SULLIVAN & CROMWELL LLP

S&C memo

July 28, 2023

SEC Adopts New Cybersecurity Disclosure Rules for Public Companies

Rules Will Require Disclosure of Material Cybersecurity Incidents Within Four Business Days, as well as Annual Cybersecurity Risk Management, Strategy and Governance Disclosures

SUMMARY

On July 26, 2023, the Securities and Exchange Commission adopted new rules (the "Final Rules") requiring registrants to disclose material cybersecurity incidents and material information regarding cybersecurity risk management, strategy and governance.[1] The SEC had originally released its proposed rules governing cybersecurity related topics (the "Proposed Rules") on March 9, 2022, which are discussed in our Memorandum to Clients, dated March 11, 2022.[2] The Final Rules track the Proposed Rules in many respects, with certain significant changes, and represent a significant expansion of the SEC's existing cybersecurity disclosure framework.

The Final Rules will require:

- disclosure under a new Item 1.05 of Form 8-K of the material aspects of the nature, scope and timing and material impact, or reasonably likely material impact, of a cybersecurity incident within four business days of determining that the incident is material;
- disclosure in Form 10-K of processes for assessing, identifying and managing material risks from cybersecurity threats; and
- disclosure in Form 10-K of governance practices relating to cybersecurity risks, including by a company's management and board of directors.

The Final Rules will subject foreign private issuers to the same disclosure requirements in their Form 20-Fs. However, foreign private issuers will not be subject to the prompt disclosure requirements of new Item 1.05 of Form 8-K. Instead, foreign private issuers will be required to furnish on Form 6-K information on material

cybersecurity incidents that they otherwise disclose in a non-U.S. jurisdiction to any stock exchange or to security holders (in the same way as they furnish Form 6-Ks for other material disclosures made in the home country).

Significantly, in response to numerous comments, the Final Rules will not require disclosure of three significant provisions that had been in the Proposed Rules: disclosure in the Form 8-K as to whether the cybersecurity incident is still ongoing, its remediation status, or whether data at issue were compromised; disclosure of immaterial incidents that may in the aggregate be material; and disclosure of the board's cybersecurity expertise. Concerns regarding the original proposed language, which the SEC has now modified or removed, are outlined in our prior Memorandum to Clients on the Proposed Rule.

The Final Rules will become effective 30 days following publication of the adopting release in the Federal Register. All registrants (other than smaller reporting companies, which will have an additional 180 days) will need to begin complying with the disclosure requirements relating to material cybersecurity incidents in Item 1.05 of Form 8-K and in Form 6-K on the later of (i) 90 days after the date of publication of the adopting release in the Federal Register or (ii) December 18, 2023. Registrants will be required to provide disclosures responsive to new Item 106 of Regulation S-K and the comparable requirements in Form 20-F beginning with annual reports for fiscal years ending on or after December 15, 2023 (for December 31 fiscal year end filers, the 2023 Form 10-K filed in early 2024).

BACKGROUND

Existing Disclosure Framework

In 2011, the SEC issued interpretive guidance noting that U.S. securities laws require disclosure of material computer-system intrusions and information-technology risks, even though the laws do not explicitly address cybersecurity. In 2018, applying its traditional principles-based approach to disclosure requirements, the SEC issued further interpretive guidance stating, among other things, that to the extent material, companies should specifically describe cybersecurity incidents and the nature of their boards' roles in overseeing management of cybersecurity risks and emphasizing the need for comprehensive disclosure policies and procedures relating to cybersecurity. In response to the 2011 and 2018 guidance, many registrants include cybersecurity-related disclosures in their annual and quarterly reports, generally in the form of risk factors and disclaimers about forward-looking statements, as well as in disclosures in their proxy statements regarding board or committee oversight of cybersecurity risks. However, in adopting the Final Rules, the SEC noted in the adopting release (the "Adopting Release") that the SEC "remain[ed] convinced that investors need timely, standardized disclosure regarding cybersecurity incidents materially affecting registrants' businesses, and that the existing regulatory landscape is not yielding consistent and informative disclosure of cybersecurity incidents from registrants."

The Proposed Rules and SEC Background

On March 9, 2022, the SEC released the Proposed Rules at a time when the SEC was becoming increasingly concerned about the timely disclosure of cybersecurity risks and incidents as those risks were becoming more pronounced and incidents continued to grow in scale and impact.[3] The SEC noted in the Proposing Release that "cybersecurity is among the most critical governance-related issues for investors, especially U.S. investors."[4] In the SEC's view, "investors would benefit from more timely and consistent disclosure about material cybersecurity incidents," and "from greater availability and comparability of disclosure by public companies across industries regarding their cybersecurity risk management, strategy and governance practices in order to better assess whether and how companies are managing cybersecurity risks."[5] Although the Proposed Rules were generally consistent with the SEC's historical principles-based approach to cybersecurity incident disclosures, they would have imposed explicit timing and content requirements on cyber-related incident disclosures and added required disclosures of cybersecurity risk management, strategy and governance without regard to materiality.

The Proposed Rules were issued against the backdrop of increased enforcement efforts by the SEC. In the last few years, the number of enforcement actions brought by the SEC has risen sharply, alleging inadequate disclosure controls and procedures, and failure to make timely disclosure of material information relating to cybersecurity incidents.[6] Recent years have also seen focused attention on investigating potential cybersecurity issues. For example, following the discovery of the compromise of SolarWinds software in December 2020, through which a threat actor thought to be based in the Russian Federation had infiltrated U.S. federal agencies and reportedly over 18,000 companies, the SEC has been engaged in a widely reported inquiry regarding the SolarWinds compromise.[7] Just this week, Judge Amit Mehta of the U.S. District Court for the District of Columbia ordered a law firm to identify seven of its clients to the SEC as part of an SEC investigation into possible insider trading or other securities violations resulting from a 2020 cyberattack on the law firm that may have compromised material nonpublic information.[8]

Broader National Context

The Final Rules follow recently issued cybersecurity standards and disclosure requirements, including:

- ***Notification Requirements:***
  - the passage of the *Cyber Incident Reporting for Critical Infrastructure Act*, signed into law March 15, 2022, which mandates that critical infrastructure entities report certain cybersecurity incidents to the government within 72 hours and requires 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";[9]
  - cybersecurity disclosure requirements imposed by the Department of Homeland Security in 2021 for companies in a range of critical infrastructure sectors, including certain requirements that cybersecurity incidents be disclosed to CISA within 24 hours;[10]
  - rules proposed in 2023 by the SEC's Division of Trading and Markets and the Federal Communications Commission ("FCC") to strengthen data breach reporting requirements, which

would require "immediate" notification under the SEC rule, and notification "as soon as practicable" under the FCC's rule;[11]

- rules adopted by federal banking regulators in 2021 mandating disclosure to the agencies of certain significant cybersecurity incidents within 36 hours;[12] and
- last month, an amendment to a proposed regulation by the New York State Department of Financial Services, which would mandate the implementation of certain cybersecurity controls for covered entities and enhance notification requirements, including requiring notification to the superintendent within 72 hours of determining that certain cybersecurity events have occurred.[13]

- ***Affirmative Cybersecurity Standards:***
  - cybersecurity amendments for airports, aircraft operators, and railroad carriers imposed by the Transportation Security Administration requiring covered entities to develop and implement plans to improve their cybersecurity resilience and prevent disruption to their infrastructure;[14]
  - guidance from the Treasury's Office of Foreign Assets Control that offers a mitigated enforcement response where a company that unknowingly made a ransomware payment in violation of sanctions regulations had an adequate cybersecurity program prior to the attack and disclosed and cooperated fully with law enforcement during and after the attack;[15]
  - guidance from the Treasury's Financial Crimes Enforcement Network ("FinCEN") stating that ransomware attacks and related transactions should be reported immediately to law enforcement and FinCEN;[16] and
  - new privacy laws passed by state legislatures in California, Colorado, Connecticut, Indiana, Iowa, Texas, Tennessee, Utah, and Virginia and under consideration in Illinois, Oregon, New York, and other jurisdictions.

The Final Rules and other new federal and state requirements follow a series of high profile cybersecurity attacks that have harmed U.S. national security and the private sector in recent years. These include the SolarWinds attack; Russian ransomware gang Cl0p's breach of the MOVEit secure file transfer software that is reported to have impacted hundreds of companies and organizations and tens of millions of individuals;[17] and, most recently, the compromise of Microsoft by a suspected Chinese threat actor, resulting in access to thousands of U.S. government emails.[18]

OVERVIEW OF THE FINAL RULES

The Final Rules track the Proposed Rules and amendments in many respects, but include some significant changes, including a streamlining of the scope of cybersecurity incident disclosures, requiring updated cybersecurity incident disclosures on an amended Form 8-K instead of on Forms 10-Q and 10-K for domestic registrants (and on Form 6-K for foreign private issuers, to the extent those foreign private issuers are required to disclose in foreign jurisdictions), the omission of the proposed aggregation of immaterial incidents for materiality analyses, and the removal of disclosure requirements concerning board cybersecurity expertise.

New Form 8-K Requirements

The Final Rules add a new Item 1.05 to Form 8-K that will require disclosure of material cybersecurity incidents within four business days after a registrant determines that it has experienced a material cybersecurity incident.

Content. Item 1.05 will require the registrant to describe "the material aspects of the nature, scope, and timing of the cybersecurity incident, and the material impact or reasonably likely material impact" on the registrant, including its financial condition and results of operations. This is a significant narrowing of the scope of the Item 1.05 disclosure articulated in the Proposed Rules, which would have required significantly more information to be disclosed, in some cases without regard to materiality. While the Adopting Release does not provide specific examples of incidents that may require disclosure on Form 8-K, the Proposing Release had provided the following non-exhaustive list, which may be helpful for companies in considering the sorts of incidents potentially covered by the Final Rules:

- An unauthorized incident that has compromised the confidentiality, integrity or availability of an information asset (data, system or network); or violated the registrant's security policies or procedures. Incidents may stem from the accidental exposure of data or from a deliberate attack to steal or alter data;
- An unauthorized incident that caused degradation, interruption, loss of control, damage to or loss of operational technology systems;
- An incident in which an unauthorized party accessed, or a party exceeded authorized access, and altered, or has stolen sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the registrant;
- An incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data; or
- An incident in which a malicious actor has demanded payment to restore company data that was stolen or altered.

The Final Rules include an Instruction 4 to Item 1.05, clarifying that a registrant will not be expected to disclose specific, technical information about its planned response to a cybersecurity incident or its cybersecurity systems, related networks and devices or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident.

In another important change from the Proposed Rules, the SEC did not adopt a requirement for disclosure regarding a cybersecurity incident's remediation status, whether it is ongoing, and whether data were compromised.

Timing. The new disclosure requirement will be tied to the date the registrant determines the cybersecurity incident is material, rather than the date of discovery of the incident. However, a registrant will be required to make a materiality determination regarding a cybersecurity incident "without unreasonable delay" after discovery of the incident. In the Adopting Release, the SEC notes that the "instruction was intended to address any concern that some registrants may delay making such a determination to avoid a disclosure

obligation" and provides a few examples of "unreasonable delays," including the intentional deferral of a board or committee meeting or extension of incident severity assessment deadlines. Consistent with the Proposed Rules, the SEC is also amending Form S-3 to provide that untimely filing of an Item 1.05 Form 8-K will not result in loss of Form S-3 eligibility.

Materiality Determination. In the Adopting Release, the SEC underscores that the reference to an incident having, or being reasonably likely to have, a material impact on a registrant, including its "financial condition and results of operations," is not exclusive, and that registrants will need to consider both quantitative and qualitative factors, taking into consideration the total mix of information and all relevant facts and circumstances, when assessing materiality of a cybersecurity incident. Harm to a registrant's "reputation, customer or vendor relationships, or competitiveness" and the potential for "litigation or regulatory investigations" are noted as examples that may constitute a reasonably likely material impact on the registrant.

The SEC notes in the Adopting Release that "[d]oubts as to the critical nature" of the relevant information "will be commonplace" and should "be resolved in favor of those the statute is designed to protect, namely investors."

With respect to incidents on third-party vendor systems, the SEC also notes in the Adopting Release that it is "not exempting registrants from providing disclosures regarding cybersecurity incidents on third-party systems they use, nor [is it] providing a safe harbor for information disclosed about third-party systems." However, the Adopting Release clarifies that registrants generally will not be required to conduct additional inquiries outside of their regular channels of communication with third-party service providers pursuant to those contracts and in accordance with registrants' disclosure controls and procedures. This policy is consistent with the SEC's general rules relating to information that is difficult to obtain.[19]

Reporting Delay Provisions. In a change from the Proposed Rules, the Final Rules include a provision pursuant to which registrants may delay making an Item 1.05 Form 8-K filing if the Attorney General determines that the disclosure poses a substantial risk to national security or public safety and notifies the SEC of the determination in writing. Disclosure may be delayed for a time period specified by the Attorney General, up to 30 days (which may be extended in certain cases) following the date when the disclosure was otherwise required to be provided. The Adopting Release emphasizes the SEC's belief that designating the Department of Justice as the single point of contact for such determinations is "critical to ensuring that the rule is administrable" and notes the SEC's intention to establish an interagency communication process with the Department of Justice to allow the Attorney General to communicate such determinations with the SEC in a timely manner.

In addition, in the Final Rules, the SEC has added a new paragraph (d) to Item 1.05, which provides that registrants subject to the FCC's rule requiring notification in the event of breaches of customer proprietary network information ("CPNI"), who are required to notify the United States Secret Service ("USSS") and the

Federal Bureau of Investigation ("FBI") within seven days after reasonable determination of a CPNI breach, may delay making an Item 1.05 Form 8-K disclosure up to the seven business day period following notification to the USSS and FBI upon written notification to the SEC.

Requirement to Update Previously Disclosed Cybersecurity Incidents on Form 8-K Amendment. In order to mitigate commenters' concerns with proposed Item 106(d)(1), which would have required registrants to disclose "any material changes, additions, or updates" to previously provided disclosure regarding one or more cybersecurity incidents pursuant to Item 1.05 of Form 8-K in the registrant's Quarterly Report on Form 10-Q or Annual Report on Form 10-K, the new Instruction 2 to Item 1.05 of Form 8-K instead requires a registrant to include in its Item 1.05 Form 8-K a statement identifying any information called for in Item 1.05(a) that is either not determined or unavailable at the time of the required filing and then file an amendment to its original Form 8-K containing such information within four business days after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available.

No Requirement to Disclose Cybersecurity Incidents That Have Become Material in the Aggregate. In a significant departure from the Proposed Rules, the SEC did not adopt proposed Item 106(d)(2), which, as discussed in our March 11, 2022 Memorandum to Clients, would have required disclosure in a registrant's Quarterly Report on Form 10-Q or Annual Report on Form 10-K of previously undisclosed, individually immaterial cybersecurity incidents when a determination is made that such incidents are material when viewed in the aggregate, due to concerns that the proposed aggregation requirement was vague and difficult to apply. However, the Adopting Release emphasizes that the term "cybersecurity incident" is to be construed broadly, and that the definition of "cybersecurity incident" extends to "a series of related unauthorized occurrences" such that Item 1.05 disclosure may nonetheless be triggered by a series of individually immaterial cybersecurity incidents. Specifically, the SEC notes that if a company has been materially affected by what may appear as a series of related cyber intrusions, Item 1.05 may be triggered even if the material impact or reasonably likely material impact was divided among the multiple intrusions such that each intrusion, assessed individually, was immaterial. The SEC also provides the following examples of incidents that, in the aggregate, may be material: (1) if the same malicious actor engages in a number of small, continuous cyberattacks related in time and form against the same company, which, collectively, are either quantitatively or qualitatively material; and (2) if there are a series of related attacks from multiple actors exploiting the same vulnerability, which collectively impede the company's business materially.

New Form 10-K Disclosure Requirements (For Foreign Private Issuers, Form 20-F)

Amendments to Form 10-K and Form 20-F Regarding Cybersecurity Processes and Governance. New Item 106 of Regulation S-K will require disclosure in Annual Reports on Form 10-K (and on Form 20-F for foreign private issuers) of cybersecurity risk management, strategy and governance, including:

- ***Processes for identifying and managing cybersecurity risks.*** Disclosure will be required to describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, (i) whether and how such processes have been integrated into the registrant's overall risk management system or processes; (ii) whether the registrant engages assessors, consultants, auditors or other third parties in connection with any such processes; and (iii) whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider. However, the SEC notes that this is a non-exclusive list of potential disclosures and registrants should disclose other information as necessary for a reasonable investor to understand the registrant's cybersecurity processes. Disclosure will also be required as to whether cybersecurity risks have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations or financial condition and, if so, how.
- ***The board of directors' role in cyber governance.*** Item 106(c) will require disclosure regarding the board of directors' oversight of risks from cybersecurity threats, including (i) whether the entire board of directors, specific board members or a board committee is responsible for the oversight of cybersecurity risks and (ii) the processes by which the board of directors or such committee is informed about cybersecurity risks. In an important change from the Proposed Rules, the SEC did not adopt a requirement for registrants to disclose whether any member of the board of directors has cybersecurity expertise and, if so, the director's name and details sufficient to fully describe the nature of the expertise.
- ***Management's role in cyber governance.*** Item 106(c) will require disclosure of management's role in assessing and managing material cybersecurity risks and related policies, procedures and strategies, including:
  - Whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents, and the relevant expertise of such persons or members;
  - The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection and remediation of cybersecurity incidents; and
  - Whether such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risk.

Proposed Item 106(d)(1) would have required disclosure of changes to the registrant's policies and procedures as a result of previous cybersecurity incidents. This proposal was not adopted by the Commission in response to comments voicing concerns that the requirement was unnecessary and overly broad.

Foreign Private Issuers. The Final Rules also amend Form 6-K to add "material cybersecurity incidents" as a reporting topic; however, as with all other Form 6-K disclosure items, foreign private issuers are only required to disclose on Form 6-K cybersecurity incidents to the extent that they are required to disclose them elsewhere. As a result, for many foreign private issuers, the additional compliance burden for this particular requirement is expected to be minor. For instance, issuers subject to the Market Abuse Regulation ("MAR") in the European Union will already be subject to prompt disclosure or publication obligations under MAR. When a foreign private issuer must file a 6-K but seeks to delay its report, it must also seek a determination from the U.S. Attorney General that disclosure would pose a substantial risk to national security or public safety in the same way as U.S. registrants.

iXBRL. Information disclosed under the Final Rules will need to be tagged using inline XBRL beginning one year after initial compliance with the applicable disclosure requirement, described below.

TIMING

The Final Rules will become effective 30 days following publication of the adopting release in the Federal Register. All registrants (other than smaller reporting companies, which have an additional 180 days) must begin complying with the incident disclosure requirements in Form 8-K Item 1.05 and in Form 6- K on the later of 90 days after the date of publication of the adopting release in the Federal Register or December 18, 2023. Registrants will be required to provide disclosures responsive to new Item 106 of Regulation S-K and the comparable requirements in Form 20-F beginning with annual reports for fiscal years ending on or after December 15, 2023.

IMPLICATIONS

Disclosure of Cybersecurity Incidents on Form 8-K

As previewed in our Memorandum to Clients on the Proposed Rules, the four-business-day window to disclose material cybersecurity incidents on Form 8-K may raise challenges in a number of contexts.

- ***Materiality Determinations.*** The question of whether a particular cybersecurity incident, or series of incidents, is material may not be easy to determine depending on the circumstances. As the facts and the company's understanding of the nature and impact of a cybersecurity incident may quickly evolve, companies may be challenged to identify and assess the materiality of a cybersecurity incident in order to report on a timely basis, and may need to update that disclosure as the incident evolves.
- ***Ongoing Cybersecurity Incidents.*** In certain circumstances, companies experiencing an ongoing cybersecurity incident may have a concern that the very fact of public disclosure of the incident may expose them to additional security risk or harm. For example, if the company must disclose an incident before it has been able to eradicate malicious actors from its systems, it could potentially face risk that the malicious actors take additional action in response to the disclosure, including taking steps to more carefully evade detection and eradication. As another example, a company that is required to disclose a data extortion or ransomware attack in the midst of responding to it may face risk that the perpetrators change their behavior to the company's detriment in response to the disclosure, for example, by increasing the size of their payment demand or otherwise heightening their threats to disclose stolen data or further harm the company.
- ***Incidents Involving Other Disclosure Obligations and Relationship Management.*** The four-business-day disclosure window will put additional pressure on registrants who will need to balance the competing demands of meeting obligations with respect to the timing and content of communications with regulators and state attorneys general, containing and remediating the cyber breach, managing relationships with customers and relevant counterparties, and notifying impacted customers and individuals. Foreign private issuers might need to seek a determination that delay is appropriate from the U.S. Attorney General even where foreign law enforcement agencies would be the principal agencies investigating the attack and its implications for national security or public safety.
- ***Incidents Involving Personally Identifying Information.*** The four-business-day disclosure window may create particular challenges in connection with incidents involving unauthorized access to or disclosure of individuals' personally identifying information. It is not uncommon for a

company that has experienced such an incident to need additional time to determine the nature and scope of the information accessed. As a result, the Form 8-K disclosure may lead to incoming questions and requests from potentially affected individuals that the company is not in a position to answer, including as to whether and to what extent any particular individual was affected. That situation could expose the company to reputational or other harms, and divert internal resources and attention at a time when the company is already strained in responding to a material cybersecurity incident.

Disclosure Controls and Procedures

Registrants should also evaluate their existing cyber-incident reporting and cyber risk-assessment disclosure controls and procedures in light of the Final Rules. In particular, registrants should consider whether:

- their existing disclosure controls would escalate information in a timely fashion in light of the new, time-sensitive disclosure requirements in Item 1.05 of Form 8-K;
- their existing disclosure controls and procedures adequately cover security incidents that may occur on third-party platforms;
- there is an appropriate framework in place to identify patterns in cybersecurity incidents over time and incorporate issues identified by front-line cybersecurity professionals into disclosure controls and procedures; and
- their existing controls and procedures allow for timely and appropriate materiality determinations to be made, especially in the context of a series of related cybersecurity incidents that result or are reasonably likely to result in a material impact to the registrant.

Given its heightened investigation and enforcement activity, the SEC can be expected to continue to scrutinize the adequacy of companies' disclosures regarding cybersecurity matters, including with respect to the new disclosure requirements set forth in the Final Rules.

* * *

ENDNOTES

1 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, SEC Release Nos. 33-11216; 34-97989; File No. S7-09-22 (July 26, 2023) (the "Adopting Release"). *See also* SEC Fact Sheet: Public Company Cybersecurity; Final Rules (July 26, 2023), *available at* https://www.sec.gov/files/33-11038-fact-sheet.pdf. The Final Rules were adopted by a 3 to 2 vote.

2 We published a memorandum discussing the Proposed Rules in March 2022. Sullivan & Cromwell LLP, *SEC Proposes New Cybersecurity Disclosure Rules for Public Companies* (Mar. 11, 2022), *available at* https://www.sullcrom.com/SullivanCromwell/_Assets/PDFs/Memos/sc-publication-sec-proposes-new-cybersecurity-disclosure-rules-for-public-companies.pdf.

3 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, SEC Release Nos. 33-11038; 34-943529; IC-34529 (March 9, 2022) (the "Proposing Release"). *See also* SEC Fact Sheet: Public Company Cybersecurity; Proposed Rules (Mar. 9, 2022), *available at* https://www.sec.gov/files/33-11038-fact-sheet.pdf.

4 *Id.* at 11.

5 *Id.* at 12.

6 *See* SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack that Impacted Charitable Donors (Mar. 9, 2023), https://www.sec.gov/news/press-release/2023-48; SEC Charges Issuer With Cybersecurity Disclosure Controls Failures (June 15, 2021), https://www.sec.gov/news/press-release/2021-102; SEC Charges Issuer with Misleading Investors About Cybersecurity Incident and for Inadequate Disclosure Controls, Sullivan & Cromwell Memo (Aug. 18, 2021), *available at* https://www.sullcrom.com/SullivanCromwell/_Assets/PDFs/Memos/sc-publication-SEC-brings-cybersecurity-charges-against-issuer.pdf; and SEC Sanctions Firms in Three Actions for Deficient Cybersecurity Controls, Sullivan & Cromwell Memo (Sept. 1, 2021), *available at* https://www.sullcrom.com/SullivanCromwell/_Assets/PDFs/Memos/SC-Publication-SEC-Sanctions-Firms-For-Deficient-Cybersecurity-Controls.pdf.

7 *See* SolarWinds Corporation, Current Report (Form 8-K) (June 23, 2023), *available at* https://www.sec.gov/Archives/edgar/data/1739942/000173994223000079/swi-20230623.htm.

8 *SEC* v. *Covington & Burling, LLP*, No. 23-MC-00002 (APM), 2023 WL 4706125 (D.D.C. July 24, 2023).

9 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.

10 *See* Press Release, Department of Homeland Security, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (May 27, 2021), *available at* https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators; Press Release, Department of Homeland Security, DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators (Dec. 2, 2021), *available at* https://www.dhs.gov/news/2021/12/02/dhs-announces-new-cybersecurity-requirements-surface-transportation-owners-and.

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

ENDNOTES (CONTINUED)

12 In November 2021, the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC) and the Federal Reserve Board of Governors jointly issued a final rule that requires banking organizations and service providers to notify their primary regulator within 36 hours after determining that a "cyber-security incident that rises to the level of a notification incident has occurred." Financial Institution Letter, Computer-Security Incident Notification Final Rule (Nov. 18, 2021), https://www.fdic.gov/news/financial-institution-letters/2021/fil21074.html. *See* Federal Banking Agencies Issue Final Rule Regarding Cyber Incident Notification Requirements (Nov. 22, 2021), *available at* https://www.sullcrom.com/files/upload/sc-publication-federal-banking-regulators-mandate-cybersecurity-incident-notification.pdf.

13 Cybersecurity Resource Center: Proposed Second Amendment to 23 NYCRR Part 500, DFS, https://www.dfs.ny.gov/industry_guidance/cybersecurity; Revised Proposed Second Amendment to 23 NYCRR 500, https://www.dfs.ny.gov/system/files/documents/2023/06/rev_rp_23a2_text_20230628.pdf.

14 *See* Press Release, Transportation Security Administration, TSA Issues New Cybersecurity Requirements for Airport and Aircraft Operators (Mar. 7, 2023), *available at* 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), *available at* https://www.tsa.gov/news/press/releases/2022/10/18/tsa-issues-new-cybersecurity-requirements-passenger-and-freight.

15 *See* OFAC Updates Ransomware Advisory, Sullivan & Cromwell Memo (Sept. 23, 2021), *available at* https://www.sullcrom.com/SullivanCromwell/_Assets/PDFs/Memos/SC-Publication-OFAC-Updates-Ransomeware-Advisory-Designates-Crypto-Exchange.pdf.

16 *See* FinCEN Updates Ransomware Advisory, Sullivan & Cromwell Memo (Nov. 11, 2021), *available at* https://www.sullcrom.com/SullivanCromwell/_Assets/PDFs/Memos/sc-publication-fincen-updates-advisory-regarding-reporting-ransomware-payments.pdf.

17 *See* Zach Simas, *Unpacking the MOVEit Breach: Statistics and Analysis*, EMSISOFT BLOG (Jul. 18, 2023), https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/ [https://web.archive.org/web/20230727173014/https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/].

18 *See* Charlie Bell, *Mitigation for China-based threat actor activity*, THE OFFICIAL MICROSOFT BLOG (Jul. 11, 2023), https://blogs.microsoft.com/on-the-issues/2023/07/11/mitigation-china-based-threat-actor/ [https://web.archive.org/web/20230727012204/https://blogs.microsoft.com/on-the-issues/2023/07/11/mitigation-china-based-threat-actor/].

19 Proposing Release at 31; *see also* 17 CFR 230.409 and 17 CFR 240.12b-21, which provide that information need only be disclosed insofar as it is known or reasonably available to the registrant.

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.