May 9, 2022

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

RE: **Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure; Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22 (March 9, 2022)**

Dear Ms. Countryman:

Virtu Financial, Inc.[1] ("Virtu") respectfully submits this letter in response to the above-referenced rule proposal issued by the Securities and Exchange Commission (the "SEC" or "Commission") on March 9, 2022 (the "Proposal").[2] In the Proposal, the Commission seeks public comment on prescriptive and inflexible disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies. More specifically, the Proposal would require the following:

- Current reporting about material cybersecurity incidents on Form 8-K;
- Periodic disclosures regarding, among other things:
  - A registrant's policies and procedures to identify and manage cybersecurity risks;
  - Management's role in implementing cybersecurity policies and procedures;
  - Board of directors' cybersecurity expertise, if any, and board oversight of cybersecurity risk; and
  - Updated disclosures about previously reported material cybersecurity incidents.

First and foremost, like many public companies that operate in today's challenging world replete with nation states and criminals seeking to wreak cyber havoc, Virtu takes its cyber security obligations seriously and already discloses in its public filings the cyber risks it faces and its efforts

[1] Virtu is a leading financial firm that leverages cutting edge technology to deliver liquidity to the global markets and innovative, transparent trading solutions to its clients. Virtu operates as a market maker across numerous exchanges in the U.S. and is a member of all U.S. registered stock exchanges. Virtu's market structure expertise, broad diversification, and execution technology enables it to provide competitive bids and offers in over 25,000 securities, at over 235 venues, in 36 countries worldwide. Virtu broadly supports innovation and enhancements to transparency and fairness that increase liquidity and promote competition to the benefit of all marketplace participants.

[2] U.S. Securities and Exchange Commission, Proposed Rule, *Cyber Security Risk Management, Strategy, Governance, and Incident Disclosure*, Release No.34-94382; File No. S7-09-22 (March 9, 2022), *available at* https://www.federalregister.gov/documents/2022/03/23/2022-05480/cybersecurity-risk-management-strategy-governance-and-incident-disclosure.

to combat and manage those risks.[3] Further, Virtu is a strong advocate of comprehensive disclosures that enable investors to make educated and fact-based determinations in their respective financial decisions. However, the Proposal is the latest example of a recent and troubling Commission trend exceeding its legal authority by exercising unnecessary and unneeded micro-management of the affairs of public companies.

Commissioner Peirce, in her typical eloquent and succinct manner, described this ongoing problem in her dissent from the Proposal:

> ***We must approach this topic, of course, through the prism of our mission. We have an important role to play in ensuring that investors get the information they need to understand issuers' cybersecurity risks if they are material. This proposal, however, flirts with casting us as the nation's cybersecurity command center, a role Congress did not give us.***
>
> ***Our role with respect to public companies' activities, cybersecurity or otherwise, is limited. The Commission regulates public companies' disclosures; it does not regulate public companies' activities. Companies register the offer and sale, and classes of securities with the Commission; they themselves are not registered with us, and we do not have the same authority over public companies as we do over investment advisers, broker-dealers, or other registered entities.***[4]

The Commission has many experienced and knowledgeable staff members that prepare well-intended and meaningful guidance and proposals on matters that aid companies and the investing public. This Proposal is not one such example – respectfully, the staff does not have the necessary expertise to appropriately guide public companies on how to manage their cyber programs. As Commissioner Peirce stated "[r]egulators may have a role to play in working with companies on cybersecurity, but we are not regulators with the necessary expertise".[5] It is more appropriately the domain of company management to designs systems and protections based on their respective business model and associated risks. Instead, the Commission is seeking to expand its role as a prudential regulator by taking a seat at the management table of companies.

Further, the Proposal calls for the premature disclosure of information that could cause a company and its shareholders harm. The Proposal ignores that companies must have the unfettered ability to conduct investigations and coordinate with law enforcement in the event of a cyber breach. To mandate disclosure under prescriptive time frames would inevitably impact this critical need for a company to undertake such steps, posing significant risk of harm to the company and its shareholders.

---

[3] See, Virtu Financial, Inc. 2021 Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act, at pp 9-10, 23.

[4] *See* SEC Commissioner Hester M. Peirce, *Dissenting Statement on Cybersecurity Risk Management Strategy, Governance, and Incident Disclosure Proposal* (March 9, 2022), *available at* https://www.sec.gov/news/statement/peirce-statement-cybersecurity-030922.

[5] *Id.*

A. The Proposal is unnecessary in light of existing disclosure regulations and previously issued Commission guidance

Broadly speaking, the Proposal raises an initial key question: what is the problem issue that needs to be addressed? That is, what is the problem that the Proposal is seeking to solve? First, as noted in the Proposal, public companies are already required to adhere to the general disclosure requirements set forth in Regulation S-K and S-X for reporting material items to shareholders. Moreover, the Commission has already issued two interpretative guides to public companies concerning the application of existing disclosure and other requirements under the current regulatory regime governing cyber risks and incidents:

- In 2011, the Division of Corporation Finance issued interpretative guidance (the "2011 Staff Guidance") to public companies concerning disclosure obligations related to cyber security;[6] and
- In 2018, the Corporation Finance staff expanded upon the 2011 Staff Guidance and specifically referenced the existing regulatory requirements in Regulation S-K and S-X that require disclosure of cyber incidents (the "2018 Staff Guidance").[7]

The Commission contends that it has "observed certain cybersecurity incidents that were reported in the media but were not disclosed in a registrant's filings."[8] The staff cites two studies that purportedly evidence a "growing concern that material cybersecurity incidents are underreported and that existing reporting may not be sufficiently timely."[9] However, the staff also noted that "[re]gistrants' disclosures of both material cybersecurity incidents and cybersecurity risk management and governance have improved since the issuance of the 2011 Staff Guidance and the 2018 Interpretative Release."[10]

We respectfully submit that the solution to address the Commission's concerns about cyber incident underreporting is to reemphasize the 2011 and 2018 Staff Guidance and utilize its enforcement powers to ensure that public companies continue to report material cyber incidents. Prescriptive additional regulation is not the answer.

B. The four-day reporting requirement for "material" cyber incidents may negatively impact shareholders and companies

The Commission proposes amending Form 8-K to require companies to disclose information about a cyber incident within ***four business days*** after the company determines that it

---

[6] CF Disclosure Guidance: Topic No2-Cybersecurity (Oct. 13, 2022), *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[7] Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 18, 2018) *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[8] *See* the Proposal at p. 16.

[9] *See* Proposal at p.20.

[10] *See* the Proposal at p.17.

has experienced a material cyber incident. The following information would be required to be included in the Form 8-K, to the extent such information is known at the time of the filing:

- when the incident was discovered and whether it is ongoing;
- a brief description of the nature and scope of the incident;
- whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;
- the effect of the incident on the company's operations; and
- whether the company has remediated or is currently remediating the incident.

There are a number of troubling aspects to this aggressive four business day requirement. First, during the initial days of a cyber incident, a company may not have a full understanding of the nature of the issue. A forensic firm retained by the company may be in the midst of an analysis that is undeveloped and unfinished. Simply put, it may be too premature to conclusively determine what has occurred and how significant the issue may be to the company's operations. Forcing a company to disclose an uncertain and dynamic situation has the potential to cause significant harm to shareholders – investors would ostensibly be forced to make an investment decision on incomplete, uncertain, and evolving information.

Further, requiring a company to disclose details of remediations could, in fact, frustrate the overall goal of protecting the company. If the remediation is not complete, the disclosure could alert cyber attackers that the company is still vulnerable and exposed, resulting in additional hacks. Lastly, Commissioner Peirce noted in her dissent, the Proposal does not consider the need to cooperate with, and sometimes defer to or take specific instructions from, federal government and state government prosecutors or officials. Ongoing governmental investigations may need to stay confidential for a certain period of time (again sometimes at the request of a prosecutor) and maintaining confidentiality could increase the chances of recovery of stolen funds or prevention of additional wrongdoing.

C. The "materiality" examples are helpful guidance but highly subjective.

The Proposal provides the following examples of cyber incidents that may need to be disclosed:

- an unauthorized incident that has compromised the confidentiality, integrity, or availability of an information asset (data, system, or network); or violated the registrant's security policies or procedures. Incidents may stem from the accidental exposure of data or from a deliberate attack to steal or alter data;
- an unauthorized incident that caused degradation, interruption, loss of control, damage to, or loss of operational technology systems;
- an incident in which an unauthorized party accessed, or a party exceeded authorized access, and altered, or has stolen sensitive business information, personally identifiable

information, intellectual property, or information that has resulted, or may result, in a loss or liability for the registrant;

- an incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data; or
- an incident in which a malicious actor has demanded payment to restore company data that was stolen or altered.[11]

While these examples provide helpful guidance on whether an incident may be material to the Commission, they may result in over-reporting of incidents by registrants due to their substantial subjectivity. If a company is concerned with determining whether a matter is in fact material and the situation "fits" within one of these examples, the company may decide to report in an abundance of caution. For example, if an employee were to leave a company and in so doing refused to immediately return a company device containing its intellectual property, the company may be forced to make an 8-K disclosure even if the employee eventually agrees to comply with the company's request. An incident such as this may cause investors to act irrationally, thinking that the event is more damaging to the company than it is in actuality, resulting in unnecessary volatility.

D. Mandating the disclosure of policies and procedures may aid the cyber criminals and not benefit investors.

Proposed new Item 106(b) of Regulation S-K would require a company to disclose in its Form 10-K, as applicable, whether:

- it has a cybersecurity risk assessment program and if so, provide a description of such program;
- it engages assessors, consultants, auditors or other third parties in connection with any cybersecurity risk assessment program;
- it has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider (including, but not limited to, those providers that have access to the company's customer and employee data), including whether and how cybersecurity considerations affect the selection and oversight of these providers and contractual and other mechanisms the company uses to mitigate cybersecurity risks related to these providers;
- it undertakes activities to prevent, detect, and minimize the effects of cybersecurity incidents;
- it has business continuity, contingency and recovery plans in the event of a cybersecurity incident;
- previous cybersecurity incidents have informed changes in its governance, policies and procedures, or technologies;
- cybersecurity-related risks and incidents have affected or are reasonably likely to affect its results of operations or financial condition and if so, how; and

[11] *See* the Proposal at p.24.

- cybersecurity risks are considered as part of its business strategy, financial planning, and capital allocation and if so, how.

Commissioner Peirce pointedly addressed the concerns with this requirement in her dissent:

> ***The proposed rules also require companies to disclose their policies and procedures, if they exist, for the identification and management of risks from cybersecurity threats. Again, while cloaked as a disclosure requirement, the proposed rules pressure companies to consider adapting their existing policies and procedures to conform to the Commission's preferred approach, embodied in eight specific disclosure items. The enumerated disclosure topics likely make sense for many public companies, but securities regulators are not best suited to design cybersecurity programs to be effective for all companies, in all industries, across time. The proposal's detailed disclosure obligations on these topics will have the undeniable effect of incentivizing companies to take specific actions to avoid appearing as if they do not take cybersecurity as seriously as other companies. The substance of how a company manages its cybersecurity risk, however, is best left to the company's management to figure out in view of its specific challenges, subject to the checks and balances provided by the board of directors and shareholders.***[12]

Virtu respectfully submits that a public company should be allowed to contour its cyber program to its business and related vulnerabilities instead of being forced to mechanically address the requirements set by the Commission. Further, requiring registrants to go into the level of detail contemplated by the Proposal could provide a roadmap to cyber criminals on how to expose and take advantage of a company. Again, the policy objectives advanced by the Proposal could have been much more effectively achieved through an update to the 2011 Staff Guidance and 2018 Staff Guidance materials rather than through an overreaching and prescriptive rulemaking.

E. The alleged rationale for requiring enhanced disclosures does not justify mandating board composition or other prescriptive governance requirements.

In addition, the Proposal would require disclosure in a company's Form 10-K of information about its cybersecurity governance, including a description of the board's oversight of cybersecurity risks and management's role in assessing and managing cybersecurity-related risks and in implementing the company's cybersecurity policies, procedures, and strategies. Moreover, proposed new paragraph (j) of Item 407 of Regulation S-K would require disclosure in annual reports, annual meeting proxy statements, and information statements on Schedule 14C if any member of the company's board of directors has expertise in cybersecurity, including the name(s) of any such director(s) and any detail necessary to fully describe the nature of the expertise. The

[12] *See* SEC Commissioner Hester M. Peirce, *Dissenting Statement on Cybersecurity Risk Management Strategy, Governance, and Incident Disclosure Proposal* (March 9, 2022), *available at* https://www.sec.gov/news/statement/peirce-statement-cybersecurity-030922

Proposal does not define what constitutes "cybersecurity expertise" but instead includes a list of criteria (but not an exclusive list) that a company should consider in reaching a determination on whether a director has expertise in cybersecurity.

Although the purported impetus for the Proposal is the Commission's perceived view that companies are not reporting material cyber incidents, there is no corresponding concern articulated by the Commission necessitating drastic governance changes at the board level. The Proposal seeks to unnecessarily impose a requirement of cybersecurity expertise for a board member. A company should have the ability to determine the composition and roles of its board members instead of being artificially directed by a Commission requirement that addresses one risk out of many that a company may face in its operations. Simply put, the Commission should not be permitted to micromanage the governance operations of a public company.

* * *

While Virtu strongly supports the goals of enhancing transparency and company disclosure, we believe the Proposal is a continuation of the paternalistic trend by the Commission to govern the inner workings of public companies. As noted above, registrants are already required to disclose material cyber incidents. Moreover, the Proposal would mandate the disclosure of information that could harm instead of assist shareholders and investors. For all the foregoing reasons, we request that the Commission convert the Proposal into additional interpretive guidance that could truly aid and assist companies and investing public combat the ever-growing cyber threat.

Respectfully submitted,

Thomas M. Merritt
Deputy General Counsel

cc: The Honorable Gary Gensler, Chair
The Honorable Hester M. Peirce, Commissioner
The Honorable Allison H. Lee, Commissioner
The Honorable Caroline A. Crenshaw, Commissioner