CYBERSECURITY AND DATA PRIVACY

EMERGING TECHNOLOGY CHALLENGES FOR FINANCIAL INSTITUTIONS

A Regulatory Perspective for Banks, Non-Bank Lenders, Mortgage Brokers, and Tech Enabled Service Providers

Northeast Mortgage Summit

February 26-27, 2025

Mohegan Sun, Uncasville, CT

Garris Horn LLP

INTRODUCTION

Cybersecurity and Data Privacy Risks in Financial Services

Regulatory Compliance: Security and Privacy Requirements

Understanding Regulatory Enforcement

Cybersecurity and Data Privacy Policies and Procedures

Importance of Security and Privacy Obligations in Contracts

REGULATORY COMPLIANCE OVERVIEW

CYBERSECURITY AND DATA PRIVACY OBLIGATIONS

Each financial institution and third-party service provider needs to understand the specific regulatory authority that they are subject to in order to understand how to manage cybsecurity and data privacy obligations

Federal Banking Agencies

OCC, NCUA, FDIC and Federal Reserve Board

Consumer Financial Protection Regulators

The Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC)

State Banking Regulators

Enforcement of State Security and Privacy Laws

State Attorneys General

Enforce Cybersecurity, Data Privacy, and Consumer Protection Laws.

OFFICE OF THE COMPTROLLER OF THE CURRENCY (OCC)

Who is Subject to OCC Enforcement?

National banks; Federal Savings Associations; and Federally Chartered Branches of Foreign Banks

Enforceable Laws

Gramm-Leach-Bliley Act (GLBA) Safeguards Rule – Requires financial institutions to protect consumer financial data.

Bank Secrecy Act (BSA) – Mandates security controls to detect and prevent financial crimes.

Computer-Security Incident Notification Rule – Requires timely reporting of cybersecurity incidents to regulators.

Consumer Financial Protection Act (CFPA) (UDAAP) – OCC can refer deceptive cybersecurity practices to CFPB for enforcement.

Available Penalties and Damages for Violations

Civil Money Penalties (CMPs):

Up to $2.5 million per day for willful violations.

Mandatory Security Upgrades

Required implementation of stronger security controls.

Consumer Compensation

Reimbursement for financial losses due to breaches.

Institutional Corrective Actions

Regulatory scrutiny, enhanced capital requirements, or restrictions on operations.

NATIONAL CREDIT UNION ADMINISTRATION (NCUA)

Who is Subject to NCU Enforcement?

Federally Insured Credit Unions

Enforceable Laws

GLBA Safeguards Rule – Requires CU's to maintain an information security program.

Federal Credit Union Act (FCUA) – Authority to supervise CU's and enforce risk management policies.

Computer-Security Incident Notification Rule – CU's must report significant cybersecurity events.

CFPA (UDAAP) – NCUA may refer deceptive cybersecurity practices to the CFPB.

Available Penalties and Damages for Violations

Civil Money Penalties (CMPs):

Up to $1 million per day for severe security breaches

Cease-and-Desist Orders

Immediate cybersecurity remediation requirements.

Consumer Restitution

Compensation for financial losses suffered by credit union members

Revocation of Federal Credit Union Charter

For repeated cybersecurity noncompliance.

FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)

Who is Subject to FDIC Enforcement?

State-Chartered Banks and Thrifts that are not members of the Federal Reserve System (state non-member banks); and Insured State Savings Associations

Enforceable Laws

Gramm-Leach-Bliley Act (GLBA) Safeguards Rule – Requires financial institutions to protect consumer financial data.

Bank Secrecy Act (BSA) – Mandates security controls to detect and prevent financial crimes.

Computer-Security Incident Notification Rule – Requires timely reporting of cybersecurity incidents to regulators.

Consumer Financial Protection Act (CFPA) (UDAAP) – FDIC can refer deceptive cybersecurity practices to CFPB for enforcement.

Available Penalties and Damages for Violations

Civil Money Penalties (CMPs):

Fines up to $2.5 million per day for systemic cybersecurity failures.

Cease-and-Desist Orders

Immediate correction of cybersecurity deficiencies.

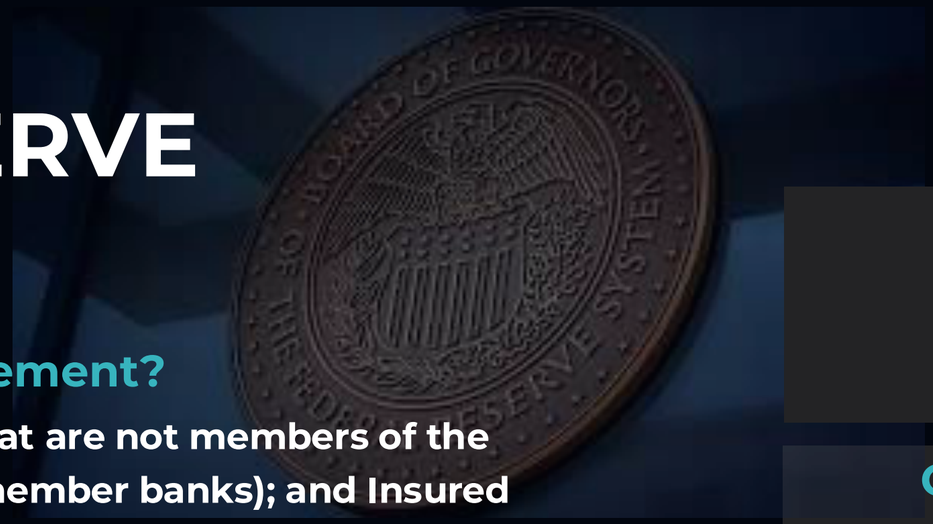
Restitution and Consumer Compensation

Reimbursement for financial losses due to breaches.

Institutional Corrective Actions

Regulatory scrutiny, enhanced capital requirements, or restrictions on operations.

FEDERAL RESERVE BOARD (FRB)



Who is Subject to FRB Enforcement?

State-Chartered Banks and Thrifts that are not members of the Federal Reserve System (state non-member banks); and Insured State Savings Associations

Enforceable Laws

GLBA Safeguards Rule – Requires financial institutions to secure consumer data.
Dodd-Frank Act – Enhanced Prudential Standards – Requires large institutions to implement risk-based cybersecurity measures.
Bank Holding Company Act (BHCA) – Authorizes Federal Reserve oversight of cybersecurity risk management at BHCs.
Computer-Security Incident Notification Rule – Requires timely reporting of cybersecurity incidents to regulators.
Consumer Financial Protection Act (CFPA) (UDAAP) – FRB can refer deceptive cybersecurity practices to CFPB for enforcement.

Available Penalties and Damages for Violations

Civil Money Penalties (CMPs):

Fines up to $2.5 million per day for knowing violations

Restitution Orders

Mandatory compensation to affected consumers for security lapses.

Disgorgement of Profits

Requiring banks to forfeit ill-gotten gains from noncompliant security practices.

Increased Supervision and Reporting Requirements

Regulatory scrutiny, enhanced capital requirements, or restrictions on operations.

CONSUMER FINANCIAL PROTECTION BUREAU (CFPB)

Who is Subject to FRB Enforcement?

Non-Bank Financial Institutions, including IMBs, Servicers, and Payday Lenders; Credit Reporting Agencies; Debt Collectors; and, Large Banks and Financial Service Providers under CFPB jurisdiction

Enforceable Laws

Consumer Financial Protection Act (CFPA) – Prohibits unfair, deceptive, or abusive acts or practices (UDAAPs).

GLBA Privacy and Safeguards Rules – Requires covered financial institutions to protect consumer financial data.

Fair Credit Reporting Act (FCRA) – Governs credit reporting agencies and consumer data protection.

Electronic Fund Transfer Act (EFTA) – Ensures security in electronic banking transactions.

Available Penalties and Damages for Violations

Civil Money Penalties (CMPs):

Fines up to $1 million per day for reckless or knowing violations.

Restitution and Consumer Compensation

Requires financial institutions to reimburse consumers harmed by data breaches.

Injunctive Relief

Orders mandating cybersecurity improvements and enhanced consumer protections.

Public Enforcement Actions

CFPB can publicly disclose violations, damaging reputations and investor confidence.

FEDERAL TRADE COMMISSION (FTC)

Who is Subject to FTC Enforcement?

Non-Bank Financial Institutions and Third-Party Service Providers handling Consumer Financial Data; Payment Processors, Cloud Storage Providers, and IT Vendors working with Financial Institutions; Debt Collectors, Credit Reporting Agencies, and Data Aggregators; and, FinTech Companies Offering Financial Services

Enforceable Laws

GLBA Safeguards Rule – Requires non-bank financial institutions to implement cybersecurity controls.

FTC Act – Prohibits unfair or deceptive cybersecurity practices.

Consumer Financial Protection Act (CFPA) (UDAAP) – FTC can take enforcement action against deceptive cybersecurity practices.

Fair Credit Reporting Act (FCRA) – Governs cybersecurity and data protection for credit reporting agencies.

Available Penalties and Damages for Violations

Civil Money Penalties (CMPs):

Up to $50,120 per violation for unfair or deceptive acts.

Injunctive Relief

Court orders requiring improved cybersecurity policies and oversight.

Restitution and Consumer Compensation

Reimbursement for financial harm caused by a data breach.

Ban on Engaging in Certain Activities

Prohibition from handling consumer financial data if security failures persist.

STATE REGULATORS AND ATTORNEYS GENERAL (AGS)

Available Penalties and Damages for Violations

Civil Money Penalties (CMPs):

Fines based on the number of affected consumers and severity of the violation.

Restitution and Consumer Compensation

Reimbursement for financial harm caused by cybersecurity failures.

Injunctive Relief

Court orders requiring businesses to overhaul security programs.

Revocation of Licenses

The ability to revoke state licenses for non-compliant financial institutions.

Who is Subject to State Civil Liability and Enforcement?

Non-bank financial institutions operating within the state; State-chartered banks; Mortgage lenders, servicers, and brokers; Debt collectors and credit reporting agencies; and FinTech companies handling consumer financial data

Enforceable Laws

Consumer Financial Protection Act (CFPA) – Grants state AGs the power to enforce federal consumer protection laws independently of the CFPB.

Gramm-Leach-Bliley Act (GLBA) Safeguards Rule – Certain states enforce their own versions of the rule or supplement federal enforcement.

State-Level Unfair, Deceptive, or Abusive Acts or Practices (UDAAP) Laws – Used to prosecute cybersecurity failures and deceptive privacy policies.

Key Regulatory ComplianceTakeaways

01 State AGs and regulators can independently enforce the CFPA and 17 other federal consumer protection laws, including their implementing regulations and regulatory orders.

02 All four agencies, and the Federal Reserve, may enforce the GLBA Safeguards Rule, requiring financial institutions to protect consumer financial data.

03 Each agency enforces cybersecurity incident notification rules specific to their regulated entities.

04 The OCC, NCUA, FDIC, and Federal Reserve can refer deceptive cybersecurity practices to the CFPB under the CFPA (UDAAP).

05 Each regulator has authority to impose civil penalties, require consumer restitution, and enforce corrective actions for cybersecurity failures.

06 Repeat or willful cybersecurity violations may result in enhanced oversight, operational restrictions, or charter revocation.

Cybersecurity and Data Privacy Policies and Procedures

Entities Required to Implement Policies and Procedures

Banks and Credit Unions

Non-Bank Financial Institutions (e.g., Mortgage Lenders, Servicers, Payday Lenders, FinTech Companies)

Technology-Enabled Third-Party Service Providers handling Consumer Financial Data

POLICIES AND PROCEDURES

Information Security Program (GLBA Compliance): Comprehensive risk-based security framework. Encryption of sensitive consumer data. Access control measures and least-privilege access enforcement.

Data Breach Response and Notification Policy: Incident detection, isolation, remediation, response and reporting protocols. Regulatory and consumer notification timelines. Crisis communication and remediation steps.

Third-Party Vendor Management Policy: Due diligence and risk assessment of service providers. Security audits and contractual cybersecurity obligations. Compliance monitoring and breach accountability.

Consumer Privacy and Data Protection Policy: Consumer consent and data minimization strategies. Transparency in data collection and usage. Consumer rights to access, delete, or modify personal information. Security controls testing and validation.

Cybersecurity Risk Management Program: Defines governance, oversight, risk assessment frameworks. Risk assessment, threat monitoring, risk mitigation and reporting, including periodic security controls assessments and regulatory compliance audits.

Employee Training and Awareness Program: Cyber hygiene best practices. Phishing attack simulations. Compliance training on data security regulations.

Regulatory Compliance and Audit Policy: Regular internal and third-party cybersecurity audits. Documentation and evidence retention for regulatory inspections and audit readiness. Ongoing compliance monitoring and update process based on evolving regulations.

Business Continuity and Disaster Recovery (BC/DR) Policy: Process for maintaining critical operations during cyber incidents (resilience). Data backup and recovery procedures. Contingency planning for ransomware and system failures. Regular testing and updating of BC/DR plans.

Contracting with Technology and Technology Enabled Service Providers

01

Data Security and Compliance Obligations

Compliance with GLBA, CFPA, and applicable federal and state laws. Security certifications (ISO 27001, SOC 2).

02

Data Access and Encryption

Encryption of data at rest and in transit. Access control frameworks (RBAC, least privilege).

03

Incident Notification and Response:

Breach notification timeframes. Forensic investigation responsibilities.

04

Regulatory Audit and Inspection Rights

Right to audit the SaaS provider's security controls. Obligation to cooperate with financial institution regulatory audits.

05

Third-Party Vendor Management

Approval process for subcontracting. Ensuring subcontractors adhere to financial institution security policies.

06

Data Retention and Secure Disposal

Clear data retention policies aligned with FI's regulatory requirements. Data deletion requirements upon contract termination.

07

Indemnification and Liability

Allocation of liability in case of a security breach. Cyber insurance requirements.

Emerging Technology Challenges and Cybersecurity Risks

Artificial Intelligence (AI)

- AI-driven fraud detection vs. risks of AI bias (fair lending).
- Security concerns in AI decision-making models.

Blockchain and Decentralized Finance (DeFi)

- Data privacy implications of on-chain transactions.
- Risks of smart contract vulnerabilities.
- Data Immutability

Quantum Computing Threats

- Future risk of quantum computing breaking current encryption standards.
- Potential regulatory responses to post-quantum cryptography.

Cloud Computing Risks

- Regulatory concerns in cloud-hosted financial services.
- Data sovereignty issues in multi-cloud environments.
- API Security Concerns

Contracting with Technology and Technology Enabled Service Providers

01

Cybersecurity and Data Privacy Are Regulatory Priorities

Federal and state regulators actively enforce data security laws, with severe penalties for noncompliance.

02

Comprehensive Risk Management and Compliance Are Essential

A well-documented cybersecurity program, risk assessments, and third-party oversight are crucial for financial institutions and service providers.

03

Incident Readiness and Response Are Critical

Firms must have proactive threat monitoring, breach response plans, and regulatory notification protocolsto mitigate cyber risks

04

Emerging Technologies Present Both Risks and Compliance Challenges

The rise of AI, blockchain, and cloud computing necessitates enhanced data security controls, regulatory engagement, and adaptive risk strategies.

THANK YOU

Old Lyme, CT 06371

+18607074380

JLevonick@garrishorn.com

www.garrishorn.com

LinkedIn www.linkedin.com/in/johnlevonick/