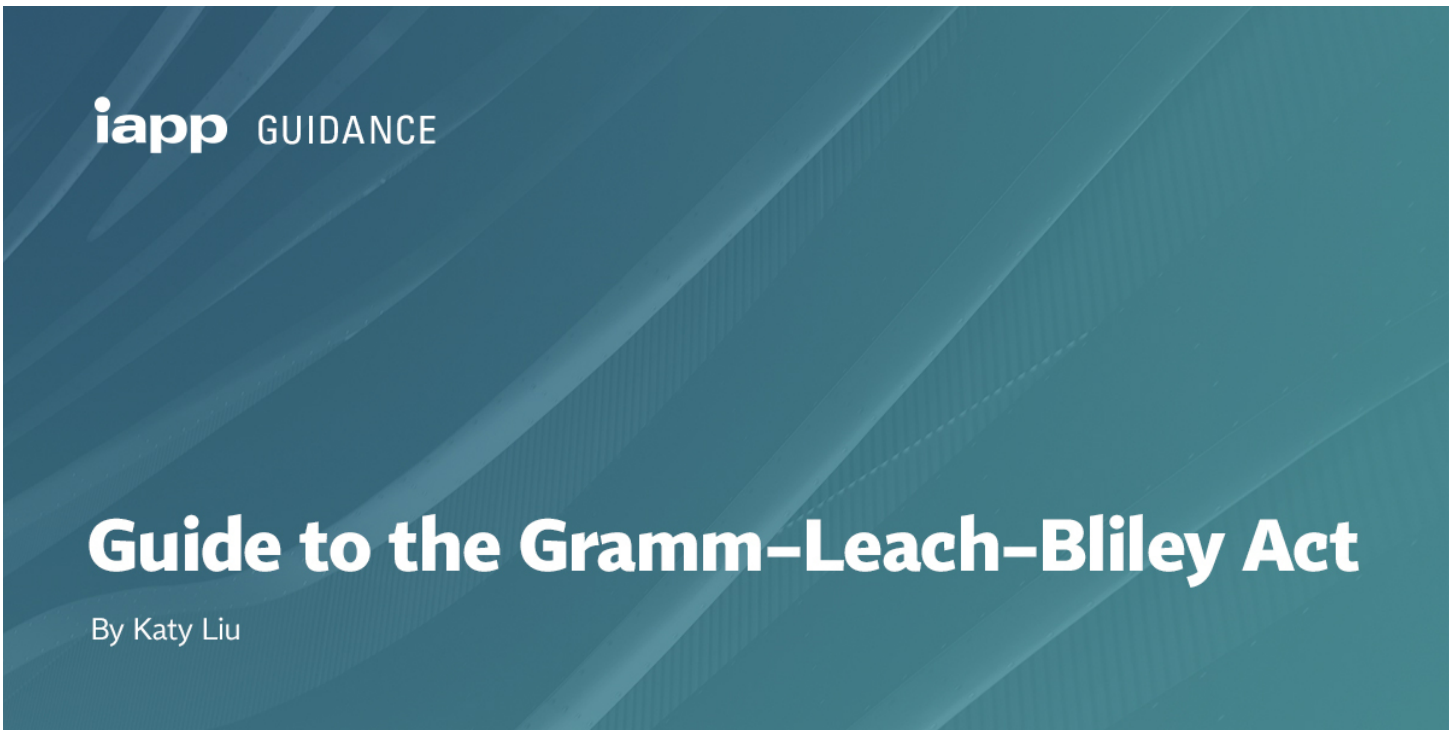
Resource**Center (/resources)**

All the privacy tools and information you need in one easy-to-find place

(https://www.linkedin.com/company/iapp---international-association-of-privacy-professionals/) (https://twitter.com/PrivacyPros) (https://www.instagram.com/iappprivacypros/?hl=en) (https://www.facebook.com/IAPPprivacypros) (https://www.youtube.com/user/IAPPvideos)

Guide to the Gramm–Leach–Bliley Act

Katy Liu (https://iapp.org/about/person/0011a00000DlCzlAAF)



This guide provides an overview of the main provisions of the GLBA.

Easily navigate within this guide through the following sections:

Overview

What is it?

The GLBA is a federal law that became effective in the United States In 1999. The GLBA is also known as the Financial Services Modernization Act of 1999.

Privacy pros zero in on Title V, Subtitle A of the GLBA (https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf) (15 U.S.C. 6801 et seq). Title V boldly introduces the topic of "Privacy" and the "Disclosure of Nonpublic Personal Information."

Under Title V, Subtitle A, Section 501 describes the "Protection of Nonpublic Personal Information," stating that "each financial institution has an affirmative and continuing obligation "to respect the privacy of its customers and to protect the security and confidentiality of those customers' non-public personal information" (15 U.S.C. § 6801). Also, financial regulatory agencies have to "establish appropriate administrative, technical, and physical safeguard standards" that will:

- Ensure the security and confidentiality of customer records and information.
- Protect against any anticipated threats or hazards to the security or integrity of such records.
- Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer (15 U.S.C. § 6801, 15 U.S.C. § 6804).

GLBA requires that financial institutions share their privacy policies and practices with consumers in writing. Also, if the financial institution wants to share consumer nonpublic personal information with nonaffiliated third parties, the financial institution must give consumers the right to opt out from the information sharing.

States may enforce stricter rules than the GLBA. Financial institutions should understand the GLBA, rules issued by applicable financial regulatory agencies, and the rules of the states in which they operate.

Who must comply with it?

Financial institutions, brokers, dealers, and people providing insurance services, including investment companies and investment advisors.

Enforcement

When the GLBA became effective in 1999, federal financial regulatory agencies were required to enforce the GLBA (http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/html/PLAW-106publ102.htm) (15 U.S.C. § 6805).

In 2011, the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) transferred rule-making authority for most of Subtitle V of the GLBA to the Consumer Financial Protection Bureau (https://www.consumerfinance.gov/?utm_source=bing&utm_medium=cpc&utm_term=cfpb&utm_content=Brand&utm_campaign= the Board of Governors of the Federal Reserve System, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, Federal Deposit Insurance Corporation, and the Federal Trade Commission (in part) (see 12 C.F.R. § 1016).

Below is a table that shows whether the Dodd-Frank Act transferred rule-making authority for Subtitle V from a federal regulatory agency to the CFPB.

Regulatory Agency	Regulated Parties	Rule-making transfered to CFPB

Office of the Comptroller of the Currency	National banks, Federal branches and Federal agencies of foreign banks and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisors)	Yes
Board of Governors of the Federal Reserve System	Federal Reserve system member banks (other than national banks), branches and agencies of foreign banks (other than Federal branches, federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act, and bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers)	Yes
Federal Deposit Insurance Corporation	Banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System), insured State branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies and investment advisors)	Yes

*Effective July 21, 2011, the Office of Thrift Supervision merged (http://www.occ.gov/tools-forms/tools/examinations/ots-archive-search.html) with the Office of the Comptroller of Currency	Savings associations the deposits of which are insured by the Federal Deposit Insurance Corporation and any subsidiaries of such savings associations (except brokers, dealers, persons providing insurance, investment companies and investment advisors)	Yes
National Credit Union Administration	Any federally insured credit union and any subsidiaries of such an entity	Yes
Federal Trade Commission	Any other financial institution not subject to the jurisdiction of any agency or authority listed above	In part – the FTC has authority for certain motor vehicle dealers
Securities and Exchange Commission	Any broker or dealer, investment companies, investment advisors registered with the SEC for the Investment Advisors Act of 1940	No
Commodity Futures Trading Commission	Futures commission merchants, retail foreign exchange dealers, commodity trading advisors, commodity pool operators, introducing brokers, major swap participants and swap dealers that are subject to the jurisdiction of the Commission	

The Financial Privacy Rule

The Financial Privacy Rule is another name for the GLBA's requirement that financial institutions must give customers and consumers the right to opt out, or not allow, a financial institution to share the customer/consumer's information with nonaffiliated third parties prior to sharing it. (15 U.S.C. § 6802).

What is nonpublic personal information?

NPI is personally identifiable financial information that is not available in public records that (a) a consumer gives to a financial institution (b) for any transaction or service performed for the consumer, or (c) is otherwise obtained by the financial institution in relation to providing the customer with a financial product or service.

NPI includes "lists, descriptions, or grouping of consumers (and publicly available information pertaining to them)" created using nonpublic personal information.

How does the GLBA regulate information sharing?

A financial institution cannot share a consumer's NPI with a nonaffiliated third party without first notifying the consumer and giving the consumer a chance to opt out of information sharing. The notice must be clear and conspicuous, and the consumer must be given time to review the information and say no to information sharing (15 U.S.C. § 6801).

A financial institution may not share account numbers, access numbers and access codes for credit cards, deposit accounts and the like with third parties "for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer." (15 U.S.C. § 6801) Such information may be shared with a credit reporting agency.

Are there exceptions to the GLBA privacy notice requirements?

Yes. NPI may be shared without a consumer/customer's permission in certain cases. For example, NPI may be shared if the NPI is provided to a third party to perform services for the financial institution. In that case, the financial institution must inform the consumer about the information-sharing arrangement and that there is a confidentiality agreement protecting the information between the financial institution and the nonaffiliated third party (15 U.S.C. § 6802 (https://www.law.cornell.edu/uscode/text/15/6802)).

(https://www.law.cornell.edu/uscode/text/15/6802), and consult with legal counsel.

What is the difference between a customer and a consumer?

A consumer is an individual who receives or has received a financial product or service from a financial institution mainly for personal, family or household purposes. An example is a person who cashes "a check at a check-cashing company," or a person who makes a wire transfer at a financial institution.

A consumer becomes a customer when there is a continuing customer relationship between a financial institution and the consumer. All customers are consumers. A customer includes a person who opens "a credit card account with a financial institution," an individual who leases "an automobile from an auto dealer," or a person who obtains "the services of a tax preparer or investment adviser."

What are the privacy notice requirements for consumers?

Consumers do not have an on-going relationship with the financial institution. The only time a financial institution must give a consumer a privacy notice is consumer if the financial institution wants to share the consumer's nonpublic personal information with a nonaffiliated third party. In that case, the financial institution must provide the consumer with a privacy notice with information about how to opt-out from information sharing before the financial institution shares any information. If the consumer does not exercise the opt-out right, the financial institution is free to share the consumer's nonpublic personal information with nonaffiliated third parties.

What are the privacy notice requirements for customers?

Customers have an on-going relationship with a financial institution. For customers, financial institutions must provide an initial privacy notice at the start of the customer relationship and provide annual privacy notices.

A privacy notice describes the financial institution's policies and practices for sharing nonpublic personal information with nonaffiliated *and* affiliated third parties, and includes:

- The categories of persons to whom the information is or may be shared with.
- The financial institution's policies and practices for sharing information about customers who stop being customers.

- How the institution protects the confidentiality and security of nonpublic personal information.
- Any other information required under section 603(d)(2)(A) of the Fair Credit Reporting Act (FCRA).

What is a nonaffiliated third party?

A party that is not related by common ownership or corporate control.

Under the GLBA, financial institutions must give consumers and customers a privacy notice with opt-out rights if they want to share nonpublic personal information with nonaffiliated third parties.

Can a nonaffiliated party that receives information share the information with another nonaffiliated party?

Yes, but only if the financial institution who provided the information to the nonaffiliated third party could have shared the information with the second nonaffiliated third party directly.

Is a model privacy form available and what is safe harbor?

Yes, a model privacy form is available. If an institution uses the model privacy form, the institution "obtains a "safe harbor" and will satisfy the disclosure requirements for notices (https://www.ftc.gov/news-events/press-releases/2009/11/federal-regulators-issue-final-model-privacy-notice-form)" (FTC, Federal Regulators Issue Final Model Privacy NoticeForm, published Nov. 19, 2009).

For more context about why and how a model privacy form was developed, see the Supplemental Information section of the Final Model Privacy Form under the Gramm-Leach-Bliley Act Rule (https://www.ftc.gov/sites/default/files/attachments/press-releases/federal-regulators-issue-final-model-privacy-notice-form/privacymodelform_rule.pdf). In 2006, the Financial Services Regulatory Relief Act amended the GLBA. The Relief Act amendment directed financial regulatory agencies to collaborate and develop a model privacy notice. In 2009, eight regulatory agencies amended each of their rules to adopt a model privacy form.

Can a financial institution post its annual privacy notice online?

an alternative method for delivering annual privacy notices (https://s3.amazonaws.com/files.consumerfinance.gov/f/201410_cfpb_final-rule_annual-privacy-notice.pdf). This alternative method does not apply to financial institutions regulated by the Securities and Exchange Commission, Commodity Futures Trading Commission or Federal Trade Commission.

In general, financial institutions regulated by the Bureau of Consumer Financial Protection may use an alternative delivery method if the financial institution will not share nonpublic personal information in a manner that will trigger GLBA opt-out rights, and if the financial institution uses the model form or model privacy notice (*see* 76 FR 79025 (https://www.gpo.gov/fdsys/granule/FR-2011-12-21/2011-31729), Dec. 21, 2011).

What is the FAST Act and how does it affect annual privacy notice requirements?

The FAST Act (https://www.gpo.gov/fdsys/pkg/BILLS-114hr22enr/pdf/BILLS-114hr22enr.pdf), or Fixing America's Surface Transportation Act, became law in December 2015. Under the FAST Act's "Eliminate Privacy Notice Confusion" section (§75001), financial institutions may skip the requirement of providing an annual privacy notice under certain circumstances. In general, a financial institution does not need to send an annual privacy notice if the financial institution shares NPI under limited circumstances and if the financial institution has not changed its privacy policy and practices from that described in the financial institution's most recent privacy notice.

How is the Fair Credit Reporting Act related to the GLBA?

The Fair Credit Reporting Act (http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf) is a U.S. federal privacy law that applies to consumer reporting agencies and consumer report information (e.g., information affecting a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living that is used or expected to be used for reasons including assessing credit worthiness). The FCRA gives consumers an opt-out right for information shared with both affiliated and nonaffiliated third parties whereas the GLBA gives consumers an opt-out right for information shared with nonaffiliated third parties only.

Determine whether your financial institution is defined as a consumer reporting agency under the FRCA; if so, privacy requirements for both laws apply

What is it?

In 2006, the Financial Services Regulatory Relief Act (Relief Act) amended the GLBA. The Relief Act amendment directed financial regulatory agencies to collaborate and develop a model privacy notice. In 2009, eight regulatory agencies amended each of their rules to adopt a model privacy form.

For more context about why and how a model privacy form was developed, see the *Supplemental Information* section of the Final Model Privacy Form under the Gramm-Leach-Bliley Act Rule (https://www.ftc.gov/sites/default/files/attachments/press-releases/federal-regulators-issue-final-model-privacy-notice-form/privacymodelform_rule.pdf).

Can a financial institution post its annual privacy notice online?

Yes — if the financial institution meets certain requirements, the institution may use an alternative method for delivering annual privacy notices (https://s3.amazonaws.com/files.consumerfinance.gov/f/201410_cfpb_final-rule_annual-privacy-notice.pdf). This alternative method does not apply to financial institutions regulated by the Securities and Exchange Commission, Commodity Futures Trading Commission or Federal Trade Commission.

In general, financial institutions regulated by the Bureau of Consumer Financial Protection may use an alternative delivery method if the financial institution will not share nonpublic personal information in a manner that will trigger GLBA opt-out rights, and if the financial institution uses the model form or model privacy notice (*see* 76 FR 79025 (https://www.gpo.gov/fdsys/granule/FR-2011-12-21/2011-31729), Dec. 21, 2011).

What is the FAST Act and how does it affect annual privacy notice requirements?

The FAST Act (https://www.gpo.gov/fdsys/pkg/BILLS-114hr22enr/pdf/BILLS-114hr22enr.pdf), or Fixing America's Surface Transportation Act, became law in December 2015. Under the FAST Act's "Eliminate Privacy Notice Confusion" section (§75001), financial institutions may skip the requirement of providing an annual privacy notice under certain circumstances. In general, a financial institution does not need to send an annual privacy notice if the financial

changed its privacy policy or practices from that described in the financial institution's most recent privacy notice.

How is the Fair Credit Reporting Act related to the GLBA?

The Fair Credit Reporting Act (http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf) is a U.S. federal privacy law that applies to consumer reporting agencies and consumer report information (e.g., information affecting a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living that is used or expected to be used for reasons including assessing credit worthiness). The FCRA gives consumers an opt-out right for information shared with both affiliated and nonaffiliated third parties whereas the GLBA gives consumers an opt-out right for information shared with nonaffiliated third parties only.

If your financial institution is defined as a consumer reporting agency under the FRCA, privacy requirements for both laws apply.

Privacy Protection for Customer Information — Pretexting & Fraudulent Access

What is pretexting and how does the GLBA regulate the fraudulent access of financial information?

Pretexting involves a person making up a story and tricking another person into providing nonpublic information.

Under the GLBA, a person may not obtain or try to obtain customer information about another person "by making a false, fictitious, or fraudulent statement or representation to an officer, employee," agent, or customer of an institution (15 U.S.C. § 6821 (https://www.law.cornell.edu/uscode/text/15/6821)). The GLBA also prohibits a person from knowingly using "forged, counterfeit, lost, fraudulently obtained" documents to obtain consumer information (*Id.*).

financial information. Individuals who "knowingly and intentionally violate" or "attempt to violate" the regulation may be fined, imprisoned, or both.

Tags:

Pease International Tradeport, 75 Rochester Ave.
Portsmouth, NH 03801 USA • +1 603.427.9200