Overview

Relationship of GLBA to State Privacy, Data Breach, and Insurance Laws

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

Bloomberg Law

Relationship of GLBA to State Privacy, Data Breach, and Insurance Laws

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

GLBA and State Financial Privacy Laws

Section 6807(a) of the Gramm-Leach-Bliley Act of 1999 (GLBA) expressly states that the privacy protections in GLBA "shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State" as long as the state law or regulation is not inconsistent with GLBA. 15 U.S.C. § 6807(a). Subsection (b) clarifies that any state law, regulation or order is not inconsistent with GLBA if it "affords any person" greater protection than is provided under GLBA. 15 U.S.C. § 6807(b).

California's Special Notice (Opt-out/Affiliate) Requirements

California enacted the California Financial Information Privacy Act (Cal. Fin Code §§ 4050-4060) in 2003, which provided state residents with two protections not contained in GLBA. The first provision permitted consumers to opt-out of affiliate sharing. The second provision gives consumers the right to opt-in to sharing with non-affiliates. Note that the affiliate-sharing provisions was challenged under the Fair Credit Reporting Act, and was ultimately held not to apply to "consumer report information" under FCRA. (Am. Bankers Ass'n v. Lockyer, 541 F3d 1214, 1216 (9th Cir. 2008), cert. denied, 557 U.S. 935 (2009).) As a result, California residents can prohibit affiliate-sharing of information that is not "consumer report" information, and many financial institutions have a separate California form that is modeled on the federal form but follows California's requirements.

For information on the various privacy laws of each state, see State Privacy & Data Security Chart Builder and related In Focus page.

Vermont's Special Notice

Vermont's Financial Privacy Act (8 Vt. Stat. Ann. §§ 10201 – 10206) also differs from GLBA. Like California, it requires an opt-in before consumer data can be shared with non-affiliates, and the consumer can withdraw that consent at any time. Financial institutions are not required to offer the consumer the ability to opt out, but have the option to allow consumers to select certain information and/or certain non-affiliates for opting-in. Regulation B-2018-01 Section 11. The financial institution's notice must identify the financial products and services to which the opt-in applies. The notice must also describe the methods to revoke any opt-in consent.

With respect to GLBA's model form privacy notice, Vermont's Regulation B-2018-01 Section 7.G gives financial institutions two options: First, they can indicate that they do not share information about consumers' creditworthiness to affiliates for their "everyday purposes" and that they do not share personal information with non-affiliates for them to market to the consumer. Second, the financial institution can add the following in the "Other Important Information" box of the model form:

For Vermont Members/Customers.

- We will not disclose information about your creditworthiness to our affiliates and will not disclose your personal information, financial information, credit report, or health information to nonaffiliated third parties to market to you, other than as permitted by Vermont law, unless you authorize us to make those disclosures.
- Additional information concerning our privacy policies can be found at [*website link*] or call [*telephone number*].

GLBA and State Data Breach Notification Laws

On March 29, 2005, the Office of the Comptroller of the Currency (OCC), Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), and Office of Thrift Supervision (OTS) issued guidance relating to data breaches, entitled Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Guidance). In 2023, all 50 states, Washington, D.C., Guam, Puerto Rico, and U.S. Virgin Islands have "data breach" laws, but that was not the case when this Guidance issued in 2005. The federal regulators set forth a national standard for financial institutions subject to their jurisdiction. The guidance defined a customer notification event when "an incident of unauthorized access to customer information involves customer information systems maintained by an institution's service providers."

The Guidance states that each financial institution's notification program should, at a minimum, have five elements:

1. Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;
2. Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined below;
3. Consistent with the Agencies' Suspicious Activity Report (SAR) regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;
4. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and
5. Notifying customers when warranted.

The Guidance places an obligation on financial institutions to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Substantial harm or inconvenience is most likely to result from improper access to sensitive customer information because this type of information is most likely to be misused, as in the commission of identity theft. For purposes of this Guidance, sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.

This definition is similar to the state data breach laws as they existed in 2005. Since 2005, many states have adopted additional factors, including health insurance information and date of birth.

Much like the state data breach laws, the Guidance requires financial institutions to notify the customers whose data has been affected, or if that cannot be determined, to notify the group of customers affected. For example, if a financial institution can determine that only customers whose data had been added or amended since X date had their data affected, the financial institution need only notify those customers. In contrast, if the hacker deleted some of the files showing what the hacker had accessed, the financial institution would need to notify the customers to which the hacker likely had access or—if the financial institution did not have sufficient contact information—use alternate notifications, such as website banners. The Guidance also specifies the contents of the notice:

1. A description of the incident in general terms and the type of customer information that was the subject of unauthorized access or use.
2. A general description of what the institution has done to protect the customers' information from further unauthorized access. In addition, the financial institution's customer notice should include
3. A telephone number that customers can call for further information and assistance.

4. A reminder to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft to the institution.

5. A recommendation that the customer review account statements and immediately report any suspicious activity to the institution;

6. A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud;

7. A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;

8. An explanation of how the customer may obtain a credit report free of charge; and

9. Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the customer to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that customers may use to obtain the identity theft guidance and report suspected incidents of identity theft.

With respect to the delivery of the notice, the Guidance is general:

> Customer notice should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

Most state data breach laws exempt entities subject to GLBA and/or entities in compliance with the Guidance. The eight states that do not have these exceptions are:

- Alaska (Alaska Stat. § 45.48.010 – 090);
- Arkansas (Ark. Code Ann. § 4-110-105);
- California (Cal. Civ. Code § 1798.82);
- Connecticut (Conn. Gen. Stat. Ann. § 36a-701b);
- Maine (10 Maine Rev. Stat. Ann. § 1348);
- Montana (Mont. Code Ann. § 30-14-1704);
- New Jersey (New Jersey Stat. Ann. § 56:8-163); and
- Texas (Tex. Bus. & Com. Code § 521.053).

GLBA and State Comprehensive Privacy Laws

The comprehensive state privacy laws that have been enacted since 2020 (including, but not limited to, California, Virginia, Colorado, Utah, Connecticut, and Iowa) all include exceptions relating to GLBA. All except California exclude entities subject to GLBA. California excepts the data (not the entity) that is subject to GLBA.

State Insurance Law Requirements

The federal McCarran–Ferguson Act, 15 U.S.C. §§ 1011-1015, provides that "Acts of Congress" which do not expressly purport to regulate the "business of insurance" will not preempt state laws or regulations that regulate the "business of insurance." GLBA does not directly provide for the regulation of insurance, but does address insurance in three sections:

- Coordination, consistency, and comparability:

  Each of the agencies authorized under paragraph (1) to prescribe regulations shall consult and coordinate with the other such agencies and, as appropriate, and with [1] **representatives of State insurance authorities designated by the National Association of Insurance Commissioners**, for the purpose of assuring, to the extent possible, that the regulations prescribed by each such agency are consistent and comparable with the regulations prescribed by the other such agencies.

  15 U.S.C.§ 6804(a)(2) (emphasis added);

- Enforcement:

  Subject to subtitle B of the Consumer Financial Protection Act of 2010 [12 U.S.C. 5511 et seq.], this subchapter and the regulations prescribed thereunder shall be enforced by the Bureau of Consumer Financial Protection, the Federal functional regulators, **the State insurance authorities,** and the Federal Trade Commission with respect to financial institutions and other persons subject to their jurisdiction under applicable law, as follows:

  15 U.S.C.§ 6805(a) (emphasis added); and

- Absence of State action:

  If a State insurance authority fails to adopt regulations to carry out this subchapter, such State shall not be eligible to override, pursuant to section 1831x(g)(2)(B)(iii) of title 12, the insurance customer protection regulations prescribed by a Federal banking agency under section 1831x(a) of title 12.

  15 U.S.C.§ 6805(c) (emphasis added).

The National Association of Insurance Commission (NAIC) took the position that GLBA called on state insurance regulators to promulgate similar privacy regulations:

> The NAIC adopted the Privacy of Consumer Financial and Health Information Model Regulation on September 26, 2000. The model regulation was drafted in response to requirements set forth in Title V of the Gramm-Leach-Bliley Act (P.L. 106-102) (GLBA), which was signed into law by President Clinton on November 12, 1999. **GLBA calls on the state insurance regulators to issue regulations protecting the privacy of insurance consumers' personal information**.
>
> NAIC, "NAIC Privacy of Consumer Financial and Health Information Model Regulation – Frequently Asked Questions" (Jan. 2001), https://www.naic.org/documents/prod_serv_legal_pcf_op.pdf (emphasis added).

The U.S. GAO also took the position that GLBA required state insurance authorities to adopt the regulations, as it wrote in 2002 in response to an inquiry from Representative John Dingell:

> Subtitle A calls upon federal regulators to (1) issue regulations implementing disclosure-related requirements and (2) establish standards for safeguarding the privacy and integrity of customer information and records. **The act also requires state insurance authorities to enforce its provisions by adopting regulations for both information disclosure and information safeguards.** As of March 2002, all of the states and the District of Columbia have acted to ensure that insurance companies under their jurisdiction meet Subtitle A's disclosure and notice requirements. In addition some states have included or retained provisions in their regulations or laws that they feel provide greater protections, or more restrictive requirements than those contained in Subtitle A. Only one state, New York, has established standards for protecting the security and confidentiality of insurance customer information as of March 2002. Another state, California, has issued proposed regulations establishing such standards.
>
> U.S. General Accounting Office, "Financial Privacy: Status of State Actions on Gramm-Leach-Bliley Act's Privacy Provisions (12-APR-02, GAO-02-361)" (Apr. 12, 2002) https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-02-361/html/GAOREPORTS-GAO-02-361.htm (emphasis added).

Consequently, many insurers take the position that GLBA exceptions in state data breach laws and comprehensive state privacy laws apply to insurers. States have also begun adopting laws and/or promulgating regulations specifically applicable to insurance with respect to security obligations and breach reporting. For information on the specific breach notification requirements of each state, including those specifically applicable to the insurance industry, see State Data Breach Notification Requirements Chart Builder.