Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Big Data in Financial Services: Privacy and Security Regulation

November 15, 2019

Congress has shown interest in data privacy and security issues in the financial services industry, including an upcoming House Financial Services task force hearing. Recent data breaches at large financial institutions and credit reporting agencies have increased concern about the privacy and security of the large amounts of consumer financial information (known increasingly as *big data*) that companies gather, use, and store. Some of this information is public, whereas other information is considered personal and nonpublic. No single law provides a framework for regulating data privacy in the United States. Instead, myriad laws cover different industries.

In the financial services industry, several federal and state laws cover data privacy; most comprehensively, the Gramm-Leach-Bliley Act (GLBA; P.L. 106-102) directs financial regulators to implement disclosure requirements and security measures to safeguard private information. This Insight summarizes GLBA's regulatory implementation and discusses policy issues for Congress.

GLBA and the Financial Regulators

GLBA provides a framework for regulating data privacy and security practices in the financial services industry. This framework is built upon two pillars: (1) privacy standards that impose disclosure limitations on financial institutions concerning consumers' information and (2) security standards that require institutions to implement certain practices to safeguard the information from unauthorized access, use, and disclosure. The two major rules for implementing this framework are known as the Privacy Rule (Regulation P) and the Safeguards Rule, respectively. These rules are promulgated, supervised, and enforced by different government agencies, and in some cases different agencies have rulemaking and supervisory authority over the same entity.

Rulemaking

Rulemaking authority to implement the Privacy Rule through Regulation P is vested in four agencies. The Federal Trade Commission (FTC) has the rulemaking authority for the Safeguards Rule. **Table 1** provides a crosswalk of the federal agencies and who they may regulate under each rule.

Congressional Research Service
https://crsreports.congress.gov
IN11199

Table 1. Rulemaking Authority for GLBA

Federal Regulator	Privacy Rule	Safeguards Rule
Consumer Financial Protection Bureau (CFPB)	Depository and nonbank financial institutions involving consumer financial products or services in the CFPB's jurisdiction	None
Securities and Exchange Commission (SEC)	Securities companies	None
Commodity Futures Trading Commission (CFTC)	Futures-related companies	None
Federal Trade Commission (FTC)	Motor vehicle dealers	Financial institutions significantly engaged in financial activities (e.g., bank and nonbank lenders, real estate appraisers, professional tax preparers, courier services, credit reporting agencies, and ATM operators)

Source: 15. U.S.C. §6804; 12 C.F.R. §1016.1(b).

Regulation P requires financial institutions to

- provide initial, annual, and revised privacy policy notices to customers and
- set the conditions for when a financial institution may or may not disclose nonpublic personal information.

The Safeguards Rule requires financial institutions to

- design and implement a safeguards program and
- identify and assess the risks to customer information in each relevant area of the company's operation, including service providers and changes in the firm's operations.

Supervision and Enforcement

Agencies responsible for privacy and safeguard rulemaking are sometimes not the same agencies responsible for implementing these rules for a particular entity. For instance, as discussed in **Table 1**, the FTC has rulemaking authority for the Safeguards Rule; however, supervisory authority for the rule is shared among the banking and credit union regulators. Further, most of the financial regulators have some supervisory or enforcement authority to ensure that the institutions in their respective jurisdictions comply with the Privacy and Safeguards Rules (see **Table 2**).

Table 2. Supervision and Enforcement Authority for GLBA

Federal Regulator	Privacy Rule	Safeguards Rule
CFPB	Supervision and enforcement authority over depository and nonbank financial institutions involving consumer financial products or services in the CFPB's jurisdiction	None
Depository agencies	Supervision and enforcement authority over banks or credit unions in their jurisdiction	Supervision and enforcement authority over banks or credit unions in their jurisdiction

Federal Regulator	Privacy Rule	Safeguards Rule
SEC	Enforcement authority over brokers, dealers, and investment advisors or companies in their jurisdiction	Enforcement authority over securities companies in their jurisdiction
FTC	Enforcement authority over other entities not covered above by another federal regulator, such as motor vehicle dealers or other nonfinancial companies	Enforcement authority over other entities not covered above by another federal regulator, such as nonbank consumer financial institutions or other nonfinancial companies

Source: 15. U.S.C. §6805.

Note: The depository agencies include the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Reserve, and the National Credit Union Administration.

Potential Policy Considerations for Congress

The fact that several regulators implement, supervise, and enforce GLBA provisions has raised questions over the "patchwork" of regulatory standards for consumer privacy and security. As Congress continues to explore this issue, a few policy considerations may be informative:

Data Security Standards—One area of debate is whether data security standards should be prescriptive and government defined or flexible and outcome based. Some argue that a prescriptive approach can be inflexible and harm innovation, but others argue that an outcome-based approach might lead to institutions having to comply with a wide range of data standards. For instance, the FTC recently submitted proposed amendments to the Privacy and Safeguards Rules to provide more certainty to financial institutions and to better protect consumers. Two commissioners dissented over the amendments to the Safeguards Rule, raising caution over the impact more prescriptive cybersecurity standards might have on innovation.

Financial Data and Consumer Redress—GLBA covers only nonpublic personal information held by financial institutions significantly engaged in financial activities. However, as the industry's data use has grown, some have debated whether the law covers all sensitive individual financial information. For example, data brokers can compile public and private data from different sources, much of which may not be subject to GLBA's provision, but combining these data might reveal financially sensitive information about a consumer. Further, consumers have a limited ability to know, control, or correct financial data, which can make it difficult to obtain redress for violations such as data breaches.

Author Information

Andrew P. Scott
Analyst in Financial Economics

Disclaimer