Schulte Roth&Zabel LLP

919 Third Avenue
New York, NY 10022
212.756.2000
212.593.5955 fax

www.srz.com

June 5, 2023

Via Electronic Mail: rule-comments@sec.gov

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

RE: Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information (File No. S7-05-23)

Dear Ms. Countryman:

We are responding to the request of the Securities and Exchange Commission (the "Commission") for comments to the proposed rule amendments to Section 248.30 of Regulation S-P that would require brokers and dealers ("Broker-Dealers"), investment companies, and investment advisers registered with the Commission ("RIAs," with "Broker-Dealers" collectively "Covered Institutions") to adopt written policies and procedures for incident response programs to unauthorized access to or use of customer information, including procedures for providing timely notification to individuals affected by an incident involving sensitive customer information (the "Proposed Rules").[1]

Schulte Roth & Zabel LLP is an international law firm with offices in New York, London and Washington, D.C. Our clients include many RIAs and Broker-Dealers that will be affected by the Proposed Rule as well as institutional investors and limited partners. We regularly advise clients with respect to regulatory obligations and responsibilities, including with respect to cybersecurity, data privacy, and related disclosures.

These comments, while informed by our experience in representing our clients, represent our own views and are not intended to reflect the views of the clients of the firm. We recognize the time and effort invested by the Commission and the Staff of the Division of Trading and Markets and the Division of Investment Management (the "Staff") in formulating the Proposed Rule and appreciate the opportunity to comment.

[1] *Privacy of Consumer Financial Information and Safeguarding Customer Information;* Release No. 34-97141 (March 15, 2023) (the "Proposing Release").

On March 15, 2023, the Commission issued the Proposed Rules to, among other things, require Covered Institutions to adopt reasonably designed incident response programs, policies and procedures for assessment, control and containment of a cyber-intrusion, and to ensure incident response plans provide for sufficient customer notification. We respond below to several of the questions raised in the Proposing Release and respectfully request that the Commission tailor the Proposed Rules, as follows:

The Scope of Incident Response Plans. The Proposing Release asks whether incident response programs should be more limited in scope so that they would only address incidents that involve unauthorized access to or use of a subset of customer information (e.g., sensitive customer information).[2] We believe that incident response plans should be limited to sensitive customer information (and not encompass all nonpublic customer information). Sensitive customer information is, by definition, information that is "reasonably likely risk of substantial harm or inconvenience to an individual identified with the information".[3] The notification requirements in the Proposed Rules are triggered when sensitive customer information has been accessed or used. Incident response programs, however, are required for unauthorized access or use of any customer information, which is defined much more broadly to include any record containing nonpublic personal information about a customer of a financial institution.[4] Because sensitive customer information is the information likely to cause substantial harm or inconvenience to a customer and that requires notification to customers, it follows that incident response plans should be tailored to sensitive customer information.

The Scope of The Proposed Definition of Service Provider. The Proposed Rule defines the term "service provider" to include any person or entity that is a third party[5] and receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a Covered Institution.[6] This definition would include affiliates of Covered Institutions if they are permitted access to customer information through their provision of services. The Proposing Release asks whether a Covered Institution's affiliates should be excluded from the definition of "service provider."[7] We believe that the proposed definition of "service provider" should exclude a Covered Institution's affiliates. Such an exclusion is consistent with the distinction the Gramm-Leach-Bliley Act ("GLBA") makes between sharing nonpublic personal information with affiliates versus with non-affiliated third parties. Including "affiliates" in the definition of "service provider" would collapse that distinction.[8] We note that affiliates are typically included within the scope of a Covered Institution's cybersecurity policies and procedures and would also be covered by an applicable incident response plan. As such, it would

[2] *Id.* at 25.
[3] Proposed Rule 248.30(e)(9).
[4] Proposing Release at 19.
[5] The use of the term "third party" in the definition of "service provider" creates confusion as to whether affiliates are included (though the Proposing Release suggests that they are).
[6] Proposed Rule 248.30(e)(10).
[7] Proposing Release at 35.
[8] Section 6808 of GLBA required the Secretary of the Treasury, in conjunction with the Federal functional regulators and the Federal Trade Commission, to conduct a study of information sharing practices among financial institutions and their affiliates and deliver a report to Congress on or before January 1, 2002. Congress chose not to make any amendment to GLBA regarding the sharing of customer nonpublic personal information among affiliates.

be inefficient and distracting for an affiliate to be focused on service provider disclosure obligations to the Covered Institution when, in all likelihood, the Covered Institution or its personnel would be closely involved with any affiliate's cyber incident response plan.

Delegation of Providing Notice. The Proposing Release asks whether it is appropriate to permit Covered Institutions to delegate their customer notification obligations to their service providers.[9] Covered Institutions should be permitted to reach commercial agreements that delegate notice obligations to service providers, as long as the notice actually provided to customers with potentially impacted data satisfies the Covered Institution's notice obligations. If the service provider was the victim of a cyber-attack that included unauthorized access to Covered Institution sensitive customer information, then the service provider would be better situated to notify the affected customers (and likely would have a duty to do so, independent of its agreement with the Covered Institution). Nearly all data breach notices require the entity that was the victim of the cyber-attack to provide a narrative that describes the nature of the data breach and the steps taken to limit the harm caused by the attack, as well as the steps taken to identify and secure compromised data. A Covered Institution would have limited ability to provide meaningful notice to its impacted customers without a full and complete understanding of its service provider's response to the cyber-attack. Also, a comprehensive response to a cyber-incident that includes unauthorized access to customer data can be a time-consuming undertaking that can include state, federal, and international reporting obligations. Often, the varied and potentially voluminous customer notification process can be managed best by specialists acting on behalf of organizations that have been subjected to a cyber-attack. Cybersecurity incident response specialists are often better positioned to manage notice obligations quickly and efficiently, which benefits both the affected institution and any customers whose data might have been compromised.

Service Provider Notice To Covered Institutions. The Proposed Rule would require Covered Institutions to adopt policies and procedures mandating that contracts with certain of their service providers include requirements that the service provider 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. The Proposing Release asks if a different timeframe such as "as soon as practicable" should be used.[10] The time that service providers have to notify Covered Institutions should not be mandated by rule, but should be left to Covered Institutions and their service providers to negotiate, and should account for the nature of the service provided, and the type of customer data that a service provider might possess. Service providers that are required to provide notice to covered institutions only 48 hours after a data breach is discovered are left with the impractical challenge of allocating resources to making disclosures to counterparties (i) when resources could be better allocated to identifying and containing the scope of the data breach, and (ii) before the service provider has a complete picture of the impact of a data breach. Service providers that are compelled to make disclosures to Covered Institutions within 48 hours of the discovery of a data breach are often left reporting the fact that a breach occurred, but are unable to identify specific customers who might have been impacted, or whether any sensitive customer information was compromised during the data breach. If the Staff does not believe notice "as soon

[9] *Id.* at 38.
[10] *Id.*

as practicable" is acceptable, then service providers should at least be permitted to make disclosures to Covered Institutions within 48 hours of identifying unauthorized access to specifically identifiable sensitive customer information that would actually trigger the Covered Institution's 30-day notice period for contacting its affected customers.

Compliance Date. The Proposing Release suggests that the compliance date for the Proposed Rules should be twelve months after the effective date of any adoption, in order to give Covered Institutions sufficient time to develop and adopt appropriate procedures to comply.[11] To promote efficiencies, we suggest that the compliance date for the Proposed Rule be harmonized and coordinated with the compliance date for the Proposed Rules and Amendments to Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (File No. S7-04-22).

* * *

We would be pleased to respond to any inquiries you may have regarding our letter or our views on the Proposed Rule more generally. Please feel free to direct any inquiries to Kelly Koscuiszka and Philip J. Bezanson at (212) 756-2000.

Respectfully submitted,

SCHULTE ROTH & ZABEL LLP

cc: The Honorable Gary Gensler
The Honorable Caroline Crenshaw
The Honorable Jaime Lizárraga, SEC Commissioner
The Honorable Hester Peirce, SEC Commissioner
The Honorable Mark T. Uyeda, SEC Commissioner
William Birdthistle, Director, Division of Investment Management

[11] *Id.* at 131.