Google Cloud

June 5, 2023

Submitted via email to rule-comments@sec.gov (Files S7-06-23 and S7-05-23)

U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090.

Re: Exchange Act Cybersecurity and Regulation S-P Proposals

On March 15, 2023, the Securities and Exchange Commission (Commission) proposed new requirements 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 to address their cybersecurity risks (hereinafter referred to as "Exchange Act Cybersecurity Proposal"). On the same day, the Commission proposed amendments to Regulation S-P to "enhance the protection of customer information by, among other things, requiring broker-dealers, investment companies, registered investment advisers, and transfer agents to provide notice to individuals affected by certain types of data breaches that may put them at risk of identity theft or other harm" (hereinafter referred to as "Regulation S-P Proposal").

The two sets of proposals, while each with a distinct scope and purpose, have a fair degree of overlap.[1] One notable area of overlap between the proposals is in the area of engagement with, and obligations relating to, third-party service providers. The changes proposed to the Exchange Act Cybersecurity Proposal would, *inter alia*, require subject financial institutions (FIs) to assess cybersecurity risks associated with their use of services from third-party providers. The proposal would also require subject FIs to conduct oversight of such service providers "pursuant to a written contract" including certain specified practices "designed to protect the covered entity's information systems and information residing on those systems" (e.g., relating to management of access to subject information systems etc.).

[1] According to the Commission "The Exchange Act Cybersecurity Proposal would have several policies and procedures requirements that are designed to address similar cybersecurity-related risks to these proposed requirements of Regulation S-P. First, under the Exchange Act Cybersecurity Proposal, a Covered Entity's policies and procedures would require measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems and the information residing on those systems. Second, under the Exchange Act Cybersecurity Proposal, a Covered Entity's policies and procedures would require incident response measures designed to detect, respond to, and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure, among other things, the protection of the Covered Entity's information systems and the information residing on those systems."

The proposals to Reg S-P would similarly "require covered institutions, pursuant to a written contract between the covered institution and its service providers, to require the service providers to take appropriate measures that are designed to protect against unauthorized access to or use of customer information, including notification to the covered institution in the event of any breach in security resulting in unauthorized access to a customer information system maintained by the service provider to enable the covered institution to implement its response program."

As a provider of cloud services to the financial industry, Google Cloud welcomes the Commission's proposals. Effective cybersecurity practices and system safeguards, including incident response and notification, are critical for the financial markets and services industry and the regulators tasked with oversight of this sector. To this end, achieving greater global convergence regarding cybersecurity and system safeguard standards, including incident response and reporting, are essential to ensuring that industry actors have clarity and certainty regarding regulatory expectations. This certainty will allow public and private sector stakeholders to focus on the primary objective of detecting, preventing, mitigating, and responding to cyber incident and technology-related risks that pose a reasonable likelihood of materially impacting the operations or security of markets and related intermediaries.

Google Cloud maintains a rigorous process for identifying, mitigating, and in the event one occurs, responding to and remediating data incidents as part of our overall security and privacy program. Our cybersecurity and system safeguards practices are developed with our customers and end-users in mind, and with the core objective of ensuring system integrity. Google Cloud welcomes the opportunity to provide comments on both sets of proposed rules, informed by our experience in this area.

I. Observations and Comments

As noted above, effective cybersecurity and system safeguards, including with respect to incident response and notification, are critical for the financial markets and services industry and the regulators tasked with supervising regulated intermediaries. We urge that the following principles and considerations inform the regulatory effort to modernize these requirements.

1. **Definition of Cybersecurity Incident.** The Exchange Act Cybersecurity Proposal defines "cybersecurity incident" 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." (Emphasis added) We urge the Commission to replace "jeopardizes" with "that results in actual harm to."

As the Commission recognises, "jeopardizes" means to "place at risk" which broadens significantly the scope of obligations beyond those that result in actual harm. This creates a potentially confusing overlap with the concept of a cybersecurity threat.

Further, in the context of incident reporting, in particular, this could have unintended consequences. Specifically, the Exchange Act Cybersecurity Proposal does not have an explicit notification requirement applicable to service providers vis-a-vis their FI customers. However, it does provide that "[a] covered entity must give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring." Given the focus of "significant cybersecurity incident" on the specific impacts to the FI, only the FI will be in a position to determine if a cybersecurity incident is, in fact, significant. As a result, the current definition of "cybersecurity incident" could compel FIs to require service providers to notify the market entity of all cybersecurity incidents – not only those that result in actual harm but also those that present a threat of harm.[2]

Although the service provider should continue to monitor them, events that (could have but) did not result in actual harm should be excluded from the scope of customer notifications. The fact that an event has not resulted in actual information/systems harm is often evidence that the service provider's controls are operating as intended. Reporting of all such events would significantly increase the operational burden on all involved parties, including FIs (who would be receiving excessive volumes of non-actionable information), without a clear benefit. This is likely to distract FIs from true incidents and, at worst, could itself lead to heightened security risks by compromising live investigations of as yet unconfirmed incidents.

[2] While this notification requirement applies to financial institutions, where they are using the services of a third-party supplier, the requirement could result in the requirement being flowed down to service providers in some form. With that in mind, we note that tying notification to the point at which the covered entity has a "reasonable basis to conclude" that a significant cybersecurity incident has occurred or is occurring imposes an objective standard on what is by its nature a highly subjective process. The reality of incident response is that decisions must often be taken relatively quickly based on constantly evolving information. A "reasonably believes" standard could introduce too much uncertainty and invite second-guessing of decisions that are, by necessity, made quickly and potentially without key facts that are only known later. This could incentivize over-reporting that will not benefit covered entities, regulators or other stakeholders. This is recognised in the Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, which ties notification to the point at which the regulated entity determines that a notification incident has occurred: "The OCC must receive this notification from the banking organization as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred." We urge the Commission to consider changing this language from "a reasonable basis to conclude" to "determines" consistent with the banking regulations.

The change proposed to the "cybersecurity incident" definition would also serve to harmonize regulatory approaches across the financial sector. The Federal banking agencies in the Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers have adopted the following definition: "[c]omputer-security incident is an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits."

2. **Third-Party Service Provider Considerations & Contracts.** We applaud the Commission's recognition that third-party service providers, including cloud service providers (CSPs), are playing an increasingly important role in supporting and enhancing financial markets. We further agree that specific attention should be focused on ensuring that regulatory expectations are clear and consistent with respect to providers' role in ensuring that FI customers are able to meet requirements under the proposals.

   To this end, contracts are important tools both for (a) validating the capabilities of a service provider upfront, as well as (b) risk management during the life of the service relationship. However, mandating that contracts between FIs and service providers include provisions requiring providers to implement all the same measures as apply directly to the FIs could (a) create issues that could slow or halt adoption of certain technologies if requirements are not technology neutral, and (b) have negative impacts on security in the long term if requirements are overly specific and overtaken by the speed of technological innovation.

   The practices required to be included in service provider contracts pursuant to the Exchange Act Cybersecurity Proposal (see proposed Section 242.10(b)(1)(i) through (v)) are written from the perspective of the covered entity and not the service provider. This may not be problematic in the context of business process outsourcing where the service provider takes on an entire process/function end-to-end and therefore has the visibility and control to implement measures just as the covered entity could. However, in the public cloud context, responsibility for a number of these practices are within the covered entity's sole control or ability to perform.

   To address customer and regulator expectations of privacy and security, by design, a public cloud infrastructure provider does not have visibility into the type of data the customer is processing on its services. This means the provider would not be able to:

   - perform risk assessments based on the type of information residing on systems ((i)(A));

   - protect information based on the sensitivity level of that information((iii)(A)(1)); or

- assess The impact of a cybersecurity incident on the covered entity's customers, counterparties, members, users ((iii)(A)(5)).

Instead the provider would offer the FI customer security tools that the customer could use to configure the level of security etc required based on their use case.

In the same vein, a public cloud provider would not be able to implement such things as multi-factor authentication (see proposed Section 242.10(b)(ii)(B)) and password management ((see proposed Section 242.10(ii)(C)) on the customer's behalf. These are tools that public cloud providers make available to customers, but customers must make the decision to deploy them.

Mandating covered entities to contractually require all service providers to implement all of these practices when these practices are not compatible with all service delivery models would unnecessarily hinder adoption.

Rather than prescribe the specific practices that must be included in the contract, we suggest that (a) contracts should require service providers to implement and maintain appropriate measures that are consistent with industry standards, and (b) each covered entity should oversee their providers to assess if the provider addresses the relevant practices to an adequate standard. This activity can be supported with third party certifications and standards.

We note that the Commission is exploring allowing this kind of reliance on industry "assurances and certifications," in lieu of specific written contractual provisions, that a service provider is taking appropriate measures to manage cybersecurity risk (*see e.g.,* Exchange Act Cybersecurity Proposal Question 36). We strongly support that approach for the reasons above.

Last, we urge the Commission to consider making any new obligations with respect to contracting forward looking so as not to disrupt contracts already in existence by requiring renegotiation. In considering timeframes for implementation, as well, the Commission should give due regard to the extensiveness of the requirements and the reasonable time that will be needed for new commercial contractual provisions to be negotiated in line with them.

3. **Incident Notification by Service Providers.** An important aspect of an effective incident response process is ensuring that true positives/actual incidents are promptly flagged to affected customers (and subsequently to regulators, where necessary) and that these are not drowned out by false positives/non-material incidents. This helps service providers, FIs, and,

ultimately, regulators focus on the incidents that matter and not expend resources on false or *de minimis* matters. To this end, some amount of reasonable investigation is usually required to distinguish true positives/material incidents from false positives/non-material incidents and to determine whether there is a reasonable likelihood of such material harm.

The Regulation S-P Proposal requires service providers to provide "notification to the covered institution as soon as possible, but no later than 48 hours after becoming aware of a breach, in the event of any breach in security resulting in unauthorized access to a customer information system maintained by the service provider to enable the covered institution to implement its response program." We urge the Commission to make clear that the trigger in this instance (becoming "aware" of a breach that results in unauthorized access) will almost always involve some expenditure of time and resources for investigation to determine that such a breach has occurred. To that end, changing the language from "becoming aware" to "determining" may help to minimize pressure to report before due investigation is able to be conducted.

This proposed change would also serve the interest in harmonizing regulatory approaches across the financial sector. The Federal banking agencies in the Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers have adopted the following requirement: "[a] bank service provider is required to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider *determines* that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours." (Emphasis added)[3]

4. **Encryption Safe Harbor.** In connection with the Reg S-P Proposal, the Commission asks "[s]hould we except from the definition of 'sensitive customer information' encrypted information, as certain states do?" We believe that this is a useful exception for the Commission to consider. At present, state-of-the-art encryption provides effective protection against disclosure of data even if the encrypted data is exposed. Where a provider or FI determines that such encryption was in use with respect to exposed data, notifying FI customers of the exposure would serve little purpose other than to generate confusion as to the consequences and possible damage.

5. **Disclosure of cybersecurity risks and incidents.** The Exchange Act Cybersecurity Proposal requires covered FIs to "provide a summary description of each significant

[3] We note that the Exchange Act Cybersecurity Proposal do A covered entity must give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.

cybersecurity incident that has occurred during the current or previous calendar year." We urge the Commission to make clear that the need to publicly disclose incidents must be balanced against what is best for the effectiveness of incident response. We do not believe the Commission's intent is to mandate disclosure of information that may be counter-productive to incident response (particularly if the incident is ongoing). To this end, we propose that the Commission include the following additional language (see bold): "**Provided that no description should include information that will prejudice the response to the significant cybersecurity incident,** the description of each significant cybersecurity incident must include the following information. . . ."

6. **Consistency Across Domestic (and International) Regulations.** Building upon the prior recommendation, consistency regarding incident notification standards and requirements, as well as cybersecurity and system safeguards, across domestic and global regulators is critical in enhancing clarity, reducing costly and inefficient fragmentation, and ensuring the objective of identifying and mitigating actual cyber and technology risks. To this end, we applaud the FSB's recent work on incident notification[4] and the coordination across the U.S. banking regulators in promulgating recent rules. We further urge alignment with regulatory rule-making on incident reporting associated with the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022.[5] In order to advance consistency and regulatory convergence, we recommend the establishment and use of voluntary fora to help drive uniformity and for information sharing about threats/incidents that can be hosted jointly with other domestic and international regulators.

II. Conclusion

We appreciate the opportunity to provide our views on the Commission's Exchange Act Cybersecurity Proposal and Regulations S-P Proposal. We have a shared interest in making sure that cybersecurity risks are mitigated, system safeguards are implemented, and material incidents are properly reported. By pursuing convergence with respect to regulatory requirements consistent with domestic and global best practices, the Commission can most effectively and efficiently satisfy these objectives.

[4] Financial Stability Board (FSB), *Consultative Document: Achieving Greater Convergence in Cyber Incident Reporting* (Oct. 17, 2022), available at https://www.fsb.org/wp-content/uploads/P171022.pdf.
[5] Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), available at https://www.congress.gov/bill/117th-congress/house-bill/2471/text.