SULLIVAN & CROMWELL LLP

S&C memo

March 22, 2023

SEC Proposes New Disclosure Rule for Market Entities, and Amendments to Regulations SCI and S-P, to Address Cybersecurity Risks to the U.S. Securities Markets

Proposed Rule Would Require New and Enhanced Cybersecurity Incident Reporting, and Amendments Would Require the Implementation of Policies and Procedures to Address Cybersecurity Risks

SUMMARY

On March 15, 2023, the Securities and Exchange Commission ("SEC") proposed a new rule regarding cybersecurity risk-management for broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents (collectively, "Market Entities") ("Proposed Rule 10"). Among other things, Proposed Rule 10 would require Market Entities to make an "immediate" notification to the SEC of a "significant cybersecurity incident" and, for most Market Entities, to report "detailed information" and updates to the SEC, as well as public disclosures of cybersecurity risks and significant cybersecurity incidents.[1]

Also on March 15, the SEC proposed amendments to Regulation SCI which would expand the scope of entities subject to Regulation SCI and specify cybersecurity policies and procedures required to be implemented by these entities.[2] Additionally, the SEC proposed amendments to Regulation S-P intended to "enhance the protection of customer information" held by broker-dealers, investment companies, registered investment advisers, and transfer agents.[3]

The 60-day notice-and-comment period for each of these new proposed rules will begin on the date of publication of each respective proposing release in the Federal Register.[4] Additionally, the SEC reopened the notice-and-comment period on proposed cybersecurity risk management rules under the Investment Advisors Act of 1940 and the Investment Company Act of 1940 it originally proposed on February 9, 2022; the notice-and-comment period for these proposed rules will remain open until May 22, 2023.[5]

BACKGROUND

As set forth in its proposing release for Proposed Rule 10, the SEC recognizes that cybersecurity risks increasingly create the potential of significant harm to Market Entities, investors, and other market participants.[6] The SEC seeks to protect the U.S. securities markets and investors from the threat posed by cybersecurity risks by mandating that entities covered by Proposed Rule 10 implement new cybersecurity policies and procedures and comply with new notification requirements regarding reporting incidents to the SEC and the public.[7]

The proposed rules are the latest in a series of SEC rulemakings and enforcement actions in the realm of cybersecurity, an area of heightened focus for the SEC. In 2022 alone, the SEC issued three rulemaking projects implicating cybersecurity, including proposals designed to address cybersecurity risk with respect to investment advisers and investment companies, to expand Regulation SCI to certain government securities trading platforms, and to significantly expand cybersecurity disclosure requirements for SEC registrants.[8] In the past two years, the SEC has brought an unprecedented series of cybersecurity-focused enforcement actions in these areas, including actions focused on public company disclosure and disclosure controls and procedures with respect to cybersecurity, as well as cybersecurity risk management by investment advisers and investment companies.

The SEC's heightened rulemaking and enforcement activity in cybersecurity parallels that of other federal agencies, Congress, and the White House under the Biden Administration, as cyber risks and harms have continued to escalate and threaten the U.S. public and private sectors. The proposed rules follow the 2021 implementation of a final rule by the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation imposing mandatory reporting requirements on banking organizations regarding cybersecurity incidents ("Federal Bank Regulators' Cyber Incident Reporting Rule"). Other regulatory agencies at both the federal and state level have also been particularly focused on cybersecurity risks in recent years, including the Transportation Security Administration,[9] the Federal Communications Commission,[10] the Federal Trade Commission, and the New York State Department of Financial Services ("DFS"). In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act, mandating that the Cybersecurity and Infrastructure Security Agency ("CISA") "develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA."[11] The White House has also acted by Executive

Order and through other measures to elevate cybersecurity standards across the private sector and enhance cybersecurity for other U.S. critical infrastructure.[12]

OVERVIEW OF THE SEC'S PROPOSED RULE AND AMENDMENTS

A. PROPOSED RULE 10

Proposed Rule 10 would apply to "Market Entities," defined as "broker-dealers, the Municipal Securities Rulemaking Board, clearing agencies, major security-based swap participants, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents."[13] Proposed Rule 10 also includes additional requirements for so-called "Covered Entities," encompassing all Market Entities except for "certain types of small broker-dealers."[14]

1. Written Cybersecurity Policies and Procedures

Proposed Rule 10 would require Market Entities to maintain and enforce written policies and procedures "reasonably designed to address their cybersecurity risk," and to review and assess the design and effectiveness of those policies and procedures on an annual basis.[15] Proposed Rule 10 also provides specific guidance as to the required contents and substance of a Covered Entity's written policies and procedures: a Covered Entity's policies and procedures would need to provide for (i) written documentation of periodic risk assessments of the Covered Entity's information systems, (ii) monitoring of its information systems and controls designed to minimize the risk of unauthorized access to its information systems, (iii) measures designed to detect, mitigate, and remediate cybersecurity threats and vulnerabilities to its information systems, (iv) measures to respond to a cybersecurity incident, and (v) procedures for documenting any cybersecurity incidents.[16]

2. Immediate Reporting of a Significant Cybersecurity Incident

Most notably, Proposed Rule 10 would require Market Entities to provide the SEC with "immediate written electronic notice" upon having a reasonable basis to conclude that a "significant cybersecurity incident" had occurred or is occurring.[17] These notices to the SEC would be kept "nonpublic to the extent permitted by law."[18]

Under Proposed Rule 10, a "cybersecurity incident" is defined as "an unauthorized occurrence on or conducted through a Market Entity's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems,"[19] leveraging much of the same language used in the Federal Bank Regulators' Cyber Incident Reporting Rule. Further, under Proposed Rule 10, a "significant cybersecurity incident" is (i) a "cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the ability of the Market Entity to maintain critical operations," or (ii) "a cybersecurity incident, or a group of cybersecurity incidents, that leads to the unauthorized access or use of the information or information systems of the Market Entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to

result in: (1) substantial harm to the Market Entity; or (2) substantial harm to a customer, counterparty, member, registrant, or user of the Market Entity, or to any other person that interacts with the Market Entity."[20]

In the proposing release, the SEC offers guidance on the intended meaning of "significant cybersecurity incident." Specifically, the SEC states that despite the broad definition of "cybersecurity incident" (which is based on the National Institute of Standards and Technology definition), the two-pronged definition is designed to limit the reporting requirement to those cybersecurity incidents that "prevent[] the Market Entity from performing functions that rely on the system operating as designed," such as "a ransomware attack," or that compromise confidential information in a manner that "could lead to the improper use of this information to harm the persons to whom it pertains . . . or provide the unauthorized user with an unfair advantage over other market participants," such as providing that user with the ability to trade "based on confidential business information."[21]

Within 48 hours of having a reasonable basis to conclude that a significant cybersecurity incident had occurred or was occurring, Covered Entities would be required to complete and submit to the SEC Part I of a proposed Form SCIR[22] including "information about the significant cybersecurity incident and the Covered Entity's efforts to respond to and recover from the incident."[23] Notably, a Covered Entity would be required to file an amended Part I to Form SCIR when "(1) any information previously reported to the [SEC] on Part I of proposed form SCIR pertaining to the significant cybersecurity incident becomes materially inaccurate; (2) any new material information pertaining to the significant cybersecurity incident previously reported to the [SEC] on Part I on proposed Form SCIR is discovered; (3) the significant cybersecurity incident is resolved; or (4) an internal investigation pertaining to a significant cybersecurity incident is closed."[24]

3. Public Disclosure of Cybersecurity Risks and Significant Cybersecurity Incidents

Additionally, pursuant to Proposed Rule 10, Covered Entities would be required to publicly disclose "summary descriptions of their cybersecurity risks" and the "significant cybersecurity incidents" they experienced in the current or previous calendar year on Part II of the proposed Form SCIR.[25] Part II would need to be filed with the SEC, posted on a Covered Entity's website, and, in the case of Covered Entities that carry or introduce broker-dealers, provided to customers at account-opening, annually, and whenever the Form SCIR is updated.[26]

Proposed Rule 10 defines "cybersecurity risk" broadly to include "financial, operational, legal, reputational, and other adverse consequences that could stem from cybersecurity incidents, cybersecurity threats, and cybersecurity vulnerabilities."[27] Further, it defines "cybersecurity threat" to mean "any potential occurrence that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a Market Entity's information systems or any information residing on those systems."[28] Proposed Rule 10 defines "cybersecurity vulnerability" to mean "a vulnerability in a Market Entity's information systems, information system security procedures, or internal controls, including, for example, vulnerabilities in their

design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident."[29]

B. PROPOSED AMENDMENTS TO REGULATION SCI

Also on March 15, the SEC proposed amendments to Regulation SCI, which was first adopted in 2014 to strengthen the technology infrastructure of the U.S. securities markets.[30] The SEC's proposed amendments to Regulation SCI would expand the scope of entities subject to Regulation SCI, strengthen the requirements of Regulation SCI, and "expand the types of SCI events" that would "trigger immediate notification" to the SEC, in addition to imposing a handful of additional requirements.[31]

1. Expansion of Regulation SCI's Application

Regulation SCI currently applies to a wide variety of securities market actors, including exchanges, securities associations, certain non-exempt clearing agencies, and certain disseminators of market data. The amended Regulation SCI would expand its applicability to include registered security-based swap data repositories, registered broker-dealers with assets or transaction activity in excess of a certain threshold, and all clearing agencies exempted from registration.[32]

Further, the proposed amendments would amend the definition of "systems intrusion" under Regulation SCI in order to cover additional "cybersecurity events such as certain distributed denial-of-service attacks."[33]

2. Required Policies and Procedures for SCI Entities

At present, entities subject to Regulation SCI ("SCI entities") must maintain comprehensive policies and procedures reasonably designed to ensure the resiliency, security, and integrity of their systems to "maintain operational capability and promote the maintenance of fair and orderly markets."[34] Among other things, SCI entities are required to make reports to the SEC to facilitate the SEC's market oversight, take corrective action to address systems issues, and notify parties affected by any such issues.[35] Under the proposed amendments, an SCI entity would need to update its policies and procedures to include, for example, an "inventory, classification, and lifecycle management program for SCI systems and indirect SCI systems," a "program to manage and oversee third party providers, including cloud service providers," a "program to prevent unauthorized access to SCI systems and information therein," and "identification of current SCI industry standards with which each such policy and procedure is consistent, if any."[36]

3. Updates to SCI Review Requirements

The proposed amendments to Regulation SCI would also require that an SCI entity conduct an SCI review at least once every calendar year, with the exception of certain penetration testing reviews that may be conducted once every three years, and "assessments of SCI systems directly supporting market regulation or market surveillance," which may be conducted "at a frequency based upon the risk assessment

conducted as part of the SCI review, but in no case less than once every three years."[37] Under the amended Regulation SCI, these SCI reviews would need to be conducted by "objective personnel."[38]

C. PROPOSED AMENDMENTS TO REGULATION S-P

The SEC has also proposed amendments to Regulation S-P, which sets forth requirements designed to protect the privacy of consumers' financial information. Regulation S-P requires broker-dealers, investment companies, and registered investment advisers ("S-P entities") to maintain written policies and procedures to safeguard "customer records and information" (the "safeguards rule"), and dispose of "consumer report information" in a manner that prevents unauthorized access (the "disposal rule"), among other things.[39] The SEC's proposed amendments to Regulation S-P are intended to "enhance the protection of customer information" and institute new customer notification requirements in the event their information is compromised.[40]

1. Required Data Breach Notification

Significantly, the proposed amendments to Regulation S-P would create a new "[f]ederal minimum standard" in breach notification by requiring covered entities to notify individuals whose information "was or is reasonably likely to have been accessed or used without authorization . . . as soon as practicable, but not later than 30 days after a covered institution becomes aware" of the compromise of the information,[41] unless the covered entity determines that the sensitive customer information has not been and is not reasonably likely to be used in a manner that would result in "substantial harm or inconvenience."[42] The SEC envisions that the exception will apply only in "limited circumstances" where an entity can "provide a sufficient basis" for such a determination."[43] Covered entities should retain any documentation of a determination that notification is not required for three years, but would not be required to submit this documentation to the SEC.[44]

2. Coverage of "Customer Information" under the Safeguards Rule and the Disposal Rule

Under the amended Regulation S-P, "customer information" would be required to be protected in accordance with both the safeguards rule and the disposal rule.[45] Specifically, customer information would replace the term "customer records and information" in the safeguards rule, and be added to the disposal rule.[46] Customer information would "encompass any record containing 'nonpublic personal information' (as defined in Regulation S-P) about a 'customer of a financial institution.'"[47]

3. Incident Response Plans

As proposed, the amended Regulation S-P would also require S-P entities to adopt written incident response plans "reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information."[48] In particular, the plan would be required to set forth procedures for assessing the nature and scope of such an incident, and procedures for containing and controlling such incidents.[49]

4. Coverage of Transfer Agents Under Regulation S-P

In addition to broker-dealers, investment companies, and registered investment advisers, Regulation S-P would be expanded to include transfer agents as covered institutions subject to the safeguards rule and the disposal rule.[50] Previously, only transfer agents registered with the SEC were subject to the disposal rule, and none were subject to the safeguards rule.[51]

D. REQUEST FOR COMMENTS

The SEC is seeking comments on the proposed rules. With respect to Proposed Rule 10, the SEC has specifically requested comment on the scope of the proposed definition of "Covered Entities," "significant cybersecurity incident," and numerous other terms, and whether Rule 10 should apply to additional securities markets participants.[52] With respect to Regulation S-P, the SEC has specifically requested comment on whether the proposed "becoming aware" timing requirement for notification should remain as written, or whether it should begin to run at some other time, such as "after the covered institution 'reasonably should have been aware' of the incident" or "after completing its assessment of the incident or containment."[53] Finally, with respect to Regulation SCI, the SEC has requested comment "on the relation between the requirements of Regulation SCI (as it currently exists and as it is proposed to be amended), proposed Rule 10, and Regulation S-P (as it currently exists and as it is proposed to be amended)."[54]

IMPLICATIONS

If adopted as proposed, Proposed Rule 10 would have significant implications for the Market Entities subject to its requirements. The new standard it proposes for the reporting of a "significant cybersecurity incident" adds to numerous, overlapping federal and state cyber incident reporting requirements for entities in various industries that incorporate different standards. Market Entities would need to evaluate the standard carefully with respect to any potentially significant cybersecurity incident, particularly since, unlike certain other regulatory reporting requirements such as the Federal Bank Regulators' Cyber Incident Reporting Rule and the DFS Cybersecurity Requirements for Financial Services Companies, Proposed Rule 10 would also require companies to publicly file and disclose on their website, at a minimum, any "significant cybersecurity incident" they have experienced in the past year.

In addition, while Proposed Rule 10 requires immediate notification only after the Market Entity has reasonably determined that it has experienced a reportable incident, and thus allows that it may take some time for a Market Entity to make such a reasonable determination, the standard may be challenging to meet depending on the circumstances. For example, key personnel at a Market Entity might reasonably have differing views on whether a particular incident meets the reporting standard, raising questions as to whether or when the Market Entity has made the relevant determination; separately, if key personnel need to be diverted from crisis response work on a given incident to contribute to the analysis and reporting, it could be more challenging to provide immediate notification.

Public companies subject to Proposed Rule 10 would need to carefully consider how the materiality analysis, which generally governs what information may be required to be disclosed regarding current events, relates to the analysis of what cybersecurity incidents are "significant." Similarly, public companies will need to evaluate how the materiality analysis, which generally governs their cybersecurity and other risk factor disclosures, relates to the requirement under Proposed Rule 10 that they publicly file and disclose on their websites a "summary description" of their "cybersecurity risks," a term that, as currently proposed, is broadly defined and incorporates neither a materiality standard nor a minimum threshold.

Proposed Rule 10 also leaves significant questions unanswered about how its requirements for the submission of an amended Form SCIR on a "significant cybersecurity incident" should be interpreted. The proposing release does not offer guidance on how Covered Entities should assess what new information is appropriately considered material with respect to a previously reported incident, or when "any information" previously reported on a Form SCIR regarding an incident should be deemed "materially inaccurate." Given how quickly Covered Entities will be required to submit the initial Form SCIR, for example, and that the form will include both information about the significant cybersecurity incident and the Covered Entity's efforts to respond to, and recover from, the incident, Covered Entities may continue to learn new information on an ongoing basis, and engage in significant activity to respond to and recover from the incident, after the initial Form SCIR is submitted. It is also not uncommon in responding to a cybersecurity incident for companies to learn information that causes their initial understanding of facts to change, including as to the nature, scope, and root cause of an incident. In this context, the questions of what information is material, and when the materiality determination can appropriately be made with reasonable certainty, may be challenging to answer under certain circumstances.

With respect to the proposed amendments to Regulation S-P, the SEC's new "federal minimum standard" requiring entities subject to Regulation S-P to notify affected individuals of a breach of sensitive personal information within 30 days or less may, depending on the circumstances, be challenging to meet and raise collateral issues. With respect to timing, for example, an entity responding to a data breach may identify that an individual's personal information has been compromised but need to undertake additional investigation and analysis to identify the nature and scope of the affected information and prepare responses to questions the individual may reasonably be expected to ask upon receiving notification. Entities that provide such information piecemeal, or that are unprepared to answer customers' questions, could be subject to criticism, reputational harms, and additional costs. Relatedly, the 30-day deadline may, under certain circumstances, create a risk of straining or diverting critical company resources otherwise devoted to responding to a cybersecurity incident. Notably, in imposing this "federal minimum standard," the amendments would require quicker notification than the notification laws of 47 states that impose less stringent or no specific deadlines for breach notification.

* * *

ENDNOTES

1 Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, SEC Release No. 34-97142 (Mar. 15, 2023) (the "Rule 10 Release"), at 1; Press Release, Securities and Exchange Commission, SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets (Mar. 15, 2023), https://www.sec.gov/news/press-release/2023-52.

2 Fact Sheet, Securities and Exchange Commission, Regulation SCI: Proposed Expansion and Updates, at 1-2 (Mar. 15, 2023), https://www.sec.gov/files/34-97143-fact-sheet.pdf.

3 Press Release, Securities and Exchange Commission, SEC Proposes Changes to Reg S-P to Enhance Protection of Customer Information (Mar. 15, 2023), https://www.sec.gov/news/press-release/2023-51.

4 Fact Sheet, Securities and Exchange Commission, Addressing Cybersecurity Risks to the U.S. Securities Markets, at 2 (Mar. 15, 2023), https://www.sec.gov/files/34-97142-fact-sheet.pdf; Fact Sheet, Securities and Exchange Commission, Regulation SCI: Proposed Expansion and Updates, at 2; Fact Sheet, Securities and Exchange Commission, Proposed Enhancements to Regulation S-P, at 2 (Mar. 15 2023), https://www.sec.gov/files/34-97141-fact-sheet.pdf.

5 Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 88 Fed. Reg. 16921 (Mar. 21, 2022).

6 Rule 10 Release, at 7-23.

7 *Id*. at 23, 53-58.

8 *See* Amendments Regarding the Definition of ''Exchange'' and Alternative Trading Systems (ATSs) That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities, 87 Fed. Reg. 15496 (Mar. 18, 2022); Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590 (Mar. 23, 2022); Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 13524 (Mar. 9, 2022) ("Investment Management Cybersecurity Release").

9 *See* Press Release, Transportation Security Administration, TSA Issues New Cybersecurity Requirements for Airport and Aircraft Operators (Mar. 7, 2023), https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202; Press Release, Transportation Security Administration, TSA Issues New Cybersecurity Requirements for Passenger and Freight Railroad Carriers (Oct. 18, 2022), https://www.tsa.gov/news/press/releases/2022/10/18/tsa-issues-new-cybersecurity-requirements-passenger-and-freight.

10 *See* Press Release, Federal Communications Commission, FCC Proposes Updated Data Breach Reporting Requirements (Jan. 6, 2023), https://www.fcc.gov/document/fcc-proposes-updated-data-breach-reporting-requirements.

11 *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

12 Exec. Order No. 14,208 (May 12, 2021); Fact Sheet, President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks (May 12, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/; Fact Sheet, The White House, Biden-Harris

ENDNOTES (CONTINUED)

Administration Announces National Cybersecurity Strategy (Mar. 2, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/; THE WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY (2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf; Fact Sheet, The White House, Biden-Harris Administration Expands Public-Private Cybersecurity Partnership to Chemical Sector (Oct. 26, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/26/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-chemical-sector/; National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, The White House (July 28, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/; Fact Sheet, The White House, Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure (July 28, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/.

13 Fact Sheet, Securities and Exchange Commission, Addressing Cybersecurity Risks to the U.S. Securities Markets, at 1.

14 *Id*. at 2.

15 *Id*. at 1.

16 *Id*. at 2.

17 *Id*. at 2.

18 Rule 10 Release, at 139-140.

19 *Id*. at 76-77.

20 *Id*. at 79-81.

21 *Id*. at 79-81.

22 *Id*. at 143.

23 Fact Sheet, Securities and Exchange Commission, Addressing Cybersecurity Risks to the U.S. Securities Markets, at 2.

24 Rule 10 Release, at 147-48.

25 Fact Sheet, Securities and Exchange Commission, Addressing Cybersecurity Risks to the U.S. Securities Markets, at 2.

26 *Id*. at 2.

27 Rule 10 Release, at 83.

28 *Id*. at 81.

29 *Id*. at 82.

30 Press Release, Securities and Exchange Commission, SEC Proposes to Expand and Update Regulation SCI (Mar. 15, 2023), https://www.sec.gov/news/press-release/2023-53.

31 *Id*.

32 Fact Sheet, Securities and Exchange Commission, Regulation SCI: Proposed Expansion and Updates, at 2.

33 *Id*. at 2.

34 *Id*. at 1.

35 *Id*. at 1-2.

ENDNOTES (CONTINUED)

36 *Id*. at 2.

37 Regulation Systems Compliance and Integrity, SEC Release No. 34-97143 (Mar. 15, 2023 (the "Reg. SCI Release"), at 139-40.

38 Fact Sheet, Securities and Exchange Commission, Regulation SCI: Proposed Expansion and Updates, at 2.

39 Fact Sheet, Securities and Exchange Commission, Proposed Enhancements to Regulation S-P, at 1.

40 Press Release, Securities and Exchange Commission, SEC Proposes Changes to Reg S-P to Enhance Protection of Customer Information.

41 Fact Sheet, Securities and Exchange Commission, Proposed Enhancements to Regulation S-P, at 1-2.

42 *Id*. at 2.

43 Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, SEC Release Nos. 34-97141; IA-6262; IC-34854 (Mar. 15, 2023) (the "Reg. S-P Releases"), at 42.

44 Reg. S-P Releases, at 42, 231.

45 Fact Sheet, Securities and Exchange Commission, Proposed Enhancements to Regulation S-P, at 2.

46 Reg. S-P Releases, at 74.

47 *Id*. at 74-75.

48 Fact Sheet, Securities and Exchange Commission, Proposed Enhancements to Regulation S-P, at 2.

49 *Id*. at 2.

50 Press Release, Securities and Exchange Commission, SEC Proposes Changes to Reg S-P to Enhance Protection of Customer Information; Fact Sheet, Securities and Exchange Commission, Proposed Enhancements to Regulation S-P, at 1-2.

51 Press Release, Securities and Exchange Commission, SEC Proposes Changes to Reg S-P to Enhance Protection of Customer Information.

52 Rule 10 Release, at 89-264.

53 Reg. S-P Releases, at 63.

54 Reg. SCI Release, at 179.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 900 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.