individual's net worth to reflect financial sophistication, the new rules reflect the SEC's view that certain experience and knowledge may also demonstrate financial sophistication. Davis Polk published a **client memorandum** discussing the amendments to the definition of "accredited investor" and "qualified institutional buyer."

Industry Update

OCIE Publishes Risk Alert on Cybersecurity: Safeguarding Client Accounts Against Credential Compromise

On September 15, 2020, the Office of Compliance Inspections and Examinations ("**OCIE**") issued a risk alert to share its observations of the recent increase in instances of "credential stuffing", the associated risks, and how firms can mitigate those risks. Credential stuffing is a method of cyber-attack in which bad actors obtain lists of usernames, email addresses and passwords from the dark web and then attempt to use the same log-in credentials to gain access to other websites. If a bad actor is successful in entering a firm's systems through this method, the bad actor can steal assets from customer accounts, access

confidential customer information (including login credentials that they can then sell to other bad actors on the dark web), and perform other nefarious deeds.

Summary of Observations

OCIE has observed an increase in credential stuffing attacks and notes that a firm's susceptibility to credential stuffing attacks could lead to negative financial, regulatory and legal ramifications, while also putting its investors at risk. OCIE observes that firms' internet-facing websites are especially vulnerable targets because bad actors can initiate transactions or transfer funds from a compromised customer's account if a credential stuffing attack is successful. Moreover, Personally Identifiable Information is often available on firms' internet-facing websites, which can provide bad actors with information they can use for credential stuffing attacks on other websites.

Credential stuffing attacks are most successful when individuals use the same password (or similar passwords with only minor variations) across multiple online accounts or when individual use login credentials that are easily guessed (such as email addresses or full names).

OCIE encourages registrants to update their Regulation S-P and Regulation S-ID policies to address this risk.

Firms' Responses to Credential Stuffing

OCIE has observed that firms have implemented several strategies for strengthening their security against credential stuffing. Such examples include:

- Policies and procedures that require that passwords meet certain strength criteria;
- Multi-Factor Authentication ("**MFA**"), in which a person seeking to access an account must satisfy multiple verification methods;
- CAPTCHA, or "Completely Automated Public Turing test to tell Computers and Humans Apart", verifications such as requiring a user to identify pictures of a particular object within a grid of pictures before permitting access to an account, which can help combat automated scripts that attempt to enter accounts;
- Controls to detect and prevent such attacks, such as monitoring for a higher-than-usual number of login attempts or a higher-than-usual number of failed logins, using a Web Application Firewall, or implementing additional controls that can mitigate damage if an account is taken over (such as limiting online fund transfers); and
- Monitoring the dark web for lists of leaked user IDs and passwords, and testing to evaluate whether current user accounts are susceptible to credential stuffing attacks.

Other Considerations in Preparing for Credential Stuffing Attacks

OICE encourages firms to evaluate their current cyber security practices and to consider whether the firm's customers and staff are properly educated regarding how they can protect their accounts. Such strategies can include:

- Encouraging clients and staff to create strong, unique passwords (i.e., not a password used for another website) and to change a password if there is an indication that it has been compromised; and
- Encouraging clients and staff to be alert to instances where their mobile devices no longer work. Though text messages are often used as a MFA verification method, a bad actor may attempt to transfer the phone number to another device to satisfy MFA in connection with an attack.

Conclusion

The OCIE encourages firms to review their current account protection safeguards and to consider consumer outreach to educate them of actions they may take to help minimize future risks.

- **See a copy of the Risk Alert**

Litigation

Token Issuer Settles SEC Allegations of Failing to Register under Section 5 of the Securities Act

On September 15, 2020, the SEC issued an order (the "**Unikrn Order**") instituting and settling cease-and-desist proceedings against Unikrn, Inc. ("**Unikrn**") for allegedly offering and selling digital tokens as investment contracts (i.e., securities) without having filed a registration statement or qualifying for an exemption from registration under the Securities Act.

According to the Unikrn Order, Unikrn operates an online eSports gaming and gambling platform. Between June 2017 and October 2017, Unikrn allegedly raised $31 million through the sale of its digital tokens in a pre-sale phase and an initial coin offering.

The SEC alleges that in June 2017, Unikrn initiated the "pre-sale" phase of its digital token offering by reaching out to current shareholders and inviting them to participate in the offering. The pre-sale was originally marketed to shareholders, wealthy individuals and digital asset investment funds, and Unikrn also allegedly advertised its offering to the general public through social media outlets. In the advertisements, Unikrn allegedly highlighted its founders' successes and record of "picking winners." Unikrn also allegedly described its efforts to expand the token which would lead to an increase in value, and hired a blockchain marketing firm who allegedly promoted the offering as a "good long-term hold."

Although the terms of the purchase agreement required purchasers to represent that they were buying the tokens for their utility and not as an investment, the SEC concluded that the marketing promotions led offering participants to have a reasonable expectation of profit from Unikrn's efforts to expand the token's uses and increase its value. As a result, the SEC concluded that Unikrn's tokens were offered and sold as investment contracts, and therefore securities, and that Unkirn violated Sections 5(a) and 5(c) of the Securities Act by failing to register the offering or qualify for an exemption. Unikrn agreed to permanently disable the tokens within 10 days of the date of the Unikrn Order, to publish notice of the Unikrn Order on its website and social media channels within 10 days of the date of the Unikrn Order, and to request removal of its tokens from digital asset trading platforms. Unikrn was ordered to pay a civil money penalty of $6,100,000.

Commissioner Hester M. Peirce issued a dissenting opinion with respect to the Unikrn Order, and expressed her concern that the consequences of the Unikrn Order may be to "enervate innovation and stifle the economic growth that innovation brings." She noted that the determination of whether an instrument is an investment contract, and therefore a security, is a subjective analysis that does not provide clear enough guideposts for entrepreneurs to follow. Because of this, the Commissioner called for the SEC to design a safe-harbor that would "effectively combine the [SEC]'s interest in protecting investors with developers' ambition to experiment."

- **See a copy of the Unikrn Order**
- **See a copy of the Commissioner's statement**

Investment Adviser and its Chief Compliance Officer Settle SEC Charges Arising Out of Alleged Failure to Conduct Compliance Reviews, and Altering Compliance Reports Provided to SEC Examiners

On September 17, 2020, the SEC issued an order (the "**GGHC Order**") instituting and settling cease-and-desist proceedings against Gilder Gagnon Howe & Co LLC ("**GGHC**"), a registered investment adviser and broker-dealer, and its chief compliance officer, Bonnie M. Haupt ("**Haupt**"). GGHC allegedly failed to conduct certain reviews of clients' accounts for excessive commissions, as required by GGHC's compliance policies and procedures, and Haupt allegedly altered reports provided to SEC exam staff so that it would appear that GGHC performed these reviews even though it had not.

According to the GGHC Order, as of December 31, 2017, GGHC managed approximately $9.75 billion in assets; approximately 80% of those assets were held in accounts that paid commissions on a pay-per-trade basis. GGHC employs an active trading strategy which may result in high turnover. In late 2016, FINRA conducted an examination of GGHC and found that the firm had not demonstrated it was actively monitoring accounts for cost-to-equity ratios and turnover rates. In response GGHC, in early 2017, instituted a policy that GGHC's chief compliance officer, or her designee, would review and document monthly cost-to-equity ratios and turnover rates using a "Turnover Report," and escalate to GGHC management all accounts with a cost-to-equity ratio above 6%.

The SEC alleges that GGHC and Haupt did not conduct any monthly reviews of cost-to-equity ratios in 2017, and that Haupt did not escalate to management any of the allegedly "numerous" accounts with cost-to-equity ratios above 6%. GGHC and Haupt also allegedly failed to conduct reviews of turnover rates for eleven of the twelve months of 2017.

In November 2017, the SEC staff began an examination of GGHC. During the exam, staff requested that GGHC provide Turnover Reports from June through November 2017. Exam staff also asked GGHC to provide a written explanation of the firm's procedures to review client accounts regarding fees. In response to these requests, Haupt allegedly provided Turnover Reports for January through November 2017, which Haupt had altered so that they would appear to have been reviewed monthly, at the end of the month covered. Later, during an investigation by SEC's Enforcement Division, GGHC produced the altered reports in response to an SEC document request. Haupt allegedly admitted to altering the reports in sworn testimony before the SEC enforcement staff.

As a result of the actions described above, the SEC alleges that GGHC willfully violated section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder, and that Haupt willfully aided and abetted GGHC's violations. GGHC and Haupt agreed to cease and desist from further violations, and to be censured. Haupt agreed to be barred from association with any broker-dealer or investment advisor, subject to the right to reapply for association in the future. GGHC agreed to pay a civil money penalty of $1.7 million; Haupt agreed to pay a civil money penalty of $45,000.

- **See a copy of the GGHC Order**

Investment Adviser Settles SEC Allegations of Custody Rule Violations

On September 4, 2020, the SEC issued an order (the "**SQN Order**") instituting and settling cease-and-desist proceedings against SQN Capital Management, LLC ("**SQN Capital**"), a registered investment adviser, arising out of SQN Capital's alleged failure to distribute audited financial statements of its managed funds within the timeframe required by Rule 206(4)-2(b)(4) under the Advisers Act (the "**Custody Rule Exception**").

According to the SQN Order, SQN advised several funds, including the two funds at issue in the SQN Order, the SQN Special Opportunity Fund, LLC (the "**SO Fund**") and the SQN Portfolio Acquisition Company, LLC (the "**PA Fund**"), which together accounted for $21.2 million of the approximately $918 million in SQN Capital's assets under management as of May 2020.

The SEC alleges that although SQN Capital engaged a Public Company Accounting Oversight Board-registered firm to conduct annual audits of the financial statements of the SO Fund and the PA Fund, the audit firm did not complete the audits until significantly after the timeframe required by the Custody Rule Exception (i.e., 120 days following the end of the relevant fiscal year). The SQN Order states that for certain years, audits had been completed more than a year late, and that for certain years the audits had not been completed at all.

As a result of these alleged failures, the SEC charged SQN Capital with willfully violating Section 206(4) of the Advisers Act and rules 206(4)-2 and 206(4)-7 thereunder. SQN Capital agreed to cease and desist from further violations, to be censured, and to pay a civil money penalty of $75,000.

- **See a copy of the SQN Order**

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

Nora M. Jordan	212 450 4684	**nora.jordan@davispolk.com**
James H.R. Windels	212 450 4978	**james.windels@davispolk.com**
John G. Crowley	212 450 4550	**john.crowley@davispolk.com**
Amelia T.R. Starr	212 450 4516	**amelia.starr@davispolk.com**
Leor Landa	212 450 6160	**leor.landa@davispolk.com**
Gregory S. Rowland	212 450 4930	**gregory.rowland@davispolk.com**
Michael S. Hong	212 450 4048	**michael.hong@davispolk.com**
Lee Hochbaum	212 450 4736	**lee.hochbaum@davispolk.com**
Sarah E. Kim	212 450 4408	**sarah.e.kim@davispolk.com**
Marc J. Tobak	212 450 3073	**marc.tobak@davispolk.com**
