Federal Banking Agencies Issue Final Rule on Computer-Security Incident Notifications

Five Things To Know

On Thursday, November 18, 2021, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (collectively, the "Agencies") issued a final rule requiring banking organizations and bank service providers to notify their primary federal regulator and affected banking organization customers, respectively, after determining that a reportable computer-security incident has occurred. These reporting requirements are intended to ensure that regulators are able to identify and take preemptive action against emerging threats to the financial system and that banking organizations receive prompt notice when a service provider experiences a computer-security incident that has caused, or is reasonably likely to cause, a material disruption to covered services.

The final rule's compliance date is May 1, 2022.

1 The final rule requires a banking organization to notify its primary federal regulator shortly after the banking organization determines that it has experienced a "computer-security incident" that is a "notification incident" – terms that cover a broad range of systems disruptions that result in actual harm and have materially disrupted or degraded operations or are reasonably likely to do so.

Under the final rule, a banking organization must file a report with its primary federal regulator as soon as possible and no later than 36 hours after determining that the banking organization has experienced a computer-security incident that rose to the level of a notification incident. The reporting requirement is triggered when the banking organization *determines* that it has experienced a computer-security incident that requires notification, not when the incident occurred. The preamble to the final rule anticipates that a banking organization will take a reasonable amount of time to determine that it has experienced a notification incident.

A computer-security incident is an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits. To rise to the level of a notification incident, a computer-security incident must have materially disrupted or degraded, or must be reasonably likely to materially disrupt or degrade, a banking organization's:

- ability 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;
- business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or
- operations, 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.

A notification incident could include an operational failure or error that does not result from a malicious breach of a banking organization's systems. The preamble to the final rule encourages banking

organizations to contact their primary federal regulator when in doubt as to whether a notification incident has occurred.

Banking organizations subject to the final rule include insured depository institutions, uninsured national banks and federal savings associations, bank holding companies, savings and loan holding companies, and the U.S. operations of foreign banks, such as U.S. branches and agencies.

---

2 A banking organization is still expected to notify law enforcement agencies of certain cyber incidents.

The final rule does not supplant other reporting regimes that may apply to computer-security incidents, such as the requirement that a banking organization file a Suspicious Activity Report with the Department of Treasury's Financial Crimes Enforcement Network for certain transactions, or the expectation that a banking organization notify the relevant law enforcement agencies of a computer-security incident that may be criminal in nature.

---

3 The final rule requires a bank service provider to notify affected banking organization customers of certain computer-security incidents.

Under the final rule, a bank service provider must notify at least one bank-designated point of contact at each affected banking organization *as soon as possible* after the bank service provider determines that it has experienced a computer-security incident that materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours. A service provider need not provide notification of scheduled maintenance, testing, or software updates that it previously communicated to a banking organization customer.

A bank service provider generally means any person that performs covered services, which consist of services that are subject to the Bank Service Company Act, including 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. A financial market utility that is designated as systemically important under Title VIII of the Dodd-Frank Act (and is therefore subject to a separate regulatory regime) is exempt from the final rule.

After receiving a notification from a bank service provider, an affected banking organization may be required to file a report with the appropriate federal regulator if the banking organization determines that it has experienced a notification incident.

---

4 While the final rule requires prompt notification, notice procedures are relatively open-ended.

The final rule requires that banking organizations and bank service providers give notice shortly after determining that a reportable computer-security incident has occurred, but does not contain prescriptive notice procedures. For banking organizations, the final rule does not include a specific format for notifications, specifying only that a notification must be made through email, telephone, or other method that each Agency can prescribe, and that the notification can be directed either to the Agency's supervisory office or to another designated point of contact. Additionally, the notification need only report that the banking organization has determined that it experienced a computer-security incident that rose to the level of a notification incident. The preamble to the final rule explicitly notes that a banking

organization's notification "does not require an assessment or analysis." The final rule leaves room for the Agencies to adopt more specific processes in the future.

For bank service providers, the final rule specifies only that a bank service provider must notify a banking organization-designated point of contact at each affected banking organization customer, and does not prescribe a particular medium or format for that notification. If a banking organization has not designated a point of contact, the bank service provider must notify the banking organization's Chief Executive Officer, Chief Information Officer, or two individuals of comparable responsibilities, through any reasonable means.

---

5 The final rule reflects the trend of banking regulators scrutinizing the conduct of bank service providers.

In recent years, banking organizations have increasingly outsourced support functions to third parties and partnered with third parties such as fintech companies to provide services to customers. In response to this trend, federal and state banking regulators have devoted greater focus and resources to the oversight of bank service providers and the risks that service providers can pose to banking organizations. Much of the supervisory focus on bank service providers derives from the Agencies' authority under the Bank Service Company Act, and has, until now, primarily manifested itself in the form of guidance, examination activity, and supervisory communications that address how banks should oversee their service providers. The final rule is believed to be the first substantive federal banking regulation that applies directly and uniquely to the activities of bank service providers, and could presage future efforts by the Agencies to regulate these entities directly.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Financial Services practice:

Randy Benjenk	+1 202 662 5041	rbenjenk@cov.com
Nikhil V. Gore	+1 202 662 5918	ngore@cov.com
Jeremy Newell	+1 212 841 1296	jnewell@cov.com
Michael Nonaka	+1 202 662 5727	mnonaka@cov.com
Karen Solomon	+1 202 662 5489	ksolomon@cov.com
D. Jean Veta	+1 202 662 5294	jveta@cov.com
Blair Hotz	+1 202 662 5969	bhotz@cov.com