WINSTON & STRAWN LLP

Data Breach and Data Security Law

Within 48 U.S. states and the District of Columbia, **data breach and data security laws** require organizations and government agencies to provide notifications of security breaches when they involve personally identifiable information. Companies may also be required by state data breach laws to act to minimize the effects of a breach. The FTC can investigate companies that do not adhere to their stated privacy policies and do not have safeguards to protect customer data, but no broad federal law exists regarding breach notifications. However, these U.S. data security laws and government agency rules are enforced:

- Gramm-Leach-Bliley (GLB) Act, requiring financial institutions to ensure the security and confidentiality of personal information
- Federal Trade Commission Safeguards Rule, requiring certain financial institutions to establish measures to keep customer information secure
- HIPAA Breach Notification Rule, requiring HIPAA-covered entities and associates to provide notification following a breach of unsecured, protected health information
- FTC Health Breach Notification Rule, requiring health-related businesses, which are not under HIPAA regulation, to notify customers following a breach of electronic health information

Related Capabilities

Privacy & Data Security | Privacy: Regulated Personal Information (RPI)