Online Lenders Alliance

Maintaining Data Security in an Ever-Changing World

July 16, 2024

Kim Phan
Troutman Pepper
kim.phan@troutman.com
(202) 274-2992

Alexander Cox
Locke Lord
alex.cox@lockelord.com
(860) 541-7756

COMPLIANCE UNIVERSITY

Online Lenders Alliance

FEDERAL SECURITY DEVELOPMENTS

COMPLIANCE UNIVERSITY

COMPLIANCE UNIVERSITY

OLA Online Lenders Alliance

FTC GLBA Data Breach Notification Rule

- NON-BANK FINANCIAL INSTITUTIONS ONLY!
- Notice of any unauthorized acquisition of unencrypted data affecting over 500 consumers must be provided no later than 30 days after discovery.
- The notice must contain the following information:
  - (1) the name and contact information of the reporting financial institution;
  - (2) a description of the types of information that were involved in the notification event;
  - (3) if the information is possible to determine, the date or date range of the notification event;
  - (4) the number of consumers affected;
  - (5) a general description of the notification event; and
  - If applicable, 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.

- NOTICES WILL BE POSTED TO FTC'S PUBLICLY AVAILABLE DATABASE.

COMPLIANCE UNIVERSITY

Online Lenders Alliance

SEC Cybersecurity Disclosure Rule

- Notice to the SEC within 4 days
- Disclosure of material cybersecurity incidents on Form 8-K
- Requires disclosure of cybersecurity incidents within four business days of a materiality determination (not discovery)
- Must include the nature, scope, and timing of the incident; and any reasonably likely material impacts on financial condition or operations
- Only disclosure delay for substantial risk to national security or public safety as determined by the U.S. attorney general
- Periodic disclosure of cybersecurity risk management, strategy, and governance in Form 10-K annual reports
- Requires sufficient detail for a reasonable investor to understand processes for assessing, identifying, and managing material risks from cybersecurity threats
- Must include descriptions of the board's oversight of cybersecurity risk and management's role in assessing, managing, and reporting to the board about material cybersecurity risk

CISA Cyber Incident Reporting Proposed Rule

- On March 15, 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was signed into law.
- Proposed rules would require covered entities designated as critical infrastructure (including the financial sector) to report to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA):
  - Within 72 hours after reasonably believing that a covered cyber incident has occurred, and
  - Within 24 hours after a ransom payment has been made.
- Reporting must include specified content.
- Record preservation requirements for no less than two years.
- Public comment period ends on June 3, 2024.

COMPLIANCE UNIVERSITY

OLA Online Lenders Alliance

NIST Cybersecurity Framework Update

- As our business grows, how often are we reviewing our cybersecurity strategy?
- Do we need to upskill our existing staff, hire talent, or engage an external partner to help manage cybersecurity?
- What are our most critical business assets to protect?
- What technologies or services are personnel using to accomplish their work?
- Are we restricting access and privileges only to those who need it?
- How are we securely sanitizing and destroying data and data storage devices?
- How is our business monitoring its logs and alerts to detect potential cyber incidents?
- Have we practiced our incident response plan?
- How do we ensure that recovery steps are not introducing new vulnerabilities?

Online Lenders Alliance

FEDERAL PRIVACY DEVELOPMENTS

COMPLIANCE UNIVERSITY

CFPB FCRA Proposed Rule

- On June 11, 2024, the CFPB proposed draft rules under the Fair Credit Reporting Act (FCRA) banning medical debts from consumer reports.
- On September 21, 2023, the CFPB had issued a proposed outline for its FCRA rulemaking. Many of the topics contained in that outline were not included in the draft rules:
  - Redefining "consumer reporting agency" to include data brokers and credit header data.
  - New interpretations of "permissible purpose" relating to written instructions, legitimate business need, and data breaches.
  - Imposing new furnisher obligations to investigate legal disputes and systemic disputes.

COMPLIANCE UNIVERSITY

OLA Online Lenders Alliance

CFPB Section 1033 Proposed Rule

- On October 19, 2023, the CFPB issued the draft rules.
  - Data provider requirements to deploy developer interfaces.
  - Authorized third-party obligations to obtain consent, capture revocations, limit secondary uses, and delete consumer financial records without reauthorization on an annual basis.
- Supplemental rulemakings to address mortgage, auto finance, and student loans.

- On June 5, 2024, the CFPB issued a final rule on recognizing standard-setting bodies for the development of data formats to be used by industry participants under the Section 1033 rules.

Online Lenders Alliance

STATE SECURITY DEVELOPMENTS

COMPLIANCE UNIVERSITY

COMPLIANCE UNIVERSITY

OLA Online Lenders Alliance

State Breach Notification Law Update

- Utah now requires AG notification. (5/1/24)
- Texas AG shortened to 30 days. (9/1/23)
- Florida Adds biometric and geolocation information. (7/1/24)
- Pennsylvania adds online credentials, medical, and health insurance information. (5/2/23)

COMPLIANCE UNIVERSITY

Online Lenders Alliance

Changes to the NY DFS Cybersecurity Regulation

Effective November 1, 2023, Compliance began Dec 1, 2023.

- 30 days (December 1, 2023) new requirements for the annual certification of compliance, and notices of extortion payments (Section 500.17).
- One year (November 1, 2024) new governance requirements (Section 500.4), encryption (Section 500.15), and incident response and business continuity (Section 500.16); and for the changes to the limited exemptions (Section 500.19(a)).
- 18 months (May 1, 2025) vulnerability scans (Section 500.5(a)(2)), access privileges (Section 500.7), and monitoring and training (Section 500.14(a)(2) and (b)).
- Two years (November 1, 2025) multi-factor authentication (Section 12), asset management and data retention (Section 500.13(a)).

Requirements overhaul, changes to limited exemptions

- Class A, Small Business (MFA/training), Governance, MFA, Training, Partial compliance,

Notification changes

- Ransomware and extortion payments

Online Lenders Alliance

STATE PRIVACY DEVELOPMENTS

COMPLIANCE UNIVERSITY

COMPLIANCE UNIVERSITY

Online Lenders Alliance

New State Comprehensive Privacy Laws

- Texas and Oregon Effective 7/1/24
- Montana Effective 10/1/24

Applicability changes

- Texas bringing a new standard
- GLBA entity exemption nuances, new pattern.

Same issues, expanded jurisdictions; 1/25 (DE, IA, NE, NH NJ)

COMPLIANCE UNIVERSITY

OLA Online Lenders Alliance

Privacy Assessments and Colorado

"Data Protection Assessments" or similar

- To be required in CA (Pending final regulations)
- In 2024, required in CO, CT, MT, VA, OR, TX
- Colorado AI Disclosures, more impact assessments (2026)

Regulations from CO provide guidance, other states rely (publicly CT & OR)

- Documentation, US to resemble EU/UK

OLA
Online Lenders Alliance

Thank you!

Questions??

COMPLIANCE UNIVERSITY