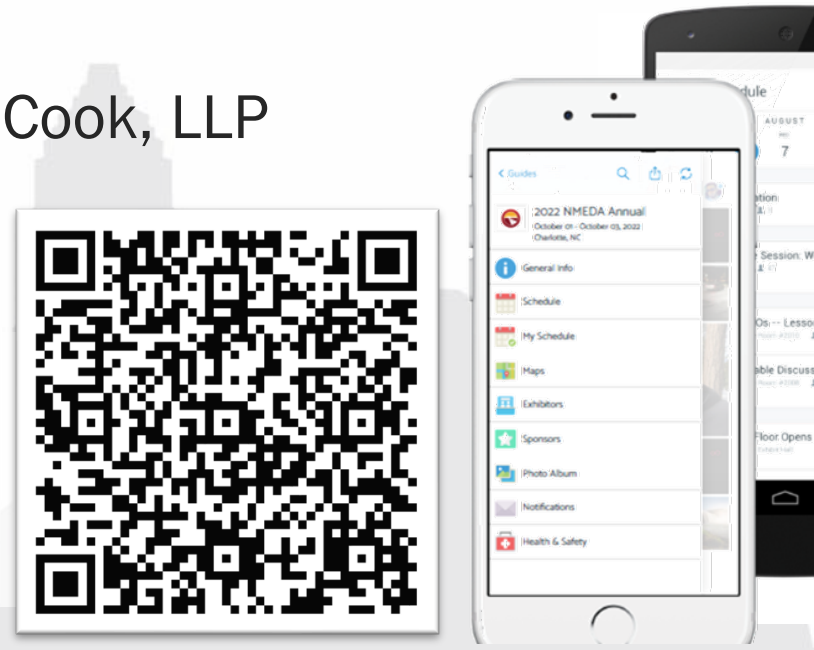
Time is ticking – Are you ready for the FTC's sweeping changes to the Safeguards Rule?

Presenter:

K. Dailey Wilson, Senior Associate – Hudson Cook, LLP

Download the Conference App

Submit session feedback right in the app!



Disclaimer

This presentation is provided for informational purposes only. The presentation is not intended to be an exhaustive review of all laws on any subject. We have made every effort to ensure that the information in this presentation is complete and accurate with respect to the topic(s) addressed. Hudson Cook, LLP and the individual presenter(s) are not responsible for any errors in or omissions from the information provided.

Nothing in this presentation should be construed as legal advice from Hudson Cook, LLP or the individual presenter, nor is the presentation a substitute for legal counsel on any matter. Legal advice must be tailored to specific facts and circumstances. No attendee of this presentation should act or refrain from acting solely on the basis of any information included in this presentation. Attendees should seek appropriate legal or other professional advice on legal matters specific to their business.

The views and opinions in this presentation are those of the presenter and do not necessarily represent official policy or position of Hudson Cook, LLP or of its clients.

Safeguards Rule Basics

Safeguards Rule: Pre-2021 Changes

- The Safeguards Rule requires a financial institution to develop, implement, and maintain a comprehensive information security program that consists of the administrative, technical, and physical safeguards the financial institution uses to:
  - *Access* customer information;
  - *Collect* customer information;
  - *Distribute* customer information;
  - *Process* customer information;
  - *Protect* customer information;
  - *Store* customer information;
  - *Use* customer information;
  - *Transmit* customer information;
  - *Dispose of* customer information; or
  - Otherwise *handle* customer information.

NMEDA 2022 ANNUAL CONFERENCE

Safeguards Rule: Pre-2021 Changes

- Must be a written program
  - Must be appropriate 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;
  - Reasonably designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of the information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer;
    - Include risk assessment and design/implement safeguards to control the risks identified through the risk assessment;
    - must regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures;
    - Must designate an employee or employees to coordinate the information security program; and
    - Take reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for customer information and require those service providers by contract to implement and maintain such safeguards.

Safeguards Rule: 2021 Rulemaking
Adoption of the Rule

- **Issue Date**: FTC approved October 27, 2021

- **Effective Dates**: For new *substantive* provisions, 1 year after publication in the Federal Register (published 12/9/2021, so **deadline is 12/9/2022**)
  - Sections 314.4(a) (designation of qualified individual), 314.4(b)(1) (written risk assessment), 314.4(c)(1)-(8) (implementation of specific safeguards, including MFA), 314.4(d)(2) (continuous monitoring or penetration testing), 314.4(e) (training and oversight), 314.4(f)(3) (periodic assessment of service providers), 314.4(h) (written incident response), and 314.4(i) (requirement of qualified individual to report in writing to board))
  - *Non-substantive* changes became effective 30 days after publication (January 10, 2022)

Safeguards Rule: 2021 Rulemaking
Who does the Rule apply to?

- The Rule applies to "financial institutions."
  - The term "financial institutions" is defined to mean any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k).
  - Under the Bank Holding Company Act, "activities that are financial in nature" include lending money. 12 U.S.C. § 1843(k)(4)(A). May be an employee, affiliate, or service provider.
  - "Activities that are financial in nature" also include any activity that the Federal Reserve Board has determined by order or regulation to be so closely related to banking or managing or controlling banks as to be proper incident thereto. 12 U.S.C. § 1843(k)(4)(F). 12 C.F.R. § 225.28(b)(1) provides that "making, acquiring, brokering, or servicing loans or other extensions of credit" is an activity that is so closely related to banking or managing or controlling banks as to be a proper incident thereto.

Safeguards Rule: 2021 Rulemaking
Exemption

- Exempts financial institutions that maintain customer information concerning fewer than 5,000 consumers from certain requirements, including the requirements:
  - to conduct a written risk assessment;
  - to conduct continuous monitoring or periodic penetration testing and vulnerability assessments;
  - to establish a written incident response plan; and
  - to regularly report in writing to the board of directors or equivalent governing body.

Safeguards Rule: 2021 Rulemaking
Qualified Individual

- Requires financial institutions to appoint a "qualified individual."
  - Qualified individual is responsible for overseeing, implementing, and enforcing the information security program.
  - Must be a single individual – multiple people cannot be appointed as the "qualified individual."
  - May be an employee, affiliate, or service provider.
  - No particular level of education, experience, or certification is required.

Note: Requirements that do not apply to exempt institutions are noted with an asterisk (*) in this presentation

Safeguards Rule: 2021 Rulemaking
Written Risk Assessment*

- Must base information security program on a risk assessment.
  - Must be in writing.
  - Must include:
    - Criteria for evaluating and categorizing identified security risks or threats.
    - Criteria for assessing the confidentiality, integrity, and availability of information systems and customer information, including the adequacy of existing controls; and
    - A description of how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address those risks.

Safeguards Rule: 2021 Rulemaking
Changes to Program Requirements

- Adds provisions regarding how to develop and implement specific aspects of an information security program.
  - Requires financial institutions to **encrypt** all customer information held or transmitted by the financial institution over external networks and at rest.
  - Requires financial institutions to implement **multifactor authentication** for all information systems.
  - Requires financial institutions to develop, implement, and maintain procedures for the **secure disposal** of customer information.

Safeguards Rule: 2021 Rulemaking
Regular Testing and Monitoring*

- Financial institutions must regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.
  - Must include continuous monitoring or periodic penetration testing and vulnerability assessments.
    - *Penetration Testing*: a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems.
    - Vulnerability assessments must be conducted every 6 months; whenever there are material changes to operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.

Safeguards Rule: 2021 Rulemaking
Policies, Procedures and Training

- Must implement policies and procedures to ensure that personnel are able to enact the information security program by:
  - Providing personnel with security awareness training;
  - Using qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and perform or oversee the information security program;
  - Providing information security personnel with security updates and training sufficient to address relevant security risks; and
  - Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

Safeguards Rule: 2021 Rulemaking
Oversee Service Providers

- Must oversee service providers by:
  - Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;
  - Requiring your service providers by contract to implement and maintain safeguards; and
  - Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.

Safeguards Rule: 2021 Rulemaking
Written Incident Response Plan*

- Requires financial institutions to establish a written incident response plan, which must include:
  - The goals of the incident response plan;
  - The internal processes for responding to a security event;
  - The definition of clear roles, responsibilities, and levels of decision-making authority;
  - External and internal communications and information sharing;
  - Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
  - Documentation and reporting regarding security events and related incident response activities; and
  - Evaluation and revision of the incident response plan as necessary following a security event.

Safeguards Rule: 2021 Rulemaking
Reporting Requirements*

- The Qualified Individual must report, in writing, regularly and at least annually, to the board of directors or other equivalent governing body regarding:
  - Overall status of the information security program;
  - Compliance with the Safeguards Rule;
  - Material matters related to the information security program, including issues related to risk assessment, risk management and control decisions, service provider arrangements, results of any testing, security events, management's response to security events, and recommendations for any changes to the information security program.

Next Steps

Next Steps

- Hire or appoint a “qualified individual”.
- Take an inventory of what you already have:
  - Existing written information security program?
  - Existing security measures (both physical and technological)?
  - Existing network elements (applications, databases, operating systems, etc.)?
  - What kinds of data are currently maintained?
  - Who are the “users”?
- Conduct a written risk assessment.
- Revise or establish a written information security program based on the risk assessment.

Next Steps

- Revise or establish a written incident response plan.
- Implement any necessary physical or technological safeguards, like encryption software, multifactor authentication, etc.
- Develop and implement a training program for employees.
- Develop a service provider oversight program, including contractual requirements that service providers implement and maintain safeguards.

QUESTIONS?

Contact Information

Dailey Wilson
Hudson Cook, LLP
Ooltewah, TN
☎ 423.490.7567
✉ dwilson@hudco.com

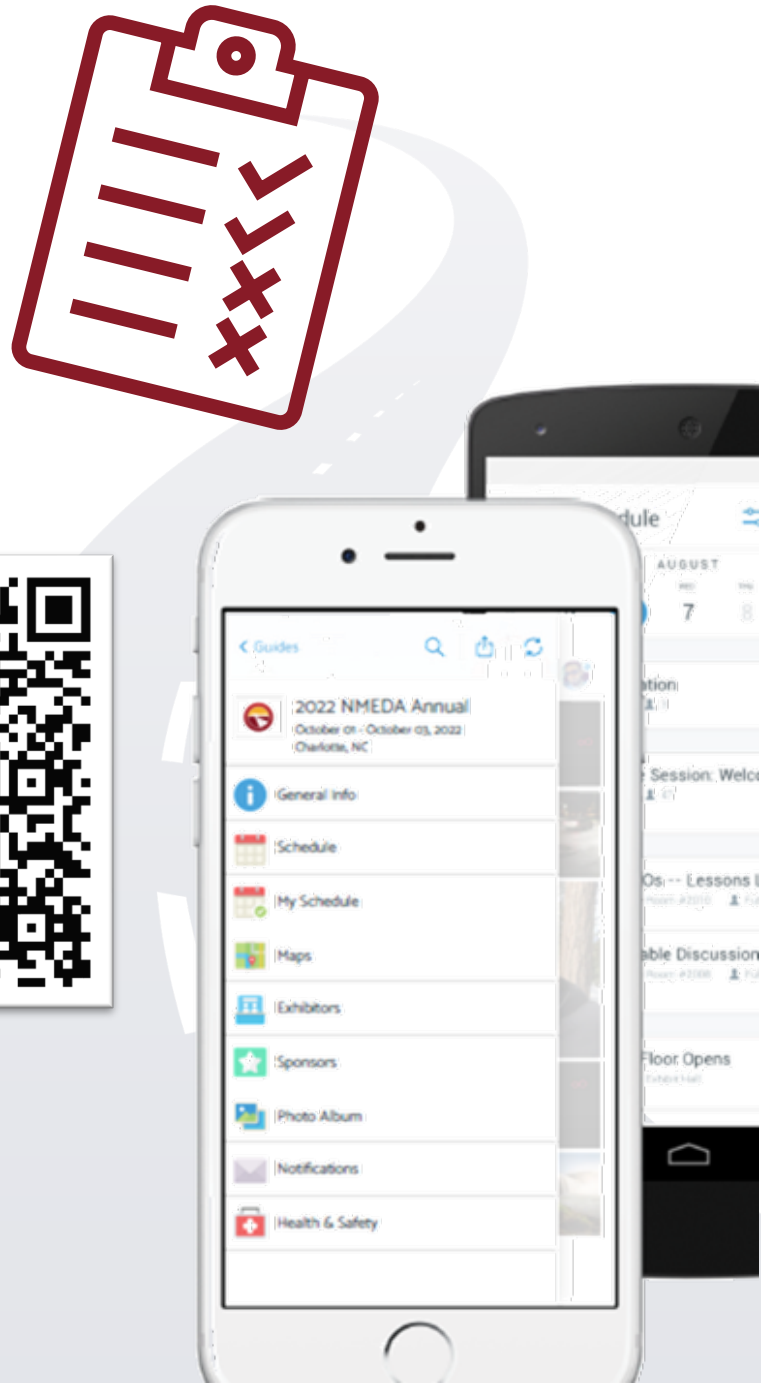
NMEDA 2022 ANNUAL CONFERENCE

DON'T FORGET YOUR SURVEY!

- Use the conference app and complete the survey found in the "schedule" for this session

OR

- Complete a paper survey



THANK YOU!

NMEDA 2022 ANNUAL CONFERENCE