SEC/SRO UPDATE: SEC PROPOSES CYBERSECURITY RULES; SEC PROPOSES SHORT SALE DISCLOSURE RULE; SEC PROPOSES CYBERSECURITY RISK MANAGEMENT RULES AND AMENDMENTS FOR REGISTERED INVESTMENT ADVISERS AND FUNDS; SEC CHARGES INFINITY Q FOUNDER WITH ORCHESTRATING MASSIVE VALUATION FRAUD

By John A. Elofson and Stephanie G. Danner

John A. Elofson is a partner and Stephanie G. Danner is an associate at the law firm of Davis Graham & Stubbs LLP in Denver, Colorado. The authors thank Patrick Tredinnick, a paralegal at Davis Graham, for his assistance in preparing this article. Contact: john.elofson@dgslaw.com or stephanie.danner@dgslaw.com.

SEC Proposes Cybersecurity Rules

On March 9, 2022, the SEC proposed rule amendments intended to enhance and standardize rules regarding disclosure of cybersecurity risk management and related topics.[1] SEC Chair Gary Gensler described the purpose of the rules by stating that "cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks. A lot of issuers already provide cybersecurity disclosure to investors. I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner."[2]

Key elements of the proposed rules are requirements for companies to provide:

- *Current reporting about material cybersecurity incidents*: The rules would add a new item in Form 8-K pursuant to which a company would have to disclose any material cybersecurity incidents within four days of determining that such an incident occurred. Required disclosures would include when the incident was discovered, the scope of the incident, whether any data was stolen, altered, accessed, or used for any unauthorized purpose, the effect of the incident on the company's operations and whether the registrant has remediated the incident.

- *Periodic disclosure about cybersecurity policies*: Form 10-K would be amended to require (i) disclosure of a company's policies and procedures for identifying and managing cybersecurity risks, (ii) its "cybersecurity governance," including the board of directors' oversight role regarding cybersecurity risks and how those risks and related issues are communicated to the board, and (iii) management's role, and relevant expertise, in assessing and managing cybersecurity-related risks and implementing related policies, procedures and strategies. Relatedly, Regulation S-K would be amended to require disclosure of information regarding the cybersecurity expertise, if any, of members of the board of directors. The description of policies and procedures would include whether the company engages third parties in connection with its cybersecurity efforts, its policies regarding oversight of vendors and other counterparties, and whether and how previous incidents have informed its policies.

- *Updates regarding previously-reported cybersecurity incidents*: The rules would amend Forms 10-K and 10-Q to require updated disclosure regarding previously reported cybersecurity incidents, and when a series of undisclosed immaterial incidents have become collectively material. The updated disclosure would include, but not be limited to, the company's remediation

efforts, any existing or potential material effects of the incident, and any related changes to the company's policies and procedures.

The SEC has previously issued interpretive guidance regarding how its existing rules may require cybersecurity-related disclosures—which appear most frequently in the "risk factors" section of SEC filings—but the proposed rules would be the first to address cybersecurity issues specifically.

SEC Proposes Short Sale Disclosure Rule

On February 25, 2022, the SEC proposed a new rule under the Securities Exchange Act of 1934, as amended, to require institutional investment managers exercising investment discretion over short positions meeting specified thresholds to report on a proposed Form SHO information relating to short positions and certain daily activity affecting such positions.[3] SEC Chair Gary Gensler stated that "[p]roposed Rule 13f-2 would make aggregate data about large short positions available to the public for individual equity securities. This would provide the public and market participants with more visibility into the behavior of large short sellers."[4] The proposed rule comes on the heels of highly-publicized short selling events involving so-called "meme stocks" such as GameStop that resulted in an unusual level of public interest in short selling strategies and scrutiny of the SEC's oversight by prominent politicians across the political spectrum.[5]

The SEC's proposing release states that short sales—sales of securities that the seller does not own—can provide important benefits to the market by providing hedging options and improving pricing efficiency, but can also be used for manipulative purposes. Existing SEC Regulation SHO imposes certain requirements in connection with short sales, and in particular addresses the risk that the short seller will be unable to obtain the security subject to the sale by the time of settlement. But proposed Rule 13f-2 would go beyond existing requirements to provide greater public transparency relating to short selling activity. Among other benefits, the SEC believes that greater transparency may facilitate regulatory oversight of potentially manipulative activity such as "short squeeze" and "short and distort" schemes. At the same time, according to the SEC, public disclosure of individual short positions could unduly chill short selling and have other unintended consequences. Accordingly, the proposed rule attempts to strike a balance between these competing considerations by facilitating the public disclosure of short selling data on an aggregated rather than an individual basis.

Under the rule, investment managers meeting a specified reporting threshold would be required to file a Form SHO with the SEC within 14 calendar days after the end of a month. The identity of the managers reporting on Form SHO would not be made public and would be treated as confidential. The reporting threshold would be set at (i) for reporting issuers, a gross short position of $10 million or more or a position covering 2.5% or more of the class of security outstanding or (ii) for non-reporting issuers, a gross short position of $500,000 or more. The calculations would not take into account derivative or long positions in the same security. The SEC would then, on a delayed basis, publish aggregated information derived from the reported data, including the number of shares and dollar value of the aggregated gross short positions and a summary of reported hedging information.

Relatedly, the SEC is proposing a new rule under Regulation SHO pursuant to which a broker-dealer would be obligated to mark a purchase order as "buy to cover" if the purchaser has a gross short position in the security in the account for which the purchase is being made. The SEC believes that this requirement would allow it to better understand what it calls the "lifecycle" of short sales by identifying trades that close out short positions. The increased transparency is expected to enhance the SEC's ability to understand and police potentially manipulative trading strategies.

SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds

On February 9, 2022, the SEC voted to propose rules related to cybersecurity risk management for registered investment advisers, and registered investment companies and business development companies (collectively, "funds"), as well as amendments to certain rules that govern investment adviser and fund disclosures.[6]

According to the SEC's associated press release, the proposed rules and amendments "are designed to enhance cybersecurity preparedness and could improve investor confidence in the resiliency of advisers and funds against cybersecurity threats and attacks."[7] The proposal includes new Rule 206(4)-9 under the Investment Advisers Act of 1940 (the "Advisers Act"), and new Rule 38a-2 under the Investment Company Act of 1940 (the "Investment Company Act") (proposed Rules 206(4)-9 and 38a-2 collectively, the "proposed cybersecurity risk management rules").[8]

Under the proposed cybersecurity risk management rules:

- advisers and funds would be required to adopt and implement written cybersecurity policies and procedures designed to address cybersecurity risks that could harm advisory clients and fund investors;
- Form ADV Part 2A would be amended to require disclosure of cybersecurity risks and incidents to an adviser's clients and prospective clients;
- Form N-1A, Form N-2, Form N-3, N-4, Form N-6, Form N-8B-2, and Form S-6 would be amended to require funds to include a description of any significant fund cybersecurity incidents that have occurred in the last two fiscal years in the fund's registration statements;
- Rule 204-2 of the Advisers Act would be amended to require advisers to maintain certain records related to the proposed cybersecurity risk management rules and the occurrence of cybersecurity incidents;
- funds would be required to maintain copies of its cybersecurity policies and procedures and other related records specified under proposed Rule 38a-2 of the Investment Company Act; and
- advisers would be required to report significant cybersecurity incidents affecting the adviser or its fund or private fund clients on a new confidential Form ADV-C.

The public comment period will remain open until April 11, 2022.

SEC Charges Infinity Q Founder with Orchestrating Massive Valuation Fraud

On February 17, 2022, the SEC charged James Velissaris, the former Chief Investment Officer (the "CIO") and founder of Infinity Q Capital Management ("Infinity") with allegedly overvaluing assets by more than $1 billion.[9]

The SEC's complaint (the "Complaint")[10] alleges that between 2017 to February 2021, the CIO "engaged in a fraudulent scheme to overvalue assets held by the Infinity Q Diversified Alpha mutual fund and the Infinity Q Volatility Alpha private fund"[11] by "altering inputs and manipulating the code of a third-party pricing service used to value the funds' assets."[12] The SEC also alleges that the CIO collected more than $26 million in profit distributions through the fraudulent conduct and without disclosing his activities to investors.[13]

According to the SEC's accompanying press release (the "Press Release"), in February 2021, the CIO was removed from his role with Infinity Q after SEC Staff confronted the firm with information suggesting that the CIO had been adjusting the third-party pricing model.[14]

The Complaint was filed in the U.S. District Court

for the Southern District of New York and charges the CIO with violating antifraud and other provisions of federal securities laws. The Complaint seeks permanent injunctive relief, return of allegedly ill-gotten gains, and civil penalties. The SEC also seeks to bar the CIO from serving as a public company officer and director. In parallel actions, the U.S. Attorney's Office for the Southern District of New York announced on February 17, 2022, criminal charges against the CIO, and the Commodity Futures Trading Commission ("CFTC") announced civil charges against him.

ENDNOTES:

[1]See https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

[2]See https://www.sec.gov/news/press-release/2022-39.

[3]*See* https://www.sec.gov/rules/proposed/2022/34-94313.pdf.

[4]*See* https://www.sec.gov/news/press-release/2022-32.

[5]*See, e.g.*, Trading Curbs Reverse GameStop Rally, Angering Upstart Traders, *N.Y. Times*, Jan. 30, 2021, *available at*: https://www.nytimes.com/2021/01/28/business/gamestop-robinhood.html.

[6]*See* https://www.sec.gov/news/press-release/2022-20.

[7]SEC Press Release 2022-20.

[8]*See* https://www.sec.gov/files/33-11028-fact-sheet.pdf.

[9]*See* https://www.sec.gov/news/press-release/2022-29.

[10]*See* https://www.sec.gov/litigation/complaints/2022/comp-pr2022-29.pdf.

[11]*Supra* Note 9.

[12]*Supra* Note 9.

[13]*Supra* Note 9.

[14]*Supra* Note 9.