The FTC's Sweeping Changes to the Safeguards Rule – Time to Reexamine Your Information Security Program

By: Dailey Wilson

On October 27th, the Federal Trade Commission ("FTC") finalized its long-awaited updates to the Safeguards Rule. The Safeguards Rule implements provisions of the Gramm-Leach-Bliley Act requiring 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 Rule will require financial institutions to dust off their existing information security program 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, required elements of an effective safeguards program, the requirement to establish a written incident response plan, and the requirement submit an annual report to the financial institution's governing body regarding the safeguards program.

Qualified Individual

The Safeguards Rule will require financial institutions to designate a single "qualified individual" to be responsible for overseeing, implementing, and enforcing its information security program. The previous version of the Rule allowed financial institutions to designate multiple employees to coordinate its information security program. The Rule now requires appointment of a single individual to oversee the information security program, thereby clarifying the lines of reporting in enforcing the program, avoiding gaps in responsibility in managing data security, and improving communication.

The qualified individual may be an employee, affiliate, or service provider. The Rule does not define the term "qualified" and in fact, no particular level of education, experience, or certification is required by the Rule. Instead, what qualifications are necessary will depend upon 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 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 institution would then 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 design and based on its risk mitigation guidelines, implement appropriate safeguards.

Changes to Program Requirements

The 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 is appropriate based on the financial institution's size and complexity. The Rule now requires financial institutions to implement specific elements within its safeguarding program. For example, financial institutions must encrypt all customer information held or transmitted by the financial institution both in transmit 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).

Continued on page 18

Continued from page 14

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 response to and recover from a security event. The written incident response plan must include certain elements, including: (1) goals of incident response plan; (2) internal processes for responding to security event; (3) definition of clear roles, responsibilities, and levels of decision-making authority; (4) external and internal communications and information sharing; (5) identification of requirements for 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) evaluation and revision as necessary following a security event.

** K. Dailey Wilson is an associate in the Tennessee office of Hudson Cook, LLP. She can be reached at 423.490.7567 or by email at dwilson@hudco.com.*

Dailey Wilson
Associate of Hudson Cook, LLP