Optiver

ADDRESS
130 E Randolph Street
Suite 1400
Chicago, IL 60601

PHONE
1 (312) 821-9500

Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

Date
2 June 2023

Subject
RE: 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 Rule No. 34-97142; File No. S7-06-23

Dear Ms. Countryman,

Optiver US LLC[1] ("Optiver") appreciates the opportunity to comment on the Securities and Exchange Commission's (the "SEC" or "Commission") proposal (File No. S7-06-23) to establish a framework that ensures entities that are critical to maintaining the efficiency and stability of financial markets are adequately able to mitigate cybersecurity risks. Given the increasing role that technology plays in financial markets, Optiver agrees with the Commission on the value of establishing cybersecurity standards. However, we would caution that a broad implementation may result in unintended consequences and introduce additional risks. Specifically, Optiver would highlight that public disclosure of cybersecurity risks and significant incidents has the potential to draw the attention of nefarious individuals looking to identify and exploit the very systems the proposed rule intends to protect.

Public Disclosure of Cybersecurity Risks and Significant Cybersecurity Incidents

The Commission states in the proposal that the intent of public disclosure is to help alleviate information asymmetry, and in doing so, enable customers, counterparties, members, registrants, and users to better assess the effectiveness of Covered Entities' cybersecurity preparations and the cybersecurity risks of doing business with any one of them[2]. While Optiver acknowledges the Commission's efforts to address any information asymmetry that may exist, public disclosure of

[1] Established in 1986, Optiver is a global market maker with offices in Amsterdam, London, Chicago, Austin, Sydney, Shanghai, Hong Kong, Singapore and Taipei. With close to 2,000 employees, Optiver provides liquidity to financial markets using our own capital, at our own risk, trading a wide range of products: listed derivatives, cash equities, ETFs, bonds and foreign currencies.
[2] 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 – Page 354

Optiver

this nature risks alerting nefarious individuals to specific information that could support future or ongoing cyberattacks. To address this issue, we would encourage the Commission to amend the proposal to require that any disclosure of cybersecurity risks and events (current or historical) by a Covered Entity occur bilaterally, under a nondisclosure agreement, between market participants with whom they do business. Further, not every risk or incident will be applicable to all customers, counterparties, members, registrants or users. As a result, Optiver would encourage the Commission to refine the proposal to require disclosure only of risks and incidents directly to market participants impacted by such risks and/or incidents. Finally, in order to maintain the integrity of these disclosures, Optiver would recommend that Covered Entities be required to maintain records of these disclosures for the current and previous calendar year.

Recommendation

Optiver generally agrees with the Commission that there is significant value in establishing a cybersecurity framework to mitigate any adverse impacts to the health and efficiency of financial markets. However, we would encourage the Commission to balance the value of public disclosure against the risks it could entail, as well as determine whether the goal of removing information asymmetry could be addressed more appropriately by a private disclosure process and a risk-based framework for identifying which information needs to be shared with relevant parties.

Optiver values the opportunity to support and provide further comment on the aforementioned proposal. Please contact Liam Smith, Head of Corporate Strategy, Optiver US LLC, at liamsmith@optiver.us should you have any questions about this letter.

Respectfully,

Alexander Itkin
Chief Technology Officer
312 821-9500
alexitkin@optiver.us