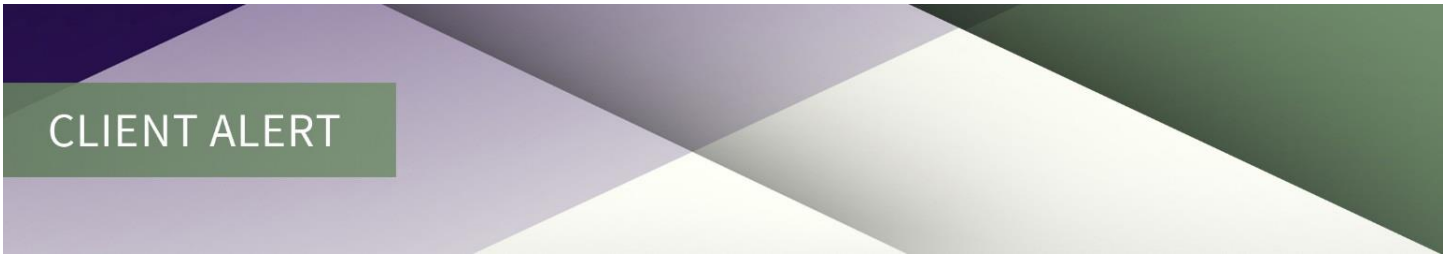

Financial Regulators Propose Breach Notification Requirements for Banks and Bank Service Providers

January 8, 2021

AUTHORS

Daniel K. Alvarez | Elizabeth Bower | Elizabeth P. Gray | Richard M. Borden
David S. Katz | Michelle Bae

On December 15, 2020, the Board of Governors of the Federal Reserve System (Board), the Office of the Comptroller of the Currency, Department of the Treasury (OCC), and the Federal Deposit Insurance Corporation (FDIC) (collectively, the "agencies") issued a proposed rule to impose new cybersecurity incident notification requirements on banking organizations and their service providers. The proposed rule would formalize incident notification requirements for many financial institutions and their federal regulators and set a new bar – 36 hours from discovery – for how quickly incidents must be reported.

Background

Currently, when a banking organization becomes aware of an incident involving unauthorized access to or use of sensitive customer information, it is generally expected to notify the primary federal regulator "as soon as possible" through the filing of Suspicious Activity Reports. The Gramm-Leach-Bliley Act notification standard sets forth similar timing requirements with respect to unauthorized access to or use of sensitive customer information.

For banking organizations, the proposed rule expands the scope of incidents that require notification and expedites the notification timing to no later than 36 hours of a determination of a notification incident. The proposed rule will allow the agencies to receive notification of incidents that disrupt banking organizations' operations but do not compromise

sensitive customer information. The proposed rule also modifies the notification requirements for bank service providers. Under the proposed rule, bank service providers would include both bank service companies and third-party providers under the Bank Service Company Act (BSCA).

Proposed Notification Requirements

The proposed rule establishes two separate notification requirements on banking organizations and bank service providers, as summarized below.

Notification Requirements for Banking Organizations

- *Covered Entities*. Under the proposed rule, "banking organizations" are entities as defined under each agency's regulations, which include: (1) under the OCC regulations, national banks, federal savings associations, and federal branches and agencies; (2) under the Board regulations, all U.S. bank holding companies and savings and loan holding companies, state member banks, the U.S. operations of foreign banking organizations, and Edge and agreement corporations; and (3) under the FDIC regulations, all insured state non-member banks, insured state-licensed branches of foreign banks, and state savings associations.

- *Notification Thresholds*. The proposed rule would require a banking organization to notify its primary federal regulator of any "computer-security incident" that rises to the level of a "notification incident" as soon as possible and no later than 36 hours after the organization believes in good faith that a notification incident has occurred.

A "computer-security incident" occurs if either of the below applies:

(i) An incident results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; *or*

(ii) An incident constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Further, a "notification incident" that would trigger notification requirements is a computer-security incident that a banking organization believes in good faith could *materially* disrupt, degrade, or impair:

(i) 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;

(ii) Any business line of a banking organization, including associated operations, services, functions and support, and that would result in a material loss of revenue, profit, or franchise value; *or*

(iii) 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.

The proposed rule provides additional guidance on subsidiaries of banking organizations that experience notification incidents. With respect to a banking organization that is a subsidiary of another banking organization that is subject to the notification requirements, the subsidiary must notify its primary federal regulator and its parent banking organization of the notification incident. The parent banking organization would need to make a separate assessment as to whether it also has suffered a notification incident that triggers the notification requirements under the proposed rule. With respect to a non-banking organization that is a subsidiary of a banking organization, although the non-banking subsidiary would not be subject to the notification requirements under the proposed rule regarding a notification incident it experiences, the parent banking organization must assess whether the parent needs to notify its primary federal regulator of the incident.

- *Examples of Notification Incidents.* The proposed rule provides a non-exhaustive list of events that would be considered notification incidents. Key examples include large-scale distributed denial-of-service attacks that disrupt customer account access for an extended period of time (e.g., more than four hours), and a computer hacking incident that disables banking operations for an extended period of time.

- *Notification Timing*. The proposed rule provides clarification regarding the "good faith" standard of the 36-hour requirement to notify the primary federal regulator of a notification incident. The agencies explain that they do not expect that banking organizations would generally be able to determine that a notification incident has occurred immediately upon becoming aware of a computer-security incident. Only after making a determination that the incident rises to a level of a notification incident after taking a reasonable amount of time to assess the incident would the requirement to report within 36 hours begin.

- *Content and Form of Notice*. The proposed rule emphasizes that the notification requirement is intended to provide an early alert to the primary federal regulator of a notification incident, and the notice would not need to include an assessment of the incident. The notice would not require specific information about the incident, and sharing general information about what is known at the time by banking organizations would be sufficient. As to the form of notice, it could be provided in either written or oral communication, including through any technological means (e.g., email or telephone), to a designated point of contact identified by the banking organization's primary federal regulator.

Notification Requirements for Bank Service Providers

- *Covered Entities*. The proposed rule applies to bank service providers that provide services described in the BSCA to banking organizations. The services that are subject to the BSCA include data processing, back office

services, and check and deposit sorting and posting. The bank regulatory agencies have interpreted that the services covered by Section 3 of the BSCA also include Internet banking and mobile banking services.

- *Notification Thresholds*. Bank service providers would be required to notify at least two individuals at affected banking organization customers immediately after experiencing a computer-security incident that they believe in good faith could disrupt, degrade, or impair the provision of services subject to the BSCA for four or more hours. This could possibly be a lower threshold than the "notification incident" threshold, which includes a materiality standard for banking organizations.

- *Notification Timing*. Bank service providers are required to immediately notify affected banking organizations of a computer-security incident that meets the above standard.

- *Content and Form of Notice*. When notifying at least two individuals at affected banking organization customers, bank service providers are not expected to assess whether the incident rises to the level of a notification incident for their customers. The proposed rule expects only that bank service providers would make a best effort to share general information about what is known at the time.

The proposed rule recognizes that banking organizations have become increasingly reliant on bank service providers to provide essential technology-related products and services. For example, if a bank service provider that is used by a banking organization for its core banking platform to operate business applications is experiencing widespread system outages and the recovery is undeterminable, such incident would be considered a "notification incident" under the proposed rule.

Next Steps and Takeaways

Comments to the proposed rule will be due by 90 days after its publication in the Federal Register. Banking organizations and bank service providers will need to review their internal policies and procedures, such as their incident response plans to identify "computer-security incidents" and "notification incidents," and timely notify applicable regulators or affected organizations of such incidents. Although the proposed rule considers a good faith standard in calculating the 36-hour requirement to notify the primary federal regulator, the accelerated notification timing compares with the 72-hour notification requirement for a cybersecurity event experienced by financial institutions under the New York Department of Financial Services Part 500. Additionally, bank service provider agreements will require review and possible modifications to ensure that their banking organization customers are promptly notified of certain computer-security incidents.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Elizabeth Bower
202 303 1252
ebower@willkie.com

Elizabeth P. Gray
202 303 1207
egray@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com

David S. Katz
202 303 1149
dkatz@willkie.com

Michelle Bae
202 303 1166
ebae@willkie.com