Published on *The National Law Review* https://natlawreview.com

The Broadening Data Security Mandate: SEC Incident Response Plan and Data Breach Notification Requirements

Article By:

Damon W. Silver

Melissa Pascualini

Virtually all organizations have an obligation to safeguard their personal data against unauthorized access or use, and, in some instances, to notify affected individuals in the event such access or use occurs. Those obligations are, in some instances, relatively nebulous, and organizations—for better or worse—have flexibility to determine what pre-incident safeguards and post-incident responsive actions are “reasonable” under the circumstances.

The SEC, in its recent amendments to Regulation S-P (the Amendments), takes a different approach. The Amendments impose detailed and specific obligations on covered institutions—including broker-dealers, investment companies, registered investment advisers, and transfer agents—to (1) develop and maintain written incident response programs and (2) provide notification to affected individuals in the event their sensitive customer information is subject to unauthorized access or use (a Data Breach)

Incident Response Program

The Amendments require covered institutions to develop and maintain written information response programs. **The function of these programs is to enable covered institutions to better detect and respond to Data Breaches, including by facilitating their:**

- **assessment** of the nature and scope of these incidents, including identification of the internal systems containing customer information and the types of customer information that may have been accessed or used without authorization. The Amendments indicate that covered institutions when assessing an incident, should consider the type and extent of the unauthorized access, the impact on operations, and whether information has been exfiltrated or is no longer accessible;
- **containment and control** of the incident to prevent further unauthorized access to or use of customer information. The Amendments acknowledge that the appropriate steps for containing and controlling an incident will vary based on its nature, but identify the following as potential key action items: isolation of affected systems, enhancement of system monitoring, identifying additional compromised systems, forcing password resets, and

changing or disabling default user accounts; and
- **notification** to individuals whose "sensitive customer information" (defined below) was, or is reasonably likely to have been, accessed or used without authorization.

Notably, while the foregoing incident response program requirements apply to all consumer "nonpublic personal information"—a broad category encompassing all personally identifiable financial information a financial institution collects about an individual in connection with providing a financial product or service—the notification obligations discussed below are limited to incidents impacting "sensitive customer information."

Notification to Affected Individuals

Covered institutions must provide notice to each affected individual whose sensitive customer information was, or is reasonably likely to have been, subject to a Data Breach. **"Sensitive customer information" includes:**

- information uniquely identified with an individual, such that it can reasonably be used to authenticate the individual's identity;
- government-issued identification numbers, including a social security number, driver's license number, alien registration number, passport number, or employer or taxpayer identification number;
- a biometric record;
- a unique electronic identification number, address, or routing code;
- telecommunication identifying information or access device; or
- information identifying an individual or an individual's account, including an account number, name, or online username, in combination with other authenticating information that could be used to gain access to an individual's account.

In the event of a Data Breach, the Amendments require covered institutions to provide clear and conspicuous notice "as soon as practicable," but not later than 30 days after their discovery of the breach. **Notice to affected individuals must include the following:**

- a general description of the incident and type of sensitive customer information affected;
- the date (or estimated date/date range) of the incident;
- contact information notice recipients can utilize to obtain more information about the incident; and
- steps affected individuals can take to protect their information, including how they can obtain free credit reports, place fraud alerts on their accounts, and review their account statements for suspicious activity.

Under the Amendments, unauthorized access to or use of sensitive customer information does not always trigger the obligation to notify. Notice is *not* required if, after a reasonable investigation of relevant facts and circumstances, the covered institution determines that the sensitive customer information in question has not been, and is not reasonably likely to be, used in a manner resulting in substantial harm or inconvenience (e.g. because it was protected by encryption). The Amendments indicated that, if a covered institution reasonably determines that a specificindividual's sensitive customer information was not accessed or used without authorization, it does not need to notify that individual. However, if the covered institution is unable to identify which specific individual's sensitive customer information has been accessed or used, it must notify all individuals whose information resided on the impacted information system.

Implementation

The Amendments will take effect in early August 2024, but covered entities—depending on their size—will have an 18- or 24-month grace period to come into compliance. Larger entities, which are defined below, will need to come into compliance by December 2025, while smaller entities will have until June 2026.

Entity	Qualification to be Considered a Larger Entity
Investment companies together with other investment companies in the same group of related investment companies	Net assets of $1 billion or more as of the end of the most recent fiscal year.
Registered investment advisers	$1.5 billion or more in assets under management.
Broker-dealers	All broker-dealers that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.
Transfer agents	All transfer agents that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.

Takeaways

Though the grace periods will likely lull some entities into near-term complacency—believing they have plenty of time to get their houses in order—prudent entities will place compliance with the Amendments high on their task lists.

For entities that haven't already made a significant investment in their incident response programs, development of the robust program the Amendments require will be a heavy lift. Compliance with the assessment component, for instance, may require entities to conduct extensive data mapping to better understand what data they have, where it's stored, how it's safeguarded, and how long it's retained.

They may also need to take a close look at their current controls to detect and rapidly investigate and respond to potential Data Breaches, including those that enable the isolation of affected systems, the identification and eradication of ongoing malicious activity, and the restoration of business operations, including potential data recovery from backups.

Covered entities will also need to prepare to analyze their notification obligations and timely provide requisite notices.

To many, the above requirements will sound familiar, as they overlap to a degree with obligations imposed by state reasonable safeguard and breach notification laws. The Amendments' incident response plan prescriptions, however, are more detailed and onerous than the requirements imposed by most state laws, and their definition of "sensitive customer information" is broader than the definition of "personally identifiable information" (or the comparable term) in most states. Accordingly, even entities that have mature incident response programs in place would benefit from giving those programs a fresh look to ensure they meet the Amendments' lofty requirements.

National Law Review, Volume XIV, Number 197

Source URL:https://natlawreview.com/article/broadening-data-security-mandate-sec-incident-response-plan-and-data-breach