DORSEY
DORSEY+WHITNEY LLP

The Prudential Bank Regulators Adopt Federal Data Interruption Notice Requirements for FDIC-Insured Institutions and Service Providers

by Erin Bryan and Joseph Lynyak

Introduction

On November 23, 2021, the Office of the Comptroller of the Currency (the "OCC"), the Federal Deposit Insurance Corporation (the "FDIC") and the Federal Reserve Board (the "Prudential Regulators") exercised their collective safety and soundness authority to establish a national standard for FDIC-insured institutions (collectively, "Banks") and their bank service providers ("Service Providers") to notify the applicable Prudential Regulator of a data interruption, system failure or breach that is likely to cause loss to a Bank.

The final rule (the "Rule") is effective as of April 1, 2022, with compliance mandatory on May 1, 2022.[1] The Rule imposes different evaluative factors on Banks and Service Providers when determining whether a notice obligation is created, including qualitative judgments following an identified "data-security incident" to determine whether a required notice must be provided.

What follows is a summary of the Rule, as well as several initial observations regarding possible compliance concerns for both Banks and Service Providers.

Overview

Notwithstanding the plethora of state statutes addressing data breaches and required notifications, in the banking sector there has not existed a clear federal requirement for a Bank to notify its Prudential Regulator that a data interruption or breach of its electronic systems has occurred that might jeopardize the Bank and/or the financial system. From the perspective of the Prudential Regulators, some of the evaluative standards promulgated under various state data breach laws may have had the effect of permitting a Bank to delay deeming a data breach incident to have occurred, as well as permitting a Bank to delay notifying the applicable Prudential Regulator in sufficient time to allow the Prudential Regulator to take remedial action to prevent actual loss or damage to an individual Bank or to the U.S. banking system as a whole.

Related People

- Erin Bryan
- Joseph Lynyak

Related Capabilities

- Banking & Financial Institutions
- Consumer Financial Services
- Financial Services Regulatory
- Privacy & Social Media

In recognition of the growing use of Service Providers being employed by Banks (e.g., cloud processing for lending and deposit systems and general data account storage), the Prudential Regulators elected to include Service Providers by imposing on them an "early warning" notice to a Bank customer of a "computer-security incident" that requires the immediate attention of a Bank.

The Rule establishes a three-step process to determine whether a notice is required. First, has a computer-security incident, discussed below, occurred that results in actual harm either to a Bank's electronic system(s) or the data stored in it? Second, if the answer is in the affirmative, has the identified computer-security incident materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a Bank's operations? Third, if the answer is in the affirmative, a Bank must notify its Prudential Regulator within 36 hours from the point in time that determination is made, and a Service Provider must notify its Bank customers "as soon as possible" after that determination is made.

Bank

The Rule requires a Bank to notify its Prudential Regulator upon the occurrence of a "notification incident" arising from a "computer-security incident" at the Bank, which is defined as "an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the [electronic] system processes, stores, or transmits."

Upon the identification of a computer-security incident, a Bank must immediately determine whether the incident (including a security breach) is sufficiently significant as to create a "notification incident" that requires that a notification be made by the Bank to the Bank's Prudential Regulator.

The Rule defines a "notification incident" as follows:

Notification incident is 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 its 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) 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.

Should a Bank determine that a notification incident has occurred, the Bank must notify

its Prudential Regulatory within 36 hours of that determination. The method for notifying the applicable Prudential Regulator is intended to be direct and straightforward, and includes the use of a telephonic communication, email or other similar method.[2]

While not included in the Rule itself, the supplemental information in the *Federal Register* accompanying the Rule provides examples of electronic system disruptions or failures that will generally be deemed to *per se* constitute notification incidents:

- Large-scale distributed denial of service attacks that disrupt customer account access for an extended period of time (*e.g.*, more than 4 hours);
- A Service Provider that is used by a Bank for its core banking platform to operate business applications experiences widespread system outages and recovery time is undeterminable;
- A failed system upgrade or change that results in widespread user outages for a Bank's customers and employees;
- An unrecoverable system failure that results in activation of a Bank's business continuity or disaster recovery plan;
- A computer hacking incident that disables banking operations for an extended period of time;
- Malware on a Bank's network that: (i) poses an imminent threat to the Bank's core business lines or critical operations; or (ii) requires the Bank to disengage any compromised products or information systems that support the Bank's core business lines or critical operations from Internet-based network connections; and
- A ransom malware attack that encrypts a core banking system or backup data.

Service Providers

The Rule defines a "Service Provider" as any person or entity who provides a service to a Bank which is a covered service pursuant to the Bank Service Company Act (the "BSCA").[3] This definitional approach results in a broad scope of coverage for Service Providers regardless whether the Service Provider is itself a bank service company. The definition is intended to include Bank affiliates as well, regardless of whether such affiliates would constitute bank service companies under the BSCA.

The BSCA defines the following services that may be provided by a bank service company to a Bank:

- 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; and
- any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a Bank.[4]

In addition to these core banking functions that may be provided by a Service Provider, a bank service company may also provide any services that may be performed by a bank holding company (as interpreted by the Federal Reserve) pursuant to Section 4(c)(8) of the Bank Holding Company Act.[5]

The effect of this definitional approach is to include within the coverage of the Rule a

Service Provider who provides a service to a Bank that can be directly performed by the Bank itself. Considering that the Rule contemplates computer malfunctions associated with the operation of a Bank, it is difficult to identify any electronic system being provided by a third party related to a Bank's core operations that would not be deemed to be a covered service under the Rule.

It should be noted that when a computer-security incident is experienced by a Service Provider, the Rule subjects a Service Provider to a lower (*i.e.*, reduced) factual determination of harm than would apply to a Bank customer. First, the Service Provider must conclude that a computer-security incident has occurred, based upon the same evaluative criteria as the criteria to be employed by a Bank directly. Second, however, a Service Provider must determine whether the computer-security incident it has experienced has "materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade," the covered services provided to a Bank customer for four or more hours. Upon making this second determination, a Service Provider is required to notify at least one Bank-designated point of contact at each affected Bank customer utilizing an email address, phone number, or any other contact methodology previously provided by the Bank to the Service Provider.[6]

Observations Regarding Compliance

We offer the following observations regarding the Rule:

Comparing the Rule's Requirements with State Data Breach Laws. While the Rule's notification requirements encompass computer system interruptions that are broader than many state data breach laws, particular concerns may arise when a computer-security incident may also qualify as a data breach as defined by state law. Because many states impose liability on third parties for failing to take required action of a data breach incident, a Bank experiencing a computer-security incident under the Rule must exercise care to distinguish between differing standards that might apply.

Specifically, the standard for notifying a Prudential Regulator of a computer-security incident (*i.e.*, following a determination that a notification incident has occurred as defined by the Rule) may be lower than the factual determination required to be made that a data breach has occurred. In the case of the Rule, the Rule contemplates the quick and prompt evaluation of harm to a Bank, but without the necessity of determining why that data loss (as compared to systems functionality) has occurred. Conversely, many state laws permit an entity experiencing a possible data breach the time to conduct an investigation to determine that a data loss outside of the control of a Bank (or a Service Provider) has occurred, and generally a factual investigation to determine that a data loss has actually occurred is permitted prior to the obligation of notifying third parties commences.[7]

This possible disparity in evaluative standards between the Rule and state data breach laws could expose both a Bank and a Service Provider to an allegation that its state law data breach compliance obligations commenced based upon the Rule and not the applicable state data breach law. Accordingly, Banks and Service Providers complying

with the Rule should consider including in any notice a statement that the notice is being provided under the standards as set forth in the Rule, and compliance with any obligations under state law data breach laws will be separately considered.[8]

The Rule's Scope of Coverage for Service Providers. As noted above, the Rule employs a broad coverage approach to include in the scope of coverage under the Rule virtually any electronic system provided by a Service Provider to a Bank that potentially might cause loss to a Bank.

We note that mapping covered computer systems operated directly by a Bank for compliance purposes should not present a significant difficulty by reference to existing vendor management guidance issued by the Prudential Regulators and the FFIEC.[9] However, in regard to Service Providers, the application of the test described above may present practical difficulties both in respect of the short time-frame for determining that a notice must be provided to a Bank customer (*i.e.*, as soon as possible) as well as the potential number of notices that might be required in the instance of a large Service Provider that provides covered services to hundreds of Banks.[10]

Contractual versus the Rule's Notice Obligations for Service Providers. Considering the significant expansion of covered services now being provided by Service Providers, large Service Providers may find compliance to be difficult, and may be reluctant (or unable) to implement compliance protocols within the Rule's effective date for compliance (*i.e.*, May 1, 2022).

In that regard, Service Providers may have strong legal positions to object to strict compliance with the notice requirement under the Rule.

First, the Rule's attempt to claim jurisdiction over Service Providers that are not affiliated with a Bank may be of questionable legal effect. While compliance may be voluntary on the part of Service Providers, strict compliance may not be legally enforceable by the Prudential Regulators.

Second, Service Providers objecting to coverage under the Rule may elect to rely upon existing service contracts with Banks that frequently include data interruption and breach notification provisions—meaning that until those provisions are modified by a Bank and its Service Provider, existing contractual provisions should control and not the requirements of the Rule.[11] At a minimum, Banks may want to harmonize as much as possible the nomenclature in this area in a manner that provides reasonable guidance to both its own employees and to Service Providers.

Finally, the scope of coverage of the Rule is so broad that drafting effective policies and procedures to enable a Service Provider to achieve reasonable compliance may require significant efforts. In the instance of Service Providers that provide Bank customers core bank system services, creating a notification system for Bank customers may be practically difficult to achieve without considerable modification to policies and procedures applicable to bank-related data breaches.

[1] Available at: https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank (last accessed Dec. 10, 2021).

[2] The Prudential Regulators may issue supplemental guidance regarding an acceptable notification methodology. However, the clear intent of the notification requirements of the Rule is to effect a notice in a practical and efficient manner. (Regardless of the notification method employed, a specific notice to a Bank's examiner in charge may be prudent.)

[3] 12 U.S.C § 1861 *et seq*.

[4] 12 U.S.C. § 1863.

[5] 12 U.S.C § 1843(c)(8). The activities falling into this category are usual and typical support services traditionally provided by a bank holding company for a bank subsidiary which had been determined prior to November 12, 1999 by the Federal Reserve to be so closely related to banking as to be a proper incident thereto. Most computer and other electronic support services under this alternative authority would be a covered service under the Rule.

[6] If a Bank has not previously provided a Service Provider a designated point of contact, the required notification must be made to the chief executive officer and chief information officer of the Bank, or two individuals of comparable responsibilities (through any reasonable means).

[7] It should be noted that the discussion of state data breach laws is intended to highlight the differing standards that may exist between complying with state data breach requirements and the Rule's lower standards for notifying the Prudential Regulators. Care must be exercised by a Bank to determine its specific obligations under each state data breach statute and regulations that may apply when a computer-security incident and a possible data breach has occurred.

[8] A Bank providing a notification to a Prudential Regulator might also consider requesting that the notice be deemed confidential pursuant to safety and soundness examination considerations. The New York State Department of Financial Services (the "DFS") already allows for this, and has imposed penalties on DFS regulated companies, even if no harm resulted.

[9] *See*, Third-Party Relationships: Risk Management Guidance | OCC; Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29 | OCC; Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 2021-15308.pdf (govinfo.gov) (July 2021).

[10] We note that the Prudential Regulators may not appreciate the potential complexity for service providers to adopt effective policies and procedures. Whether latitude for achieving a reasonable degree of compliance for larger Service Providers will be afforded by the Prudential Regulators may require additional discussions with the Prudential Regulators in the next six months.

[11] While the Prudential Regulators have not directly addressed this contractual issue, informal discussions have indicated that Banks will be expected to modify contracts with Service Providers as those contracts are negotiated or renewed.