1221 Chapala Street, Office 6, Santa Barbara, CA 93101

July 20, 2020

Secretariat to the Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Submitted via E-Mail

Re: Theta Lake's Comments on the Financial Stability Board's Effective Practices for Cyber Incident Response and Recovery Consultative Document

To Whom It May Concern:

Theta Lake submits this letter in response to the Financial Stability Board's ("FSB") request for feedback on its Effective Practices for Cyber Incident Response and Recovery Consultative Document published on April 20, 2020.

Theta Lake applauds the FSB's creation of a common framework for effective cyber incident response in an effort to align protocols across the industry. As financial services activity continues to migrate to digital platforms, uniform approaches to cyber incident response will benefit firms, regulators, and investors.

We've taken a thematic approach with our comments—outlining three issues and noting where they could be incorporated into the Consultative Document. As requested by the FSB, we've paid special attention to lessons learned during the coronavirus pandemic and included those details throughout.

1. Collaboration Platform Risk

Financial services firms accelerated their transition to collaboration tools like Zoom, Microsoft Teams, and Cisco Webex to support remote working as part of COVID-19 response. The risks that collaboration platforms present for compliance, privacy, and cyber security are new and nuanced, so this first set of recommendations centers around how to manage and mitigate these risks to support incident prevention and response.

Collaboration platforms offer multiple mechanisms for interaction and sharing information. Their popularity is based, in part, on their ability to replace email and person-to-person information sharing and communications during the pandemic. Applications like Zoom and Microsoft Teams facilitate the sharing of information through video, audio, chat, white boards, and file transfers, thereby drastically improving remote communication. However, these dynamic features open up new threat vectors for intentional and unintentional data exposure. As a result, oversight of these applications should be a critical pillar of any cyber security framework.

From a regulatory compliance perspective, collaboration platforms require oversight to validate that employees are complying with business conduct rules, appropriate handling of confidential data such as PII, and investment recommendation mandates. Moreover, since employees can use collaboration tools to share sensitive information such as account details, national identification numbers, and material non-public information, as well as distribute malware links and offensive content, they pose serious privacy

and cyber security risks. We suggest updating Paragraph 9 to include policies around ongoing supervision of collaboration and other communication platforms for potential cyber security issues. A corresponding reference may be useful in Paragraph 28 to add the monitoring of communication platforms, including collaboration applications, as a component of routine oversight.

2. **Cyber Security Training**

Our second observation concerns employee cyber security training and tooling. Since phishing and social engineering attacks of escalating sophistication are being carried out to exploit employees working remotely during the COVID-19 crisis, training schemes to address these risks must be considered. In addition to passive training, tools are now available that provide interactive feedback directly to users of collaboration platforms as they take potentially risky actions like screen sharing and enabling web cams. Real time training tools built into commonly used communication systems are more effective in increasing awareness and improving employee behavior than traditional training methods. Adding references to passive and proactive training as a component of a firm's culture in Paragraph 5 would provide helpful guidance to firms grappling with the unique remote working risks of the pandemic.

3. **Preserving Legal Privilege**

Finally, with respect to forensic processes (Paragraph 16) and recording activities (Paragraph 31), we recommend adding the notion of maintaining legal privilege, where possible, when documenting incident response efforts. Particularly given recent caselaw in the US, firms should be mindful of engaging in-house and outside legal counsel to ensure that privilege is preserved when documenting key steps in the cyber security incident response process.

Theta Lake appreciates the opportunity to provide feedback to the FSB on the Consultative Document, and we look forward to having a dialogue about these issues in the near future.

Please do not hesitate to contact me with any additional questions.

Respectfully yours,

Marc Gilman

Marc Gilman
General Counsel and VP of Compliance