BLANKROME
CELEBRATING 75 YEARS

Privacy, Security & Data Protection

DECEMBER 9, 2021 • NO. 5

FTC Updates GLBA Safeguards Rule for Financial Institutions to Strengthen Security

The Federal Trade Commission ("FTC") recently updated the Safeguards Rule under the Gramm-Leach-Bliley Act ("GLBA"), which is applicable to financial institutions, to strengthen data security requirements for consumer financial information. The amendments to the Safeguards Rule ("Final Rule") come following a significant rise in data breaches and cyberattacks in recent years. In addition to the amendments, the FTC seeks comment on whether to make additional changes to the Safeguards Rule to require financial institutions to report certain data breaches and other security incidents to the FTC.

The Safeguards Rule was promulgated in 2002 under the GLBA's directive requiring the FTC and other federal agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards for certain information, and became effective in 2003. The Final Rule is the result of two years of FTC rule making activity.

Guidance: The Final Rule contains four main modifications. First, it adds provisions to guide covered financial institutions on how to develop and implement specific aspects of an overall information security program, including access controls, data inventory and classification, secure development practices, multi-factor authentication, encryption, information disposal procedures, change management, testing, and incident response. For example, while the current Rule requires financial institutions to undertake a risk assessment and develop and implement safeguards to address the identified risks, the Final Rule sets forth specific criteria for what the risk assessment must include and requires that the risk assessment be in writing. Additionally, the Final Rule requires financial institutions adopt mechanisms to ensure employee training and service provider oversight mandated by the Safeguards Rule are effective. While the Final Rule creates more specific requirements, the FTC states it is still intended to allow for flexibility so that an information security program can be tailored to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue.

Accountability: Second, the Final Rule adds requirements designed to improve the accountability of financial institutions' information security programs. For instance, while the current Rule allows a financial institution to designate one or more employees to be responsible for the information security program, the Final Rule requires the designation of a single "qualified individual." However, the Final Rule does not prescribe a particular level of education, experience, or certification for an individual to be considered "qualified."

The Final Rule also requires the qualified individual to report, in writing, regularly and at least annually to the board of directors or equivalent governing bodies to provide senior management with better awareness of their financial institutions' information security programs, thus making it more likely that the programs will receive the required resources and be able to protect customer information. The report must include: (1) the overall status of the information security program and compliance with the Final Rule and (2) material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

Partial Exemption: Third, to recognize the impact of the additional requirements on small businesses, the Final Rule exempts financial institutions that collect information on fewer than 5,000 consumers from the requirements of a written risk assessment, incident response plan, and annual reporting to the board of directors.

Expansion of Definition of Covered "Financial Institutions": Fourth, it expands the definition of "financial institution" under the GLBA to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities. This change brings "finders," companies that bring together buyers and sellers of a product or service, within the scope of the Final Rule and makes the definition of "financial institution" more analogous to that in the Bank Holding Company Act. In addition, the Final Rule defines several terms and provides related examples, including of "financial institution," in the Rule itself rather than incorporate them by reference from the Privacy of Consumer Financial Information Rule

The Final Rule will come into effect one year after the date of publication in the Federal Register.

BRight Ideas: The Final Rule authorizes the FTC to commence enforcement actions and impose civil fines and penalties in the event of non-compliance. Entities subject to the Safeguards Rule should review their current information security programs against the Final Rule's new, more prescriptive standards and begin the process of implementing changes to address any shortcomings prior to the effective date of the Final Rule.

The exemption for financial institutions collecting information on fewer than 5,000 customers seems somewhat arbitrary because often cyber criminals target the smaller service providers who are less prepared for security incidents. Since the chain is only as strong as the weakest link, this exemption will require covered institutions to double their efforts to have oversight and insurance for the activities of vendors and subcontractors that are exempt.

The GLBA and the Safeguards Rule do not preempt states from regulating cybersecurity. Accordingly, the Final Rule should be viewed as the baseline but certain states, such as New York, require additional controls and protocols for compliance with state law requirements.

Financial institutions should start preparing now for the additional security requirements needed to comply with the upgraded GLBA safeguards as they will take some time to operationalize.

For additional information, please contact:

Sharon R. Klein
949.812.6010 | sharon.klein@blankrome.com

Scott D. Samlin
212.885.5208 | scott.samlin@blankrome.com

Alex C. Nisenbaum
949.812.6011 | alex.nisenbaum@blankrome.com

Karen H. Shin
949.812.6012 | karen.shin@blankrome.com