

Gramm-Leach-Bliley Act  
15 USC, Subchapter I, Sec. 6801-6809  
Disclosure of Non-public Personal Information

---

**Sec.**

**6801. Protection of nonpublic personal information.**

- (a) Privacy obligation policy.
- (b) Financial institutions safeguards.

**6802. Obligations with respect to disclosures of personal information.**

- (a) Notice requirements.
- (b) Opt out.
- (c) Limits on reuse of information.
- (d) Limitations on the sharing of account number information for marketing purposes.
- (e) General exceptions.

**6803. Disclosure of institution privacy policy.**

- (a) Disclosure required.
- (b) Information to be included.

**6804. Rulemaking.**

- (a) Regulatory authority.
- (b) Authority to grant exceptions.

**6805. Enforcement.**

- (a) In general.
- (b) Enforcement of section 6801.
- (c) Absence of State action.
- (d) Definitions.

**6806. Relation to other provisions.**

**6807. Relation to State laws.**

- (a) In general.
- (b) Greater protection under State law.

**6808. Study of information sharing among financial affiliates.**

- (a) In general.
- (b) Consultation.
- (c) Report.

**6809. Definitions.**

---

**Sec. 6801. Protection of nonpublic personal information**

- (a) Privacy obligation policy

It is the policy of the Congress 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' nonpublic personal information.

(b) Financial institutions safeguards

In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards -

**(1) to insure the security and confidentiality of customer records and information;**

**(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and**

**(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.**

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 6803, 6805 of this title.

**NOTE:** Pub. L. 106-102, title V, Sec. 510, Nov. 12, 1999, 113 Stat. 1445, provided that: "This subtitle (subtitle A (Sec. 501-510) of title V of Pub. L. 106-102, enacting this subchapter and amending section 1681s of this title) shall take effect 6 months after the date on which rules are required to be prescribed under section 504(a)(3) (15 U.S.C. 6804(a)(3)), except -

"(1) to the extent that a later date is specified in the rules prescribed under section 504; and

"(2) that sections 504 (15 U.S.C. 6804) and 506 (enacting section 6806 of this title and amending section 1681s of this title) shall be effective upon enactment (Nov. 12, 1999)."

**Sec. 6802. Obligations with respect to disclosures of personal information**

(a) Notice requirements

Except as otherwise provided in this subchapter, a financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 6803 of this title.

(b) Opt out

(1) In general

A financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless -

(A) such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 6804 of this title, that such information may be disclosed to such third party;

(B) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such

information not be disclosed to such third party; and

(C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.

(2) Exception

This subsection shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with the requirements imposed by the regulations prescribed under section 6804 of this title, if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information.

(c) Limits on reuse of information

Except as otherwise provided in this subchapter, a nonaffiliated third party that receives from a financial institution nonpublic personal information under this section shall not, directly or through an affiliate of such receiving third party, disclose such information to any other person that is a nonaffiliated third party of both the financial institution and such receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution.

(d) Limitations on the sharing of account number information for marketing purposes

A financial institution shall not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

(e) General exceptions

Subsections (a) and (b) of this section shall not prohibit the disclosure of nonpublic personal information -

(1) as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with -

(A) servicing or processing a financial product or service requested or authorized by the consumer;

(B) maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

(C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer;

(2) with the consent or at the direction of the consumer;

(3)(A) to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein; (B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (C) for required institutional risk control, or for resolving customer disputes or inquiries; (D) to persons holding a legal or beneficial interest

relating to the consumer; or (E) to persons acting in a fiduciary or representative capacity on behalf of the consumer;

(4) to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors;

(5) to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title 31, and chapter 2 of title I of Public Law 91-508 (12 U.S.C. 1951-1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

(6)(A) to a consumer reporting agency in accordance with the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), or (B) from a consumer report reported by a consumer reporting agency;

(7) in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or

(8) to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.

(Pub. L. 106-102, title V, Sec. 502, Nov. 12, 1999, 113 Stat. 1437.)

#### REFERENCES IN TEXT

This subchapter, referred to in subsecs. (a) and (c), was in the original "this subtitle", meaning subtitle A (Sec. 501 et seq.) of title V of Pub. L. 106-102, Nov. 12, 1999, 113 Stat. 1436, which enacted this subchapter and amended section 1681s of this title.

For complete classification of subtitle A to the Code, see Tables.

The Right to Financial Privacy Act of 1978, referred to in subsec. (e)(5), is title XI of Pub. L. 95-630, Nov. 10, 1978, 92 Stat. 3697, as amended, which is classified generally to chapter 35 (Sec. 3401 et seq.) of Title 12, Banks and Banking. For complete classification of this Act to the Code, see Short Title note set out under section 3401 of Title 12 and Tables.

Chapter 2 of title I of Public Law 91-508, referred to in subsec. (e)(5), is chapter 2 (Sec. 121-129) of title I of Pub. L. 91-508, Oct. 26, 1970, 84 Stat. 1116, which is classified generally to chapter 21 (Sec. 1951 et seq.) of Title 12, Banks and Banking. For complete classification of chapter 2 to the Code, see Tables.

The Fair Credit Reporting Act, referred to in subsec. (e)(6)(A), is title VI of Pub. L. 90-321, as added by Pub. L. 91-508, title VI, Sec. 601, Oct. 26, 1970, 84 Stat. 1127, as amended, which is classified generally to subchapter III (Sec. 1681 et seq.) of chapter 41 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 1601 of this title and Tables.

#### SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 6803, 6804, 6809 of this title.

**Sec. 6803. Disclosure of institution privacy policy**

(a) Disclosure required

At the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship, a financial institution shall provide a clear and conspicuous disclosure to such consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 6804 of this title, of such financial institution's policies and practices with respect to -

(1) disclosing nonpublic personal information to affiliates and nonaffiliated third parties, consistent with section 6802 of this title, including the categories of information that may be disclosed;

(2) disclosing nonpublic personal information of persons who have ceased to be customers of the financial institution; and

(3) protecting the nonpublic personal information of consumers.

Such disclosures shall be made in accordance with the regulations prescribed under section 6804 of this title.

(b) Information to be included

The disclosure required by subsection (a) of this section shall include -

(1) the policies and practices of the institution with respect to disclosing nonpublic personal information to nonaffiliated third parties, other than agents of the institution, consistent with section 6802 of this title, and including -

(A) the categories of persons to whom the information is or may be disclosed, other than the persons to whom the information may be provided pursuant to section 6802(e) of this title; and

(B) the policies and practices of the institution with respect to disclosing of nonpublic personal information of persons who have ceased to be customers of the financial institution;

(2) the categories of nonpublic personal information that are collected by the financial institution;

(3) the policies that the institution maintains to protect the confidentiality and security of nonpublic personal information in accordance with section 6801 of this title; and

(4) the disclosures required, if any, under section 1681a(d)(2)(A)(iii) of this title.

(Pub. L. 106-102, title V, Sec. 503, Nov. 12, 1999, 113 Stat. 1439.)

**SECTION REFERRED TO IN OTHER SECTIONS**

This section is referred to in section 6802 of this title.

**Sec. 6804. Rulemaking**

(a) Regulatory authority

(1) Rulemaking

The Federal banking agencies, the National Credit Union Administration, the Secretary of the Treasury, the Securities and Exchange Commission, and the Federal Trade Commission shall each prescribe, after consultation as appropriate with representatives of State insurance authorities designated by the National Association of Insurance Commissioners, such regulations as may be necessary to carry out the purposes of this subchapter with respect to the financial institutions subject to their jurisdiction under section 6805 of this title.

(2) Coordination, consistency, and comparability

Each of the agencies and authorities required under paragraph (1) to prescribe regulations shall consult and coordinate with the other such agencies and authorities for the purposes of assuring, to the extent possible, that the regulations prescribed by each such agency and authority are consistent and comparable with the regulations prescribed by the other such agencies and authorities.

(3) Procedures and deadline

Such regulations shall be prescribed in accordance with applicable requirements of title 5 and shall be issued in final form not later than 6 months after November 12, 1999.

(b) Authority to grant exceptions

The regulations prescribed under subsection (a) of this section may include such additional exceptions to subsections (a) through (d) of section 6802 of this title as are deemed consistent with the purposes of this subchapter.

(Pub. L. 106-102, title V, Sec. 504, Nov. 12, 1999, 113 Stat.1439.)

**SECTION REFERRED TO IN OTHER SECTIONS**

This section is referred to in sections 6802, 6803, 6809 of this title.

**Sec. 6805. Enforcement**

(a) In general

This subchapter and the regulations prescribed thereunder shall be enforced by 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:

(1) Under section 1818 of title 12, in the case of -

(A) 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 advisers), by the Office of the Comptroller of the Currency;

(B) member banks of the Federal Reserve System (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 (12 U.S.C. 601 et seq., 611 et seq.), and bank holding companies and their non-bank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), by the Board of Governors of the Federal Reserve System;

(C) 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 advisers), by the Board of Directors of the Federal Deposit Insurance Corporation; and

(D) 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 advisers), by the Director of the Office of Thrift Supervision.

(2) Under the Federal Credit Union Act (12 U.S.C. 1751 et seq.), by the Board of the National Credit Union Administration with respect to any federally insured credit union, and any subsidiaries of such an entity.

(3) Under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.), by the Securities and Exchange Commission with respect to any broker or dealer.

(4) Under the Investment Company Act of 1940 (15 U.S.C. 80a-1 et seq.), by the Securities and Exchange Commission with respect to investment companies.

(5) Under the Investment Advisers Act of 1940 (15 U.S.C. 80b-1

et seq.), by the Securities and Exchange Commission with respect to investment advisers registered with the Commission under such Act.

(6) Under State insurance law, in the case of any person engaged in providing insurance, by the applicable State insurance authority of the State in which the person is domiciled, subject to section 6701 of this title.

(7) Under the Federal Trade Commission Act (15 U.S.C. 41 et seq.), by the Federal Trade Commission for any other financial institution or other person that is not subject to the jurisdiction of any agency or authority under paragraphs (1) through (6) of this subsection.

(b) Enforcement of section 6801

(1) In general

Except as provided in paragraph (2), the agencies and authorities described in subsection (a) of this section shall implement the standards prescribed under section 6801(b) of this title in the same manner, to the extent practicable, as standards prescribed pursuant to section 1831p-1(a) of title 12 are implemented

pursuant to such section.

(2) Exception

The agencies and authorities described in paragraphs (3), (4), (5), (6), and (7) of subsection (a) of this section shall implement the standards prescribed under section 6801(b) of this title by rule with respect to the financial institutions and other persons subject to their respective jurisdictions under subsection (a) of this section.

(c) 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.

(d) Definitions

The terms used in subsection (a)(1) of this section that are not defined in this subchapter or otherwise defined in section 1813(s) of title 12 shall have the same meaning as given in section 3101 of title 12.

(Pub. L. 106-102, title V, Sec. 505, Nov. 12, 1999, 113 Stat. 1440.)

REFERENCES IN TEXT

Section 25 of the Federal Reserve Act, referred to in subsec. (a)(1)(B), is classified to subchapter I (Sec. 601 et seq.) of chapter 6 of Title 12, Banks and Banking. Section 25A of the Federal Reserve Act is classified to subchapter II (Sec. 611 et seq.) of chapter 6 of Title 12.

The Federal Credit Union Act, referred to in subsec. (a)(2), is act June 26, 1934, ch. 750, 48 Stat. 1216, as amended, which is classified generally to chapter 14 (Sec. 1751 et seq.) of Title 12, Banks and Banking. For complete classification of this Act to the Code, see section 1751 of Title 12 and Tables.

The Securities Exchange Act of 1934, referred to in subsec. (a)(3), is act June 6, 1934, ch. 404, 48 Stat. 881, as amended, which is classified principally to chapter 2B (Sec. 78a et seq.) of this title. For complete classification of this Act to the Code, see section 78a of this title and Tables. The Investment Company Act of 1940, referred to in subsec. (a)(4), is title I of act Aug. 22, 1940, ch. 686, 54 Stat. 789, as amended, which is classified generally to subchapter I (Sec. 80a-1 et seq.) of chapter 2D of this title. For complete classification of this Act to the Code, see section 80a-51 of this title and Tables.

The Investment Advisers Act of 1940, referred to in subsec. (a)(5), is title II of act Aug. 22, 1940, ch. 686, 54 Stat. 847, as amended, which is classified generally to subchapter II (Sec. 80b-1 et seq.) of chapter 2D of this title. For complete classification of this Act to the Code, see section 80b-20 of this title and Tables.

The Federal Trade Commission Act, referred to in subsec. (a)(7), is act Sept. 26, 1914, ch. 311, 38 Stat. 717, as amended, which is classified generally to subchapter I (Sec. 41 et seq.) of chapter 2 of this title. For complete classification of this Act to the Code, see section 58 of this title and Tables.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 6801, 6804, 6807 of this title.

**Sec. 6806. Relation to other provisions**

Except for the amendments made by subsections (a) and (b), nothing in this chapter shall be construed to modify, limit, or supersede the operation of the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be drawn on the basis of the provisions of this chapter regarding whether information is transaction or experience information under section 603 of such Act (15 U.S.C. 1681a).

(Pub. L. 106-102, title V, Sec. 506(c), Nov. 12, 1999, 113 Stat. 1442.)

REFERENCES IN TEXT

Amendments made by subsections (a) and (b), referred to in text, means amendments made by section 506(a) and (b) of Pub. L. 106-102, which amended section 1681s of this title.

This chapter, referred to in text, was in the original "this title", meaning title V of Pub. L. 106-102, Nov. 12, 1999, 113 Stat. 1436, as amended, which enacted this chapter and amended section 1681s of this title. For complete classification of title V to the Code, see Tables.

The Fair Credit Reporting Act, referred to in text, is title VI of Pub. L. 90-321, as added by Pub. L. 91-508, title VI, Sec. 601, Oct. 26, 1970, 84 Stat. 1127, as amended, which is classified generally to subchapter III (Sec. 1681 et seq.) of chapter 41 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 1601 of this title and Tables.

#### **Sec. 6807. Relation to State laws**

(a) In general

This subchapter and the amendments made by this subchapter shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this subchapter, and then only to the extent of the inconsistency.

(b) Greater protection under State law

For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter and the amendments made by this subchapter, as determined by the Federal Trade Commission, after consultation with the agency or authority with jurisdiction under section 6805(a) of this title of either the person that initiated the complaint or that is the subject of the complaint, on its own motion or upon the petition of any interested party.

(Pub. L. 106-102, title V, Sec. 507, Nov. 12, 1999, 113 Stat. 1442.)

#### REFERENCES IN TEXT

This subchapter, referred to in text, was in the original "this subtitle", meaning subtitle A (Sec. 501-510) of title V of Pub. L. 106-102, Nov. 12, 1999, 113 Stat. 1436, which enacted this subchapter and amended section 1681s of this title. For complete classification of subtitle A to the Code, see Tables.

#### **Sec. 6808. Study of information sharing among financial affiliates**

(a) In general

The Secretary of the Treasury, in conjunction with the Federal functional regulators and the Federal Trade Commission, shall conduct a study of information sharing practices among financial institutions and their affiliates. Such study shall include -

- (1) the purposes for the sharing of confidential customer information with affiliates or with nonaffiliated third parties;
- (2) the extent and adequacy of security protections for such information;
- (3) the potential risks for customer privacy of such sharing of information;
- (4) the potential benefits for financial institutions and affiliates of such sharing of information;
- (5) the potential benefits for customers of such sharing of information;
- (6) the adequacy of existing laws to protect customer privacy;
- (7) the adequacy of financial institution privacy policy and privacy rights

disclosure under existing law;

(8) the feasibility of different approaches, including opt-out and opt-in, to permit customers to direct that confidential information not be shared with affiliates and nonaffiliated third parties; and

(9) the feasibility of restricting sharing of information for specific uses or of permitting customers to direct the uses for which information may be shared.

(b) Consultation

The Secretary shall consult with representatives of State insurance authorities designated by the National Association of Insurance Commissioners, and also with financial services industry, consumer organizations and privacy groups, and other representatives of the general public, in formulating and conducting the study required by subsection (a) of this section.

(c) Report

On or before January 1, 2002, the Secretary shall submit a report to the Congress containing the findings and conclusions of the study required under subsection (a) of this section, together with such recommendations for legislative or administrative action as may be appropriate.

(Pub. L. 106-102, title V, Sec. 508, Nov. 12, 1999, 113 Stat.1442.)

**Sec. 6809. Definitions**

As used in this subchapter:

(1) Federal banking agency

The term "Federal banking agency" has the same meaning as given in section 1813 of title 12.

(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.

(3) Financial institution

(A) In general

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.

(B) Persons subject to CFTC regulation

Notwithstanding subparagraph (A), the term "financial institution" does not include any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 et seq.).

(C) Farm credit institutions

Notwithstanding subparagraph (A), the term "financial institution" does not include the Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.).

(D) Other secondary market institutions

Notwithstanding subparagraph (A), the term "financial institution" does not include institutions chartered by Congress specifically to engage in transactions described in section 6802(e)(1)(C) of this title, as long as such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

(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.

(5) Nonaffiliated third party

The term "nonaffiliated third party" means any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution, but does not include a joint employee of such institution.

(6) Affiliate

The term "affiliate" means any company that controls, is controlled by, or is under common control with another company.

(7) Necessary to effect, administer, or enforce

The term "as necessary to effect, administer, or enforce the transaction" means -

(A) the disclosure is required, or is a usual, appropriate, or acceptable method, to carry out the transaction or the product or service business of which the transaction is a part, and record or service or maintain the consumer's account in the ordinary course of providing the financial service or financial product, or to administer or service benefits or claims relating to the transaction or the product or service business of which it is a part, and includes -

(i) providing the consumer or the consumer's agent or broker with a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product; and

(ii) the accrual or recognition of incentives or bonuses associated with the transaction that are provided by the financial institution or any other party;

(B) the disclosure is required, or is one of the lawful or appropriate methods, to enforce the rights of the financial institution or of other persons engaged in carrying out the financial transaction, or providing the product or service;

(C) the disclosure is required, or is a usual, appropriate, or acceptable method, for insurance underwriting at the consumer's request or for reinsurance purposes, or for any of the following purposes as they relate to a consumer's insurance: Account administration, reporting, investigating, or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research

projects, or as otherwise required or specifically permitted by Federal or State law; or

(D) the disclosure is required, or is a usual, appropriate or acceptable method, in connection with -

(i) the authorization, settlement, billing, processing, clearing, transferring, reconciling, or collection of amounts charged, debited, or otherwise paid using a debit, credit or other payment card, check, or account number, or by other payment means;

(ii) the transfer of receivables, accounts or interests therein; or

(iii) the audit of debit, credit or other payment information.

(8) State insurance authority

The term "State insurance authority" means, in the case of any person engaged in providing insurance, the State insurance authority of the State in which the person is domiciled.

(9) Consumer

The term "consumer" means an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual.

(10) Joint agreement

The term "joint agreement" means a formal written contract pursuant to which two or more financial institutions jointly offer, endorse, or sponsor a financial product or service, and as may be further defined in the regulations prescribed under section 6804 of this title.

(11) Customer relationship

The term "time of establishing a customer relationship" shall be defined by the regulations prescribed under section 6804 of this title, and shall, in the case of a financial institution engaged in extending credit directly to consumers to finance purchases of goods or services, mean the time of establishing the credit relationship with the consumer.

(Pub. L. 106-102, title V, Sec. 509, Nov. 12, 1999, 113 Stat. 1443.)

REFERENCES IN TEXT

The Commodity Exchange Act, referred to in par. (3)(B), is act Sept. 21, 1922, ch. 369, 42 Stat. 998, as amended, which is classified generally to chapter 1 (Sec. 1 et seq.) of Title 7, Agriculture. For complete classification of this Act to the Code, see section 1 of Title 7 and Tables.

The Farm Credit Act of 1971, referred to in par. (3)(C), is Pub. L. 92-181, Dec. 10, 1971, 85 Stat.

583, as amended, which is classified generally to chapter 23 (Sec. 2001 et seq.) of Title 12, Banks and Banking. For complete classification of this Act to the Code, see Short Title note set out under section 2001 of Title 12 and Tables.

**For Release:** May 23, 2003

## **FTC Financial Information Safeguards Rule Takes Effect**

The Federal Trade Commission's Safeguards Rule, which implements the security provisions of the Gramm-Leach-Bliley Act, becomes effective today. As of today, financial institutions subject to the Rule must have in place a comprehensive security program to ensure the security and confidentiality of customer information.

The Safeguards Rule was published in the Federal Register one year ago [67 Fed Reg 36484 (May 23, 2002)] and can be found on the Federal Trade Commission Web site at <http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html>. Financial institutions covered by the newly-effective Rule include companies that engage in a wide variety of "financial activities," such as brokering or servicing consumer loans; transferring or safeguarding money; preparing individual tax returns; providing financial advice or credit counseling; providing residential real estate settlement services; collecting consumer debts; and an array of other activities that are deemed "financial" by pre-existing regulations. A list of the financial activities that trigger the Rule can be found on the FTC's Web site. The Safeguards Rule applies both to financial institutions that collect information from their customers and to financial institutions - such as credit reporting agencies, ATM operators, and check cashing services - that receive customer information from other financial institutions.

To implement its information security program, each financial institution must:

- **Designate an employee or employees to coordinate the program;**
- **Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information and assess the sufficiency of any safeguards in place to control the risks;**
- **Design and implement safeguards to address the risks and monitor the effectiveness of these safeguards;**
- **Select and retain service providers that are capable of maintaining appropriate safeguards for the information and require them, by contract, to implement and maintain such safeguards; and**
- **Adjust the information security program in light of developments that may materially affect the program.**

Although each information security program must include these basic elements, the Rule allows companies to select specific safeguards that are appropriate to their size and complexity, the nature and scope of their activities, and the sensitivity of the customer information they maintain.

# In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act

For more information about the Financial Privacy Rule requirements, please see the FTC's [Small Business Guide](#)

Protecting the privacy of consumer information held by "financial institutions" is at the heart of the financial privacy provisions of the Gramm-Leach-Bliley Financial Modernization Act of 1999. The GLB Act requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some - but not all - sharing of their information.

Here's a brief look at the basic financial privacy requirements of the law.

## Financial Institutions

The GLB Act applies to "financial institutions" - companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance. The Federal Trade Commission has authority to enforce the law with respect to "financial institutions" that are not covered by the federal banking agencies, the Securities and Exchange Commission, the Commodity Futures Trading Commission, and state insurance authorities. Among the institutions that fall under FTC jurisdiction for purposes of the GLB Act are non-bank mortgage lenders, loan brokers, some financial or investment advisers, tax preparers, providers of real estate settlement services, and debt collectors. At the same time, the FTC's regulation applies only to companies that are "significantly engaged" in such financial activities.

The law requires that financial institutions protect information collected about individuals; it does not apply to information collected in business or commercial activities.

## Consumers and Customers

A company's obligations under the GLB Act depend on whether the company has consumers or customers who obtain its services. A *consumer* is an individual who obtains or has obtained a financial product or service from a financial institution for personal, family or household reasons. A *customer* is a consumer with a continuing relationship with a financial institution. Generally, if the relationship between the financial institution and the individual is significant and/or long-term, the individual is a customer of the institution. For example, a person who gets a mortgage from a lender or hires a broker to get a personal loan is considered a customer of the lender or the broker, while a person who uses a check-cashing service is a consumer of that service.

Why is the difference between consumers and customers so important? Because only customers are entitled to receive a financial institution's privacy notice automatically. Consumers are entitled to receive a privacy notice from a financial institution only if the company shares the consumers' information with companies not affiliated with it, with some exceptions. Customers must receive a notice every year for as long as the customer relationship lasts.

The privacy notice must be given to individual customers or consumers by mail or in-person delivery; it may not, say, be posted on a wall. Reasonable ways to deliver a notice may depend on the type of business the institution is in: for example, an online lender may post its notice on its website and require online consumers to acknowledge receipt as a necessary part of a loan application.

## **The Privacy Notice**

The privacy notice must be a clear, conspicuous, and accurate statement of the company's privacy practices; it should include what information the company collects about its consumers and customers, with whom it shares the information, and how it protects or safeguards the information. The notice applies to the "nonpublic personal information" the company gathers and discloses about its consumers and customers; in practice, that may be most - or all - of the information a company has about them. For example, nonpublic personal information could be information that a consumer or customer puts on an application; information about the individual from another source, such as a credit bureau; or information about transactions between the individual and the company, such as an account balance. Indeed, even the fact that an individual is a consumer or customer of a particular financial institution is nonpublic person information. But information that the company has reason to believe is lawfully public - such as mortgage loan information in a jurisdiction where that information is publicly recorded - is not restricted by the GLB Act.

## **Opt-Out Rights**

Consumers and customers have the right to opt out of - or say no to - having their information shared with certain third parties. The privacy notice must explain how - and offer a reasonable way - they can do that. For example, providing a toll-free telephone number or a detachable form with a pre-printed address is a reasonable way for consumers or customers to opt out; requiring someone to write a letter as the only way to opt out is not.

The privacy notice also must explain that consumers have a right to say no to the sharing of certain information - credit report or application information - with the financial institution's affiliates. An affiliate is an entity that controls another company, is controlled by the company, or is under common control with the company. Consumers have this right under a different law, the Fair Credit Reporting Act. The GLB Act does not give consumers the right to opt out when the financial institution shares other information with its affiliates.

The GLB Act provides no opt-out right in several other situations: For example, an individual cannot opt out if:

- a financial institution shares information with outside companies that provide essential services like data processing or servicing accounts;
- the disclosure is legally required;
- a financial institution shares customer data with outside service providers that market the financial company's products or services.

## **Receiving Nonpublic Personal Information**

The GLB Act puts some limits on how anyone that receives nonpublic personal information from a financial institution can use or re-disclose the information. Take the case of a lender that discloses customer information to a service provider responsible for mailing account statements, where the consumer has no right to opt out: The service provider may use the information for limited purposes - that is, for mailing account statements. It may not sell the information to other organizations or use it for marketing.

However, it's a different scenario when a company receives nonpublic personal information from a financial institution that provided an opt-out notice -- and the consumer didn't opt out. In this case, the recipient steps into the shoes of the disclosing financial institution, and may use the information for its own purposes or re-disclose it to a third party, consistent with the financial institution's privacy notice. That is, if the privacy notice of the financial institution allows for disclosure to other unaffiliated financial institutions - like insurance providers - the recipient may re-disclose the information to an unaffiliated insurance provider.

### **Other Provisions**

Other important provisions of the GLB Act also impact how a company conducts business. For example, financial institutions are prohibited from disclosing their customers' account numbers to non-affiliated companies when it comes to telemarketing, direct mail marketing or other marketing through e-mail, even if the individuals have not opted out of sharing the information for marketing purposes.

Another provision prohibits "pretexting" - the practice of obtaining customer information from financial institutions under false pretenses. The FTC has brought several cases against information brokers who engage in pretexting.

### **For More Information**

The FTC is one of eight federal regulatory agencies that has the authority to enforce the financial privacy law, along with the state insurance authorities. The federal banking agencies, the Securities and Exchange Commission and the Commodity Futures Trading Commission have jurisdiction over banks, thrifts, credit unions, brokerage firms and commodity traders. The FTC has additional details on the GLB Act, the Commission's Privacy Rule and a compliance guide for small business owners at [www.ftc.gov/privacy](http://www.ftc.gov/privacy).

## **GENERAL QUESTIONS**

### **1. Does Gramm-Leach-Bliley (GLB) apply to my company?**

GLB applies to "financial institutions," but financial institution is so broadly defined that it includes not just banks, credit unions, and securities brokers, but also real estate appraisers, insurance companies, *automobile leasing companies*, companies that operate travel agencies in connection with financial services, retailers that issue their own credit cards directly to consumers, and any other entity that is "significantly involved in financial activities."

### **2. When do the GLB regulations take effect?**

The GLB regulations went into effect on November 13, 2000, but companies have until July 1, 2001, to come into full compliance. Seven federal agencies issued regulations implementing the privacy provisions of the Act, but we are primarily concerned here with the rules put out by the Federal Trade Commission.

### **3. We are complying with The DMA's Privacy Promise; do we have to follow the GLB rules, too?**

Yes. Although there are similarities between the GLB regulations and the Privacy Promise, the GLB rules are law and the Privacy Promise is not, and in some areas the GLB rules require more than the Privacy Promise.

#### **4. WHAT DOES MY COMPANY HAVE TO DO TO COMPLY?**

Before you can share "non-public personal information" (NPPI) with anybody other than affiliates, you must provide the consumer with detailed notice (see "Privacy Notices" below) and the opportunity to say "no" (opt out).

NPPI is defined as personally identifiable financial information resulting from any transaction with the consumer or any service performed for the consumer. It even includes a simple list of the names and addresses of a financial institution's customers.

More specifically, NPPI includes:

- information that a consumer provides on an application to obtain a loan, credit card, or other financial product or service;
- account balance information, payment history, and credit or debit card purchase history;
- any information about a consumer if it reveals that the individual is or has been a customer of the financial institution;
- any information that a consumer provides in connection with the collection or servicing of a credit account.

NPPI does not include publicly available information or consumer lists put together without using any NPPI.

An affiliate is a company that is controlled by another company. Control of a company is defined as:

- the power to vote 25 percent or more of the stock;
- the ability to control the election of a majority of the company directors; or
- the power to exercise a controlling influence over the management or policies of the company.

#### **5. Are there any exceptions to the ban on disclosure of account numbers to nonaffiliated third parties for marketing purposes?**

Yes. If a customer chooses to participate in a private label credit card program (such as a Wal-Mart Visa), the merchant and the financial institution can share the consumer's account number if the consumer is told upfront who the participants in the private label credit card are.

The rules also allow disclosures of account numbers to agents or service providers (such as telemarketing firms) for the purpose of marketing the financial institution's own products or services, as long as the agent or service provider is not allowed to debit the consumer's account without the consumer's consent.

**6. Does my company have to give everybody we do business with the same kind of notice and opt out?**

No. The rules make a distinction between a "consumer" and a "customer". Generally, a "consumer" is someone who has only a brief relationship with your company, such as applying for a loan but not taking it out. A "customer", on the other hand, has an on-going relationship, such as establishing an account or actually taking out a loan.

Isolated transactions in which a financial institution sells the consumer airline tickets, travel insurance, or traveler's checks, or the consumer purchases checks for a personal account from a financial institution do not, without further contact, establish a "customer" relationship.

This difference matters because GLB regulations require companies to provide "consumers" with one upfront notice if they plan to share the consumer's NPPI with an unaffiliated third party, but "customers" must be provided with information on the company's privacy policy when the customer relationship is established and annually thereafter.

## **PRIVACY NOTICES**

**7. What information needs to be included in the privacy notice?**

The following nine items must be included in the privacy notice:

- Categories of personal information your company collects;
- Categories of personal information you disclose;
- Categories of affiliates and nonaffiliated third parties to whom you disclose the information;
- An explanation of the right to opt out of disclosures to nonaffiliated third parties;
- A description of the kind of disclosures to nonaffiliated parties that are exceptions to the rules and don't give the consumer the right to opt out.

- An explanation of the ability to opt out of disclosures of information among affiliates under the Fair Credit Reporting Act (FCRA);
- If your company discloses information to third parties (such as telemarketing agencies) to conduct marketing campaigns, etc., on your behalf, you must include a separate statement of the categories of information disclosed and the categories of third parties to whom the information will be disclosed;
- A description of your confidentiality and security policies and practices; and
- Categories of personal information about former customers that you disclose and to whom you disclose such information.

## **8. When does my company have to deliver the notice to the consumer?**

You are required to deliver both an initial notice and, in the case of an ongoing "customer" relationship, annual notices.

The initial notice needs to be delivered at a "meaningful time" for both "consumers" and "customers". For consumers, the initial notice must be delivered before your company discloses any personal information about the consumer to a non-affiliated third party. If your company does not disclose any personal information about a consumer (except under the exception described in [#5](#)), you don't have to provide an initial notice.

You must deliver the initial notice to customers when you establish a customer relationship (for example, when a consumer opens a credit card account or buys insurance) and at least once a year as long as the customer relationship lasts.

## **9. How does my company have to deliver the notice?**

Notices must be provided in writing or, if the consumer agrees, electronically.

You CANNOT provide the notice solely by an oral explanation, either in person or over the telephone. You can hand a printed copy of the notice to the consumer or mail it by either First-Class or Standard (A) mail. If you mail the notice, you must give the consumer a reasonable amount of time to opt out (see "Consumer Opt-Out" below); if you use Standard (A) mail rather than First-Class, you will have to allow additional time for an opt-out.

Alternatively, you can provide the privacy notice by e-mail if the consumer obtains his or her financial products or services electronically. If the consumer

conducts transactions almost entirely at your Web site, you can satisfy the GLB notice requirements by "clearly and conspicuously" posting a privacy notice at your Web site and requiring consumers to acknowledge receipt of the notice before you provide them with any financial product or service.

In the case of annual privacy notices for long-term customers, if the customer uses the financial institution's Web site to access financial products and services and has agreed to accept notice on the Web site, you can satisfy the annual notice requirements by posting a privacy notice describing your current privacy practices and policies in a "clear and conspicuous" manner on your Web site. "Clear and conspicuous" means you must design your Web site so that the notice or a clear link to it cannot be overlooked.

**10. Do the GLB notices need to be stand-alone documents or can they be combined with other information or material?** You are allowed to combine the notices with other information provided that, like the Web site requirements, the notice is "clear and conspicuous", which means you should make it stand out with different fonts, shading, etc.

**11. Do I ever have to provide a revised privacy notice?**

If you start doing things that weren't mentioned in your original privacy notice, including collecting a new category of personal information or disclosing information to a new category of nonaffiliated third party, you might have to distribute a revised privacy notice before you disclose any personal information.

## **CONSUMER OPT-OUT**

**12. When do I have to give customers the right to opt out?**

You must provide a "reasonable opportunity to opt out" before you disclose personal information to nonaffiliated third parties. This obligation continues throughout your relationship with a customer. If you send the opt-out notice by mail, the customer must have at least 30 days to request the opt-out after the notice is sent.

### **13. What are acceptable methods for providing the consumer with the opportunity to opt out?**

The rules allow you to use any of the methods listed below, but one thing you can't do is make the customer write a letter.

- Designate check-off boxes in a prominent position on the relevant forms with the opt-out notice;
- Include a reply form that provides the address to which the form should be mailed;
- Provide an electronic means to opt out, such as a form that can be sent via e-mail or an opt-out procedure at your Web site;
- Provide a toll-free number that consumers can call. For example, your notice could state that "if you prefer that we not disclose personal information about you to third parties, you may call the following toll-free number: 800-\_\_\_\_\_."

## **EXCEPTIONS TO NOTICE AND OPT-OUT**

**14. Are there any exceptions to the notice and opt-out requirements?** You are allowed to share personal information (other than customer account numbers) without offering an opt-out with companies that run marketing campaigns for you or companies with whom you have joint marketing agreements. However, you must notify the customer that you are making the disclosures, and you must have a contract with the other company that requires it to maintain the confidentiality of the information, using it only to carry out the marketing campaign for which you supplied the information.

As noted in [#5](#) above, there is a general prohibition on the disclosure of account numbers for marketing purposes.

### **15. Under what other circumstances are notice and opt-out not required?**

There are a series of exceptions under which notice and opt-out are not required prior to sharing personal information with nonaffiliated third parties, including:

- where the disclosure is necessary to process or service a transaction;
- to protect record security and confidentiality;
- to provide information to legal counsel and to prove that the company is complying with industry standards;

- to respond to requests from regulators, self-regulatory organizations, and law enforcement;
- to report a customer's activities to a credit bureau;
- to protect against fraud;
- to individuals or businesses with a legal interest relating to the consumer;
- in connection with a proposed or actual merger or acquisition;
- to comply with laws and legal process.

## **REUSE AND REDISCLOSURE**

**16. The rules also apply to companies such as marketers, data processors, and consumer reporting agencies that sell information, if they receive personal information from financial institutions with whom they are not affiliated. How do the regulations limit the reuse and redisclosure of personal information by these third-party companies?**

If the third party receives the personal information from a financial institution under one of the exceptions previously mentioned, the recipient may reuse or redisclose the personal information only as necessary to carry out the activity covered by the exception under which it received the information.

If the third party receives the personal information from a financial institution outside of one of the exceptions, the recipient "steps into the shoes" of the financial institution and may reuse or redisclose the information only in accordance with the privacy policies and consumer opt-out choices of the company from which the information was obtained.

## **ENFORCEMENT**

**17. Who will enforce the rules?**

The rules will be enforced by the various federal agencies that have jurisdiction over financial institutions (and companies considered financial institutions) covered by GLB (the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Securities and Exchange Commission, and the National Credit Union Administration), the State insurance

authorities, and the Federal Trade Commission (FTC). Most direct marketers would almost certainly fall under FTC jurisdiction.

**18. Can consumers sue for violations of the GLB Act or rules?**

No. Neither the original law nor the regulations contain a private cause of action provision that would allow consumers to bring a suit for violations of the GLB Act's requirements. Enforcement is left to the Federal agencies and the State insurance agencies that have jurisdiction over financial institutions covered by the rules.

**19. What role do state governments have in connection with the new law?**

The GLB Act preempts only "inconsistent" state laws. It sets a floor, not a ceiling, over which states are free to pass stricter laws.

**OTHER**

**20. What should you do to prepare for GLB's effective date?**

To prepare for the effective date of the GLB Act you should, at a minimum, do the following:

- assess what financial services and products you provide, others provide on your behalf, and what you provide on behalf of others;
- evaluate your company's practices in sharing personal information;
- draft or revise your company's privacy policy to include the information required under the GLB;
- draft mandatory disclosures for your company's privacy notice;
- establish a method to track and honor opt-out requests;
- ensure compliance with relevant state laws; and
- revise language in employment, service, joint venture, and mergers and acquisitions agreements to conform to GLB requirements.

**21. Do the regulations distinguish between data collected prior to the effective date and data collected after the effective date?**

No. Before July 1, 2001, all companies covered by the rules must provide their existing customers with both a privacy notice and a reasonable opportunity to opt out of the disclosure of their personal information regardless of when it was collected.

The rules do distinguish between existing customers and former customers. Specifically, initial notices do not have to be given to customers whose relationships have terminated prior to July 1, 2001 (if an account is inactive on July 1, 2001, then no initial notice will be required). However, because the former customers would remain "consumers," you would have to provide a privacy and opt-out notice to them if you subsequently decided to disclose their personal information (except under one of the exceptions previously described).