Webinar

Reporting a Data Breach: FTC Amendment to the Safeguards Rule

Presenters:
Eric Johnson, Partner - Hudson Cook, LLP
K. Dailey Wilson, Partner - Hudson Cook, LLP

DISCLAIMER

The Association of Dealership Compliance Officers (ADCO) provides articles, webinars, and other content, provided both by attorneys and by other outside authors, for education purposes only. ADCO does not warrant the accuracy or completeness of the content in the webinars, compliance interviews, and workshops and has no duty to correct or update such information. The views and opinions in the content contained in ADCO sponsored webinars do not constitute the views and opinion of the Association. Provided content does not constitute legal advice from such authors, presenters or from ADCO.

For legal advice on a matter, one should seek the advice of counsel.

ASSOCIATION
OF DEALERSHIP
COMPLIANCE OFFICERS

Eric L. Johnson
Partner
405.602.3812
ejohnson@hudco.com
918 S.W. 117th Street, Suite 200
Oklahoma City, OK 73170

Eric is a partner in Hudson Cook's Oklahoma City office and Editor in Chief of CounselorLibrary.com's *Spot Delivery* publication. He assists motor vehicles dealers and automotive finance companies in the development and maintenance of nationwide automobile finance programs; online motor vehicle sales programs; and Compliance Management Systems.

Eric serves as Chair to the Legal Committee for the National Automotive Finance Association and is a co-founder and co-instructor of their Consumer Credit Compliance Certification and Certificate Programs. Eric is a Fellow of the American College of Consumer Financial Services Lawyers. He also serves as President of the Governing Committee for The Conference on Consumer Finance Law and as Update Chair of the Financial Institutions and Commercial Law Section of the Oklahoma Bar Association. He is a member of the American Bar Association (Business Law Section; Banking, Commercial Finance and Consumer Financial Services Committees) and a member of the National Association of Dealer Counsel. Eric is listed in the 2023 edition of The Best Lawyers in America® in the practice areas of Banking and Finance Law, Commercial Litigation, Financial Services Regulation Law and Litigation-Banking & Finance. Eric speaks frequently across the country on the legal and business issues shaping the financial services industry.

K. Dailey Wilson
Partner
423.490.7567
dwilson@hudco.com
9431 Bradmore Lane, Suite 201
Ooltewah, TN 37363

Dailey is a partner in the firm's Tennessee office. She focuses her practice on federal and state regulatory compliance for rent-to-own providers and other alternative financial services providers. Dailey frequently assists clients with drafting consumer-facing documentation, developing internal policies and procedures, and completing audits for compliance with state and federal law. Dailey advises various financial institutions and others on compliance with data use and security laws, including the Safeguards Rule. Dailey works closely with clients to develop data security compliance strategies, including in connection with risk assessments, information security programs, written incident response plans, vendor management, and due diligence matters.

Dailey received her law degree *cum laude* in 2012 from the University of Georgia School of Law. She holds a Bachelor of Arts *magna cum laude* in History from the College of Charleston.

She is admitted to practice in Georgia and Tennessee.

HUDSON COOK

Reporting a Data Breach: 2023 FTC Safeguards Rule Changes

Eric L. Johnson and K. Dailey Wilson

November 29, 2023

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.

HUDSON COOK

SAFEGUARDS RULE BASICS

Safeguards Rule

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

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.

Safeguards Rule

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

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

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

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

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

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

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.

Safeguards Rule

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.

HUDSON COOK

2023 Amendment

2023 Amendment

What is a “Notification Event”?

- The term “notification event” means the acquisition of unencrypted customer information, or encrypted information along with the encryption key, without the authorization of the individual to which the information pertains.
  - Requires notification for the unauthorized access of *any* customer information.
  - The Safeguards Rule defines the term “customer information” to essentially mean any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates. This includes:
    - information a consumer provides to you on an application to obtain a credit transaction;
    - payment history;
    - account balance information;
    - the fact that an individual is or has been one of your customers or has obtained a financial product or service from you;
    - any information a consumer provides to you or that your or your agent otherwise obtain in connection with collecting on, or servicing, a credit account; and
    - information from a consumer report.

2023 Amendment

When is Notification Required?

- Financial Institutions must notify the FTC “as soon as possible” but no later than 30 days after the discovery of the notification event.
- A notification event is considered “discovered” as of the 1st day on which you receive knowledge of the notification event.
  - Deemed to have knowledge of a notification event if the notification event is known to any employee, officer, or other agent of the financial institution (other than the person committing the breach).
- No delay in providing notification to FTC for law enforcement investigation.

2023 Amendment

What Notification is Required?

- Must be made on an electronic form made available from the FTC on its website.
- Notification must include the following:
  - Company's name and contact information;
  - Description of the types of information that were involved in the notification event;
  - Date or date range of the notification event, if that information is possible to determine;
  - Number of consumers affected or potentially affected;
  - General description of the notification event; and
  - Whether any law enforcement official has provided the financial institution with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security and a means for the FTC to contact the law enforcement official.

2023 Amendment

Law Enforcement Delays

- Law enforcement delay only affects whether FTC publicizes information about the notification event to the public – Must notify the FTC of a notification event within the required time period no matter what.
- Law enforcement official may request an initial delay in notifying the public of up to 30 days following the date when the notice was provided to the FTC.
- Law enforcement official may request an extension up to an additional 60 days.
  - Request must be in writing.
  - FTC must determine that public disclosure of the breach continues to impede a criminal investigation or cause damage to national security.

2023 Amendment

Effective Date

- 2023 Amendment was published in *Federal Register* on November 13, 2023
- 2023 Amendment is effective May 13, 2024 (less than 6 months away)

Q&A

Contact Information

Eric Johnson
Hudson Cook, LLP
☎405.602.3812
✉ ejohnson@hudco.com

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

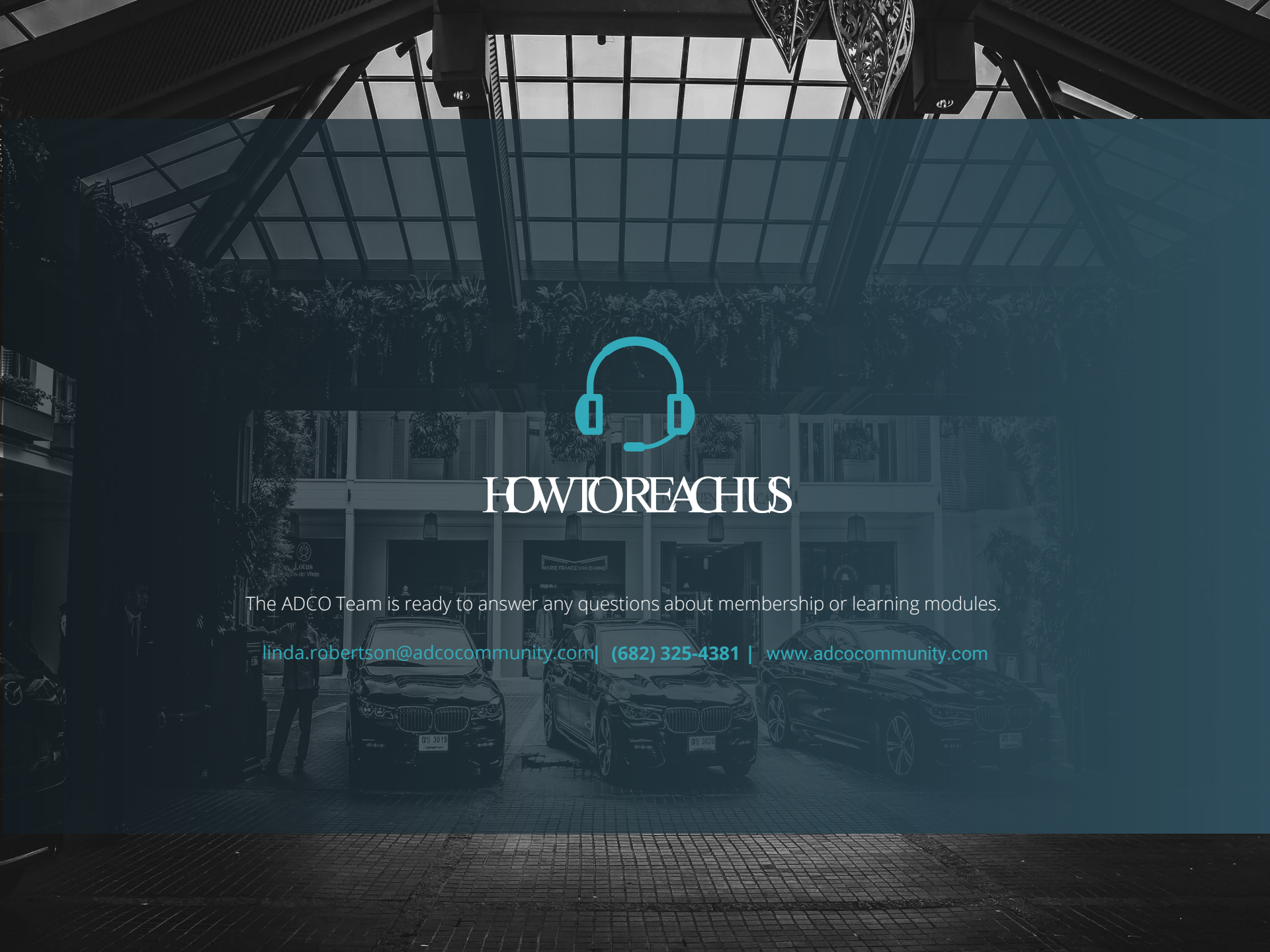
Follow Hudson Cook

THANK YOU

ABOUT ADCO

REDUCE RISK. BUILD TRUST. DELIVER VALUE

The mission of the Association of Dealership Compliance Officers is to reduce business risk for the dealer, protect the dealer's bottom line, and enhance the reputation of the dealership within the community.



HOW TO REACH US

The ADCO Team is ready to answer any questions about membership or learning modules.

linda.robertson@adcocommunity.com| **(682) 325-4381** | www.adcocommunity.com