FSSCC

Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

Via Electronic Mail to fsb@fsb.org

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

Re: Achieving Greater Convergence in Cyber Incident Reporting – Consultative Document

The Financial Services Sector Coordinating Council (FSSCC) appreciates the opportunity to respond to the Financial Stability Board's (FSB) consultation, ***Achieving Greater Convergence in Cyber Incident Reporting*** ('Consultative Document'). Fragmented requirements and the growing complexity of the incident reporting regulatory landscape globally, create challenges for the management and reporting of cyber incidents. The FSB's efforts to converge cyber incident reporting (CIR) will help strengthen the financial sector's cyber resilience and promote financial stability.

1. Introduction

Established in 2002, the FSSCC is an industry-led, non-profit, organization that coordinates critical infrastructure and homeland security activities within the U.S. financial services industry. The FSSCC collaborates closely with the U.S. Treasury Department, the U.S. Department of Homeland Security, U.S. financial regulatory agencies and law enforcement agencies to improve our collective resilience and security posture. FSSCC members consist of trade associations, financial market utilities, and financial firms. The FSSCC partners with the public sector on policy issues to enhance the security and resiliency of the United States' financial system. The U.S. Department of Homeland Security recognizes the FSSCC as a member of the Critical Infrastructure Partnership Advisory Council on behalf of the banking and finance sector.

2. Executive Summary

The FSSCC applauds the prior work that the FSB has conducted to enhance the cyber resilience of financial institutions (FIs) cyber resilience. In 2018, the ***FSB Cyber Lexicon***[1] provided a common nomenclature for cybersecurity terminologies, including 'cyber event' and 'cyber incident.' Further, in 2020, the FSB published ***Effective Practices For Cyber Incident Response and Recovery***.[2] This report was the result of the FSB's partnership with financial institutions and helped raise the floor of financial sector preparedness for cyber incidents. In 2021, the FSB published a report on ***Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence***,[3] a critical stocktake that provided clear evidence of fragmentation and the resulting challenges. As such, we are pleased to see that this 2022 consultation contains key insights on how to address the challenges of seeking convergence in the global cyber incident reporting regulatory landscape. The continued partnership between the financial services

[1] FSB Cyber Lexicon (November 2018).
[2] FSB Effective Practices For Cyber Incident Response and Recovery (October 2020).
[3] FSB Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence (October2021)

sector and financial authorities demonstrates the value of the commitment to collaboratively develop solutions that improve resilience and supports the delivery of a safe and efficient financial marketplace.

The financial services sector is committed to strengthening its cyber resilience and understands that incident reporting is a key pillar of resilience. However, disparate reporting requirements may elongate incident response times and complicate a financial institution's ability to not only remain in compliance with its incident reporting obligations, but also to effectively respond to the incident. Incident reporting often occurs in a moment of extreme chaos and stress for financial institutions. Financial institutions must identify the source of the disruption, determine the immediate steps required to restore its business operations, and identify the financial authorities and clients (both commercial partners and consumers) that require notification. These actions collectively occur while the financial institution must identify and communicate with key internal stakeholders, work towards incident remediation, and document key decision points made throughout the incident management process. If the incident is determined to be malicious, financial institutions have the added responsibility of determining how the threat actor entered their network, the actions that occurred upon entry, the impact to the financial institutions given the threat actor's actions, when to notify law enforcement, and determining when it is safe to bring systems back online. Often, the same incident response team is managing the incident, and providing the information to numerous teams seeking to report out to the regulator to remain in compliance. However, if requirements are optimized through convergence, cyber incident reporting can:

- Serve as an early warning system to the financial services sector on significant cyber incidents;
- Identify common tactics and techniques used by threat actors, and provide insights into the vulnerabilities that threat actors may exploit to gain unauthorized access into firms;
- Streamline reporting processes for financial institutions to aid in compliance objectives; and
- Position government resources to better assist impacted private sector entities.

The FSSCC supports the FSB's work in gaining greater convergence for cyber incident reporting. To that end, the FSSCC offers several specific recommendations for consideration:

- **Align Policy Objectives with Incident Information**. Financial authorities must ensure that cyber incident reporting requirements align with clear and purposeful policy objectives to improve the incident reporting process and provide greater clarity on what information financial institutions should be sharing. Doing so will help institutions properly balance their resources between reporting and mitigating the incident.
- **Align Definitions and Key Terms.** The FSB should consider updating the FSB Cyber Lexicon's definitions to reflect more common usage of terms, including the revision of "cybersecurity incident" to connote malicious activities that cause actual harm.
- **Adopt a Common Reporting Template that is Simple and Tied to Actionable Objectives.** The FSB should encourage authorities to work together to develop and adopt a common reporting template that is customizable, but only within the limits of the template itself. Establishing a set of common data points that can be used as a standard amongst global authorities could help incident response teams streamline reporting and enable them to devote more resources to incident response.
- **Limit Scope of Incident Notification Requirements to Significant Incidents of Actual Harm.** The FSB should encourage authorities to limit cyber incident notification requirements to those that meet a materiality threshold that could impact financial stability, national security, and/or public health and safety, with the understanding that institutions are in the best position to determine their own materiality thresholds.

- **Adopt Reasonable Timelines for Reporting.** Timelines for reporting should consider that once institutions discover a possible breach, it will take financial institutions a certain amount of time to assess impact and evaluate whether the incident rises to the level of notification. Once it has been established that an incident should be reported, institutions will also need a reasonable timeframe to gather and validate the information to be reported.
- **Build Trust.** The FSB should ensure authorities incorporate trust-enhancing mechanisms—like robust liability protections—and encourage authorities to establish stronger, voluntary information sharing forums and mechanisms. Voluntary information sharing is critical to ensuring the free flow of information that is timely and actionable.
- **Facilitate Bi-Directional Information Sharing Between the Public and Private Sectors.** The FSB should encourage financial authorities and financial institutions to facilitate bi-directional information sharing, where an effective "feedback loop" ensures that incident data is aggregated, analyzed, and converted into actionable intelligence that is shared back to firms to help uplift the sector as a whole.
- **Ensure Reported Cyber Incident Data is Protected and Confidential.** To foster a trusted relationship between the public and private sectors, the FSB should encourage financial authorities to implement secure protocols that adequately protect financial institutions' sensitive information. When aggregated, cyber incident data from across the financial sector becomes increasingly sensitive and valuable, and has the potential to turn financial authorities into a target of cyber threat actors. Further, financial institutions will be more likely to voluntarily share information with financial authorities and through information sharing mechanisms if their data is protected and anonymized.

3. Discussion

Align Policy Objectives and Incident Information

Cyber incident reporting requirements should align with clear and purposeful policy objectives to ensure that authorities receive the requisite level of detail on incidents within an appropriate timeframe, while limiting the detraction from the remediation efforts of the affected financial institution. Clear and purposeful policy objectives will improve the incident reporting process and provide greater clarity on what information institutions should provide to achieve the relevant objectives. Further, this clarity may assist with minimizing the instances of financial institutions under- or over-reporting their cyber incidents in contravention of stated policy objectives.

As an example, the FSB consultation's top incident reporting objective is, '*To support management of the impacts arising from an incident at one or more institutions.*[4] In order to do so, authorities would need early warning from institutions. As part of cyber incident reporting, the FSSCC recommends distinguishing the initial phase of providing an early warning as "incident notification". Incident notification enables financial institutions to signal that they are experiencing an incident of a significant threshold that could impact economic stability, threaten public health and safety, or national security. Since "notification" would be done on a shorter timeline, the information provided to authorities would necessarily be limited to the information on hand with the understanding that information in early stages of an incident is fluid and variable. As an incident unfolds and more information becomes available, the FSSCC supports the FSB's suggestion of implementing incremental reporting in a phased

[4] FSB *Achieving Greater Convergence in Cyber Incident Reporting – Consultative Document*, page 35 (October 2022).

manner for institutions to report on any significant, new changes up until incident resolution. The FSSCC cautions against authorities mandating systematic updates (e.g., every 30 minutes or every 10 days), as these types of requirements focus institutions on compliance and reporting and detract from incident mitigation activities.

Align Definitions and Key Terms

The FSSCC appreciates the FSB's support on efforts to deepen convergence amongst global authorities and agrees that a key element in achieving convergence is to identify a common lexicon. The FSB Cyber Lexicon can create cross-sector understanding of relevant cybersecurity terminology, limit confusion when discussing cybersecurity topics, and be leveraged to develop new regulations. As such, the FSSCC encourages the FSB to consider the following changes for its Cyber Lexicon.

Cyber Incident: The FSSCC agrees with the decision to remove "jeopardizes" from the definition of cyber incident to limit the scope to incidents that cause "actual" harm. When combined with materiality thresholds, this ensures financial institutions will report on significant incidents and prevent inundating financial authorities with information of limited value. The updated definition of cyber incident will also balance the effort of key financial institution resources between reporting and remediating incidents. Consistent with this definition change, the FSSCC does not support Recommendation 8[5] which extends the cyber incident definition to include 'likely' breaches. Financial institutions observe malicious attempts and probing on their networks, but reporting on those types of activities would be to report on innumerable actions daily and would serve little purpose for authorities. Instead, this type of information should be shared voluntarily in forums such as an Information Sharing and Analysis Center (ISAC), to alert other financial institutions of potential threats. The FSSCC observes that information sharing forums around the world could be strengthened, and encourages that countries seek to build or enhance these mechanisms.

The FSSCC also recommends further revisions aimed at strengthening the cyber incident definition. First, the FSSCC recommends removing point (ii) from the cyber incident definition. While violations of security policies, security procedures, or acceptable use policies may weaken the security posture (e.g., overdue security patches, weak passwords) and lead to a cyber incident, the presence of these violations by themselves are not incidents. Second, the FSSCC recommends excluding non-malicious incidents from the definition of cyber incident, specifically by deleting "or not" after the language "whether resulting from malicious activity." While FSSCC acknowledges that the definition of cyber/cybersecurity in its purest and original form does not necessarily connote "malicious," the common usage of the term has evolved, and is generally consistent with how institutions today view "cybersecurity" and have organized internal teams to meet malicious threats. Considering these two elements for the cyber incident definition creates a more precise definition and further enhances the changes recommended by the FSB.

Operational Incident: The FSSCC proposes that the FSB should add a definition for *operational incident* to its Cyber Lexicon to explicitly differentiate between a cyber incident and an operational incident. Operational incidents, such as those incidents created by technology failures (e.g., faulty hardware), production incidents (e.g., failed change management), or human error, have the potential to meet

[5] FSB *Achieving Greater Convergence in Cyber Incident Reporting – Consultative Document*, page 16 (October 2022).

defined incident reporting thresholds and warrant reporting to financial authorities. However, the FSSCC encourages the FSB to distinguish a cyber incident as an incident driven by malicious intent because the criticality for early warning of a malicious cyber incident has a different sense of urgency and action than a non-malicious operational disruption. Operational—or non-malicious—incidents also generally have different incident management policies, procedures, personnel, and reporting objectives.

The FSSCC proposes the following definition for *operational incident*:

- *Operational Incident*: An event caused by a non-malicious failure that is not part of the expected business outcome and adversely affects an information system or the information the system processes, stores, or transmits.

Cyber Event: The FSSCC recommends modifying the cyber event definition to include "network." This change will align the definition of cyber event with the NIST Cybersecurity Framework, strengthening its current alignment with NIST. The FSSCC proposes using the following definition, "*Any observable occurrence in an information system or network. Cyber events sometimes provide indication that a cyber incident is occurring.*"

Insider Threat: Further, the FSSCC proposes the following change to the insider threat definition to read, "*the threat that an individual or group, provided with authorized access to a financial institution's systems or network, will use this access, maliciously or unintendedly, to do harm to the organization's mission, reputation, capabilities, resources, personnel, facilities, information, equipment, networks, or systems*."

Third Party and *Outsourcing:* As financial institutions continue to expand their use of third-party relationships and financial authorities increase focus on the resilience of individual firms and the financial sector, there is a need to include *third party* and *outsourcing* in the Cyber Lexicon. The FSSCC recommends aligning to existing third party and outsourcing definitions per our suggestions below:

- *Third party*: Any business relationship or contract between an entity and an organization to provide a product or service.
- *Outsourcing*: Whereby a third party provides a business function, service, product, or process that would otherwise be reasonably provided by the entity itself.

Adopt a Common Reporting Template that is Simple and Tied to Actionable Objectives

The FSSCC generally supports the concept of the Format for Incident Reporting Exchange (FIRE) framework with the goal of standardizing information requirements for cyber incident reporting across jurisdictions. As mentioned in the consultation, financial institutions comply with a multitude of reporting requirements that establish key definitions, timelines, and reporting thresholds, as well as oversight and enforcement mechanisms, which may include fines and other penalties. The FSSCC recognizes the need for FIRE, or any other common cyber incident reporting template, to be customizable, given the fact that financial authorities require different data points to satisfy their individual objectives. However, the FSSCC recommends setting the common data points that would be standard across all cyber incident reporting forms (e.g., description of incident, impact, contact information), and limit variability amongst authorities that go outside of what would be articulated within FIRE. Identifying a boundary for what can be customized will help limit time spent on tailored reporting by financial institutions' incident response teams and create a more streamlined approach to cyber incident reporting.

As mentioned above, the FSSCC recommends separating the concept of *incident notification* from *cyber incident reporting*. Incident notification serves as an "early-warning" alert for financial authorities that a materially impactful incident may be occurring, and therefore, the information reported will be limited and potentially fluid and variable. Whereas cyber incident reporting occurs after an initial notification and aligns with what the FSB terms as "intermediate reporting" when more details about the incident may be available.

Limit Scope of Incident Notification Requirements to Significant Incidents of Actual Harm

The FSSCC recommends that the FSB advise that incident notification requirements be limited to notifying authorities to incidents of a material threshold tied to impacts that could threaten economic stability, national security, and public health and safety. This ensures that these incidents are reported in a timely manner to authorities and material incidents are not lost in the overreporting of incidents that are not actionable. We would also stress that institutions should be able to set their own materiality thresholds for the practical reason that they are best placed to understand how an incident could potentially impact their clients, business, supply chain, and the broader ecosystem.

Cyber incidents that hold no imminent threat or material impact should be shared voluntarily. The FSSCC underscores the importance of ensuring that this type of information is shared voluntarily as a means to build trust in the ecosystem. It also ensures that institutions are mindful of sharing valuable information as opposed to flooding the system with common vulnerabilities or innocuous threats.

Adopt Reasonable Timelines for Reporting

The FSSCC encourages the FSB to help authorities converge around reasonable timelines for reporting. The FSB's consultation accurately lays out the nuances of timelines and the areas that need to be clarified to prevent confusion (e.g., establishing the correct triggers, reporting windows, update cadence, incident closure). As the FSB lays out in Figure 1[6], timelines for reporting vary from "without undue delay" to anywhere between 2 and 72 hours, which separately creates disparate reporting update cadences. For financial institutions that operate in multiple jurisdictions, it is nearly impossible to keep up with each reporting deadline.

The FSSCC emphasizes its previous recommendation to allow for "incident notification" to streamline reporting requirements and ensure that institutions provide an early warning of a confirmed significant incident with the limited information available, while allowing intermediate reporting to be more fluid and ad hoc. The FSSCC notes that once a potential incident is discovered, it may take some time for financial institutions to determine impact and decide that an incident must be reported. For example, a financial institution may not know immediately if a service is disrupted due to a cyber incident (malicious intent) or an operational incident (non-malicious intent). Therefore, there should be flexibility built into timelines to allow for a financial institution to conduct the proper due diligence within a reasonable amount of time. Once it has been established that an incident requires regulatory notification, FSSCC recommends that FSB encourages authorities to converge around a timeframe between 36 and 72 hours, but if and only if rules make allowances for the fact that institutions may

[6] FSB *Achieving Greater Convergence in Cyber Incident Reporting – Consultative Document*, page 5 (October 2022).

need time up front to determine whether an incident must be reported. In short, timelines should avoid injecting additional complexity at a time when affected entities are focused on remediating an incident.

Build Trust

Fundamental to robust incident reporting and information sharing is the element of trust. Without trust, information flow is stilted and guarded. The FSSCC encourages authorities to build out mechanisms to strengthen trust. As an example, to share information freely, financial institutions must not be subjected to retribution or additional penalties. In addition, there should be strong liability protections in place when sharing information to limit the threat of double victimizing the breached party through onerous fines and penalties. Should authorities seek to enhance situational awareness, FSSCC encourages that they seek to build stronger relationships and more informal dialogue with the financial institutions that operate within their borders and encourage voluntary and ad hoc information sharing. When it comes to cybersecurity, both financial authorities' and financial institutions' goals are largely aligned. Given our this alignment, it is important that the teams conducting incident management and incident reporting are able to operate fluidly together. A more streamlined reporting framework assists financial institutions with this goal. Further, the ability to build trust is grounded in financial authorities' and financial institutions' ability to avoid punitive actions, inflexible reporting requirements, and actions that further victimize the financial institution. Trust can also be enhanced by financial authorities sharing common lessons learned from incident reporting to back to financial institutions.

Further, authorities should encourage their private sector to either utilize or develop information sharing forums like an FS-ISAC[7] or an Analysis and Resilience Center For Systemic Risk.[8] These forums are examples of vehicles that facilitate voluntary information sharing between financial institutions and are critical in providing insights to the threat landscape impacting the financial services sector as a whole.

Facilitate Bi-Directional Information Sharing Between the Public and Private Sectors

Financial authorities are well positioned to: 1) observe when disruption is occurring across multiple financial institutions and critical third parties, 2) understand the potential impact of cyber incidents on the sector, and 3) communicate cross-sector incident impacts to the financial institution and relevant parties. As such, the FSSCC urges the FSB to encourage bi-directional information sharing between the public and private sectors. The FSB should ensure there is an effective "feedback loop" where information reported to authorities is aggregated, analyzed, and converted into actionable intelligence that is shared with industry to foster near real-time mitigation of future cyber incidents. When authorities share this actionable intelligence with industry, it should be anonymized to avoid identification of the victim firm and done in coordination with the victim firm where possible. This will help foster a trusted relationship between the public and private sectors and bolster cyber threat situational awareness within the financial sector.

Ensure Reported Cyber Incident Data is Protected and Confidential

[7] More information on FS-ISAC can be found at: https://www.fsisac.com/

[8] More information on Analysis and Resilience Center For Systemic Risk can be found at: https://systemicrisk.org/

The FSSCC agrees with Recommendation 16[9] that financial authorities should ensure the protection of sensitive information. Cyber incident data, especially when aggregated by financial authorities, is highly sensitive and valuable, and has the potential to turn financial authorities into a high value target by malicious actors. Financial authorities must ensure that protected and confidential cyber incident information sharing is consistent with industry standards and best practices. Additionally, the FSSCC notes that a financial institution experiencing a material cyber incident may not be able to access a secure portal to share information with financial authorities, and therefore, alternative communication mechanisms should be considered.

The FSSCC urges the FSB to use the following industry standards and best practices to provide guidance to financial authorities:

- ➢ As a result of several U.S. data breaches pre- and post-SolarWinds, SIFMA developed its *Data Protection Principles*[10] that recommend, at a minimum, the following controls:
  - Data Collection: Limit the collection of sensitive data to that which is directly relevant and necessary to accomplish a specified purpose
  - Data Usage: Implement preventative and detective controls limiting access to sensitive data to authorized users
  - Data Sharing: Implement policies to protect information shared with external entities
  - Data Disposal: Securely eradicate, dispose, or destroy sensitive data when appropriate

- ➢ The U.S. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) also requires that the controls for confidentiality and protected sharing of data be implemented:
  - *"Data/Information contained within cyber incident reporting:*
    - *may be disseminated in a manner that protects personal information from unauthorized use/disclosure*
    - *submitted to the Agency shall be collected, stored and protected in accordance with federal government standards*
    - *may not be disseminated through public information requests, etc.*
    - *shall be considered the commercial, financial and propriety information of the submitting entity"*

On behalf of the FSSCC, thank you for your consideration of these recommendations and for your leadership on cyber incident notification and reporting. The FSSCC and its members are eager to collaborate with the FSB to deepen convergence of incident notification and reporting requirements among authorities, ultimately strengthening the financial sector's cyber resilience.

Sincerely,

Ron Green
Chief Security Officer, Mastercard
Chair, Financial Services Sector Coordinating Council (FSSCC)

[9] FSB *Achieving Greater Convergence in Cyber Incident Reporting – Consultative Document*, page 21 (October 2022).

[10] SIFMA *Data Protection Principles* (March 2021).