

Publications

Changing Cybersecurity Baselines?

ATTORNEYS & PROFESSIONALS

Jim Colejcole@groom.com

202-861-0175

Jennifer Ellerjeller@groom.com

202-861-6604

Allison Itamiaitami@groom.com

202-861-0159

Michael Krepsmkreps@groom.com

202-861-5415

David Levinedlevine@groom.com

202-861-5436

Arsalan Malikamalik@groom.com

202-861-6658

Ross McSweeneyrmcsweeney@groom.com

202-861-6625

George Sepsakosgsepsakos@groom.com

202-861-0182

Kevin L. Walshkwalsh@groom.com

202-861-6645

PUBLISHED

03/20/2019

SOURCE

Groom Benefits Brief

On March 5, 2019 the commissioners of the Federal Trade Commission (“FTC”) voted 3-2 to issue a proposed amendment (the “Proposal”) to its Standards for Safeguarding Customer Information Rule (the “Safeguards Rule”), a regulation establishing cybersecurity standards under the Gramm-Leach-Bliley Act of 1999 (the “GLBA”).^[1] The Proposal is significant to the retirement plan community for several reasons. First, the Proposal, if finalized, could raise the baseline for plan fiduciaries when developing prudent cybersecurity programs. Second, the Proposal builds on the increased interest in cybersecurity by regulators, Congress, and the states. We expect that other GLBA regulators, such as the banking regulators or the SEC may consider incorporating elements of the Proposal into their own regulations or guidelines.

Given the frequency of cyber-related news reports and attacks, cybersecurity has become a key issue for plan fiduciaries and service providers. As a result, the steps articulated in the Proposal may provide insights into what regulators could come to view as a baseline framework.

Overview

Since 2003, the Safeguards Rule has imposed a number of information security requirements on financial institutions subject to FTC regulation, including a general requirement that such entities maintain a “comprehensive information security program” with various administrative, technical, and physical safeguards in place to protect customer information. The Safeguards Rule requires that financial institutions maintain risk based information security programs that identify, evaluate, and assess risks related to customer information. The Safeguards Rule also requires that the financial institution implement controls within the institution’s technology.

We note, the Safeguards Rule works in concert with similar rules that have been promulgated by other agencies, and, as of March 13, 2019, those other agencies have not yet proposed similar changes. Thus, while the steps outlined in the FTC’s proposal do not apply to many financial institutions, the Proposal provides insight into changes that the other regulators could make and what plans and participants may expect.

As described below, the Proposal would significantly expand the Safeguards Rule by imposing numerous new procedural and technical requirements for information security programs. The Proposal draws heavily from cybersecurity regulations issued by the New York Department of Financial Services in February 2017, as well as from the insurance data security model law issued by the National Association of Insurance Commissioners (“NAIC”) in October 2017. The Proposal notes that the regulations and model law “maintain the balance between providing detailed guidance and avoiding overly prescriptive requirements for information security programs.”^[2] For financial institutions based in New York, much of the proposal will be familiar. We note that the dissenting commissioners argue persuasively that it may be too soon to draw conclusions about the efficacy of the New York or NAIC efforts.

Certain elements of the Proposal should be of particular interest to the retirement community. First, the FTC asks whether a revised rule should preempt state breach-notification laws. The current Safeguards Rule does not specifically require data breach notification – nor does it preempt state laws that require breach notification. Since the enactment of the initial rule, all fifty states have enacted data breach notification statutes. We would expect that many in the retirement community would welcome federal preemption in this area as opposed to managing the individualized state-level requirements. However, without preemption, we would expect that many in the retirement space would oppose new federal standards. Here, comments could be helpful in moving the FTC and other federal regulators towards taking the position that a single standard should apply.

In addition, we note that many state cybersecurity or data privacy laws currently have a carve-out for activity that is already regulated by GLBA. While many service providers in the ERISA space have taken the position that GLBA does not apply, arguably, the Proposal provides a basis for reevaluating that conclusion. In light of the fracturing regulatory landscape at the state level on cybersecurity and data privacy, some financial institutions may now prefer GLBA compliance when compared to disparate state and local initiatives.

Finally, the Proposal highlights the difference between the retirement industry and other parts of the financial service industry. These differences are important when plans and service providers design cybersecurity policies. Many plan participants are auto-enrolled into plans, defaulted into contribution rates, and defaulted into investment elections. This stands in contrast to the rest of the financial services industry where customers often affirmatively open accounts. As a result, plan fiduciaries balance the competing policy goals of securing participant information and assets against the risk that information may be so locked down that participants are unable to access their accounts. Because plan fiduciaries are tasked with prudently balancing these concerns, any time new cybersecurity standards develop, it may be appropriate to help shape those new standards. And, the retirement industry is particularly well suited to act on the FTC’s endorsement for self-regulation and to the development of industry-specific standards. We know that the retirement industry has already begun developing retirement-specific standards and we expect those efforts to continue throughout 2019.

General Applicability of Safeguards Rule

The Safeguards Rule generally applies to the handling of “customer information” by “financial institutions.” “Customer information” is broadly defined as, “any record containing nonpublic personal information . . . about a customer of a financial institution, whether in paper, electronic, or other form.”^[3] While participants are not viewed as “customers” of their plans, fiduciaries have viewed the standards that have developed under GLBA as providing a helpful framework for developing compliance programs.

Proposed Changes to the Safeguards Rule

While many aspects of the Safeguards Rule will remain unchanged, the Proposal adds a number of significant new elements. Below, we have identified the key changes:

- **Designation of Chief Information Security Officer (“CISO”).** The Proposal would require that financial institutions designate one individual—rather than allocating responsibility to multiple persons—as the CISO with responsibility for overseeing, implementing, and enforcing the entity’s information security program. In this regard, the FTC noted that limiting this role to one person would “lessen the possibility that there will be gaps in responsibility between individuals,” and that “requiring a single responsible individual will increase accountability for the security of financial institutions’ information systems.”^[4] Notably, the CISO role can be outsourced to an employee of an affiliate or service provider, provided certain oversight conditions are met.
- **Written Risk Assessment.** The Proposal would require financial institutions to maintain written risk assessments addressing “reasonably foreseeable internal and external” security risks.^[5] The written risk assessment must describe the criteria that will be used to evaluate risks and the security controls in place. The FTC notes that such criteria “should address the sensitivity and value of customer information collected, maintained or transmitted by the financial institution and possible vectors through which the security, confidentiality, and integrity of that information could be threatened.”^[6] The Proposal would also require “periodic”

reassessment of risks but permits “financial institutions to set their own schedule based on the needs and resources of their institution.”^[7]

- **Access Controls.** Information systems must authenticate users so as to limit access only to authorized users.
- **Data and Device Inventory.** The Proposal would require that financial institutions have an understanding of the data in their possession as well as the devices on which such data is stored and transmitted. The FTC notes that a financial institution must “understand which devices and networks contain customer information, who has access to them, and how those systems are connected to each other and to external networks.”^[8]
- **Physical Restrictions.** The Proposal would require that financial institutions “restrict access to physical locations containing customer information only to authorized individuals.”^[9] Such efforts “may include restricting access to work areas where personnel are using hard copies of customer information or requiring physical locks on filing cabinets containing customer information and similar protections” as well as having “policies for securing physical devices that contain personal information, such as laptops, tablets, phones, and thumb drives.”^[10]
- **Data Encryption.** The Proposal would require data encryption of all customer information. Notably, the Proposal would permit considerable flexibility in what constitutes encryption. In addition, if a financial institution determines that data encryption is “infeasible”, the Proposal would permit an alternative means to secure the data that has been reviewed and approved by the CISO.^[11]
- **In-House Application Development.** The Proposal would require adopting “secure development practices for in-house developed applications” to ensure that the applications they use to handle customer information are secure.^[12]
- **Multi-Factor Authentication.** The Proposal would require that financial institutions implement multi-factor authentication for any individual accessing customer information or an internal network that stores customer information. In this regard, the FTC notes that it “views multi-factor authentication as a minimum standard to allowing access to customer information.”^[13] The Proposal would define “multi-factor authentication” as “authentication through verification of at least two of the following types of authentication factors:

- 1) knowledge factors, such as a password;
- 2) possession factors, such as a token; or
- 3) inherence factors, such as biometric characteristics.^[14]

Notably, the Proposal seeks to provide “considerable flexibility” for implementing such factors. For example, for the knowledge factor, “financial institutions are not limited to requiring passwords for access to systems, but might also use biographical information, or other knowledge that should be limited to the authorized user.”^[15] Similarly, a possession factor “could include verifying that a recognized device is accessing the system, or the transmission of a one-time code to a device on file with the financial institution,” and “[f]or the inherence factors, fingerprints, retina scans, or voice prints can be used.”^[16] In a helpful note, the FTC confirmed that “[c]urrently used forms of multifactor authentication, such as requiring both a password and the receipt of a onetime passcode on a registered device, would meet this proposed requirement.”^[17]

- **Audit Trails.** The Proposal would require maintaining “audit trails designed to detect and respond to security events.”^[18] Audit trails must describe chronological logs of user access and activities and “must be designed to allow the financial institution to detect when the system has been compromised or when an attempt to compromise has been made” and “provide sufficient information for the financial institution to reasonably respond to the event.”^[19]
- **Data Disposal Procedures.** The Proposal would require developing procedures to securely dispose of any customer information that is no longer needed for business operations or “other legitimate business purposes.”^[20]
- **Change Management Procedures.** The Proposal would require adopting certain procedures in anticipation of business integrations (e.g., acquisitions or mergers) to “assess the security of devices, networks, and other items to be added to their information system or the effect of removing such items or otherwise modifying the information system.”^[21]
- **Monitoring Authorized Users.** The Proposal would require implementing policies and procedures to monitor user access and activity relating to customer information, in order to detect any unauthorized access or wrongdoing. The Proposal does not prescribe any specific conditions for the monitoring policy. However, the FTC noted that “[t]he monitoring should allow financial

institutions to identify inappropriate use of customer information by authorized users, such as transferring large amounts of data or accessing information for which the user has no legitimate use.”^[22]

- **Regular Testing of Safeguards.** The Proposal would require financial institutions to regularly monitor the effectiveness of its safeguards and controls by conducting either (i) continuous monitoring (which would provide for real-time monitoring of security threats and other vulnerabilities) or (ii) annual penetration testing and biannual vulnerability assessments.^[23]
- **Security Training and Education.** The Proposal would require that financial institutions (i) provide security awareness training to their employees, (ii) take measures to ensure that the individuals they employ along with those employed by affiliates or service providers are sufficiently qualified with respect to information security, (iii) provide information security personnel with ongoing training regarding security risks, and (iv) verify that information security personnel are actually taking steps to maintain current knowledge of security issues.^[24]
- **Oversight of Service Providers.** The Proposal would expand the current requirement that financial institutions assess the information security safeguards employed by service providers at the onboarding stage to require that financial institutions perform this assessment on a periodic, ongoing basis.^[25]
- **Incident Response Plans.** The Proposal would require that financial institutions establish written incident response plans that are “designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information” that is maintained by the financial institution.^[26]
- **Annual CISO Report.** The Proposal would require that the financial institution’s CISO provide a written report to the financial institution’s board of directors or equivalent governing body describing the status of the financial institution’s information security program and its compliance with the Safeguards Rule, as well as “material matters” relating to the information security program (e.g., risk assessment, results of testing, security events, recommendations for changes).^[27]

Next Steps

The FTC has requested comments on the Proposal within sixty (60) days of publication. We look forward to continuing to work with you on plan data and cybersecurity issues. If you have any questions, please contact George M. Sepsakos at 202-861-0182 gsepsakos@groom.com, Kevin L. Walsh at 202-861-6645 kwalsh@groom.com or your regular Groom attorney. 2019 is shaping up to be a year with big changes in data privacy and data security and we hope to help you stay ahead of the curve.