Statement on Proposed Cybersecurity Rule 10 and Form SCIR

Commissioner Hester M. Peirce

March 15, 2023

Thank you, Chair Gensler. No one questions the threat cybercriminals pose to our capital markets, and the need for broker-dealers and other regulated entities to protect themselves and their customers and counterparties from cyberthreats. As the proposing release notes, there are considerable reputational, psychological, and financial costs associated with these breaches.[1] Increasing reliance on technology in our markets has only heightened how important it is for firms to take steps to prevent cyberattacks and mitigate their effects. Addressing this challenge constructively requires the Commission to work with firms in a way that helps them shore up cyber-defenses and minimize the consequences of cyberattacks. Unfortunately, with this proposal, the Commission has apparently decided its role is to be an enforcer demanding that a firm dealing with a cybersecurity attack first and repeatedly attend to the Commission's voracious hunger for data. The Commission stands ready, not with assistance but with a cudgel to wield if the firm fails to comply with a complicated reporting regime, even if the firm resolves the incident by avoiding significant harm to the firm or its customers.

The Commission has an important, positive role in assisting market participants to defend themselves against cybercriminals. We are uniquely placed to be a resource for industry by providing registrants with market-wide intelligence on trends in, and potential defenses against, cybercrime. A reasonable reporting framework could facilitate that role. The onerous regulatory framework we are instead proposing, with a complicated reporting regime that is disproportionate to any reasonable need we have for immediate data, shows that we envision a quite different role for ourselves.

When we engage with a regulated entity that has suffered a cyberattack, we deal with a victim. We typically deal with a victim who has made great effort to protect its systems and its customers' data and is devoting significant resources to mitigate the harm from such an attack. Our priority should be to provide what support and information we can to assist the firm in this effort and, following resolution, to gather information that will help other firms in the future. Instead, this proposal demonstrates that our priority is to create even more legal peril for a firm in this situation, legal peril that will distract employees of the firm from mitigating the immediate threat to the firm and its customers as they navigate the aggressive deadlines and open-ended information demands of the Commission. Indeed, this rule is easier to understand as a tool to enhance our year-end enforcement statistics than a serious proposal to make the securities markets more secure.

- Upon having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring, a firm would need to provide the Commission with an immediate written notice, followed by a report within 48 hours on Part I of proposed Form SCIR. Form SCIR—which is prefaced with reminders that "Failure to file Form SCIR as required by 17 CFR 242.10 would violate the Federal securities laws and may result in disciplinary, administrative, injunctive or criminal action" and "**INTENTIONAL**

MISSTATEMENTS OR OMISSIONS OF FACTS MAY CONSTITUTE FEDERAL CRIMINAL VIOLATIONS."—includes fifteen detailed items and spans three pages. Within the first 48 hours of discovering a significant cybersecurity incident, filling out a detailed government form may not be the best use of time, but it gets worse—the person who signs faces individual liability if anything she submits is not current, true, or complete.

- The reporting demands continue until the incident is wrapped up. The firm has to amend that form to correct material inaccuracies, report new material information, report the resolution of an incident, or report the conclusion of an internal investigation. The sort of investigation we envision would be one "that seeks to determine the cause of the incident or to examine whether there was a failure to adhere to the Covered Entity's policies and procedures to address cybersecurity risk or whether those policies and procedures were not reasonably designed." Asking a firm to report information about policy and procedure failures again seems a set-up for enforcement actions. The proposal does ask whether the reporting requirements might dissuade firms from performing internal investigations.
- Firms will describe their cybersecurity risks and significant cybersecurity incidents on Part II of Form SCIR, which will be public and provided to brokerage customers annually. The proposal explains that this information would also assist customers in determining whether their engagement with that particular broker-dealer remains appropriate and consistent with their investment objectives. Alternatively, it could serve as a roadmap for cybercriminals.[2] It may make sense to alert market participants about a firm's cyberincidents, but the proposal implies that market participants should stop interacting with a victimized firm.[3]
- The proposed rule's definitions make it so broad as to be impossible to implement. For example, the rule "[r]equires measures designed to detect, mitigate, and remediate *any* cybersecurity threats and vulnerabilities" with respect to the firm's information systems and information residing on those systems. A "cybersecurity vulnerability" is "a vulnerability in a market entity's information systems, information system security procedures, or internal controls, including, for example, vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident."[4] The definition is expansive – though with the insertion of the word "including," not exhaustive -- to the point of making it unworkable. A "cybersecurity threat," equally open-ended, is "*any* potential occurrence that *may* result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of a market entity's information systems or any information residing on those systems."[5] Compliance measures that attempt to get their arms around such a conceptual blob are preordained to fall short.
- Small entities will have a particularly hard time with this rule. Although most smaller broker-dealers, for instance, will not fall within the definition of Covered Entities, more than a quarter will. The proposal may serve as one more barrier to new players entering the market and another catalyst for increased consolidation. Smaller transfer agents will also likely be overwhelmed by the rule's obligations.
- The proposal's requirements regarding service provider contracts make it harder for small entities to work with external service providers. The Economic Analysis acknowledges that "requiring affected [firms] to request oversight of service providers' cybersecurity practices pursuant to a written contract would lead some service providers to cease offering services to affected [firms]."[6]

I could not help but wonder, as I read through the more than 500 pages that make up this proposal, whether we at the Commission are living up to the proposed standards. At a minimum, should we not first attend to the severe cyber-risks associated with the Consolidated Audit Trail by excluding retail investor information from the CAT, or, at a minimum, adopting the CAT Data Security amendments before we consider adopting this rule?

I will not discuss the question of regulatory overlap here – I have done that in my statement concerning the proposed changes to Reg SP. Overlap and inefficiency, however, also contribute to my decision to vote in opposition to this proposal.

As is always the case, I look to commenters to inform my analysis of this rulemaking. Thank you to the remarkable teams in the Divisions of Trading and Markets and Economic and Risk Analysis, the Office of

General Counsel, and others throughout the Commission who contributed to this rulemaking. Though I cannot support this proposal, I am grateful for their tireless efforts.

---

[1] *See*, *e.g.*, Proposal at note 569 and accompanying text ("In 2020, the average loss in the financial services industry was $18.3 million, per company per incident. The average cost of a financial services data breach was $5.85 million.").

[2] For instance, Part II of proposed Form SCIR requires the reporting firm to describe how it "assesses, prioritizes, and addresses . . . cybersecurity risks." Would we require such a disclosure with respect to physical security risks?

[3] *See* page 178 ("Furthermore, requiring Covered Entities to update their disclosures following the occurrence of a new significant cybersecurity incident would assist market participants in determining whether their business relationship with that particular Covered Entity remains appropriate and consistent with their goals.")

[4] *See* paragraph (a)(5) of proposed Rule 10.

[5] *See* paragraph (a)(4) of proposed Rule 10.

[6] Proposal at page 414.