The FTC's New Safeguards Rule

What It Says and What You Need to Do to Get Ready

November 11, 2021

COVINGTON

BEIJING BRUSSELS DUBAI FRANKFURT JOHANNESBURG LONDON LOS ANGELES
NEW YORK PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

www.cov.com

Presenters

Andrew Smith
Partner, Washington
+1 202 662 5654
asmith@cov.com

Andrew Smith advises clients on retail financial services, data protection, advertising and consumer protection, technology, credit reporting, and e-commerce issues, and regularly represents clients before federal and state agencies—particularly the FTC and CFPB—in law enforcement and rulemaking proceedings. From 2018 to 2021, Andrew served as Director of the Bureau of Consumer Protection at the FTC, where he was in charge of enforcing privacy, data security, financial services, and marketing laws and regulations across a broad range of areas, including fair lending, technology platforms, digital advertising, payments, telemarketing, lead generation, affiliate marketing, consumer reporting, and small business financing. He also oversaw the Bureau's extensive rulemaking and workshop proceedings, including on endorsement guides, security of financial data, subscription marketing, contact lenses, and children's privacy. Andrew is a Fellow of the American College of Consumer Financial Services Lawyers, and a former Chairman of the American Bar Association Committee on Consumer Financial Services.

Caleb Skeath
Associate, Washington
+1 202 662 5119
cskeath@cov.com

Caleb Skeath advises clients on a broad range of cybersecurity and privacy issues, including cybersecurity incident response, cybersecurity and privacy compliance obligations, internal investigations, regulatory inquiries, and defending against class-action litigation. He specializes in assisting clients in responding to a wide variety of cybersecurity incidents, ranging from advanced persistent threats to theft or misuse of personal information or attacks utilizing destructive malware. He has also advised numerous clients on assessing post-incident notification obligations under applicable state and federal law, developing communications strategies for internal and external stakeholders, and assessing and protecting against potential litigation or regulatory risk following an incident. In addition, he has advised several clients on responding to post-incident regulatory inquiries, including inquiries from the FTC and state Attorneys General. Caleb also holds a Certified Information Systems Security Professional (CISSP) certification.

Agenda

1. Introductions
2. Background on Safeguards Rule
3. Overview of Updates to Safeguards Rule
4. Recommendations to Prepare for Compliance
5. Questions

Background on Safeguards Rule

Background on Safeguards Rule

- **FTC issued its Safeguards Rule in 2002 (16 CFR Part 314).**
  - Must "develop, implement, and maintain a comprehensive information security program" in writing.
  - Must be appropriate to an entity's size and complexity, the nature and scope of its activities, and the sensitivity of any customer information at issue.

- **Program requirements:**
  - Designate employee(s) to coordinate the program;
  - Identify risks and assess sufficiency of safeguards to control these risks;
  - Design and implement safeguards to control risks;
  - Regularly test or monitor the effectiveness of safeguards;
  - Oversee service providers; and
  - Evaluate and adjust program in light of testing/monitoring and material changes.

Background on Safeguards Rule

2016

FTC solicits comments on Safeguards Rule.

2019

FTC publishes NPRM proposing changes to the Safeguards Rule.

2020

FTC holds workshop on proposed changes.

October 27, 2021

FTC releases final rule to be published in Fed. Reg.

- Most substantive changes will take place one year from publication in Fed. Reg.
- Also published a Supplemental NPRM that proposes a breach reporting requirement.

Why the Revised Rule?

- No revisions in 20 years
  - Significant enforcement experience (80+ cases)
  - Significant business guidance (such as, “Stick with Security”)
  - More consensus on reasonable practices
- Increased state regulation
  - Safeguards Rule had proven a model in the past
- Concerns about enforceability
- Providing a more concrete “checklist” and process
  - While still allowing flexibility, such as through compensating controls

Safeguards Enforcement Trends

PayPal/Venmo (2018)

- Failed to provide security notices to customers; failed to timely investigate compromised accounts

DealerBuilt (2019)

- Service provider to financial institutions (auto dealers)
- Failed to design and implement basic safeguards and to test or monitor the effectiveness of such safeguards

Ascension Data & Analytics (2020)

- Failed to oversee service providers
- Did not follow its own vendor management program

Overview of Updates to Safeguards Rule

COVINGTON

Key Updates to Safeguards Rule

Expanded Scope	Includes entities engaged in activities “incidental” to financial activities (e.g. finders). Also expands definitions to cover hard-copy as well as electronic information.
Risk Assessments	Must be in writing and address specific criteria.
Program Requirements	Significant additional details on what the information security program must address.
Program Oversight	Program must be overseen by a single “Qualified Individual,” with periodic reporting to the Board.
Exemptions	Entities that maintain records on fewer than 5,000 individuals are exempt from certain requirements.

Changes to Risk Assessment Requirement

- Risk assessments must be in writing and include:
  - Criteria for evaluation and categorization of identified security risks or threats;
  - Criteria for assessment of the confidentiality, integrity, and availability of information systems and customer information, including adequacy of existing controls; and
  - Requirements describing how the risks will be mitigated or accepted, and how the information security program will address the risks.
- Risk acceptance is appropriate if:
  - The chance that it will produce a security event is very small;
  - The consequences of the risk are minimal; or
  - The cost of mitigating the risk far outweighs the benefit.

Periodic additional assessments must be conducted.

Changes to Information Security Program Requirements

Implementation and periodic review of access controls, including limiting access to only the information each individual needs to perform their duties or functions

Identification and management of data, personnel, devices, systems, and facilities in accordance with their relative importance to business objectives and risk strategy

Encryption of customer information at rest, as well as in transit over external networks

Adoption of secure development practices for internally-developed applications, as well as procedures for evaluating, assessing, or testing externally-developed applications

Implementation of multi-factor authentication for any individual accessing any information system

Implementation of secure information disposal procedures for disposal of customer information within two years, unless retention is necessary for business purposes or legal obligations

Changes to Information Security Program Requirements

Adoption of change management procedures

Monitoring and logging of user activity

Regular testing or monitoring of the effectiveness of key controls, including either:

- "Continuous" monitoring or
- Annual penetration testing combined with vulnerability assessments at least every 6 months or upon material changes to operations

Providing risk-based security awareness training to employees

Utilizing "qualified information security personnel" to manage the information security program, providing updates and training to these personnel, and verifying that these personnel maintain current knowledge of threats and countermeasures

Maintaining oversight of service providers through pre-engagement due diligence, use of contractual provisions, and periodic assessments

Establishing a written incident response plan that addresses areas specified in the Final Rule

Changes to Program Oversight Requirements

- **A Qualified Individual must be designated as responsible for program oversight, implementation, and enforcement.**
  - Final Rule removes references to CISO title.
  - Only requirement is that the individual is qualified for oversight and enforcement of program.

- **The Qualified Individual must report in writing to Board of Directors (or equivalent).**
  - Report must occur at least annually.
  - Report must include:
    - The overall status of the program and compliance with the Final Rule.
    - Material matters related to the program, 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 program.

Proposed Breach Notification Requirements

Requires institutions to report security events to the FTC within 30 days of discovery if:

- Misuse of customer information has occurred or is reasonably likely; and
- At least 1,000 consumers may be affected.

Notification must include:

- The name and contact information of the reporting financial institution; A description of the types of information that were involved in the security event;
- The date or date range of the security event; and
- A general description of the security event.

Notifications must be submitted through an online form.

- FTC would make the information received publicly available.

SNPRM to be issued and open for comment for 60 days following publication in the Federal Register.

Recommendations to Prepare for Compliance

COVINGTON

Recommendations to Prepare for Compliance

Conduct a gap analysis

- Identify policies, processes, tools, and personnel already in place that address requirements
- Identify requirements that are not met and develop a plan to address them prior to effective date

Consider options for limiting exposure to requirements

- Exception for entities with fewer than 5,000 customer records
- Implementing network segmentation to isolate customer information

Focus on specific required artifacts that document compliance with requirements

- Technical controls (e.g. encryption, MFA)
- Written policies/procedures required as part of program (e.g. incident response plan)
- Periodic risk assessments, vulnerability assessments, and pen testing

Prepare for potential implementation of a breach notification requirement

- Anticipate that artifacts and documentation may be subject to regulatory scrutiny
- Balance assertions of privilege versus need to demonstrate compliance

Questions