June 5, 2023

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

Re: 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; Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information (Release Nos. 34-97142; 37-97141)

Dear Ms. Countryman:

The American Securities Association (ASA)[1] submits these comments in response to recent rule proposals from the Securities and Exchange Commission (SEC) regarding new mandates related to cybersecurity policies and procedures for broker-dealers and other entities.

The SEC's proposed new SEC notification and public disclosure requirements on brokers for cyber events ("Risk Management Proposal") and a proposal to standardize internal procedures and customer notification policies in the wake of a cyber breach ("Reg S-P Proposal").

I. General Concerns.

The ASA has a number of concerns associated with the Proposals, which are generally outlined below.

First, the Proposals are not supported by evidence that brokers are fundamentally failing in their obligations to safeguard investor information and notify government authorities – within applicable Federal and state law – when a significant breach of sensitive information has occurred.

Second, the Proposals will create 'noise' for customers of brokers by requiring the notification and

[1] The ASA is a trade association that represents the retail and institutional capital markets interests of regional financial services firms who provide Main Street businesses with access to capital and advise hardworking Americans how to create and preserve wealth. The ASA's mission is to promote trust and confidence among investors, facilitate capital formation, and support efficient and competitively balanced capital markets. This mission advances financial independence, stimulates job creation, and increases prosperity. The ASA has a geographically diverse membership of almost one hundred members that spans the Heartland, Southwest, Southeast, Atlantic, and Pacific Northwest regions of the United States.

disclosure of even minor incidents that fail to meet any objective definition of a "significant" breach.

Third, the Proposals fail to address or even consider the biggest cyberthreat facing investors today: The collection and storage of the personally identifiable information (PII) of every American that trades a share of stock on a U.S. exchange by the consolidated audit trail (CAT), which is a centralized database housed in Washington and accessible by thousands of individuals.

Therefore, we urge the SEC to table the Proposals indefinitely until the agency can properly assess whether targeted changes to cybersecurity-related regulation are necessary, and until the PII security and privacy concerns of the CAT are fully addressed.

Our detailed views on each of these topics are discussed in greater detail below.

II. The Proposed rulemakings expend valuable SEC resources on prescriptive new mandates while ignoring the massive threat to investors under the CAT.

When the SEC proposed these rules, Chairman Gensler said "The nature, scale, and impact of cybersecurity risks have grown significantly in recent decades…Those who seek to harm these systems have become more sophisticated as well: in their tactics, techniques, and procedures."[2] These assertions are undoubtedly true as American investors face cyberthreats from criminals, state-sponsored actors, and individuals with regular access to sensitive consumer and investor information.

Given this, it defies explanation as to why the SEC has failed to eliminate the collection of PII by the CAT. The biggest cyberthreat facing American investors today is not the lack of standardization regarding broker-dealer customer notification policies or insufficient public disclosure regarding major cyber events; *it is the vast collection and storage of American investor PII in an unsecure, centralized database that will become the target for cybercriminals and hackers from Russia and China who wish to inflict economic harm on the United States*.

Investors are also vulnerable to the misuse of their PII by individuals that will have regular access to personal information and trading records of every American investor. At a Senate Banking Hearing in 2019, the Chief Operating Officer of the CAT openly admitted that over 3,000 individuals will have regular access to CAT data and PII.[3]

Any one of those individuals could accidentally or intentionally compromise investor PII and expose investors to identify theft or other nefarious actions. The recent breach of 250,000 consumer records by a ***single employee*** at the Consumer Financial Protection Bureau shows that

[2] Statement on Enhanced Cybersecurity for Market Entities – Chairman Gary Gensler (March 15, 2023)
[3] Senate Banking Committee October 22, 2019 hearing "Oversight of the Status of the Consolidated Audit Trail"

this type of threat is NOT hypothetical.[4]

The Risk Management Proposal notes that "Personal information is an attractive target for threat actors because they can use it to steal a person's identity and then use the stolen identity to appropriate the person's assets through unauthorized transactions or to make unlawful purchases on credit or to effect other unlawful transactions in the name of the person…they also can sell personal information…to criminals who will seek to use the information for these purposes." While it may have been unintentional, the Risk Management Proposal aptly described the biggest threats emanating from the CAT and made a persuasive case for prohibiting the collection of PII.

The SEC CAT policy is misguided and dangerous and must be changed before it causes the financial and personal identities of millions of Americans to be compromised.

Any credible effort by the SEC to mitigate cyberthreats to investors should begin with removing PII from the CAT. Limiting the unnecessary collection and storage of PII in the first place is an appropriate policy to be adopted for the CAT to reduce the risk of identity theft or other harmful actions that will affect U.S. investors. Imposing prescriptive new mandates on broker-dealers and their customers will likely only serve as a costly distraction to the risks posed by the current CAT.

III. Proposals mandate numerous disclosures and notifications to regulators and customers of broker-dealers that will confuse the public about cyber- incidents.

The Risk Management Proposal would mandate that brokers provide immediate notice to the SEC regarding a "significant cybersecurity incident." The definition of a "significant cybersecurity incident" is extremely broad and would encompass events that cause 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."[5]

A requirement to provide immediate notice to the SEC in the midst of an ongoing investigation is especially problematic. Brokers may not know the full extent of information involved in a cybersecurity incident within the window of reporting required under the Risk Management Proposal. As such, this requirement would make it impossible, in some cases, for brokers to be able to provide the SEC with the most accurate information regarding an incident.

Brokers would subsequently be required to publicly disclose details surrounding significant cybersecurity incidents that occurred during the current or previous year. The application of reporting requirements for incidents that involve a *single* customer, counterparty, member, registrant, or anyone that interacts with a broker is unnecessary and could lead to a high volume of incident reports filed with the SEC and public disclosures by brokers – even if those incidents did not implicate or threaten a broker's customer base or ability to carry out its core functions.

[4] "CFPB Says Employee Breached Data of 250,000 Consumers in Major Incident" – Politico (April 19, 2023)
[5] Risk Management Proposal at 480-481

At a minimum, the SEC should narrow the criteria for reporting incidents to include only those that actually disrupt or disable the ability of broker-dealers to perform core functions and operations.

Further, both the Risk Management Proposal and Reg S-P Proposal are void of any discussion about how current broker-dealer cybersecurity and customer notification policies are deficient or in need of a regulatory fix.

Brokers take very seriously their commitment to safeguard customer information and to disclose material information regarding a breach when necessary. But no government or private sector institution is completely immune to cyberattacks. When these incidents do occur and in particular when they affect sensitive customer information, brokers have an obligation to report and notify customers, in accordance with and when permitted under current law.

Additionally, as Commissioner Peirce pointed out in her dissenting statement on the Risk Management Proposal, small broker-dealers will have a difficult time complying with these new mandates.[6] This is of particular concern given that small firms that do not have infinite compliance budgets are much more sensitive to new regulatory mandates, particularly mandates that may result in little benefit to the customers of these firms. Yet, similar to other recently proposed rules, the SEC has done little analysis about the impact of these proposals on small broker-dealers, competition within the brokerage industry, and whether they could contribute to barriers for new entrants into the markets.

IV. The Proposals fail to consider other regulatory obligations regulated entities have relating to cyber incidents and other outstanding SEC proposals on cybersecurity.

Broker-dealers, as with other entities, are already subject to certain federal and state laws regarding cybersecurity and the disclosure of information surrounding cyber incidents. Congress recognized under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022 the importance of a coordinated government approach towards cybersecurity.

Under CIRCIA, the Cybersecurity & Infrastructure Security Agency (CISA) is required to work with other Federal agencies to "deconflict and harmonize" cyber incident reporting obligations. Yet it is unclear at best whether the SEC has coordinated or communicated with CISA or any other federal agency regarding the proposals and the potential for new mandates to duplicate or conflict with existing regulatory requirements.

Even more concerning, the SEC has not even considered the interaction of the Risk Management Proposal and Reg S-P Proposal with its *own* rules, including a proposal related to cyber incident disclosure for public companies that was released in March 2022 (the March 2022 Proposal) and is

[6] Statement on Proposed Cybersecurity Rule 10 and Form SCIR – Commissioner Hester Peirce (March 15, 2023)

expected to be finalized soon.[7]

Since many broker-dealers are also public reporting companies under the Exchange Act, it is imperative that the SEC not overburden brokers with immaterial reporting requirements and, more importantly, that it not harm or mislead investors by imposing reporting rules that conflict with one another. If the SEC elects to finalize its March 2022 Proposal, it would be more prudent to assess how those new standards work in practice *prior to* imposing additional obligations on these same entities.

As currently drafted, the Risk Management Proposal and Reg S-P Proposal will also likely compel many brokers to renegotiate contracts with service providers or hire new service providers to assist them with cyber monitoring and compliance with these new standards. Yet the proposed rulemakings include no discussion or estimate of the costs this would impose on brokers on brokers, and the proposed one-year time frame for compliance is unrealistic given the time it would take for brokers to conduct due diligence and renegotiate any contracts with outside service providers.

Conclusion.

While we appreciate the SEC's concern over cybersecurity and the threat to investors, we are concerned that the SEC has misplaced its priorities with these proposals. The most impactful investor protection initiative the SEC can take would be to stop placating the career bureaucrats clamoring for access to this data and immediately eliminate the collection of American retail investor PII from the CAT.

The SEC could then carefully analyze the myriad proposals impacting broker-dealers and, in conjunction with other federal agencies with cybersecurity expertise, determine whether these new mandates are necessary and in the best interests of investors and U.S. national security. As a result, this Commission should withdraw the proposals until those important steps are taken first.

We also urge this Commission to stop moving forward with ill-conceived ideas that do nothing but empower a professional class of lawyers and consultants whose hourly rates seem to increase every time a new rule is adopted. As always, the ASA looks forward to being a resource for SEC commissioners and staff on these critical issues.

Sincerely,

Christopher A. Iacovella

Christopher A. Iacovella
Chief Executive Officer
American Securities Association

[7] 87 FR 16590