Protection of Consumer Information - Overview

The legal framework that regulates the collection, use, disclosure, disposal, and security of personal and financial consumer information is complicated. There is no single law addressing these diverse aspects of protecting consumer information; rather, multiple layers of federal and state law regulate consumer protection and data security in different manners and contexts. Enforcement falls under the jurisdiction of many different federal and state entities, including the Consumer Financial Protection Bureau, the Federal Trade Commission, the functional federal regulators for various financial institutions, e.g., FDIC, NCUA, Federal Reserve Board, etc., and state insurance regulators. To the extent permitted under federal law, states may also have additional provisions enforced by Attorneys General, state financial regulators, or other public agencies and departments.

Overarching the host of federal laws is the Federal Trade Commission Act. This law prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce. Whereas other federal laws apply to specific types of businesses or in particular legal contexts, the FTC Act and enforcement action by the Federal Trade Commission more broadly applies to business practices across industries that cause harm to consumers. In the past several years, the FTC has brought enforcement proceedings under the Act and other laws against companies involved in prominent data breaches. The FTC typically charges these companies with unfair and deceptive trade practices—whether because the company misrepresented the scope or effectiveness of its data security program or consumer protection practices, or because the company failed to comply with its own policies.

In addition to the FTC Act, two major suites of federal statutes and regulations address the use and protection of consumer financial information: The first suite, the Fair Credit Reporting Act and associated rules, applies to consumer reporting agencies, consumer reports, and persons who use or furnish consumer credit information. In general, the act requires that: (1) consumer reporting agencies provide access to consumer credit information, take steps to ensure the accuracy of that information, and observe requirements designed to mitigate identity theft; (2) consumer reports include correct information and are available only for specific permitted purposes; (3) users observe statutory requirements for permissible, legitimate use of a report and certify to the use; and (4) furnishers of consumer credit information supply correct information and observe requirements to facilitate disputes and correction of inaccurate information and mitigate identity theft.

The second suite, the Financial Services Modernization Act, also referred to as Gramm-Leach-Bliley, and its associated rules, applies broadly to financial institutions, which includes both banking institutions and also other businesses that are significantly engaged in providing financial products or services—a category that includes, for example, check-cashing businesses; payday lenders; mortgage brokers; nonbank lenders; personal property or real estate appraisers; professional tax preparers courier services; retailers that extend credit; automobile dealers that lease vehicles for more than 90 days; and any other business that is significantly engaged in a financial activity described in section 4(k) of the Bank Holding Company Act of 1956. A financial institution subject to GLB must provide notice of its privacy policies and is limited in its ability to disclose nonpublic personal information. Additionally, the "Safeguards Rules" adopted under authority of GLB require financial institutions to implement an information security program that includes administrative, technical, and physical safeguards to ensure the security and confidentiality of, and prevent unauthorized access to, customer records and information. Of particular

significance, the GLB requirements also apply to persons with whom a financial institution shares nonpublic personal information, including consumer reporting agencies.

Another regulatory layer of federal statutes and rules impose requirements on the collection, use, and disclosure of consumer information in specific legal contexts. For example, the Children's Online Privacy Protection Act relates specifically to websites that collect information from children under age 13. The Driver's Privacy Protection Act limits disclosures of personal information by State departments of motor vehicles. The Family Educational Rights and Privacy Act restricts the disclosure of educational records. The Federal Privacy Act imposes extensive requirements on the collection and use of personal information by agencies of the federal government. Finally, the Health Insurance Portability and Accountability Act imposes duties and limits relating to personal health information.

The final layer of federal law creates crimes for the collection or misuse of personal information. For instance, the Computer Fraud and Abuse act prohibits unauthorized access to computers and trafficking in passwords. The Electronic Communications Privacy Act prohibits the unauthorized interception, use, or disclosure of wire, oral, or electronic communications, and unauthorized access to stored electronic records. The Federal Identity Theft and Assumption Deterrence Act makes it a federal crime to produce or possess false identity documents and to use another person's identity to commit a crime. The Video Privacy Protection Act prohibits the unauthorized disclosure of consumer information relating to video rentals, sales, and viewing history, such as on internet sites like Facebook and Netflix.

In addition to these federal laws, states generally have authority to impose additional requirements, which in many cases are more stringent than federal law. For example, 13 states have laws that apply to any business that has access to consumer personal information and require the business to implement a data security program similar to the GLB Act. Almost every state, including Vermont, has a data breach notification law, which requires notice to consumers (and often to the state Attorney General) when a data breach occurs.

Like many other states, Vermont has scores of state laws across most legal subject areas that seek to limit the disclosure of personal or confidential information by government-related activities. Specific Vermont laws mandate the protection of, and limit the use and disclosure of, social security numbers; require businesses to take reasonable steps to destroy records with personal information; limit a consumer's liability for unauthorized use of a credit card; and create a State law crime of identity theft.

Vermont law goes beyond the requirements of federal law in many areas. For example, with respect to financial institutions, insurance companies, and securities professionals, Vermont not only requires regular notices of privacy policies, but also requires Vermont consumers to "opt in" to allow those companies to disclose personal information to nonaffiliated third parties. Vermont also imposes on these entities the duty to have an information security program similar to the GLB Act.

Finally, with respect to credit reports and credit reporting agencies, Vermont limits the use of credit information for employment purposes, and with limited exceptions, requires written consent from the consumer before a person can obtain his or her credit report. Like many states, Vermont allows a consumer to place a "security freeze" on his or her credit file, imposes certain state-specific notice requirements for consumers, caps the amount and applicability of certain fees, and mandates one free annual credit report from each consumer reporting agency.