GELBER

June 2, 2023

Via Electronic Submission

Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090
rule-comments@sec.gov

Re: Cybersecurity Risk Management Rules for Broker-Dealers, et al. (88 Fed. Reg. 20212)
File No. S7-06-23

Dear Secretary Countryman:

Gelber Securities, LLC ("**Gelber**") welcomes the opportunity to comment on the proposed rule release from the Securities and Exchange Commission (the "**Commission**"), "Cybersecurity Risk Management Rules 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" (the "**Proposal**").[1] Gelber is a privately funded proprietary trading firm based in Chicago, Illinois. Gelber is registered with the Commission as a broker-dealer and is a member of the Financial Industry Regulatory Authority ("**FINRA**"). Its parent company, Gelber Group, LLC, was founded in 1982 and is a member of various futures exchanges in the U.S. and abroad. Gelber is one of the industry's most successful and enduring proprietary trading firms.

Gelber supports the Commission's objectives to promote robust cybersecurity risk management for broker-dealers and other entities covered by the Proposal (referred to herein as "**Firms**") through proposed Rule 10 ("**Rule 10**"). We also appreciate the Commission's recognition that it should avoid imposing on Firms "a one-size-fits-all approach to addressing cybersecurity risks."[2] This letter focuses on certain overly broad definitions and prescriptive mandates in Rule 10 that we believe run afoul of this important consideration and we believe will thwart the Commission's objectives. Our suggested changes to Rule 10 and Form SCIR appear in bulleted sentences below.

[1] 88 Fed. Reg. 20212 (April 5, 2023).
[2] *Id.* at 20239.

1. Definitions

a. The Commission should narrow the proposed definition of "information" and replace the term "personal information" with "nonpublic personal information."

Rule 10 hinges on the definition of "information." This term appears throughout the Rule and directly impacts what Firms must do with respect to risk assessments, policies and procedures, notifications, reporting and disclosures. The proposed definition of "information" is extremely broad, resulting in many other aspects of the Rule being overly broad and problematic.

Rule 10(a)(6) defines "information" as "any records or data related to the market entity's business residing on the market entity's information systems, including, for example, personal information received, maintained, created, or processed by the market entity." Rule 10(a)(9) defines "personal information" as "any information that can be used, alone or in conjunction with any other information, to identify a person, including, but not limited to, name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, government passport number, driver's license number, electronic mail address, account number, account password, biometric records, or other non-public authentication information." Taken together, these two definitions encompass virtually all information that a Firm has – even publicly available information such as the Firm's business address and the names and e-mail addresses of its officers and employees – regardless of whether that information would likely cause harm if compromised in a cybersecurity incident.[3]

To address this overbreadth, the Commission should:

- *Replace the term "personal information" with the term "nonpublic personal information" and begin the definition of that term with the phrase "any nonpublic information...."*
- *Revise the definition of "information" to mean "any records or data related to the market entity's business residing on the market entity's information systems, including, for example, nonpublic personal information received, maintained, created, or processed by the market entity, the compromise of which would create of be reasonably likely to create actual harm to the market entity or its clients or customers." (Newly proposed language underlined.)*

[3] As a proprietary trading firm, Gelber has no customers or users. Most "personal information" on our information systems is that of our officers and employees.

Narrowing these definitions in this manner will better align Rule 10 with the types of information likely to cause material harm if compromised in a cybersecurity incident. If these definitions are not narrowed, it will be difficult, at best, for Firms to appropriately and adequately tailor their cybersecurity risk management programs based upon material risks. The problems that would result from the proposed overly broad definitions are more apparent below in our discussion of other provisions in Rule 10.

b. The Commission should either revise its definition of "cybersecurity incident" to include actual harm or replace it with the term "significant cybersecurity incident" in Rule 10(b)(1)(v).

Rule 10(b)(1)(v) requires Firms to have policies and procedures to detect, respond to and recover from any cybersecurity incident, and "written documentation of any cybersecurity incident, including the covered entity's response to and recovery from the cybersecurity incident." Rule 10(a)(2) defines "cybersecurity incident" as "an unauthorized occurrence on or conducted through a market entity's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems."

This proposed definition, particularly in combination with the expansive definition of "information," could lead to any unauthorized occurrence triggering Rule 10(b)(1)(v)'s requirements related to cybersecurity incidents, even when there is no material threat, actual harm or meaningful disruption to a Firm's business. To avoid overtaxing Firms' resources by requiring them to address and document trivial matters, the Commission should either:

- *Revise the definition of "cybersecurity incident" to mean an unauthorized occurrence that results in actual harm to a market entity or its clients (not merely one that "jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems"); or*
- *In Rule 10(b)(1)(v), replace the term "cybersecurity incident" with the term "significant cybersecurity incident" (which the Commission has defined to include the concept of substantial harm).*[4]

[4] Rule 10(a)(10) defines "significant cybersecurity incident" as "a cybersecurity incident, or a group of related cybersecurity incidents, that: (i) Significantly disrupts or degrades the ability of the market entity to maintain critical operations; or (ii) Leads to the unauthorized access or use of the information or information systems of the market entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to result in: (A) Substantial harm to the market entity; or (B) 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."

Focusing Firms' regulatory obligations on incidents that produce actual harm will avoid imposing overly burdensome obligations on Firms, while capturing relevant incidents within the scope of Rule 10(b)(1)(v).

2. Cybersecurity Policies and Procedures

We agree with the Commission's observations that: (a) policies and procedures for cybersecurity risk management "generally should be tailored to the nature and scope of the [Firm's] business and address the [Firm's] cybersecurity risks"; and (b) "cybersecurity threats are constantly evolving and measures to address those threats continue to evolve."[5] Policies and procedures that are appropriately tailored to a Firm's business and material risks, and that are not wedded to today's technology, will create more effective cybersecurity programs and better protect the interests of Firms and the markets more broadly. With these critical points in mind, we have the following comments regarding Rule 10(b)(1), which addresses cybersecurity policies and procedures.

a. <u>The Commission should not require Firms to create detailed inventories or conduct a risk assessment of every service provider.</u>

As a first step in conducting risk assessments, Rule 10(b)(1)(i)(A)(1) requires Firms to "[c]ategorize and prioritize cybersecurity risks based on an inventory of the components of the covered entity's information systems and information residing on those systems...." While some type of inventory may be useful, detailed inventories of all system components and all information should not be required in order to commence a risk assessment. The inventories proposed in Rule 10B)(1)(i)(A)(1) would be particularly burdensome and costly for Firms given the overly broad definition of "information" discussed above.

As another commenter noted in response to the Commission's cybersecurity proposal for investment advisers, requiring covered entities to categorize risks based on an inventory of components of their information systems "goes well beyond [the NIST Cybersecurity Framework], and other industry standards, including the standards set forth in NIST 800-53. Assessment of network risks, as opposed to component risks, is a well-understood cybersecurity activity."[6] NIST allows for appropriate flexibility in the initial stage of risk assessments by calling for companies to "[c]ategorize the system and information processed, stored, and

[5] 88 Fed. Reg. at 20239.
[6] Letter from Jennifer W. Han, Chief Counsel and Head of Global Regulatory Affairs, Managed Funds Association, to Vanessa A. Countryman, Secretary, U.S. Securities and Exchange Commission, dated April 11, 2022, at 12 (commenting on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies).

transmitted by the system based on an analysis of the impact of loss."[7] The Commission should adopt similar language and:

- *Revise Rule 10(b)(1)(i)(A)(1) to require Firms to "categorize and prioritize cybersecurity risks associated with the covered entity's information systems and the information processed, stored and transmitted by those systems based on an analysis of the impact of loss."*

Rule 10(b)(1)(i)(A)(2) requires Firms to identify and perform a risk assessment for every service provider that receives, maintains or processes the Firm's "information." Because "information" is broadly defined to include even names and email addresses of a Firm's officers and employees, this provision would require Firms to perform a risk assessment of every service provider, even those that present little to no cybersecurity risk (*e.g.*, caterers, office supply companies, real estate brokers). Again, this goes well beyond existing cybersecurity standards and would drain the resources available to Firms to address critical, higher-risk vendors.

The better approach is to give Firms appropriate flexibility to perform cybersecurity risk assessments based on the Firm's specific business functions, risks and operating environments. To further this less prescriptive and more standard approach, we believe the Commission should:

- *Revise Rule 10(b)(1)(i)(A)(2) to require Firms to "identify and evaluate cybersecurity risks associated with the covered entity's service providers."*

b. <u>The Commission should not mandate the use of specific security tools, and it should require procedures for the "creation" (rather than "distribution") of passwords.</u>

Rule 10(b)(1)(ii) addresses user security and access. Subpart (B) requires Firms to require their users "to present a combination of two or more credentials for access verification", a procedure known as multi-factor authentication ("**MFA**"). We urge the Commission to avoid making today's technology such as MFA a regulatory requirement for years to come since that technology will become outmoded. Multiple reports already exist concerning methods utilized by hackers to thwart MFA.[8] We suggest that the Commission:

- *Remove the reference to MFA from Rule 10(b)(1)(ii)(B) or make clear that MFA is simply one tool that Firms might choose to utilize but it is not a regulatory requirement.*

---

[7] NIST 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations" (Dec. 2018), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.
[8] *See, e.g.*, "SIM Swap Attacks Are Making SMS Two-Factor Authentication Obsolete," Jan. 16, 2020, available at https://www.phishlabs.com/blog/sim-swap-attacks-two-factor-authentication-obsolete/.

The Commission has asked whether the proposed requirement in Rule 10(b)(1)(ii)(C) for Firms to have procedures for the "distribution" of passwords is problematic. The term "creation" would be more apt since it would enable Firms to allow their users to create their own passwords, which is a common practice. We therefore suggest that the Commission:

- *Replace the word "distribution" with the word "creation" in Rule 10(b)(1)(ii)(C).*

c. Firms should not be required to amend their written contracts with service providers or to oversee all service providers, regardless of the level of risk presented.

We are extremely concerned about proposed requirements regarding service providers and service provider contracts in Rule 10(b)(1)(iii)(B). We believe those requirements would lead to the loss of Firms' ability to continue working with numerous service providers, not because the service providers present material cybersecurity risk, but because they are not able or willing to amend their contracts to comply with the Commission's terms.

Rule 10(b)(iii)(B) requires that, for any service provider that receives, maintains or processes a Firm's information (or is otherwise permitted to access the Firm's information systems and information residing on those systems), the Firm must have a written contract that requires that service provider to "implement and maintain appropriate measures, including the practices described" Rule 10(b)(1)(i) through (v). Because "information" is broadly defined to include names and e-mail addresses of Firm officers and employees, we would need to renegotiate our contracts with all of our service providers, even law firms, accounting firms, water supply companies, copier repair services, and other service providers that supply essential business services but do not present an appreciable level of cybersecurity risk. Any vendor who agreed to these new contract terms would, in turn, have to renegotiate all of its contracts with all of its service providers to include compliance with Rule 10(b)(1)(i) through (v), and so on down the line. At least one commenter has called into question the Commission's legal authority to regulate the contract terms of covered entities, let alone "to indirectly regulate, through contractual provisions, persons that it lacks legal authority to regulate directly."[9]

Our experience with our service providers suggests that the vast majority of them would be unable or unwilling to incorporate compliance with Rule 10(b)(1)(i) through (v) into our contracts with them. The Proposal assumes that Firms can simply "change service providers and bear the associated switching costs",[10] but that is not realistic. It is highly unlikely that any

[9] Letter from Susan M. Olson, General Counsel, Investment Company Institute, to Vanessa A. Countryman, Secretary, U.S. Securities and Exchange Commission, dated May 23, 2023, at 14-15 (commenting on Cybersecurity Risk Management for Broker-Dealers et al).
[10] 88 Fed. Reg. at 20300.

providers of professional services, such as law firms and accounting firms, would agree to be contractually obligated to comply with Rule 10(b)(1)(i) through (v). In service categories with limited competition, there may not be suitable alternatives to supply important services. Some categories of vendors (*e.g.*, those whose services are offered exclusively online) only offer "click through" or "clickwrap" contracts, which are not negotiable.

Even if we could switch to different service providers, the Commission has overlooked significant costs that Firms would incur if forced to take this step. To help the Commission better understand such costs, we offer as one example (out of our dozens of service providers) our business relationship with a vendor that supplies contract management services (referred to herein as "**Vendor A**"). After months of reviewing potential service providers, we selected Vendor A based on its specific service offering (which, for our business needs, is superior to and not fungible with that of its competitors), its clientele (which include, among others, a branch of the U.S. Armed Services, Fortune 500 companies, and state and local governments), and its exemplary cybersecurity practices (which include, among others, SOC 2 certification and approval for deployment on the Secure Network at the U.S. Department of Defense).

We have invested hundreds of hours designing and building our contract database housed by Vendor A and working with Vendor A to design and deliver training and related materials to those at Gelber who use the database. We have a multi-year contract with Vendor A that locks in favorable pricing. Based on informal discussions regarding the Proposal, we are informed that Vendor A would not agree to a written contract that requires them to comply with Rule 10(b)(1)(i) through (iv). If forced to switch to a new service provider, our costs would include the loss of our database at Vendor A, the loss of our multi-year contract with Vendor A, and spending hundreds of hours to build and train on a new database at a vendor that provides an inferior (for our needs) offering and whose cybersecurity program may be inferior to that of Vendor A. Alternatively, we would be forced to host the database solely on on-premise servers, which would generally increase cybersecurity risks.

Given the high costs and questionable benefits of this approach, we believe the provisions of Rule 10 related to the cybersecurity risk management of service providers should be principles-based so that each Firm can tailor its vendor management program to (i) focus on service providers that present the most significant cybersecurity risk, and (ii) adopt effective risk mitigation strategies that appropriately reflect commercial realities. Accordingly, we urge the Commission to:

- *Revise Rule 10(b)(1)(iii)(B) to remove any required contractual terms and to simply require Firms to have policies and procedures that are reasonably designed to address cybersecurity risks presented by their service providers.*

d. The Commission should either revise its definition of "cybersecurity incident" or replace it with the term "significant cybersecurity incident" throughout Rule 10(b)(1)(v).

Rule 10(b)(1)(v) requires firms to take certain measures in connection with any "cybersecurity incident." As explained at pages 3-4 above, the Commission should either revise the definition of "cybersecurity incident" to require actual harm or replace that term with "significant cybersecurity incident" throughout Rule 10(b)(1)(v).

e. The Commission should not require Firms to use encryption.

The Commission has requested comment on whether it should require Firms to encrypt certain information on their information systems.[11] While encryption can be a useful tool in certain circumstances, the Commission should avoid prescribing whether and how Firms must use it. Broadly applied to specified categories of information, encryption could have serious negative performance impacts on a Firm's information systems. Also, encryption may be of questionable utility depending upon (i) the type of encryption required, and (ii) the specific details of a Firm's information systems. For these reasons, Firms should be allowed to determine for themselves how best to deploy encryption as a security tool.

3. Notice and Reporting of Significant Cybersecurity Incidents

Rule 10(c) addresses Firms' notification and reporting requirements when a "significant cybersecurity incident" occurs. Subpart (1) requires immediate written electronic notice to the Commission and certain others after the Firm reasonably determines that it has experienced a reportable incident. Subpart (2) requires submission of Form SCIR Part I through the Commission's EDGAR system within 48 hours of a Firm having reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring, with additional filings required as the incident unfolds. We share Commissioner's Peirce's concern that the "legal peril" created by the proposed notification and reporting regime "will distract employees of the firm from mitigating the immediate threat to the firm ... as they navigate the aggressive deadlines and open-ended information demands from the Commission."[12] To address these concerns, we urge the Commission to revise Rule 10(c) as suggested below.

[11] *Id.* at 20247.
[12] Statement of Commissioner Hester M. Peirce on Proposed Cybersecurity Rule 10 and Form SCIR (March 15, 2023).

a. The Commission should revise Rule 10(c)(1) to account for the possibility that a Firm's computer systems and business operations may be temporarily shut down after a cyberattack, making it impossible to provide "immediate written electronic notice."

Rule 10(c)(1) requires Firms to "give the Commission immediate written electronic notice" of a significant cybersecurity incident when the Firm has a reasonable basis to conclude that the incident has occurred or is occurring. This requirement overlooks the fact that, immediately after a cyberattack, a Firm's computer systems may be temporarily shut down, or the perpetrator may still be in the Firm's systems with access to electronic submissions made to the Commission.

To account for these possibilities, the Commission should adopt the notification approach used by U.S. federal banking regulators in their cybersecurity rules for banking organizations (the "**Interagency Guidelines**"). Those rules provide banking organizations with alternative means to notify their banking regulator of a computer-security incident "through email, telephone, or other similar methods" that the banking regulator may prescribe.[13] These multiple methods of communication were included in order to balance "the need for banking organizations to have some flexibility, including if a communication channel is impacted by the incident, with the agencies' need to ensure that they actually receive the notification."[14] Also, rather than requiring "immediate" notice, the Interagency Guidelines allow for notification "as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred."[15] Along these same lines, we suggest that the Commission:

- *Revise Rule 10(c)(1) to require Firms to provide for notification "through email, telephone or other similar methods that the Commission may prescribe" and allow such notification to occur "as soon as possible and no later than 36 hours after the covered entity has a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring."*

b. The Commission should change the deadline for the initial filing of Form SCIR Part I from 48 hours to four business days.

Rule 10(c)(2) requires Firms to submit Form SCIR Part I through EDGAR no later than 48 hours after having a reasonable basis to conclude that a significant cybersecurity incident occurred or is occurring. As noted above, after a cyberattack, a Firm's computer systems and business operations may be temporarily shut down, making it impossible for the Firm to comply with this

[13] *See* "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers," 86 Fed. Reg. 66424 (Nov. 23, 2021).
[14] *Id.* at 66433.
[15] *Id.*

requirement, and if the perpetrators are still in the Firm's system, they may have access to the Firm's EDGAR submissions.

Furthermore, Form SCIR Part I contains 15 questions, most of which call for detailed information about the incident. A tight and inflexible 48-hour window for responding to these questions may impede a Firm's efforts to contain the incident and may result in the good-faith submission of information that later proves to be inaccurate and/or incomplete. As the Cybersecurity and Infrastructure Security Agency ("**CISA**") has noted, especially during the 48-hour period after a cyberattack is uncovered, "[i]nformation will change rapidly as new evidence is discovered" and "personnel may become fatigued, and resources strained"[16]

The Interagency Guidelines impose limited notification requirements on banking organizations when a reportable incident occurs and do not require the submission of any regulatory forms. In issuing these cybersecurity notification rules, federal banking regulators highlighted that "[s]uch a limited notification requirement will alert the agencies to such incidents without unduly burdening banking organizations with detailed reporting requirements, especially when certain information may not yet be known to the banking organizations."[17]

We urge the Commission to avoid adding to the pressures that Firms experience when a cyberattack occurs by burdening them with the detailed reporting requirements of Form SCIR Part I. If the Commission insists on moving forward with this new Form, it should provide a period of at least four business days from uncovering a significant cybersecurity incident to make the submission. This aligns with the period of four business days that the Commission has proposed for a public company to submit a Form 8K after the company determines that it has experienced a material cybersecurity incident.[18] We urge the Commission to:

- *Revise Rule 10(c)(2)(i) to give a covered entity up to four business days after having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring to file Form SCIR Part I.*

[16] "'First 48': What to Expect When a Cyber Incident Occurs," available at https://www.cisa.gov/sites/default/files/video/safecom_first_48_22_1109_final_508c.pdf.
[17] 86 Fed. Reg. at 66432.
[18] *See* "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," 87 Fed. Reg. 16590 (Mar. 23, 2023).

c. The Commission should not require information about cybersecurity insurance on Form SCIR Part I.

Question 14 on Form SCIR Part I requires Firms to indicate whether a significant cybersecurity incident is covered by insurance. As an initial matter, it is questionable whether information about a Firm's cybersecurity insurance (or lack thereof) serves any significant regulatory purpose. Moreover, bad actors may target the Commission's reporting systems to obtain information about which Firms have cybersecurity insurance, and then target those Firms for attack.[19] As the Commission is aware, its EDGAR system has been penetrated by hackers on at least one occasion.[20] If the Commission has a particularized need for information regarding a Firm's insurance coverage, it should obtain such information through a channel that is more secure (and less likely to be targeted by bad actors). We encourage the Commission to:

- *Remove question 14 from Form SCIR Part I.*

d. Firms should not be required to continuously amend their initial Form SCIR Part I submissions to reflect "material" developments.

Rule 10(c)(2)(ii) requires Firms to file an amended Form SCIR Part I no later than 48 hours after each of the following: (A) any previously reported information becomes "materially inaccurate"; (B) any "new material information" about the significant cybersecurity incident is discovered; (C) the incident is resolved; or (D) an internal investigation into the incident is closed. Requiring numerous amendments to Form SCIR Part I, each with a 48-hour reporting window, would multiply the burdens that Firms face when attempting to contain and recover from significant cybersecurity incidents, and the influx of amendments would be of questionable benefit to the Commission.

In responding to the Commission's parallel rule proposal for investment advisers, one commenter referred to such a "continuous reporting requirement" as perhaps "the single most onerous and unnecessary aspect of the Proposal."[21] As that commenter observed, numerous amendments would be necessary given that significant cybersecurity incidents are fast moving,

---

[19] *See*, *e.g.*, "Companies May Be Flagging Themselves For Hackers By Buying Cybersecurity Insurance" (July 15, 2021), available at https://www.npr.org/2021/07/15/1016572979/companies-may-be-flagging-themselves-for-hackers-by-buying-cybersecurity-insuran.

[20] *See* U.S. Securities and Exchange Commission v. Ieremenko, D.N.J., Civil Action No. 19-cv-505 (Jan. 15, 2019).

[21] Letter from Gail C. Bernstein, General Counsel, Investment Advisers Association, to Vanessa A. Countryman, Secretary, U.S. Securities and Exchange Commission, dated April 11, 2022, at 29 (commenting on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies).

information is rarely known all at once and typically changes rapidly.[22] Particularly if Firms are required to submit an initial Form SCIR Part I within 48 hours of discovering an incident, they will continue to uncover new information on an ongoing basis after the initial filing. Rule 10 offers no guidance on how Firms should assess what new information is "material" with respect to a previously reported incident, or when "any information" previously reported regarding an incident should be deemed "materially inaccurate." Employees within a Firm may disagree as to what information is "material" or "materially inaccurate", leading to potential overreporting in an effort to avoid enforcement action for failure to comply with Rule 10(c)(2)(ii)(A) and (B).

By giving Firms at least four business days (rather than 48 hours) to submit the initial Form SCIR Part I, as suggested above, the Commission should obtain more complete and accurate information about significant cybersecurity incidents from the initial filings, thus decreasing the need for continuous amendments as incidents unfold. If the circumstances surrounding particular incidents require the Commission to receive additional updates, the Commission (and/or FINRA, in the case of broker-dealers) can contact Firms to request further information. Otherwise, Firms should only be required to amend Form SCIR Part I when a significant cybersecurity incident is resolved or an internal investigation into the incident is closed. We therefor urge the Commission to:

- *Eliminate subparts (A) and (B) from Rule 10(c)(2)(ii) so that Firms are only required to submit an amended Form SCIR Part I when a significant cybersecurity incident is resolved or an internal investigation into the incident is closed.*

4. Public Disclosures

a. <u>The Commission should either eliminate Form SCIR Part II or not make these filings public and not require Firms to post these filings on their websites.</u>

Rule 10(d) requires Firms to make public disclosures concerning: (1) cybersecurity risks that could materially affect the Firm's business and operations and how the Firm assesses, prioritizes and addresses those risks; and (2) each significant cybersecurity incident that the Firm experienced during the current or previous calendar year, including persons affected, the date it was discovered and whether it is ongoing, whether data was stolen or altered or accessed, the effect of the incident on the Firm's operations, and whether the Firm has remediated or is remediating the incident. Firms would make these disclosures by filing Part II of Form SCIR with the Commission, and the Commission would make these filings publicly available.[23] In

[22] *Id.*
[23] The Proposal states that "[t]he Commission would make these [Form SCIR Part II] filings public." 88 Fed. Reg. at 20257.

addition, a Firm would have to post its Form SCIR Part II filings "on an easily accessible portion of its business internet website that can be viewed by the public without the need of entering a password or making any type of payment or providing any other consideration."[24]

The Commission offers two reasons for requiring Firms to make these public disclosures. First, the Proposal states that "individuals naturally may visit a company's business website when seeking timely and updated information about the company, particularly if the company is experiencing an incident that disrupts or degrades the services it provides."[25] Second, the Proposal states that "individuals may naturally visit a company's business internet website as part of their due diligence process in determining whether to use its services."[26]

Neither of these reasons applies to proprietary trading firms like Gelber. Gelber does not offer any services to the public nor does it have any customers or users.[27] Our counterparties are sophisticated market entities (*i.e*., exchanges, trading platforms, clearing firms, prime brokers and other broker-dealers). While our counterparties may check our website for certain basic information as part of their due diligence processes, they routinely require us to furnish information that is confidential in nature and is not posted on our website. They can easily request information about our cybersecurity risks and any cybersecurity incidents as part of their regular due diligence processes if they choose to do so. We ask the Commission to avoid burdening proprietary trading firms with regulatory requirements designed for Firms with customers or users.

Moreover, we share Commissioner Peirce's concern that mandatory public disclosure of information about Firms' cybersecurity vulnerabilities and risk management strategies, along with specific information about potentially ongoing cybersecurity incidents, "could serve as a roadmap for cybercriminals."[28] In other words, if this information is made public, it may provide the cyber "bad actor" community with an easily accessible and exploitable blueprint of each Firm's cybersecurity vulnerabilities and defenses, and make Firms an even more likely target for cyberattacks. It may also serve to notify a perpetrator that its attack has been discovered and make it more likely that the perpetrator will be able to cover its tracks.[29] To the best of our

[24] Rule 10(d)(2)(ii).
[25] 88 Fed. Reg. at 20257.
[26] *Id*.
[27] We leave it to Firms with customers or users to address appropriate methods for disclosing information about their cybersecurity risks and incidents to their customer or user base.
[28] *Supra* note 12.
[29] *See* Ari Schwartz, "The Securities and Exchange Commission Obstructs National Security," Wall St. J. (Sep 30, 2022).

knowledge, no other regulator in the financial services sector requires companies to make this type of information publicly available.[30] The Commission should not do so either.

As to the Commission's need for the information contained in Form SCIR Part II, the Proposal states that "[c]entralized EDGAR filing could make it easier for Commission staff and others to assess the cybersecurity risk profiles of different types of Covered Entities and could facilitate trend analysis of significant cybersecurity incidents."[31] Given that the Commission will have detailed information about significant cybersecurity incidents from Form SCIR Part I, Form SCIR Part II is not needed to facilitate trend analysis of incidents.

With regard to assessing risk profiles of different types of Covered Entities, we do not understand the need for an EDGAR filing concerning cybersecurity risk more so than other categories of risk faced by Firms (*e.g.*, market risk, liquidity risk, legal risk, credit risk, compliance risk). If Commission staff wants to assess cybersecurity risk profiles of different types of Firms, it will have means other than Form SCIR Part II to obtain the necessary information. For example, Firms will be required to document their cybersecurity risk management programs and to create and keep records of those programs which will be subject to examination.

For all of the above reasons, we believe that the Commission should:

- *Eliminate Rule 10(d) and Form SCIR Part II in its entirety; or*
- *Exempt proprietary trading firms from Rule 10(d); or*
- *Revise Rule 10(d) to eliminate any requirement for Firms to make Form SCIR Part II filings publicly available (on their websites or otherwise), and do not allow the Commission to make Form SCIR Part II filings publicly available.*

[30] *See, e.g., supra* note 13 (Interagency Guidelines do not require public disclosures regarding cybersecurity incidents or risk management programs); New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies, 23 CRR-NY 500, et seq. (NYDFS does not require covered entities to make public disclosures regarding cybersecurity incidents or risk management programs); National Futures Association Interpretive Notice 9070 – NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (NFA does not require member firms to make public disclosures regarding cybersecurity incidents or risk management programs).

[31] 88 Fed. Reg. at 20257.

b. The Commission should require no more than regularly scheduled, periodic updates of Form SCIR Part II.

Rule 10(d)(4) requires Firms to "promptly" update the disclosures on Form SCIR Part II when the information initially provided "materially changes," including after a new significant cybersecurity incident occurs or when information about a previously disclosed incident "materially changes." We refer to the discussion at pages 11-12 above regarding the difficulties inherent in determining what information should be deemed "material" in the circumstances of cybersecurity incidents, particularly when the Commission offers no guidance in that regard. If the Proposal is adopted as is, Firms will not only have to submit continuous amendments to Form SCIR Part I as they grapple with significant cybersecurity incidents, they will also need to submit continuous amendments to Form SCIR Part II and post those amended forms on their websites. In addition to creating undue regulatory burdens, this will allow perpetrators of ongoing incidents to follow along in real time with a Firm's efforts to investigate and remediate the attack.

These problems could be ameliorated by only requiring high-level, aggregated information about a Firm's significant cybersecurity incidents within the past year on Form SCIR Part II, so that multiple amendments need not be made and posted as a particular incident unfolds. We also suggest that, if Form SCIR Part II is to be used at all, Firms should only be required to make regularly scheduled periodic amendments, such as annually. Accordingly, we recommend that the Commission:

- *Revise Rule 10(d)(4) so that Firms are required to make annual updates to Form SCIR Part II if the information previously disclosed has changed.*

We thank the Commission again for the opportunity to submit these comments in response to the Proposal. If the Commission has any questions regarding this letter, please contact the undersigned at (312) 692-2840 or Ldunsky@gelbergroup.com.

Sincerely,

/s/ Lisa Dunsky

Lisa A. Dunsky
General Counsel
Gelber Securities, LLC