Data Privacy and Data Security – What Every Compliance Professional Should Know

July 18, 2023

1

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. The individual presenter(s) and their respective law firms, Hudson Cook, LLP and Troutman Pepper, are not responsible for any errors in or omissions from the information provided.

Nothing in this presentation should be construed as legal advice, 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 presenters and do not necessarily represent official policy or position of Hudson Cook, LLP, Troutman Pepper, or their clients.

2

Complying with the FTC Safeguards Rule

Safeguards Rule Basics

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 was 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)

- HOWEVER, FTC granted extension to December 9th compliance date. **New compliance date is June 9, 2023**.

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). Examples include collection agency services, credit bureau services, acquiring debt in default, and providing educational courses and instructional materials to consumers on individual financial matters.

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.

Regular Testing and Monitoring*

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.

CFPB Guidance

CFPB Circular 2022-04: August 11, 2022

- States that inadequate security for sensitive customer information collected, processed, maintained, or stored by a company can constitute an unfair practice.
  - Inadequate authentication, password management, or software update policies or practices are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers.
  - Financial institutions are unlikely to be able to justify weak data security practices based on countervailing benefits to consumers or competition.
  - Inadequate data security can be an unfair practice in the absence of breach or intrusion.

CFPB IT Examination Procedures

- Published September 20th, 2021.
- CFPB Examination Procedures include an evaluation of the technology controls of an institution and its service providers.
  - Includes inquiries regarding:
    - whether the institution has an information security program;
    - whether the institution has an effective risk management program, including risk identification, risk assessment, and risk mitigation;
    - whether compliance policies and procedures are designed to effectively manage IT controls and compliance risk in the products, services, and activities of the institution; and
    - whether the institution has effective IT training for employees.

Lessons from FTC Data Security Actions

19

- FTC frequently uses its UDAP authority to take action for perceived data security failures.
  - Since 2019, the FTC has taken 12 cybersecurity actions.
- FTC has used both the unfairness and deception prongs.
  - Unfairness is often used when a data breach has occurred.
  - Deception is used when entities make misleading claims about their data security practices on their websites or in their privacy policies.

OLA
Online Lenders Alliance

20

Lesson 1 – No One is Safe

- Of the 12 data security actions the FTC has taken since 2019, only 2 of those have arisen under the Safeguards Rule.
- The FTC uses its UDAP authority to take action against non-financial institutions for data security failures.
  - Recent subjects of FTC actions include: CafePress, Drizly, and Chegg.
- The FTC will also hold individuals liable.
  - James Cory Rellas, CEO of Drizly, was found individually liable for failing to use appropriate information security practices.
    - Rellas did not implement, or properly delegate the responsibility to implement reasonable security practices.
    - Rellas hired senior executives dedicated to finance, legal, marketing, retail, human resources, product, and analytics, but failed to hire a senior executive responsible for information security.

Lesson 2 – MFA is Expected

- FTC frequently orders entities to implement multi-factor authentication ("MFA") for both consumers and employees.
- MFA Takeaways From Recent Orders:
  - Phishing-resistant forms of MFA, like security keys, are preferred.
  - Legacy authentication practices, like security questions, should be replaced with MFA.
  - Steer away from forms of MFA that require provision of telephone numbers.
  - Do not use information collected for MFA for any other purpose.

Lesson 3 – Implement Encryption

- FTC increasingly requiring customer information to be encrypted both in transit and at rest.
  - Many email communications are already encrypted in transit. BUT, if your email system is not encrypting customer information you should move towards a system that does ASAP.
  - Encryption at rest is not as common.
    - Data at rest is information stored on hard drives, cloud storage, databases, etc. that is not being actively used. Data at rest is attractive to hackers because it often includes highly sensitive customer information.
  - FTC has begun encouraging use of "Zero Trust" security models.
    - "Zero Trust" is based on the idea that just because you are on a network doesn't mean you should automatically be trusted to access everything.
    - Instead, users should have to be authenticated and authorized to access a system and connections should be encrypted. This means if a hacker is able to get into the system, the hacker won't automatically have access to the entire network.

Lesson 4 – Develop a Data Retention Schedule and Disposal Plan

- FTC routinely requires entities to develop a data retention schedule addressing the following:
  - The purpose or purposes for which each type of information is collected;
  - The specific business needs for retaining each type of information; and
  - A timeframe for deletion of each type of information that precludes indefinite retention of information.
- Routinely destroying unneeded customer information limits the amount of customer information that can be exposed in the event of a data breach.
- Knowing the types of customer information you store helps you determine the types of safeguards necessary to adequately protect that information.

Lesson 5 – Don't Make Express Claims About Security

- A review of recent FTC data security actions reveals that companies are often making claims about the level of security they employ.
  - Example: "Chegg takes commercially reasonable security measures to protect the Personal Information submitted to us, both during transmission and once we receive it."
  - Example: "Security. All information we collect is securely stored within our database, and we use standard, industry-wide, commercially reasonable security practices such as 128-bit encryption, firewalls, and SSL (Secure Socket Layers)."
  - Example: "CafePress also pledges to use the best and most accepted methods and technologies to insure your personal information is safe and secure."
- The best practice is to not make any express statements about the level of security you employ.
- If you do make data security claims, make sure they are accurate and that you can back them up.

OLA Online Lenders Alliance

FTC Privacy Rulemaking

- On August 16, 2022, the FTC announced an advance notice of proposed rulemaking (ANPR) to request public comment on the prevalence of harmful commercial surveillance and data security practices.
  - Initiated under section 18 of the FTC Act to limit privacy abuses, curb lax security practices, and ensure that algorithmic decision-making does not result in unlawful discrimination.
- On September 8, 2022, the FTC also hosted a public forum regarding its ANPR on commercial surveillance and data security practices that harm consumers and competition.
- The FTC invited public comments on whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies:
  - (1) collect, aggregate, protect, use, analyze, and retain consumer data, as well as
  - (2) transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive.
- The ANPR's extended public comment period closed on November 21, 2022. FTC Staff are reviewing the public comments. There is no announced timeline on next steps.

CFPB Privacy Rulemaking

- Section 1033 Rulemaking - Consumer Access to Financial Records
  - Characterized as a rulemaking on Personal Financial Data Rights
  - Will establish standards to promote the development and use of standardized formats for information made available to consumers
  - Focus: (1) promote open banking and (2) facilitate data aggregation
- Timeline
  - October 2016: Initial Request for Information
  - October 2017: Consumer Protection Principles for Consumer-Authorized Financial Data Sharing and Aggregation
  - February 2020: Consumer Access to Financial Records Symposium
  - October 2022: Advance Notice of Proposed Rulemaking
  - February 2023: Small Business Review Panel for Personal Financial Data Rights
  - October 2023: notice of proposed rulemaking

Federal Privacy Legislation

- No major legislation introduced so far in 2023.
- On March 1, 2023, the House Energy & Commerce Committee's Subcommittee on Innovation, Data and Commerce held a hearing to discuss reintroducing the American Data Privacy and Protection Act (ADPPA) from last year.
- Key issues requiring resolution:
  - Preemption of state privacy laws
  - Private right of action

State Privacy Laws Timeline

January 1, 2023

- California Privacy Rights Act amendments to the California Consumer Privacy Act
- Virginia Consumer Data Protection Act

July 1, 2023

- California Privacy Rights Act enforcement date
- Colorado Privacy Act
- Connecticut Act Concerning Personal Data

December 31, 2023

- Utah Consumer Privacy Act

July 1, 2024

- Texas Data Privacy and Security Act

October 1, 2024

- Montana Consumer Data Privacy Act

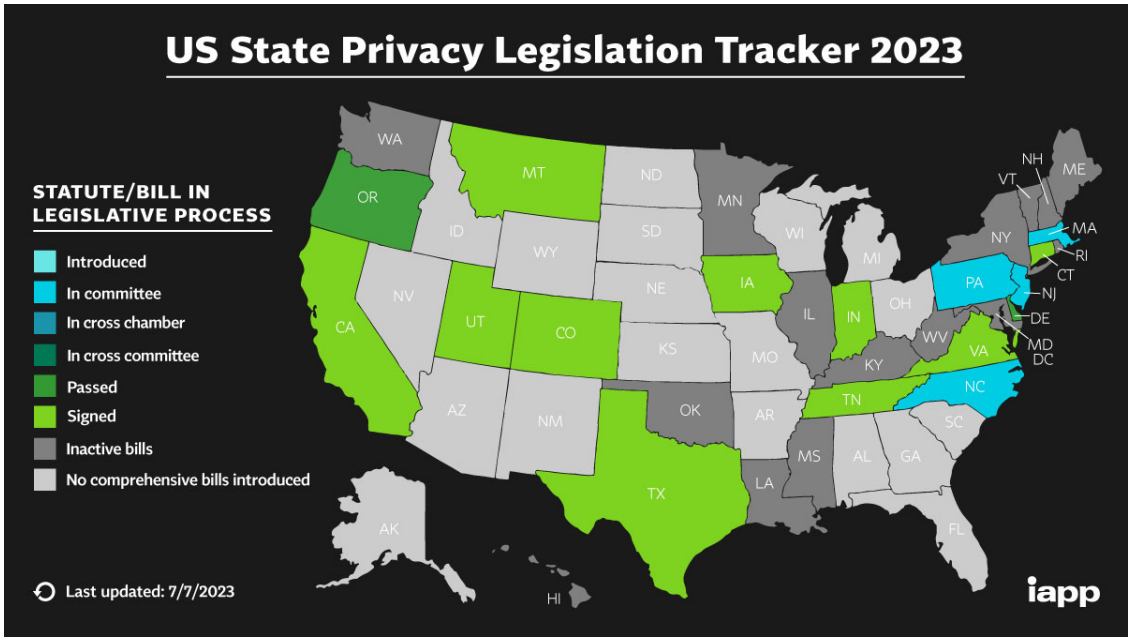
January 1, 2025

- Colorado Privacy Act regulations
- Iowa Consumer Data Protection Act
- Tennessee Information Protection Act

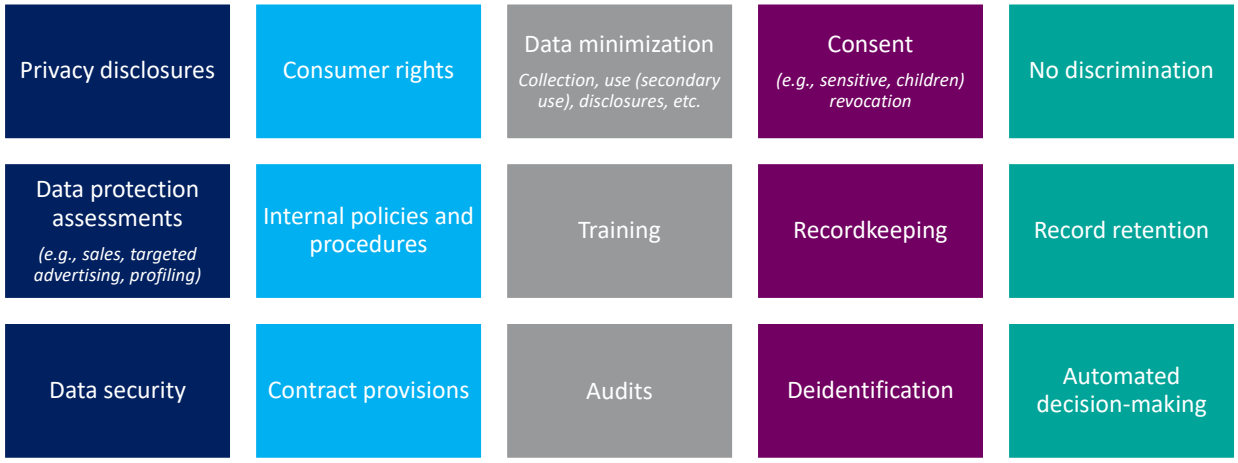
January 1, 2026

- Indiana Consumer Data Protection Act

State Privacy Legislation



State Privacy Laws – Business Requirements



State Privacy Laws – Enforcement

- California
  - California Privacy Protection Agency / Attorney General
  - Up to $2,500 per violation
  - *Sephora* $1.2 million settlement and consent order
  - Warning letters
- Colorado
  - Attorney General / District Attorneys
  - Up to $20,000 per violation
  - Warning letters

Questions?

Presenters

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

Kim Phan
Partner
Troutman Pepper
☎ 202.274.2992
✉ kim.phan@trouman.com

OLA
Online Lenders Alliance