April 12, 2021

Chief Counsel's Office
Attn: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E-218
Washington, DC 20219

The Honorable Ann E. Misback
Secretary, Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

The Honorable James P. Sheesly
Assistant Executive Secretary
Attn: Comments
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Re: ***Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*** *(**OCC:** Docket ID OCC-2020-0038, RIN 1557-AF02; **Federal Reserve System:** Docket No. R-1736, RIN 7100-AF; **FDIC:** RIN 3064-AF59)*

Google Cloud welcomes the opportunity to provide comments on the proposed rulemaking entitled "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers." (26 Fed. Reg. 2299) (January 12, 2021) ("Incident Notification Requirements") issued jointly by the Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and Board of Governors of the FederalReserve System (collectively referred to herein as the "Banking Regulators").

I. Introduction

Effective incident response is critical for the financial services industry. As a provider of cloud services to the financial services industry, Google Cloud maintains a rigorous process for preventing and managing data incidents as part of our overall security and privacy program. We also believe

strongly in supporting the establishment of effective regulatory frameworks governing incident response. The Incident Notification Requirements proposed by the Banking Regulators are an important initiative in that regard.

We offer below some responses to the questions presented by the Banking Regulators regarding the proposed Incident Notification Requirements and the state of play on incident response in the industry. A number of high level principles inform our responses:

1. An important aspect of an effective incident response process is ensuring that true positives/material incidents are flagged to affected customers and that these are not drowned out by false positives/non-material incidents. This helps bank service providers, banking organizations, and, ultimately, regulators focus on the incidents that matter and not expend resources on false or *de minimis* matters.

2. Some amount of reasonable investigation is usually required to distinguish true positives/material incidents from false positives/non-material incidents.

3. Voluntary fora for information sharing about threats/incidents are important and should be considered, instead of incident notification, for purposes of raising general industry awareness and sensitivity.

Google Cloud offers below a number of suggestions to shape the Incident Notification Requirements in line with these principles.

II. Responses to Questions Presented

1. How should the definition of "computer-security incident" be modified, if at all? For example, should it include only occurrences that result in actual harm to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits? Should it include only occurrences that constitute an actual violation of security policies, security procedures, or acceptable use policies?

The proposed Incident Notification Requirements define "computer-security incident" as "an occurrence that: (1) results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits; or (2) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." Under the proposed Incident Notification Requirements, a banking organization receiving notifications of "computer-security incidents" from a bank service provider

must determine whether the incident rises to the level of a "notification incident" and, if it does, must report the incident to the organization's primary Banking Regulator.[1]

A number of elements make the definition of "computer-securityincident" in the Incident Notification Requirements extremely broad and could result in frequent and voluminous reporting by bank service providers. Specifically, the Incident Notification Requirements:

- Encompass not only those occurrences that have any actual harm, but also any occurrences that have the *potential* to cause harm to information or information systems; and

- Encompass *violations* as well as *imminent threat of violations* of *security policies, security procedures or acceptable use policies*.

Google Cloud appreciates that this definition of "computer-security incident" needs to be read in the context of the additional language in the Incident Notification Requirements specifying that the banking service provider need notify the customer only of any "computer-security incident that it believes in good faith could disrupt, degrade, or impair services . . . for four or more hours." While the four-hour language may have been included in an effort to add a materiality element to the rule and, thus, constrain the scope of notifications that would need to be made, it is not clear that the language will in fact have that effect.

Importantly, the definition of computer-security incident relates to occurrences that have actual or potential impacts on *data*, *systems*, or *security policies*, *security procedures*, or *acceptable use policies*. However, the four-hour language relates to disruption, degradation, or impairment of *services*. The mismatch in scope of the two sets of provisions makes it difficultto understand which incidents would in fact need to be notified to customers.

The breadth of the categories included in the definition of "computer security incident" and the lack of an effective materiality requirement will likely result in an extensive volume of notifications being generated from bank services providers to bank customers, which could have significant unintended consequences.

Bank service providers' attention and resources would be focused on providing notifications that often will not be material, considering the kinds of "notification events" that are ultimately of concern to the Banking Regulators, rather than on determining impact and designing remediations. Moreover, bank customers will be put in the position of having to sort through large volumes of notifications from (likely numerous) bank service providers to make determinations of whether they

[1] A "notification incident" is defined as an incident that the organization believes in good faith could materially disrupt, degrade, or impair— (1) The ability of the banking organization to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; (2) Any business line of a banking organization, including associated operations, services, functions and support, and would result in a material loss of revenue, profit, or franchise value; or (3) Those operations of a Banking organization, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States."

rise to the level of a "notification incident," resulting in increasing compliance burdens on the bank service providers and a growing prospect that true notification incidents will be lost in the haystack.

To avoid these kinds of unintended consequences and to better tailor the Incident Notification Requirements to address the concerns identified, Google Cloud urges the Banking Regulators to consider a few modifications:

- Include only occurrences that result in actual harm. Occurrences that only have the potential to cause harm should be excluded from the scope of notifications required from the bank service providers, although the providers should continue to monitor these events. The fact that an event has not resulted in actual data/systems compromise is evidence that the bank service providers' controls are operating as intended and that escalation to the Banking Regulators is unnecessary. Making these occurrences reportable would significantly increase the operational burden on all involved parties, including banking customers (who would be receiving excessive volumes of non-actionable information), without a clear benefit.

  Nonetheless. financial institutions and their providers should continue information sharing and exchanging best practices, including with respect to unsuccessful incidents as well as aggregated post-mortems on addressed attacks. The Banking Regulators should facilitate such exchange through relevant voluntary fora.

- Eliminate the separate reporting category for security policies, security procedures, and acceptable use policies: It is difficult to conceive of a "violation or imminent threat of violation of security policies, security procedures, or acceptable use policies" having the kind of material impacts that could result in a "notification event" unless they first have some impact on customer data or on information systems. This is particularly true of "acceptable use policies" that often include requirements entirely unrelated to security. Including "security policies, security procedures, or acceptable use policies" as an additional reporting category expands the scope of reportable "computer-security incidents," and hence the volume of notifications, without clear benefit. The requirement to report occurrences that result in harm to data/systems should capture all material incidents.

- Establish Materiality Requirements Specific to Each Type of Reportable Occurrence: The provision clarifying that the banking service provider need notify the customer only of any "computer-security incident that it believes in good faith could disrupt, degrade, or impair services . . . for four or more hours" is helpful in establishing a "materiality" boundary for some cases -- specifically, those in which the primary impact of an occurrence is on the *availability* of information or an information system. In the case of occurrences that impact the confidentiality or integrity of information or the information system, however, the four hour provision may not serve as an effective measure of materiality. Consider, for example, a hypothetical breach that results in significant data exfiltration but not in any cognizable impact on the availability of the service being provided.

Google Cloud urges the Banking Regulators to consider developing alternative materiality criteria for these situations. These criteria should take into account the different types of bank service providers and, crucially, what information will and will not be available to them when making the assessment. For example, for privacy reasons, a cloud service provider supplying infrastructure-as-a-service to a banking organization may have little visibility into the impact that an incident will have on the banking organization. In that situation, shaping the materiality criteria in terms of the impact on the banking organization would be ineffective and, again, likely to lead to over-reporting. Rather, to the greatest extent possible, materiality should be based on agnostic criteria that can be applied even by third parties in such a situation -- for example, enumerating the specific kinds of harms that are encompassed by the provision (e.g., "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, data").

We believe these modifications could help achieve a better balance between the scope of reporting (and, in particular, the critical shared interest in avoiding over-reporting) and ensuring that critical and material incident information is getting to banking organizations and to regulators.

2. ***How should the 36-hour timeframe for notification be modified, if at all, and why? Should it be made shorter or longer? Should it start at a different time? Should the timeframe be modified for certain types of notificationincidents or banking organizations (for example, should banks with total assets of less than $10 billion have a different timeframe)?***

Although the 36-hour timeframe applies to notifications by banking organizations of "notification incidents" to their primary Banking Regulator, not notifications of "computer security incidents" by bank service providers to their bank customers, Google Cloud appreciates the recognition by the Banking Regulators that a banking organization is unlikely to "be able to determine that a notification incident has occurred immediately upon becoming aware of a computer security incident." The Banking Regulators note that "a banking organization would take a reasonable amount of time to determine that it has experienced a notification incident" and that "only once the banking organization has made such a determination would the requirement to report within 36 hours begin."

Ensuring that the Notification Requirements allow an opportunity for reasonable investigation is important to helping ensure that material incidents are flagged to the regulators and are not obfuscated by an influx of false positives or non-material matters. Google Cloud urges the Banking Regulators to also apply the same rationale to the notification requirements that apply to the notification of "computer-security incidents" by bank service providers to their banking customers and to ensure that sufficient time for investigation is built into that requirement. See response to Questions 3 and 6 below.

3. ***Is the proposed requirement that banking organizations and bank service providers notify the appropriate party when they "believe in good faith" that they are experiencing or have experienced a notification incident or computer-security incident, as applicable, sufficiently clear such that banking organizations and bank service***

providers understand when they should provide notice? How should the "believes in good faith" standard be modified, if at all? Forexample, should the standard be "reasonably believes" for either banking organizations or bank service providers?

The proposed Incident Notification Requirements specify that a bank service provider notify an affected banking organization customer "immediately after the bank service provider experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided . . . for four or more hours." Google Cloud supports the use of the term "believes in good faith" to modify the notification requirement in this context.

One of the very first steps in Google Cloud's incident response is conducting, as quickly as possibly, a triage assessment of the incident and assessing its severity (which may be adjusted as more information is known). Google Cloud's customer notifications are tied to its best efforts assessments of these issues based on the information available to it. The nature of the "good faith" standard is such that it recognizes that, often, the information upon which assessments are made is changing and incomplete (especially at early stages of incident response) and that an assessment of sufficiency needs to take this context into account.

By contrast, a "reasonably believes" standard could introduce too much uncertainty and invite second-guessing of decisions that are, by necessity, made quickly and potentially without key facts that are only known later, incentivizing prophylactic over-reporting that will not benefit bank service providers, their banking organization customers, or the Banking Regulators.

As discussed below in response to Question 6, however, the structure of the sentence, and in particular the phrase "immediately after the bank service provider experiences a computer-security incident" introduce uncertainty as to the exact timeframe that is applicable to the notification provided by the bank service provider. For the reasons discussed in that response, Google Cloud urges the Banking Regulators to consider using language other than "immediately after." Google Cloud urges the Banking Regulators to consider using, instead, language that is more in line with the notion that bank service providers need to be able to make a good faith assessment of impact following an occurrence and that, in many cases, the information may not be available to make such an assessment "immediately" after an occurrence.

4. ***Do existing contracts between banking organizations and bank service providers already have provisions that would allow banking organizations to meet the proposed notification incident requirements?***

The proposed notification incident requirements do not align entirely with existing approaches, in particular when it comes to events impacting confidentiality/integrity (as opposed to availability). Therefore provisions in existing contracts are unlikely to fully address the proposed requirements.

For instance:

- for the reasons noted in the response to Question 1 above, in our experience providers do not in practice notify customers of potential harm, violations of security policies etc that do not result in any harm or violations of security policies etc. In particular, given the usual content of acceptable use policies, it is not typical to notify a customer of an acceptable use policy violation by another customer absent any harm to the customer being notified.

- for the reasons noted in the response to Question 6 below, in our experience providers are typically not able to notify customers immediately after an event that impacts the confidentiality/integrity of information of informationsystems. Typically, providers will commit to doing this promptly or without undue delay after an incident has been investigated and declared.

Although contracts vary, our experience is that providers do, however, provide notification of events that actually impact the availability of information and information systems. Again, although this is done promptly, it is usually not possible to do so "immediately" given the need for reasonable investigation (as recognized by the Banking Regulators in connection with the "notification incident" timelines -- see Question 2 above).

Finally, our experience is that multi-tenant contexts, like public cloud services contracts, typically utilize one-to-many tools such as dashboards to communicate service availability events and scalable 1:1 tools such as emails/support tickets to communicate events impacting customer data.

5. ***Should the proposed rule for bank service providers require bank service providers to notify all banking organization customers or only those affected by a computer-security incident under the proposed rule?***

Google Cloud urges the Banking Regulators to limit the scope of the notification requirement to banking organization customers affected by a computer-security incident. Expansion to include all banking organization customers could (1) generate significant confusion about the scope and impact of an incident, potentially consuming bank organization resources unnecessarily; (2) draw bank service provider resources away from critical incident identification, coordination, and resolution activities; and (3) result in significantly more noise/false positives being reported to banking regulators.

If the intent behind notifying a broader group were to facilitate information sharing, there may be better ways to do so that would not have the negative impacts described above. For example, the broader group of financial institutions, providers and Banking Regulators could continue information sharing and exchanging best practices through relevant voluntary fora.

6. ***Within what timeframe should bank service providers provide notification to banking organizations? Is immediate notification after experiencing a disruption in services provided to affected banking organization customers and to report to those organizations reasonable? If not, what is the appropriateamount of time for a bank service provider to determine it has experienced a material disruption in service that impacts its banking organization customers, and why?***

Under the proposed Incident Notification Requirements, a bank service provider must notify each affected banking organization customer "immediately after the bank service provider experiences a computer security incident that it believes in good faith could disrupt, degrade, or impair services . . . for four or more hours."

The term "immediately after" suggests that no time could have elapsed between when a computer-security incident occurred and when notification has to happen. However, as discussed in response to Question 3 above, there is almost always some period of time in which facts need to be gathered in order to make an informed assessment (even if preliminary) as to nature, scope, and impact of an incident. Making a determination "in good faith" that a computer-security incident "could disrupt, degrade, or impair services provided . . . for four or more hours" (or exceeds some other materiality threshold) may not be possible "immediately after" the bank service experiences a computer-security event."

As such, the use of the term "immediate" creates confusion as to the point in time at which a bank service provider needs to provide notice. It is notable in this regard, that both this question (about the effect of the "immediately after" language) and Question 3 above (about the effect of the "good faith" language) both relate to the timeframes that apply to the bank service provider. The two phrases have different time connotations and it is unclear which is controlling.

To clarify the applicable timeframe, Google Cloud urges the Banking Regulators to consider alternative language that conveys that notification should occur "promptly" and "without undue delay" once a good faith determination is made as to materiality (whether the four hour standard or some other). This should convey the sense of urgency without suggesting that bank service providers submit notifications without any attempt to collect the kind of information that will help determine whether the computer-security incident is one that is material.

Importantly, as discussed in response to Question 2, the Banking Regulators recognize the importance of allowing time for reasonable investigation in the context of notifications by banking organizations of "notification incidents" to their primary Banking Regulator. Specifically, the Banking Regulators acknowledge that a banking organization is unlikely to "be able to determine that a notification incident has occurred immediately upon becoming aware of a computer security incident." The Banking Regulators note that "a banking organization would take a reasonable amount of time to determine that it has experienced a notification incident" and that "only once the banking organization has made such a determination would the requirement to report within 36 hours begin." Google Cloud urges the Banking Regulators to apply the same rationale to the notification requirements that apply to the notification of "computer-security incidents."

7. ***The agencies understand that many existing contracts between banking organizations and bank service providers contain notification provisions regarding material incidents***

and that, generally, bank service providers use automated systems to notify banking organizations of service disruptions. The agenciesare seeking information on how bank service providers currently notify banking organizations of service disruptions under existing contracts between bank service providers and banking organizations. Do those contracts contemplate the provision of noticeto at least two individuals at an affected banking organization? Is the method of noticespecified in existing contracts (for example, email, telephone, etc.) sufficient to allow bank service providers to provide notice of computer security incidents to atleast two individuals at affected banking organizations? If not, how best could therequirement for bank service providers to notify at least two individuals at affected banking organizations be achieved most efficiently and cost effectively for both parties?

Google Cloud notifies customers of data incidents by delivering notification(s) to customers electronically. Service disruptions are notified on a public dashboard (customer can enable RSS feed alerts) and, depending on severity and whether the customer has subscribed to a qualifying support level, may also be communicated directly to affected customers via a support ticket or notification email address supplied by customers.

Google Cloud urges the Banking Regulators to permit use of such electronic means to provide notification. This is critical to allow notifications at scale. To ensure that more than one individual receives the notification, banking organizations can ensure that the transmission is accessible by multiple individuals (e.g., by routing notification email addresses to an alias with more than one individual recipient, by ensuring multiple individuals enable RSS feed alerts).

8. ***Describe circumstances in which a bank service provider would become aware of a material disruption that could be a notification incident for banking organization customers but the banking organization customers would not be aware of the incident. Would it be overly burdensome to certain bank service providers, such as smaller bank service providers, to provide notice of material disruptions,degradations, or impairments to their affected banking organization customers and, if so, why?***

Banking organization customers are likely to become aware of a material disruption that has an impact on availability of data/systems early on in an incident, potentially at the same time as a bank service provider. However, this may not be true of a material disruption that has an impact primarily on confidentiality or integrity of data.

III. Conclusion

Google Cloud appreciates the opportunity to provide feedback on the proposed Incident Notification Requirements. We look forward to continuing to work with the Banking Regulators as the proposal is finalized and implemented.

Sincerely,

Behnaz L. Kibria
Senior Policy Counsel