The FTC’s Sweeping Changes to the Safeguards Rule

January 20th, 2022 | and K. Dailey Wilson

On October 27, the Federal Trade Commission finalized its long-awaited updates to the Safeguards Rule. The Safeguards Rule implements provisions of the Gramm-Leach-Bliley Act mandating the safeguarding of customer information, requiring a financial institution to develop, implement, and maintain a comprehensive written information security program appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of its customer information. Auto dealers and finance companies have always been subject to the requirements of the Safeguards Rule by virtue of offering credit transactions.

While the changes are not effective for one year, dealers and finance companies should familiarize themselves with the new requirements sooner rather than later. The 2021 changes to the Safeguards Rule will require financial institutions to dust off their existing information security programs and likely make some significant changes. This article addresses five key changes to the Safeguards Rule—qualified individuals, the requirement to conduct written risk assessments, the required elements of an effective safeguards program, the requirement to establish a written incident response plan, and the requirement to submit an annual report to the financial institution’s governing body regarding the safeguards program.

Qualified Individual

The Safeguards Rule will now require financial institutions to designate a single “qualified individual” to be responsible for overseeing, implementing, and enforcing their information security programs. The previous version of the Safeguards Rule allowed financial institutions to designate multiple employees to coordinate their information security programs. The new requirement to appoint a single individual clarifies the lines of reporting in enforcing the program, avoids gaps in responsibility in managing data security, and improves communication.

The qualified individual may be an employee, affiliate, or service provider. The Safeguards Rule does not define the term “qualified,” and no particular level of education, experience, or certification is required. Instead, what qualifications are necessary will depend on the size and complexity of the financial institution’s information system and the volume and sensitivity of the customer information that the financial institution possesses or otherwise processes.

Written Risk Assessment

The Safeguards Rule now requires a financial institution to base its information security program on a written risk assessment. The written risk assessment must include: (1) the criteria for evaluating and categorizing identified security risks or threats; (2) the criteria for assessing the

confidentiality, integrity, and availability of information systems and customer information, including the adequacy of existing controls in the context of the identified risks or threats the financial institution faces; and (3) a description of how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks. Based on these criteria, financial institutions would assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information and then design and implement appropriate safeguards.

Changes to Program Requirements

The Safeguards Rule previously contained very little detail regarding what was specifically required for an effective safeguards program, instead leaving it to the financial institution to determine what was appropriate based on the financial institution's size and complexity. The Safeguards Rule now requires financial institutions to implement specific elements within their safeguarding programs. For example, financial institutions must encrypt all customer information held or transmitted by the financial institution both in transit over external networks and at rest. Financial institutions must also implement an authentication process requiring verification of at least two of the following authentication factors: (1) knowledge factors, such as a password; (2) possession factors, such as a token; or (3) inherence factors, such as biometric characteristics (also known as multifactor authentication).

Written Incident Response Plan

The changes to the Safeguards Rule also require a financial institution to establish a written incident response plan, designed to promptly respond to and recover from a security event. The written incident response plan must include certain elements, including: (1) the goals of the incident response plan; (2) the internal processes for responding to a security event; (3) the definition of clear roles, responsibilities, and levels of decision-making authority; (4) external and internal communications and information sharing; (5) identification of requirements for the remediation of any identified weaknesses in information systems and associated controls; (6) documentation and reporting regarding security events and related incident response activities; and (7) the evaluation and revision of the incident response plan as necessary following a security event.

Reporting

The qualified individual must report in writing, at least annually, to the financial institution's board of directors or equivalent governing body regarding the overall status of the financial institution's information security program, compliance with the Safeguards Rule, and material matters related to the information security program, including issues related to risk assessment, risk management and control decisions, service provider arrangements, results of any testing, security events, management's response to security events, and recommendations for any changes to the information security program.

These are not the only changes to the Safeguards Rule, so all financial institutions subject to the rule should review the new rule in its entirety. The adjustments necessitated by the changes to the Safeguards Rule will require an investment of both time and resources. Dealers and finance companies should not wait to begin thinking about how they will comply with the expanded

safeguarding requirements.