Rechtman CPA PLLC

[redacted]

March 17, 2023

To:
Secretary, Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: **Proposed Rule** **File Number S7-06-23**

"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"

Via email: rule-comments@sec.gov

To whom it may concern:

In response to the Proposed Rule on 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, File Number S7-06-23 (the "Proposed Rule") Rechtman CPA PLLC is pleased to provide our comments to the Securities and Exchange Commission in furtherance of creating an effective cybersecurity rule.

Contents

Executive Summary

The proposal for the new rule reads like an apology. While we agree with the balanced approach of the risk assessment requirement, one that does not over-prescribe specific controls, the overall approach in the Proposed Rule needs to change its tune from apology to demand. Instead of regulating the entities entrusted by the public at large with maintaining their assets, including intangible assets, with the best and highest quality practices, the proposal attempts to establish a notion that "Oh, *don't worry, it won't be that expensive or that expansive*." The truth is that as a regulator, the SEC is charged with regulating certain entities and not to their reaction. The cybersecurity is not a cost/benefit analysis, but rather, "*[actors] will act based on what's inspected, not what's expected*" (attributed to J. Micara c. 1999).

With these expectations in mind, we take the position that a **more expansive coverage of the Proposed Rule 10**, with reasonable definitions of the following delineation of "incident"[1] and "breach" (as defined under HIPAA, see 45 USC § 164.402 for a definition),

[1] Proposed Rule Page 139, et seq.

and the reference to **common and established risk standards** such as NIST Publication 800-30. The "reasonable basis" standard for an incident and the urgent, arbitrary "48 hours" threshold will not create better compliance. Rather, there may be a rush of disclosures, or in the alternative a "reasonable" standard may apply.

Instead, we recommend borrowing a page from the HIPAA rulebook, and apply a bi-furcated status: "incident", a potential for harm, and "breach" an established state of harm.

Our analysis largely ignores the purported cost that is asserted in the proposal with an **unrealistic range for auditing each entity**, from $1,500 to $20,000 per entity. We ignore these audit costs—which we believe are unrealistically low—because they are irrelevant. The covered entity (expanded, as per our comments herein) should take a greater sense of responsibility in investing in the security of the stakeholders' asset, and not start the discussion with the ubiquitous question, "*how much is it going to cost?*". The reality is that the cost per stakeholder is negligible, and the old adage holds true in these circumstances: "an ounce of prevention is worth a pound of correction".

> "FUN FACT 1":
>
> We believe that the costs of audits should be approximately triple what the proposal is quoting, at least $15,000, and that such audits are paramount for proper implementation. However, if that cost would be spent on inspection, the effect of the audit would be substantially higher cost/benefit to the general public *and* to the auditees themselves.
>
> "FUN FACT 2":
>
> Public companies that audit rarely result in an adverse opinion. The rate of audits that fail inspection under PCAOB Part I.A is around 20% in 2021[2]. Part I: A finding is when "Deficiencies that were of such significance that we believe the firm, at the time it issued its audit report(s), had not obtained sufficient, appropriate audit evidence to support its opinion(s) on the issuer's financial statements and/or ICFR".

[2] https://www.cpajournal.com/2022/06/13/the-new-working-world-of-the-covid-19-pandemic/ See Exhibit 4.

Overall, we believe in taking a measured approach of risk assessment and risk management, to assess an increase in budget for inspections (rather than internally sourced or paid-for audits).

About Rechtman CPA PLLC

Rechtman CPA PLLC™ provides services in fraud investigation, forensic accounting, information technology, data mining, and cybersecurity consulting. Our managing member, **Yigal M. Rechtman, CPA, CFE, CITP, CISM** applies a multidisciplinary approach combining his background in *Computer Science, Accounting, Auditing, Tax, and Forensic Accounting,* to deliver analysis and deliverables that respond to specific engagement objectives, be they a fraud report, or analysis of the application of audit standards; among other things.

Our specialty with these services includes fraud investigation for asset misappropriation, litigation consulting, HIPAA and healthcare compliance, civil, damages, insurance claims, evaluation of internal controls, risk analysis, information systems, information technology, Service Organization's Controls (SOC) under SSAE, and SOX 404A testing. We also provide tax compliance services, with a specialty in clergy-related tax matters.

Our experience is in a wide range of industries such as construction, healthcare, real estate, construction, hospitality and dining, professional services, not-for-profit, technology, closely held companies, ERISA plans, and education.

We are pleased to present our detailed analysis in the following pages. With any questions, please contact the undersigned.

Sincerely,

/s/Yigal Rechtman

Yigal M. Rechtman, CPA, CFE, CITP, CISM
Managing Member

Detailed Analysis

Comment #1: Covered entities under the proposed rule

Proposed Rule: Scope of coverage is:

> "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"[3]

Comment:

The rule's scope should also **specifically and unequivocally include sub-contracts**, platform providers, consultant, third party in service of a recordkeeper, and others with permitted access to logical or physical elements of the record keeper's assets, whether physical or electronic.

> **"FUN FACT 3"**:
>
> While the terms "contractor" and "vendor" appear throughout the proposed rule, the cost of quality compliance of such vendors is vastly understated. In footnote 782 the proposed rule states *inter-alia* that the cost[4] of the audit could be between $1,500 and $20,000.
>
> The idea of auditing, paid for by the auditee itself, is antithetical to the idea of a standard, genuinely external inspection. Assuming that only companies that have their inner workings looked at will bother to have an effective compliance, then the audit ranks a distant second to the inspection process.

Considering an axiomatic postulation that inspection is better than internally-sourced audit, the range of costs both underestimates the actual cost and by establishing a low bottom of $1,500 to this purported range, but also accepts the "audit-at-any-cost" mentality that is the bane of Cybersecurity experts. Rather, the cost should be assessed at the range of $15,000 to $35,000 and evaluated as

[3] Proposed Rule, summary, Page 1.

[4] Page 338, "The annual review and report costs are estimated to be around $1,500 and $20,000 based on the costs of obtaining a cybersecurity audit".

such in terms of cost/benefit analysis. Any amount lower than this range means that corners are cut, and quality suffers in such a way that an effective cybersecurity audit is not as attainable as it purports to be. However, **we believe that a funded inspection process takes away the inherent conflict when a paid-auditor is paid to do so by the company that they are auditing**.

In summary: the rule should be expansive in nature and cover at least Market Entities (par. 91), SCI Systems (par. 92), and Broker Dealers (par. 95). In addition, the new rule should cover any entity that is holding in trust, either as a fiduciary or as an agent for any asset of individuals, companies, corporations, and governmental agencies. There should be no exceptions, and there should be no so-called "self-regulation" other than self-evaluation and risk assessment.

Comment #2: Notification Requirement

Proposed Rule: "immediate notification to the Commission of the occurrence of a significant cybersecurity incident"

Comment:

The proposed rule is internally contradictory. An "incident" is an event that may or may not lead to a breach of the data. The "reasonable basis"[5] standard for an incident and the urgent, arbitrary "48 hours" threshold will not create better compliance. Rather, there may be a rush of disclosures, or in the alternative a "reasonable" standard may apply. Instead, we recommend borrowing a page from the HIPAA rulebook, and apply a bi-furcated status: "incident", a potential for harm, and "breach" an established state of harm.

For example: a trusted IT employee loses an electronic access device which is used to log-in. That is a "significant cybersecurity incident" however this is not a *breach*. Under the proposed rules, such a "significant incident" which would require "immediate" notification. However, no alleged break-ins or unauthorized access has been recorded and within a reasonable time, the device is disallowed, and a new device is issued. Under this scenario, the reports that will come through will be many and yet most insignificant.

While the definition of "incident" is present, it would be best if the proposed rule would be in sync with Federal and State rules that delineate a "incident" which is an event to which *response* is required, versus a "breach", which is an event in which "damages" are incurred and response is required.

The potential effect of such a deluge of reports is a dilution of the situations that are noteworthy by regulators and other stakeholders.

[5] Proposed Rule, pages 143, 147

Comment #3: Definition of "Cybersecurity Incident"

Proposed Rule: Definitions of "significant Cybersecurity Incident"[6] and "Cybersecurity Risk"[7]

Comment:

These definitions are nonconforming to existing regulations such as HIPAA, and several states' cybersecurity definitions, which are in sync.

Notwithstanding the issue identified above about what constitutes as an "incident" both this term, as well as the definition of risk, would better serve *all* stakeholders, including the SEC if it refers to the National Institute of Standards and Technology ("NIST") publication 800-30 *Guide for Conducting Risk Assessments*.

> "FUN FACT 4":
>
> The purported "Alternatives to the Policies and Procedures Requirements of Proposed Rule 10"[8] are not realistic. Disclosing an overview of policies and procedures (alternative "a") and/or "Limiting the scope of the proposed cybersecurity procedures… to third-party service providers" (alternative "b") are both impractical and dangerous alternatives. Instead, reference to existing risk standards (e.g., NIST 800-30) should provide a baseline for stakeholders, rather than consideration of these "false senses of realistic alternatives".
>
> Applying and over-prescribing controls is, as we have noted in a **previous comment to a SEC exposure draft** (comment page 2, ref: "over prescription"), is ineffective and bound to become obsolete.

Comment #4 Notification and Public Disclosure

Proposed Rule: "as applicable, reporting **detailed information** to the Commission about a significant cybersecurity incident, and public disclosures that would improve transparency with respect to cybersecurity risks and significant cybersecurity incidents."[9] (em. added).

---

[6] Proposed Rule, page 76

[7] Proposed Rule, page 83

[8] Proposed Rule, page 416, et seq.

[9] Proposed Rule, Page 1, and page 43 et seq.

Comment:

The risk of detailed information, especially if it is a public record, is that it could lead to additional risks to the reporting entity, and to other entities in a similar situation. More specifically, there is no magic in "no later than 48 hours"[10]. Rather, the definition of "incident", or "breach" by a better-suiting name, should be upon establishing the specifics of the incident, not by some arbitrary business days or hours.

"FUN FACT 5":

The term "Form SCIR" – the form to report a Cybersecurity Incident, appears 477 times in the Proposed Rule, compared to the term "inspection(s)" which appears 12 times in the Proposed Rule. The term "EDGAR" appears 127 times. This is a characteristic of regulation by form, not by substance.

For example: If a "bug" is discovered whereby access can be granted to sensitive data storage units by passing the normal threshold such as firewalls and access controls, that would clearly be a "significant cybersecurity incident".

Notwithstanding our comment regarding what should be disclosure worthy ('breaches' rather than 'incidents'), such as "detailed information" being disclosed, in the wrong hands can provide a roadmap to cyber-criminals to rinse-repeat the unauthorized access to similar data storage units.

The question before the rule-makers should be this: what is the **objective of disclosure?** If the objective is to advise the public, then a general disclosure should both be safe and sufficient. If the disclosure is to avoid repeat incidents, then existing tools such as the Federal Bureau of Investigation's task force, as well as non-governmental organizations such as CERN InfoSec are the better venues for such information sharing.

It is imperative that the SEC as a rule maker does not become yet another fractioned, partially resourced silo of information about past and present breaches. Rather, it is best that the information be shared by authorized, fully resourced, exchange platforms such as the FBI's *National Cyber Investigative Task Force* (https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force).

[10] Proposed Rule, page 366

Comment #5: Risk Management Policies and Procedures

Proposed Rule: "Accordingly, proposed Rule 10 would require Covered Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address the Covered Entity's cybersecurity risks"[11].

Comment

We agree, in general, that risk management is a key to successful compliance, and commend the SEC for the ability to avoid a pre-prescribed "one-size-fits-all". We further agree that a minimal set of risk elements should be present, namely[12] "(1) risk assessment; (2) user security and access; (3) information protection; (4) cybersecurity threat and vulnerability management; and (5) cybersecurity incident response and recovery." We feel that this balanced approach is most-likely-to-succeed in scope and nature.

Risk assessment should be internal and internally driven but adhere to established standards. As referenced herein, the NIST 800-30 standard is ideal for multiple reasons: it is scientific and generally accepted, it is in wide use, it overlaps with multiple laws and other standards (for example HIPAA or New York State's banking regulation NYCRR§500).

With that in mind, the *inspection* of such risk assessment and risk management processes—or a lighter version of which would be an entity-funded audit—should be broad in scope and deep in probe. Such audits (or perhaps inspections) should be carried out by informed and educated professionals and should not be mired by the "budgetary approach" that this proposal espouses. Rather, it should be objective based, not cost/benefit based for the betterment of the investing and trading public, and stakeholders too.

Comment #6: Crypto Assets

Proposed Rule: no proposed rule is identified by the Proposed Rule

Comment:

The analysis of the risks from crypto assets and smart contracts is correctly described by the Proposed Rule: there is no central database, behavioral patterns do not apply, and reversal of damages cannot be readily available. These threats are more frequent, and the damages are growing, so in totality this is a material risk that should be addressed by the Proposed Rule.

The action that should be prescribed, or demi-prescribed are at the very least:

[11] Proposed Rule page 102

[12] Proposed Rule, pages 102-103

- Awareness training, as part of an anti-phishing risk that is identified in the proposal.
- Exchange monitoring, to create triggers that could warn off a "51% hack", a known Blockchain hack (blockchain is the underlying structure of cryptocurrency.)
- An enhanced "Know your Customer" or KYC with test transactions to valid existing wallets of customers. While these can be opened and closed easily, the link of known wallets to a threat-actor activity may be able to reduce the negative impact of such a threat.
- Hardware based controls to prevent and detect Man-in-the-Middle ("MitM") attacks.
- "Air Backup" which addresses malware and ransomware threats. Albeit more difficult to administer, is an effective tool especially for smaller entities.

The Proposed Rule, other than describing the possibility of fraud and other cybersecurity threats emanating from cyber assets, does not require any real action in response to such a threat. In our view this is an oversight by the overseers in the SEC. There should be whatever maximum known effective method to mitigate the risks instead of throwing the proverbial hands up in the air and requiring nothing. In the bullet points above we describe a few—if incomplete—responses to the risks the crypto assets and smart contracts.

###

This space is intentionally blank.