GIBSON DUNN

January 4, 2021

FEDERAL REGULATORS PROPOSE RULE REQUIRING BANKING INSTITUTIONS AND SERVICE PROVIDERS TO PROVIDE RAPID NOTIFICATION FOLLOWING SIGNIFICANT COMPUTER-SECURITY INCIDENTS

To Our Clients and Friends:

On December 18, 2020, three federal banking regulators—the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("Board"), and the Federal Deposit Insurance Corporation ("FDIC")—jointly issued a notice of proposed rulemaking that would impose rapid notification requirements on banking organizations and bank service providers following "significant" computer-security incidents.

Under the proposal, "banking organizations" include all institutions subject to a primary federal bank regulator: for the OCC, national banks, federal savings associations, and federal branches and agencies of non-U.S. banks; for the Board, 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 for the FDIC, all insured state nonmember banks, insured state-licensed branches of foreign banks, and state savings associations.

The proposal defines "bank service providers" by reference to the Bank Service Company Act ("BSCA") as entities that provide BSCA-regulated services—"check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution," including "data processing, back office services, and activities related to credit extensions."[1] With the increasing significant use of third-party vendors to supply technology-related services to banks, this inclusion is important.

The proposal would require a banking organization to notify its primary federal regulator when it believes in "good faith" that it has experienced a "significant" computer-security incident—which the proposal terms a "notification incident." Notification of regulators would be required "as soon as possible and no later than 36 hours" after the organization determines that a notification incident has occurred. The proposal defines a "computer-security incident" as "an occurrence that—(i) [r]esults 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 (ii) [c]onstitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." The proposal describes a "notification incident" as a computer-security incident that "could jeopardize the viability of the operations of an individual banking organization, result in customers being unable to access their

deposit and other accounts, or impact the stability of the financial sector."[2] Notification incidents can arise from both criminal and non-malicious computer-security incidents.

The proposal would require a bank service provider to notify "at least two individuals at affected banking organization customers immediately after experiencing a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours." The bank service provider would not be required to determine if such an incident rises to the level of a "notification incident" for particular banking organizations; rather, the bank service provider would be required to inform affected banking organization customers, who would themselves have that responsibility.

Additionally, the proposal would require a banking organization subsidiary of another banking organization to notify both its primary federal regulator and its parent banking organization that the subsidiary had experienced a notification incident "as soon as possible." The proposal would then require the subsidiary's parent banking organization to make a separate assessment about whether the parent organization had also suffered a notification incident requiring it to notify its primary federal regulator as result of the incident at the subsidiary. Thus, the proposal would require both the subsidiary and parent banking organizations to separately determine whether they had each suffered a notification incident, and should both make such a determination, would require both to notify their regulators individually.

In contrast, the proposal would not require a non-bank subsidiary of a banking organization to notify its regulator following a notification incident at the non-bank subsidiary. Instead, the proposal would seemingly require the non-bank subsidiary to notify its parent banking organization. The parent banking organization would then be required to determine whether the computer-security incident at its non-bank subsidiary constituted a notification incident, and if so, to notify the parent banking organization's primary federal regulator.

Entities that wish to comment on the proposed rule must submit their comments no later than 90 days after the proposal is published in the Federal Register.

The proposed rule is the latest attempt to impose obligations on financial institutions that have suffered a cyber incident. Regulations requiring notification following a data breach have been in place for years, but, as we have previously noted, state and federal regulators have recently begun imposing rules requiring faster and more in-depth notifications following cybersecurity incidents. For example, since 2017, the New York Department of Financial Services has required financial institutions to notify the Superintendent of Financial Services "as promptly as possible but in no event later than 72 hours" following a cybersecurity incident.[3]

These proposed and enacted regulations requiring rapid notification following cybersecurity incidents highlight the need for financial institutions to be able to respond quickly to and report accurately and effectively on cyber events. Such notification requirements will help incentivize banking organizations to assess whether they have a well-functioning incident response plan and effective lines of communication among their information security, legal, and other relevant departments already in place before a cybersecurity incident occurs. This is important for organizations to be able to quickly assess

incidents—which can often be challenging to understand fully—and be positioned to notify regulators within the required time period following an incident. Among other preparation measures, cross-departmental training exercises can help improve the functionality of response processes before they are tested in an actual cybersecurity event.

---

[1] *See* 12 U.S.C. §§ 1861-1867.

[2] The proposed rule's complete definition of "notification incident" 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 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."

[3] N.Y. Comp. Codes R. & Regs. tit. 23, § 500.17 (2020).

The following Gibson Dunn lawyers assisted in the preparation of this article: Ryan T. Bergsieker, Arthur S. Long, Alexander H. Southwell and Marie D. Zoglo.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Privacy, Cybersecurity and Consumer Protection or Financial Institutions practice groups.

Financial Institutions Group:

Matthew L. Biben – New York (+1 212-351-6300, mbiben@gibsondunn.com)
Stephanie Brooker – Washington, D.C. (+1 202-887-3502, sbrooker@gibsondunn.com)
M. Kendall Day – Washington, D.C. (+1 202-955-8220, kday@gibsondunn.com)
Arthur S. Long – New York (+1 212-351-2426, along@gibsondunn.com)

Privacy, Cybersecurity and Consumer Protection Group:

United States
Alexander H. Southwell – Co-Chair, PCCP Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)

Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen – Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)

Europe
Ahmed Baladi – Co-Chair, PCCP Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox – London (+44 (0)20 7071 4250, jacox@gibsondunn.com)
Patrick Doris – London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Bernard Grinspan – Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden – London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Alejandro Guerrero – Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic – Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen – London (+44 (0)20 7071 4203, swazen@gibsondunn.com)

Asia
Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)