BOARD OF GOVERNORS

OF THE

FEDERAL RESERVE SYSTEM

WASHINGTON, D.C. 20551

DIVISION OF SUPERVISION AND REGULATION

DIVISION OF CONSUMER AND COMMUNITY AFFAIRS

SR 22-4

CA 22-3

March 29, 2022

TO THE OFFICER IN CHARGE OF SUPERVISION AT EACH FEDERAL RESERVE BANK

SUBJECT: Contact Information in Relation to Computer-Security Incident Notification Requirements

Applicability: This letter applies to all banking organizations supervised by the Federal Reserve, including those with $10 billion or less in consolidated assets. This letter also applies to bank service providers of banking organizations supervised by the Federal Reserve. However, this letter does not apply to designated financial market utilities as defined at 12 U.S.C. § 5462(4).

The Board of Governors of the Federal Reserve (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) issued a joint final rule to establish computer-security incident notification requirements for banking organizations and their bank service providers.[1] The final rule takes effect on April 1, 2022, with a compliance date of May 1, 2022.

As described in the final rule, this requirement will help promote early awareness of emerging threats to banking organizations and the broader financial system, helping the agencies react to these threats before they become systemic. This letter sets forth the Board-designated points of contact for banking organizations to notify the Board of "notification incidents."[2]

[1] *See* 86 FR 66424 (November 23, 2021), available at: https://www.govinfo.gov/content/pkg/FR-2021-11-23/pdf/2021-25510.pdf.

[2] The final rule defines a "notification incident" as a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's: (i) ability to carry out banking operations, activities, or processes, or deliver banking products and services to

A banking organization whose primary federal regulator is the Board must notify the Board about a notification incident by email to incident@frb.gov or telephone to (866) 364-0096.[3] The Board must receive this notification from a banking organization as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred.

If a banking organization is in doubt as to whether it is experiencing a notification incident for purposes of notifying the Board, the Board encourages the banking organization to contact the Board by email to incident@frb.gov or telephone to (866) 364-0096.

A banking organization should also contact its central point of contact about a notification incident.

Bank Service Providers

A bank service provider must notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, services provided to such banking organization for four or more hours.[4] A bank service provider is required to provide notice of the incident to at least one bank-designated point of contact at each affected banking organization as soon as possible. If a banking organization customer has not previously provided a bank-designated point of contact, the bank service provider must notify the Chief Executive Officer and Chief Information Officer of the banking organization customer, or two individuals of comparable responsibilities, through any reasonable means. The final rule takes effect on April 1, 2022, with a compliance date of May 1, 2022.

If a bank service provider is in doubt as to whether a material disruption or degradation in services provided to a banking organization customer for four or more hours may have a material adverse impact on a banking organization customer, the Board encourages the bank service provider to contact the banking organization customer or its own legal adviser.

---

a material portion of its customer base, in the ordinary course of business; (ii) 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 (iii) 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. The final rule defines a "computer-security incident" as 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.

[3] The Board may identify other methods by which banking organizations may provide notice of cyber incidents in the future.

[4] This notification requirement does not apply to any scheduled maintenance, testing, or software update previously communicated to a banking organization customer.

Reserve Banks are asked to distribute this letter to the supervised banking organizations in their districts and to appropriate supervisory staff. Questions regarding this letter may be sent via the Board's public website.[5]

Arthur Lindo Deputy Director Division of Supervision and Regulation	Eric S. Belsky Director Division of Consumer and Community Affairs

[5] *See* http://www.federalreserve.gov/apps/contactus/feedback.aspx.