Deloitte.

Data security as consumer protection

Perspectives related to increasing focus on data security by consumer protection regulators

Center *for* Regulatory Strategy US

The Consumer Financial Protection Bureau (CFPB), Federal Trade Commission (FTC), and federal banking agencies are increasingly focusing on the nexus of information technology (IT) security and consumer protection laws. Inadequate authentication, password management, or software update policies or practices may be a violation of federal law, including the Consumer Financial Protection Act (CFPA) and Gramm-Leach-Bliley Act (GLBA), in that it can cause substantial injury that is not easily avoidable by consumers. Financial institutions are unlikely to successfully justify weak data security practices based on countervailing benefits to consumers or competition.

Recent developments

FTC: In October 2023, the FTC updated Safeguards Rule implementing Section 501(b) of GLBA to set **specific criteria relating to the safeguards** that certain nonbank financial institutions must implement as a part of their information security programs.[1] Beginning on May 11, 2024, non-banks will need to submit notifications of data breaches or other security events affecting at least 500 customers to the FTC.

CFPB: In 2022, the CFPB published Circular 2022-04 which took the position that providing "inadequate security for the sensitive consumer information collected, processed, maintained, or stored by … a company can constitute an unfair practice" under the CFPA.[2]

Federal banking agencies: The federal banking agencies have the authority under GLBA to issue Information Technology (IT) Security Guidelines on how to comply with associated laws and regulations.[3]

COMMON FAILURE POINTS

Inadequate authentication

Inadequate password management

Inadequate software update, policies or practices

Areas of regulatory concern

Regulators are particularly concerned with the following deficiencies which could lead to regulatory actions including fines, penalties and/or litigation:[4]

- Gaps in network security that resulted in data breaches
- Lack of effective risk management practices
- Failure to remediate deficiencies within their cyber and security program
- Lack of governance or internal oversight program components not only at companies, but also at subcontractors or vendors
- Unapproved modes of communication to share sensitive information.

What is the GLBA?

GLBA is also known as the Financial Modernization Act of 1999. GLBA is a United States **federal law that requires financial institutions to explain how they share and protect their customers' private information**. To be GLBA compliant, financial institutions must communicate to their customers how they share the customers' sensitive data, inform customers of their right to opt-out if they prefer that their personal data not be shared with third parties, and apply specific protections to customers' private data in accordance with a written information security plan created by the institution. The GLBA is enforced by the FTC, the federal banking agencies, other federal regulatory authorities, and state insurance oversight agencies.

[1] Federal Trade Commission (FTC), "Standards for Safeguarding Customer Information," October 27, 2023.

[2] Consumer Financial Protection Bureau (CFPB), "Consumer Financial Protection Circular 2022-04," August 11, 2022.

[3] Federal Financial Institutions Examination Council (FFIEC), "IT Booklets," accessed March 4, 2024.

[4] Deloitte analysis of enforcement actions.

Deloitte.

Data security as consumer protection

Perspectives related to increasing focus on data security by consumer protection regulators

Center *for* **Regulatory Strategy US**

Considerations to evaluate

Review data security claims

- Focus on accuracy and supportability of data security claims, IT policies, and control standards. When performing an IT security review, regulators may review additional information relating to IT claims.

Strengthen cybersecurity practices

- Improve practices to exceed representations and mitigate enforcement risks. Even if deception is not an issue, the CFPB, FTC, and other banking regulators can target allegedly faulty data practices on an unfairness theory or under GLBA. Utilize the FTC's "Start with Security: A Guide for Business" which outlines learnings from enforcement.[5]

Focus on policies and procedures and programs

- Document cybersecurity policies, train employees, and regularly evaluate and update controls and procedures. Address consumer complaints for continuous improvement. Additionally, focus on programs in place to intake, adjudicate, respond to, and monitor customer complaints.

Actions to take / Next steps

Direct and guide

- Set IT risk and compliance foundation with IT policies and control standards for strong tone at the top creating a culture of compliance.

Educate and influence

- Influence IT risk and compliance performance through awareness, education and performance accountability.

Assess and report

- Proactively identify, assess, monitor and report on IT risk and controls performance through standard processes.

Respond and improve

- Streamline and automate IT risk processes and controls to expand risk coverage and gain better, more efficient results.

Govern and maintain

- Implement IT governance practices for enhanced IT risk and compliance results and business risk decision-making.

[5] FTC, "Start with Security: A Guide for Business," August 2023.

Contact us

Maria Marquez
Principal | Deloitte & Touche LLP
marmarquez@deloitte.com

Damian Kuczma
Managing Director | Deloitte & Touche LLP
dkuczma@deloitte.com

Alycia Steiner
Senior Manager | Deloitte & Touche LLP
alsteiner@deloitte.com

Elaine Liu
Senior Manager | Deloitte & Touche LLP
huliu@deloitte.com

Paul Sanford
Independent Senior Advisor to
Deloitte & Touche LLP
pasanford@deloitte.com