Google Cloud

December 30, 2022

Submitted via Email: fsb@fsb.org

The Financial Stability Board
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Re: CIR Convergence

Google Cloud welcomes the opportunity to provide comments on the Financial Stability Board's (FSB) consultative document entitled "Achieving Greater Convergence in Cyber Incident Reporting" (hereinafter "the Consultation"). We applaud the FSB's ongoing efforts to achieve greater global convergence in cyber incident reporting and view the consultation and its accompanying recommendations as a favorable step in that direction. We offer the following comments and feedback to help advance the FSB's important work.

I. Introduction

Effective incident response is critical for the financial services industry and the regulators tasked with oversight of this sector. To this end, achieving greater global convergence regarding related notification and reporting requirements is critical in ensuring that industry actors have clarity and certainty regarding regulatory expectations so that all public and private sector stakeholders can focus on the primary objective of detecting, preventing, and mitigating actual cyber incident risks.

As a provider of cloud services to the financial services industry, Google Cloud maintains a rigorous process for identifying, mitigating, and in the event one occurs, managing data incidents as part of our overall security and privacy program. We believe strongly in supporting the establishment of effective and consistent global regulatory frameworks governing incident response. The Consultation and ongoing work of the FSB are important efforts in this regard.

We offer below some responses to the questions presented by the Consultation and feedback on the related recommendations. Three high level principles inform our comments:

1. An important aspect of an effective incident response process is ensuring that true positives/material incidents are promptly flagged to affected customers (and subsequently regulators) and that these are not drowned out by false positives/non-material incidents. This helps service providers, financial institutions ("FIs"), and, ultimately, regulators focus

on the incidents that matter and not expend resources on false or de minimis matters. To this end, some amount of reasonable investigation is usually required to distinguish true positives/material incidents from false positives/non-material incidents.

2. Voluntary fora for information sharing about threats/incidents are important and should be considered—instead of expanded incident notification requirements—for purposes of raising general industry awareness and sensitivity. Flagging data incidents in this manner is more impactful as it enables industry peers to proactively be on alert and take appropriate steps to mitigate against similar threats.

3. While regulatory clarity is essential for FIs, it is important that the FSB and individual regulators also account for the role of service providers with respect to cyber incident notifications and distinctions that may need to be drawn when establishing regulatory expectations relevant to such providers. Our comments below reference examples of regulators recognizing these distinctions and providing helpful clarity to such providers.

II. Responses to Questions & Recommendations Presented

A. Challenges to satisfying core regulatory objectives and achieving greater convergence (Questions concerning sections 2-4)

As a threshold matter, we appreciate and agree with the FSB's documentation of the current fragmented state of reporting requirements across regulators and global jurisdictions. Indeed, in our experience, divergent reporting requirements exist even across regulators within national borders. Moreover, while the FSB focuses only on reporting requirements emanating from financial services regulators, the fact is that many firms (both FIs and providers) are also subject to broader horizontal regulations that impose incident response notification and reporting requirements. We underscore here that the lack of convergence requires industry actors—FIs and service providers—to spend crucial time and resources navigating regulatory reporting distinctions at the expense of focusing on the primary objective: detecting, preventing, and mitigating cyber incident risks.

While the Consultation takes helpful steps to increase convergence across jurisdictions, we note at the outset that the FSB could more directly recommend that regulators avoid establishing overbroad reporting triggers. The FSB could recommend, for example, that regulators focus reporting obligations on cyber incidents that cause actual material harm or that are reasonably likely to result in actual material harm. To this end, we would suggest adding the term "reasonably" before "likely" in Recommendation 8 in order to provide a well-known standard that would also be consistent with recent notification regulations adopted by regulators, including in the U.S.[1]

[1] Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Company, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* (Apr. 1, 2022),

Additionally, the fact that a trigger lacking a materiality element might be offered in conjunction with reduced initial reporting requirements does not solve for the extra process and diversion of resources such a trigger induces. We suggest that the FSB should underscore this point explicitly in Recommendation 4. Triggers that lack a materiality standard result in costly overreporting that distracts all stakeholders from detecting and preventing cyber incidents that cause actual harm. Such regulatory reporting standards should therefore be disfavored.

Based on this recommendation, we commend the FSB for proposing an amendment to the definition of "Cyber Incident." More specifically, the amended definition would now require a cyber event that "adversely affects the cyber security of an information system or the information the system processes, stores or transmits" rather than an event that merely "jeopardizes" such system security or information. Importantly, as the FSB notes, this change confirms that "potential incidents are not in scope of this definition."

We further suggest, however, that the FSB consider striking the second element used to define a cyber incident, which currently includes an event that "violates the security policies, security procedures or acceptable use policies . . ." It is difficult to conceive of a violation of a policy or procedure having the kind of material impact that should result in requiring notification unless it first has some impact on customer data or on information systems. In this way, the first element of the definition captures the primary objective of a notification regime and renders the second element both redundant and overbroad. This will accordingly expand the volume of notifications, without clear benefit. The requirement to report occurrences that result or are reasonably likely to result in actual harm to data/systems should capture all material incidents.

In addition to supporting convergence around the inclusion of a materiality trigger for reporting requirements, we further support the use of regulatory guidance to help industry stakeholders understand what types of events and scenarios a regulator would deem to be material. To this end, we commend the FSB's reference of the Hong Kong Monetary Authority's (HKMA) incident reporting guidelines as an example of best practice. As the FSB notes, the HKMA offers industry stakeholders a list of examples of incidents that the regulator either would or would not deem to require reporting. The use of such examples or similar guidance by global regulators would help ensure industry compliance, reduce rates of over-reporting and under-reporting, and drive convergence amongst regulators who are able to incorporate each other's guidance.

Indeed, such convergence could be further facilitated through the creation of global voluntary fora for information sharing about threats/incidents, raising general industry awareness and sensitivity,

---

available at https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf; *see also* 23 CRR-NY 500.17(a) (setting a "reasonably likely" standard).

and sharing examples and guidance to harmonize regulatory reporting expectations. This would be consistent with the FSB's Recommendations 12, 13 and 15.

B. Increase Regulatory Certainty and Convergence for Bank Service Providers (Question 1)

As noted above, we commend the FSB for its comprehensive survey of cyber incident reporting requirements as they relate to FIs. We further suggest, however, that the FSB similarly focus its convergence efforts on service providers in order to ensure consistent treatment of such stakeholders, particularly with respect to materiality triggers and reporting timeline expectations.

In the United States, the federal banking agencies recently issued new cyber incident reporting requirements based on the above principles in order to create consistency between the regulators and certainty regarding notification expectations. We commend the final rules for the clarity they provide specifically to service providers regarding notification expectations, including with respect to timeliness and materiality. We encourage the FSB to showcase the U.S. banking regulators' approach as a best practice and one that can advance regulatory convergence for all involved stakeholders.

More specifically, with respect to timeliness, the U.S. banking regulators determined "that a bank service provider must notify affected banking organization customers 'as soon as possible' when it 'determines' it has experienced an incident that meets the standard in the rule. Use of the term 'determined' allows the service provider time to examine the nature of the incident and assess the materiality of the disruption or degradation of covered services."[2] Importantly, the final rules applied the same materiality triggers to the service provider as to the FI, which will drive consistent understanding of cyber incident risk and consistent reporting.

We encourage the FSB to highlight best practices as have emerged in the U.S. and to encourage global regulatory convergence on notification expectations for service providers. With such clarity, service providers and FIs will then be in a position via contracting to ensure proper communication between the companies, shared understanding of regulatory expectations, and efficient cyber incident notification processes.

C. Support standardized notification forms and formats (FIRE) (Questions 9, 11)

We are supportive of the FSB's exploration of standardized notification forms and data formats. We believe that the format for incident reporting exchange (FIRE) initiative could help drive global regulatory convergence, yield cleaner and more actionable cyber incident data, and increase reporting efficiency.

---

[2] Cite.

We note, however, that as the FSB pursues this initiative, it is critical to include the perspective of service providers that will have contractual notification provisions with the FIs. It will be important to ensure that the information, formats, and fields of such standardized notifications are consistent with the capabilities and reporting practices of service providers that will be responsible, in many instances, for providing initial notifications to FI customers. We look forward to serving as a resource to the FSB as it pursues this important workstream.

III. Conclusion

We appreciate the opportunity to provide our views on this important issue of incident response reporting. We have a shared interest in making sure that incidents are managed properly and any risks resulting from incidents are appropriately mitigated. The FSB's long-standing efforts to drive convergence in regulatory requirements in this space, with an eye to increasing the effectiveness of the regulations, are deeply welcomed and we stand ready to work with the FSB and other industry stakeholders to carry these efforts forward.

Sincerely,

Behnaz L. Kibria
Senior Policy Counsel