sifma

Invested in America

April 17, 2025

Via E-mail: rule-comments@sec.gov

J. Matthew DeLesDernier
Deputy Secretary
Division of Trading and Markets
Securities and Exchange Commission
Washington, DC 20549

Re: File SR-DTC-2025-003

Dear Deputy Secretary DeLesDernier:

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to respond to the DTCC's notice of filing of a proposed rule change relating to a participant system disruption (the "Proposal"). in response to the Release No. 34-102712: Self-Regulatory Organizations; The Depository Trust Company; Notice of Filing of Proposed Rule Change Relating to a Participant System Disruption.

SIFMA agrees with the spirit of the disruption rule updates and proposes refinement to several definitions in order to prevent unintended consequences. The DTCC should also consider adjusting proposed reporting time frames to be more in line with existing regulatory rules and guidelines for incident notification.

In consideration of the concerns articulated below, our members believe it would be most appropriate for DTCC to review the industry's comments and issue a revised draft for further consultation. We respectfully request that any further consultation include longer timelines to allow the industry to fully consider the proposals.

[1] SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation, and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

sifma

Invested in America

Executive Summary

SIFMA recognizes the benefit of parties in the financial services ecosystem engaging in proactive review of existing disruption rules and communication on matters of importance. We appreciate that DTCC, in light of recent events, are reviewing the rules and considering amendments to Rule 38(A) *Systems Disconnect: Threat of Significant Impact to the Corporation's Systems of the Rules, By-Laws and Organization Certificate of DTC*.

However, many of the suggested rule changes are overly broad, and may lead to a significant burden of reporting for system disruptions that are beyond DTCC's purview. Further, some of the expanded requirements may infringe on a firm's ability to make appropriate business decisions based on their risk profiles. In addition, the DTCC should consider adjusting proposed reporting time frames to align with existing regulatory rules and guidelines for incident notification.

As discussed in more detail below, we believe the Proposal may have the following negative consequences:

- By expanding the definition of incident to all operational incidents, rather than only those caused by a malicious cyber event, the rule risks misapplying disconnection/reconnection as a response, thereby propagating disruption.

- By not aligning to any known definition of incident it adds yet another definition to an already complex regulatory environment for incident reporting.

- It sets an unnecessarily low threshold for incident notification. This will likely cause participants to overreport on low-risk incidents, obscuring DTCC's view of which incidents are significant and providing limited value.

- The rule gives DTCC legal rights to potentially interfere with system participants' ability to make the best business decisions.

To better align with existing regulatory requirements and practices, we suggest that DTCC make the following changes to the proposed amendments.

- Explicitly limit the scope of notifiable incidents to those caused by a malicious cyber event.

- Refine the scope of reportable incidents to focus on substantial incidents that impact critical services and harmonize with existing regulations.

- Refine and limit proposed reporting requirements to information directly related to an actionable purpose.

- Increase the notification timeframe to align with existing standards so that critical resources can be used to address the incident and mitigate impact.

- Provide definitions for the following terms: unauthorized access (actual or anticipated), unavailability, system failures or malfunctions system overloads, data corruption, restrictions (partial or total), and unaffiliated DTCC systems participant.

Finally, SIFMA notes that authorities should not view DTCC's choices as necessarily a best practice for all firms. A similar process or governance structure may not be suitable for all firms due to their differing abilities to mitigate the cyber risk and business impact from a third-party incident.

For these reasons, which we discuss in detail below, we strongly urge the DTCC and the Commission to consider our feedback. Our comments are organized by section of the proposed amendments to Rule 38A.

Our members have indicated that the definitions of a Participant System Disruption and Third-Party Cybersecurity Firm would bring about various challenges.

Definitions

Participant System Disruption

The proposed definition change of "Systems Disruption" to "Participant System Disruption" should be reconsidered:

> "Participant System Disruption" means the actual or reasonably anticipated unauthorized access to, or unavailability, failure, malfunction, overload, corruption, or restriction (whether partial or total) of one or more systems of a DTCC Systems Participant.

We believe that reportable incidents should be limited to those caused by malicious cybersecurity breaches. While DTCC may choose to take business continuity measures that are similar to disconnection protocols in response to a non-malicious operational incident at a participant, the term disconnection and the accompanying reconnection process are only appropriate for an incident in which confidence or trust in the participant has been lost. For example, while DTCC's proposed requirements to engage a Third-Party Cybersecurity Firm to obtain a 'detailed, comprehensive, and auditable report' can be an appropriate tool to restore trust, it would not be necessary when a disruption is caused by, e.g., a change management issue. Expanding the meaning of disconnection to include business continuity responses to non-malicious operational disruptions risks creating confusion in the sector and possibly prolonging the length of

disruption from such a non-malicious event by activating overly stringent response and assurance requirements.

SIFMA further believes that reporting on "reasonably anticipated" incidents is subjective, vague, and impractical. A strict legal reading of the proposed definition of a reportable incident would require participants to report any reasonably anticipated unavailability of a system, regardless of its cause or impact. The lack of any clear threshold on the occurrence, cause, and impact of the incident will result in large volumes of reporting and dilute DTCC's ability to identify serious incidents that threaten real harm. To address these concerns, SIFMA asks the Commission to consider aligning its definition with that of the Options Clearing Corporation.[2] The Corporation's definition of a "security incident occurrence" requires that a member notify when they become aware "that there has been an incident, or an incident is occurring, involving a cyber-related disruption or intrusion of a Clearing Member's system(s) that is reasonably likely to pose an imminent risk or threat to the Corporation's operations". Because this definition narrows the scope of reportable disruptions to actual or ongoing malicious cyber incidents with impact, it would focus DTCC's resources on identifying and managing incidents that pose a genuine risk to its operations.

Third-Party Cybersecurity Firm

We further request that DTCC amend the proposed definition of "Third-Party Cybersecurity Firm":

> "means a firm that, in the Corporation's reasonable judgement, (A) (i) is well-known and reputable; (ii) is not affiliated with DTCC, the Corporation, an Affiliate of DTCC or the Corporation, a DTCC Systems Participant, or an Affiliate of a DTCC Systems Participant; (iii) specializes in financial-sector cybersecurity; and (iv) employs Best Practices; or (B) is otherwise determined to be a Third-Party Cybersecurity Firm by the Corporation."

The proposed definition requires a third-party security firm to specialize in financial-sector cybersecurity. However, demonstrating specialization can be complex and subjective. To address this, the industry proposes requiring third-party security firms to have 'experience' in financial-sector cybersecurity. This criterion is more actionable and objective, allowing firms to demonstrate their capability through verifiable past engagements and achievements and corporations' flexibility in determining the appropriate vendor for their business.

[2] Options Clearing Corporation (OCC) Rules: Rule 213 Cybersecurity Obligations, Available:https://www.theocc.com/getmedia/9d3854cd-b782-450f-bcf7-33169b0576ce/occ_rules.pdf.March 26, 2025.

Further, we seek to understand DTCC's meaning of "affiliation with the third-party cybersecurity firm." We feel strongly that DTCC should not preclude a firm which DTCC itself has formerly or currently retains for cybersecurity incident response. This would significantly detract from system participants' ability to choose an appropriate firm. Additionally, as a practical matter, the proposed language does not state how system participants would have knowledge of what firms have an affiliation with DTCC. We welcome reconsideration of this definition.

Notifications of a Participant System Disruption

We request that DTCC reconsider elements of the section on Notification of a Participant System Disruption.

Reporting Timeframe

The proposed language in Section 2(a) is a significant change to the current required timeframe of immediate notification:

"Any DTCC Systems Participant experiencing a Participant System Disruption shall notify the Corporations of such on behalf of itself and any Affiliate of the DTCC Systems Participant, in writing, immediately, but no later than two hours after experiencing the disruption."

We urge DTCC to reconsider the two-hour reporting requirement because this standard will divert resources and attention away from assessment and remediation. Two hours is also not sufficient time for participants to gather all the information required by DTCC, nor does it allow time to properly determine impacts which could result in participants significantly over reporting incidents in order to avoid missing deadlines and risk of being non-compliant.

The DTCC proposal also does not sufficiently consider the impact and influence of a firm's impacted third and fourth parties on notification requirements. Third or fourth parties may delay or fail to provide timely notification to the financial institution hampering a firm's overall ability to timely notify DTCC and/or the SEC.

We request the DTCC to consider benchmarking against other federal and state reporting standards, such as the Office of the Comptroller of the Currency's (OCC's) standard for notification as stated in CFR §225.302: "A banking organization must notify the appropriate Board-designated point of contact about a notification incident through email, telephone, or other similar methods that the Board may prescribe. The Board must receive this notification from the banking organization as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred."

DTCC should also consider the Joint Agency Final Rule on Computer-Security Incident Notification Requirements for Banking Organizations and Their Service Providers, which requires notification no later than 36 hours after determining that a Notification Event has occurred.[3]

A state reporting standard to consider is the New York State Department of Financial Services (NYSDFS) which sets a 72-hour notification.[4] Our members have indicated that a 36-hour reporting timeframe is reasonable and would allow for adequate time to access the incident and not divert resources from solving the problem.

Unaffiliated DTCC Systems Participant

The next matter for consideration in this section is the proposed changes to Section 2(b):

"If a DTCC Systems Participant has actual knowledge that an unaffiliated DTCC Systems Participant is experiencing a Participant System Disruption, the DTCC Systems Participant shall, if legally permitted, notify the Corporation of such, in writing, immediately, but no later than two hours after obtaining such knowledge."

We request that DTCC clarify the meaning of "unaffiliated DTCC Systems Participant" which is not included in the Definitions section. The proposed definition of a DTCC systems participant covers the respective participant, affiliates that directly and indirectly connect with DTCC systems, and any third parties that directly or indirectly connect with the respective participant or its affiliate. Given this broad definition, it is unclear what is meant by an unaffiliated DTCC systems participant. Additionally, DTCC has not made clear why a system participant should report a disruption to an unaffiliated party. Our members have indicated that this requirement would add to existing reporting requirements and divert resources away from managing incidents. Further, reporting on incidents at an unaffiliated party, for which the participant is unlikely to have detailed or precise information, could lead DTCC to take actions which are disproportionate or damaging to the financial sector. Our members are firmly of the view that there should be no legal obligation to report on incidents at an unaffiliated party.

Disclosing Notices

The final concern we have with Section 2 is 2(c)(iii)(7): **"**Notifications provided pursuant to paragraphs (a) and (b) of this Section 2 shall, at a minimum, include all of the following information, and any such information unconfirmed or otherwise unknown shall be identified by the DTCC Systems participant as "Unknown":

---

[3] https://www.federalreserve.gov/newsevents/pressreleases/bcreg20211118a.htm

[4] 23 NYCRR 500: CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES 500.17 Notices to superintendent: (a) Notice of cybersecurity incident. (1) Each covered entity shall notify the superintendent electronically in the form set forth on the department's website as promptly as possible but in no event later than 72 hours after determining that a cybersecurity incident has occurred at the covered entity, its affiliates, or a third-party service provider.

(iii)(7): "Notice – whether any formal or informal notice of the Participant System Disruption or related information was provided to any third party including, but not limited to, a regulator or other supervisory enforcement or investigatory body; another DTCC Systems Participant; or a media outlet; and, if so, provide a copy of such notice or relevant information, if legally permitted".

Our members oppose this provision. DTCC should not require its participants to disclose other notices it has given on the participant system disruption. Communications between firms, their regulators and third parties are subject to confidentiality and disclosing this information adds no tangible benefit to DTCC's ability to manage the disruption.

Declaration of a Major Systems Event

The proposed revision of definition of 3(b) reads:

"Upon declaration of a Major System Event, the Corporation shall be entitled to act (or refrain from acting) pursuant to Section 4 of this Rule 38(A) to help address, correct, mitigate, or alleviate any and all risks presented by or related to the Major System Event. Action taken will be in the consideration of the risks presented to the Corporation, including, but not limited to, the risks enumerated in the definition of a Major System Event, based on the facts and circumstances, including, but not limited to, information provided pursuant to Section 2 of this Rule 38(A)."

DTCC should more clearly articulate the risks and threats for which it considers disconnection to be an appropriate mitigant. While we recognize the limitations of the rule making format, clarity on which threats to DTCC's operations the disconnection decision is meant to mitigate would provide greater certainty to the market. In particular, the sector believes that sufficient controls should be in place to mitigate the risk of contagion from a breach to a participant's systems. Rather, the primary drivers for disconnecting from a participant could include:

- Intelligence suggesting the threat actor has not been removed from the compromised organization's network and that further disruption is therefore likely;
- When continuing to send sensitive information to the compromised organization could result in a breach of that data;
- When continuing to send data, especially transaction data, may result in an increased backlog at the compromised organization or in some way exacerbate eventual reconciliation and business resumption activities.

Authority to Take Action and Required Cooperation

DTCC Authority

We note the expansive authority afforded to DTCC in section 4(a): "During or in connection with a Major System Event, the corporation may:(iii) Take, or refrain from taking, or require the subject DTCC Systems Participant to take or refrain from taking any and all action that the Corporation considers appropriate to help address, correct, mitigate or alleviate the Major System Event and, as appropriate and practical, facilitate the continuation of services which may include issuing instructions to the subject DTCC Systems Participant and requiring such DTCC Systems Participant to act on such instructions."

We request acknowledgment that system participants are best placed to determine mitigation actions. The proposal notes that DTCC might require its participants to take, or refrain from taking, all action it considers appropriate to prevent, address, correct, mitigate or alleviate the major event and facilitate the continuation of services. The failure to do so authorizes DTCC to subject the systems participant to disciplinary action. However, while the industry recognizes that there are actions that DTCC can reasonably expect its participants to take (e.g., halting a specific process), it is the affected participants, and not DTCC, who are best placed to determine specific mitigation actions it should take.

Balancing Cyber Risk and Business Impact

DTCC should explicitly acknowledge their intention to consider the balance of cyber risk and business impact in any disconnection decision. As DTCC is well aware, a disconnection decision must consider not only cybersecurity risk, but the potential business impact of disconnecting or not reconnecting. We note that in places the rule gives DTCC the right both to act, but also to refrain from acting. While this could be interpreted as license to make a balanced decision, more explicit acknowledgement that DTCC will refrain from acting or requiring the participant to act when they consider that doing so would create unacceptable business impact should be included. Given the likely systemic nature of a disconnection from DTCC and a major participant, it is all the more imperative that this consideration be explicitly acknowledged and also recognized by financial authorities.

Reconnection Requirements

Disclosure of Information Contained in Third-Party Cybersecurity Firm Report

SIFMA urges reconsideration of the proposed requirement to require a DTCC Systems Participant to DTCC to share the Third-Party Cybersecurity Firm's report. The Section 5(a) – Reconnection Requirements states:

(a) "A DTCC Systems Participant that was the subject of action pursuant to Section 4(a) of this Rule 38(A) must provide to the Corporation the following, prior to the Corporation reestablishing connectivity of the DTCC Systems Participant to DTCC Systems ("Reconnection"):

(i) A detailed, comprehensive and auditable report, from a Third-Party Cybersecurity Firm, that, at a minimum, includes:"

The information required in the third-party cybersecurity firm's report includes highly sensitive data on the control environment of the affected participant. While we understand that DTCC requires assurance that the mitigations identified by the third-party cybersecurity firm as being sufficiently addressed, a requirement to review the entire report is likely to lead to delays as legal terms and redactions are negotiated. Instead, the attestation process, in which the affected participant confirms that it has implemented controls recommended by the third-party cybersecurity firm, should be sufficient assurance.

SIFMA's publication "Reconnection Guidance for Remediating Cyber Events Impacting the Financial Ecosystem,"[5] is a useful resource for members and system participants to use to guide the communication of remediation expectations from client organizations and the remediating activities of the compromised organization. The result of a working group, these protocols were developed by subject matter experts and tested during several industry exercises led by the Analysis and Resilience Center (ARC) and are a significant tool for considering reconnection.

Executed Indemnity

The final item we wish to provide feedback on is Section 5(a)(iii): An executed indemnity to the reasonable satisfaction and judgment of the Corporation in consideration of the facts and circumstance.

Our members feel strongly that DTCC should not require an executed indemnity from the affected participant. The relationship between DTCC and its participants is of a legal nature and is governed by existing contracts that define the nature and scale of any indemnity given by the participant. Introducing indemnity through DTCC's rulebook is duplicative and has the potential to create inconsistencies with already agreed upon terms. At the very least, DTCC should clarify, and subsequently consult, what it is proposing that participants are indemnifying against and to what extent. This would enable participants to assess the legal risk associated with this proposal.

***

[5] Reconnection Guidance for Remediating Cyber Events Impacting the Financial Ecosystem, Available at: https://www.sifma.org/wp-content/uploads/2024/04/SIFMA-Reconnection-Framework-for-Remediating-Cyber-Events-Nov2023.pdf. November 2023.

SIFMA stands ready to provide any additional information or assistance that the Commission may find useful and welcomes the opportunity for collaboration. Please feel free to contact Steven Byron via phone at 212-313-1254 and via email at sbyron@sifma.org, should you have any questions.

Sincerely,

Stephen Byron
Managing Director
Head of Operations, Technology, Cyber & BCP
SIFMA