The FTC's Strengthened Safeguards Rule and the Evolving Landscape of Reasonable Data Security

November 18, 2021

On October 27, 2021, the Federal Trade Commission (the "FTC") announced significant updates to the Standards for Safeguarding Customer Information (the "Safeguards Rule" or "Amended Rule"). This rule, promulgated pursuant to the Gramm-Leach-Bliley Act, is designed to protect the consumer data collected by non-bank financial institutions, such as mortgage lenders and brokers, "pay day" lenders, and automobile dealerships, among many others ("subject financial institutions"). The Amended Rule is likely to have a far-reaching ripple effect and inform the meaning of reasonable data security requirements industry-wide. In this blog post, we highlight the Amended Rule's more novel requirements and provide an overview of the potential impacts.

Expanding Scope of the Safeguards Rule (and a Small Business Carve-Out). The FTC expanded the rule's scope by amending the definition of "financial institution" to cover institutions that are engaged in activities incidental to financial activities, as determined by the Federal Reserve Board. This new definition means the amended rule covers "finders," which are companies that "bring together buyers and sellers of a product or service," like a business operating an internet marketplace, thereby acting as an intermediary for the parties.

The Amended Rule also carves out small businesses, defined as financial institutions that collect information on fewer than 5,000 customers from certain requirements.

Out with the Old and in with the New: What's Changed. Beyond scope, the most notable amendments to the Safeguards Rule (a) adopt detailed requirements governing subject financial institutions' information security programs, including by expanding the types of data security incidents that must be covered; and (b) require subject financial institutions to appoint a single individual responsible for data security. We address these changes below.

- **Information Security Program Requirements**

  - Risk Assessments: The Amended Rule provides a tick list of affirmative requirements that subject financial institutions' information security programs must meet, starting with a written risk assessment that addresses certain criteria

for evaluating security risks or threats and that also must assess the confidentiality, integrity, and availability of information systems and customer information. The risk assessments must also describe how identified risks will be mitigated or accepted and how the information security program will address the risks.

- Safeguards: In addition to the risk assessment, subject financial institutions must ensure that their information security programs include:

  - *Access Controls*: Covered financial institutions must implement controls to authenticate and permit access only to authorized users in order to prevent unauthorized acquisition of customer information. Importantly, the Amended Rule also includes the "principle of least privilege," whereby financial institutions must limit users' authorized access to the customer information actually necessary to carry out a specific function. The FTC pointed to the risks that could result from expansive user access. Therefore, employees and vendors should *not* be given access to all customer information, even when enterprise-wide access controls are in place.

  - *Identification of Data, Personnel and Devices Enabling the Achievement of Business Purposes*: With this requirement, financial institutions must undertake a full inventory of the data in its possession and the systems where the data is collected, stored, or transmitted, and attain a complete understanding of the entity's information systems and their importance to the business.

  - *Encryption*: The Amended Rule requires encryption of all customer data at rest and in-flight externally. Data encryption can be both operationally difficult and particularly costly, but the FTC has noted the existence of numerous free or low-cost encryption solutions for data in transit and also stated that encryption for data at rest is "now cheaper, more flexible, and easier than before." Institutions do not need to encrypt data transmitted internally.

  - *Multi-Factor Authentication ("MFA"):* Institutions must implement MFA for all individuals accessing any information system. The verification must consist of a combination of at least two of the following categories: knowledge factors (e.g., passwords), possession factors (e.g., token), or inherence factors (e.g., biometric characteristics). Interestingly, the FTC declined to list commonly used SMS text messages as an example of a possession factor, noting that such a verification measure might not be appropriate where "extremely sensitive information can be obtained" through that access method. The FTC expressed concern that explicitly mentioning

SMS text message verification would be considered a safe harbor without regard to the risks.

- *Disposal Policies*: Financial institutions covered by the Amended Rule must put in place procedures for the disposal of customer information "no later than two years" after the last date of use. The FTC is allowing the retention of such data where there the information is "necessary for business operations or other legitimate business purposes."

- *Change-Management Processes*: Entities subject to the Amended Rule must adopt procedures for change management, which govern the addition, removal, and modification of elements of an information system. With this requirement, the FTC is seeking to ensure that financial institutions understand the security of devices, networks, and other items when making changes to the information system. As with many of the amendments, the FTC noted that the procedures will depend on the complexity and specifics of the financial institution's information system.

- *Logging Requirements*: The Amended Rule requires the adoption of policies and procedures to monitor and log authorized users' activity and detect unauthorized access or use of customer information by those users. The Commission was unbothered by commenters concerned with the cost of perpetual user monitoring, noting that the process could be completely automated.

- *Development Practices*: Covered financial institutions must also utilize secure development practices for internally developed applications and implement procedures to vet the security of externally developed applications when such applications transmit, access, or store customer information.

- *Continuous Monitoring and Testing Requirements*: In addition to regular monitoring or testing of safeguards, the FTC instituted a requirement of continuous monitoring of information systems. Alternatively, financial institutions can undertake (a) annual penetration testing of risks identified in the institution's risk assessment and (b) vulnerability assessments every six months and whenever there have been "material changes" to operations or changing circumstances with a "material impact" on the information security program. The FTC noted that covered institutions can mitigate costs stemming from monitoring, testing, and assessments by segmenting their network, as the requirement only applies to the information systems.

- *Vendor Management*: Under the Amended Rule, financial institutions must take "reasonable steps" to ensure vendors maintain proper safeguards,

contract to require vendors to institute such safeguards, and periodically evaluate vendors for the adequacy of their safeguards.

- *Incident Response Plans*: Given the rapid increase in the number of data security incidents, it is no surprise that the FTC included a requirement that covered financial institutions adopt a written incident response plan ("IRP"). The plan must be designed to assist the financial institution in responding to and recovering from a security event. The FTC also defined "security event" to include incidents "resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on an information system, or customer information held in physical form"— seeking to ensure that security events like ransomware attacks are fully covered by IRPs. The FTC noted that even in an incident where ransomware merely encrypts data, thereby "rendering it useless," IRPs should be followed as such attacks can indicate security flaws that could lead to actual customer harm.

- **Enhanced Accountability and Reporting**: Emphasizing accountability, the Amended Rule requires the appointment of a single "qualified individual." The FTC reasoned that a single individual would improve accountability, guard against oversights in data security management, and lead to better communication. The Commission specifically cited the 2017 Equifax breach as exactly the type of scenario this provision seeks to prevent by enhancing institutional accountability.

  This Qualified Individual must provide an annual report to the institution's board of directors or other governing body, providing the board with (1) the overall status of the information security program and Safeguards Rule compliance, and (2) material matters related to the information security program. Note that the FTC declined to impose a requirement that the board certify the contents of the Qualified Individual's report.

How Does the New Rule Differ from Other Data Security Requirements Governing Financial Institutions? The Amended Rule will apply only to non-bank financial institutions; banks, as well as bank holding companies and their subsidiaries, are subject to separate guidance and standards issued by the federal banking regulators. The federal banking regulators—were they to seek to adopt these revisions—would likely do so via a notice and comment process. However, it may be prudent for banks to consider whether to voluntarily adopt some of these standards, if they have not done so already.

In this section, we take a look at certain aspects of the Amended Rule, as it compares to four of the most significant pieces of data and cyber security guidance governing financial institutions, the federal banking agencies' Interagency Guidelines Establishing Information Security Standards, the Federal Financial Institutions Examination Council ("FFIEC") Cybersecurity Assessment Tool, and Information Technology Examination

Handbook, as well as the New York Department of Financial Services' ("NYDFS") Part 500.

- **FFIEC Standards**: The most substantial difference between the FFIEC standards and the Amended Rule is the encryption requirement. Whereas the Amended Rule requires encryption of *all customer information either in external transit or at rest*, the FFIEC generally *does not require banks to encrypt data at rest*, other than passwords.

  As mentioned above, the Amended Rule requires the financial institution to adopt secure disposal procedures. Though the FTC generally requires disposal of customer information within two years of the information's last use, the FFIEC has imposed no similarly concrete requirement. Instead, the FFIEC guidelines command compliance with the entity's own requirements and within "expected time frames."

  There is also no corresponding requirement that a bank covered by the FFIEC guidelines appoint a Qualified Individual. Rather, there is a more general requirement that the Board of Directors, or a designated committee, provide direction to management and that management keep the Board informed via an annual report.

- **NYDFS Part 500**: The Amended Rule was largely based on NYDFS Part 500, a regulation establishing cybersecurity standards for New York financial institutions, as noted by FTC Commissioners Phillips and Wilson in their joint dissent. Language in several Amended Rule provisions like penetration testing, risk assessments, and the appointment of a Qualified Individual, closely mirror their Part 500 counterparts. Notably, though, Part 500 utilizes the label Chief Information Security Officer ("CISO") to describe the Qualified Individual, a title that the Amended Rule specifically eschewed in favor of a more flexible title. In that sense, Part 500-compliant entities may be adhering to a slightly more stringent standard than what is articulated in the Amended Rule.

  However, as with the banking regulators' standards, the Amended Rule's two-year time line for information disposal imposes a more concrete requirement than that found in Part 500. In addition, Part 500 provides asset- and revenue-based exemptions not found in the Amended Rule.

  For businesses that do not fall within the scope of either regulation, it may be worth considering whether the FTC's decision to adopt standards similar to Part 500 represents writing on the wall about the direction of cybersecurity regulation.

Conclusion. Financial institutions subject to the Amended Rule should get into compliance immediately. Certain provisions, like safeguards monitoring (without the new, strict requirement of "continuous monitoring" discussed above) and separate,

periodic risk assessments, take effect thirty days after the Amended Rule's publication in the Federal Register. Other amendments, like written risk assessments, information security program requirements, continuous monitoring or penetration and vulnerability testing, the appointment of a Qualified Individual, written reports, and an incident response plan do not take effect until one year after the Amended Rule's publication.

Although the Safeguards Rule ultimately imposes few net-new requirements on entities already subject to NY DFS Part 500 or federal banking regulators' standards, its provisions represent another entry in the canon of reasonable data security practices that may be referred to by other regulators, private litigants, and courts. A business that does not fall within the Amended Rule's scope may nevertheless find it worthwhile to assess the delta between the Amended Rule and the firm's current practices. Satisfying the new requirements of the Amended Rule not only bolsters an entity's argument for having "reasonable data security," but may keep it one step ahead of the next wave of regulation.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

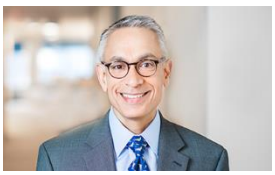
Avi Gesser
agesser@debevoise.com

Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com

Scott M. Caravello
smcaravello@debevoise.com

Corey Jeremy Goldstein
cjgoldstein@debevoise.com

WASHINGTON, D.C.



Satish M. Kini
smkini@debevoise.com

Lily D. Vo
ldvo@debevoise.com