Back-2-Basics: Responding to a Data Breach

Cybersecurity remains a top priority for regulators and the entire financial services industry. The Federal Financial Institutions Examination Council (FFIEC) agencies introduced a cybersecurity assessment tool in 2015 to help institutions determine their level of cybersecurity preparedness. Use of the tool by credit unions is recommended but voluntary, although it is being incorporated into NCUA's exam process later this year (3rd or 4th Quarter 2017).

Part 748 of NCUA's regulations requires federally insured credit unions to develop and implement "risk-based" response programs to address "instances of unauthorized access to member information in member information systems" (i.e., data breach). "Member information systems" consist of "all of the methods used to access, collect, store, use, transmit, protect, or dispose of member information," including systems maintained by the credit union's service providers (12 CFR Part 748, Appendix A, Paragraph I.C.2.d.). Appendix B to Part 748 provides credit unions with direction on how to meet this regulatory requirement.

When a credit union becomes aware of an incident of unauthorized access to "sensitive member information" in member information systems, the institution is required to conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. Sensitive member information includes data such as a member's name, address, or telephone number used in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account; or any combination of components of member information that would allow someone to log onto or access the member's account, such as user name and password or password and account number. The credit union's response program must also include procedures to notify members about incidents of unauthorized access to member information systems that could result in substantial harm or inconvenience to the member (e.g., identity theft).

Components of a response program

At a minimum, a credit union's response program should contain procedures for:

- Assessing the nature and scope of an incident, and identifying what member information systems and types of member information have been accessed or misused.

- Notifying the appropriate NCUA Regional Director, and, in the case of federally insured state-chartered credit unions, its applicable state supervisory authority, as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of "sensitive" member information.
- Notifying appropriate law enforcement authorities, in addition to filing a timely Suspicious Activity Report (SAR) in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is on-going.
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of member information (e.g., monitoring, freezing, or closing affected accounts) while preserving records and other evidence.
- Notifying members when warranted (i.e., the breach could result in substantial harm or inconvenience to the member).

Note that when an incident of unauthorized access to member information involves member information systems maintained by a contracted service provider(s), it is the credit union's responsibility to notify its members and regulator. However, a credit union may authorize or contract with its service provider to notify the credit union's members or regulators on its behalf.

Check out the following resources for more detailed information:

CUNA's e-Guide: Cybersecurity

NCUA Cybersecurity Resources

FFIEC Cybersecurity Assessment Tool

FFIEC Cybersecurity Assessment Tool Frequently Asked Questions

Source: CU Compliance Community