Overview

Gramm-Leach-Bliley Act (GLBA) Privacy & Data Security

Dan Pepper, Susan Linda Ross, and Elyssa Diamond, Norton Rose Fulbright US LLP

Bloomberg Law

Gramm-Leach-Bliley Act (GLBA) Privacy & Data Security

Contributed by Dan Pepper, Susan Linda Ross, and Elyssa Diamond, Norton Rose Fulbright US LLP.

Congress created the Gramm-Leach-Bliley Act of 1999 (GLBA, also known as the Financial Services Modernization Act of 1999) to repeal Depression-era laws that prohibited organizations from offering banking, securities, and insurance through affiliations in the same organization. The purpose of GLBA was to enhance efficiency in financial services industries. Am. Bankers Ass'n v. Gould, 412 F.3d 1081, 1087 (9th Cir. 2005) and Trans Union LLC v. Federal Trade Comm'n, 295 F.3d 42, 46-47 (D.C. Cir. 2002). In order to address concerns that these newly combined organizations would have access to large amounts of consumers' personal information, GLBA includes some privacy protections at 15 U.S.C. §§ 6801-6809, with additional protections governing fraudulent access of financial information at 15 U.S.C. §§ 6821-6827.

Privacy Notice Obligations

In general, GLBA follows a notice and opt-out consent model. The federal regulators have created a model form privacy and opt-out notice (*see* Overview – GLBA Privacy Notice Obligations). GLBA permits sharing of "nonpublic personal information" across affiliates, and consumers are not given the right to opt-out of this type of disclosure. Consumers do have the right to opt-out of sharing with other third parties, and GLBA also requires that the financial institution have a contract with any third party that receives this data, requiring the third party to maintain the confidentiality of the data (*see* Overview – Federal Trade Commission (FTC) Safeguards Rule).

Information Security Requirements

Federal regulations also require that the financial institutions "develop, implement, and maintain a comprehensive information security program." 16 C.F.R. § 314.3(a). *See* Overview – IT Security & Cloud Guidance for Financial Institutions and Overview – Federal Trade Commission (FTC) Safeguards Rule. State regulators have also built on many of these federal requirements by promulgating regulations relating to measures financial institutions must take and restrictions on uses of the data (*see* Overview - New York Department of Financial Services (NYDFS) Cybersecurity Requirements). Over time, federal regulators added requirements relating to data breaches (*see* Overview – Computer-Security Incident Notification Rule for Banking Organizations) and more recently, have expressed concern regarding over-retention of data (*see* Overview – Federal Trade Commission (FTC) Safeguards Rule).

Prohibition of "Pretexting"

Under the GLBA, it is illegal to obtain or attempt to obtain, or to attempt to disclose or cause to disclose, customer information of a financial institution by false pretenses or deception. 15 U.S.C. § 6821. Known as the "Pretexting Rule," this provision specifically relates to phishing and other related scams. In order to be compliant with the Pretexting Rule, financial institutions should educate employees to recognize social engineering and phishing scams.

Applicability to "Financial Institutions"

GLBA defines "nonpublic personal information" broadly in 15 U.S.C.§ 6809(4):

(4) Nonpublic personal information

(A) The term "nonpublic personal information" means personally identifiable financial information—

(i) provided by a consumer to a financial institution;

(ii) resulting from any transaction with the consumer or any service performed for the consumer; or

(iii) otherwise obtained by the financial institution.

(B) Such term does not include publicly available information, as such term is defined by the regulations prescribed under section 6804 of this title.

(C) Notwithstanding subparagraph (B), such term–

(i) shall include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but

(ii) shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information.

In 15 U.S.C. § 6809(3), GLBA defines a "financial institution" in terms of what the organization does: The term "financial institution" means any institution the business of which is engaging in financial activities as described in section 1843(k) of title 12. The referenced section does not list specific entity types, but instead includes a list of nine factors to be considered as to whether an activity is "financial in nature."

Regulatory Environment

Unlike many countries, the U.S. has a variety of regulators of financial institutions, based in part of whether the institution is chartered on a federal or state level, whether they are part of the Federal Reserve system, etc. A financial institution can be subject to the jurisdiction of more than one regulator.

Because the federal regulatory structure for financial institutions is fragmented, GLBA in § 6809(2) lists several "federal functional regulators":

(2) Federal functional regulator

The term "Federal functional regulator" means–

(A) the Board of Governors of the Federal Reserve System;

(B) the Office of the Comptroller of the Currency;

(C) the Board of Directors of the Federal Deposit Insurance Corporation;

(D) the Director of the Office of Thrift Supervision;

(E) the National Credit Union Administration Board; and

(F) the Securities and Exchange Commission.

Although this section of the law has not changed since 1999, the regulatory environment has. The Office of Thrift Supervision was merged into the Office of the Comptroller of the Currency. The Federal Trade Commission originally had jurisdiction over the non-insurance "financial services" that were not otherwise covered–until 2010, when the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) created the Consumer Financial Protection Bureau (CFPB). Dodd-Frank also granted most of the privacy rulemaking authority under GLBA with respect to financial institutions and other entities subject to the CFPB's jurisdiction, except securities and futures-related companies and certain motor vehicle dealers.

GLBA does not pre-empt state laws that provide greater privacy protection, 15 U.S.C. § 6807(b). *See* Overview – Relationship of GLBA to State Privacy, Data Breach, and Insurance Laws. Because there is no general federal insurance regulator, the laws and regulations relating to GLBA are all based in state requirements.

For a chart that provides a general description of which federal regulators and types of state regulators have primary responsibility for which type(s) of financial services, see Comparison Table - GLBA Privacy & Security: Federal & State Regulatory Authority. Note that an entity may be subject to more than one regulator.