



Your Financial Privacy Rights: What Banks and Other Financial Institutions Can Share

Understanding the Federal Laws That Protect Your Personal Financial Information

Your Financial Life Is an Open Book—But to Whom?

Your bank probably knows more about your financial circumstances than most of your closest friends. It knows how much money you earn, where you spend it, what bills you pay, and how much you have saved. Your credit card company knows where you shop, while your mortgage lender knows a great deal about your income, debts, and assets.

That information is valuable, not only to financial institutions but also to businesses interested in selling you products and services. Fortunately, federal law provides important privacy protections, although those protections are not absolute. Understanding what financial institutions may disclose—and what you can prevent them from sharing—is essential to protecting your financial privacy.

The Gramm–Leach–Bliley Act: A Foundation for Financial Privacy

In 1999, Congress enacted the Gramm–Leach–Bliley Act (GLBA), sometimes called the Financial Services Modernization Act. Although best known for changing the rules governing financial services, the legislation also established important protections for consumers' personal financial information.

The GLBA requires covered financial institutions to explain certain information-sharing

practices and safeguard sensitive customer information. It also gives consumers the right to restrict some disclosures to companies that are not affiliated with their financial institution.

The law covers a broad range of financial businesses, including banks, credit unions, insurance companies, securities firms, mortgage lenders, and certain other financial service providers. Different federal agencies administer and enforce its requirements, depending on the type of institution involved.

What Information Does the Law Protect?

The GLBA protects what regulators call *nonpublic personal information*. This generally includes personally identifiable financial information obtained from consumers, through financial transactions, or in connection with providing financial services.

Examples include Social Security numbers, account balances, income, loan applications, payment histories, and details of financial transactions. Information about where you shop, how much you borrow, or what financial products you own may also qualify when obtained through a covered financial relationship.

Not every piece of information about you receives the same protection. Publicly available information, such as certain property records, may fall outside the GLBA's privacy requirements, depending on how the information was obtained.

Why Your Bank Sends You Privacy Notices

If you have maintained a bank account or credit card for several years, you have probably received a document explaining the institution's privacy practices. Many consumers glance at these notices and promptly discard them, assuming they contain little more than routine legal language.

That can be a mistake. These notices explain what personal information an institution collects, why it shares that information, and whether customers can restrict particular disclosures. A standardized privacy notice includes a table identifying common sharing practices and the choices available to consumers.

Financial institutions generally must provide an initial privacy notice when establishing a customer relationship. Although annual notices were once broadly required, qualifying institutions may now omit them when their information-sharing practices meet specified conditions and their privacy policies have not changed.

When Financial Institutions Can Share Your Information

A common misconception is that banks must obtain permission before sharing any financial information. In reality, financial institutions routinely exchange information to conduct transactions, service accounts, prevent fraud, and comply with legal obligations.

Your bank may share information with companies that process electronic payments, print statements, or provide account services. A mortgage lender may disclose information to organizations administering a loan, while financial institutions may report certain information to consumer reporting agencies under applicable law.

Information may also be disclosed in response to lawful investigations, regulatory examinations, and other legally recognized circumstances. These activities generally fall within exceptions to the GLBA's consumer opt-out requirements.

The law recognizes that financial services could not function efficiently if every routine transaction required separate authorization. Its purpose is to regulate information sharing, not prohibit the ordinary exchange of information necessary to provide financial services.

Your Right to Say No: Understanding the Opt-Out Rule

One of the GLBA's most important protections concerns sharing personal financial information with *nonaffiliated third parties*. These are companies that are not part of the same corporate family as the institution holding your information.

When a financial institution proposes to share covered information with unrelated companies outside the law's exceptions, it generally must provide a privacy notice and a reasonable opportunity to opt out. The notice must explain how customers can exercise that right.

For example, a financial institution might share customer information with an unrelated company interested in marketing its products. Depending on the arrangement, customers may have the right to prevent that disclosure.

However, opting out does not prevent all information sharing. Exceptions generally permit disclosures needed to process transactions, prevent fraud, comply with the law, or conduct certain service-provider and joint-marketing activities.

Opting out can restrict certain uses of your financial information, but it does not make your account activity invisible to everyone outside your bank.

What About Companies Owned by the Same Corporation?

Many financial institutions belong to corporations offering banking, investment, insurance, and other services. These related businesses are called *affiliates*, and federal law treats information sharing among them differently from sharing with unrelated companies.

The GLBA does not generally provide a blanket right to prevent all sharing among affiliates. However, another federal law, the Fair Credit Reporting Act (FCRA), restricts certain disclosures involving creditworthiness and some marketing uses of information received from affiliated businesses.

Consequently, a financial privacy notice may offer several choices. One may concern sharing with nonaffiliated companies, another may involve creditworthiness information shared among

affiliates, and a third may address marketing by related businesses.

The Fair Credit Reporting Act: Another Layer of Protection

The Fair Credit Reporting Act regulates consumer reporting agencies and restricts how credit reports may be obtained and used. Generally, a business must have a legally permissible purpose to obtain your consumer credit report, such as evaluating a credit application or reviewing certain existing accounts.

The FCRA also gives consumers rights to obtain their credit reports and dispute inaccurate information. Consumer reporting agencies and businesses furnishing information have responsibilities concerning the investigation and correction of disputed records.

Together, the GLBA and FCRA provide overlapping protections for financial information. Understanding both is particularly useful when dealing with credit cards, mortgages, insurance, and financial marketing.

How Financial Institutions Must Protect Your Information

Privacy involves more than controlling who receives your information. Financial institutions must also safeguard sensitive records against unauthorized access, misuse, and security threats.

The GLBA's safeguarding requirements obligate covered institutions to maintain appropriate information-security programs. Depending on the institution and applicable regulations, these programs may involve risk assessments, employee training, encryption, access controls, monitoring, and oversight of service providers.

The Federal Trade Commission's Safeguards Rule establishes detailed requirements for many nonbank financial institutions under its jurisdiction. Banks and certain other regulated institutions are subject to information-security requirements administered by their respective regulators.

These protections have become increasingly important as financial services move online. Stolen computers, compromised passwords, dishonest employees, and cyberattacks can expose sensitive information belonging to thousands of consumers.

What Happens After a Financial Data Breach?

When criminals obtain financial information, the consequences can extend far beyond the institution whose systems were compromised. Stolen account credentials, Social Security numbers, and identifying information may be used to commit fraud or open unauthorized accounts.

Federal and state laws impose various notification and reporting requirements when certain breaches occur. The applicable obligations depend on the institution, the information involved, and the circumstances of the incident.

Consumers receiving a breach notification should determine what information was exposed and take appropriate precautions. These may include changing passwords, monitoring accounts, reviewing credit reports, placing fraud alerts, or freezing credit files.

A credit freeze can be particularly useful when identifying information has been compromised. It generally restricts access to a consumer's credit report for purposes of opening new credit accounts, although it cannot prevent every form of fraud.

What Consumers Can Do to Protect Their Financial Privacy

Federal law provides important protections, but consumers should not assume that every disclosure requires permission or that institutions automatically choose the most restrictive sharing practices.

Begin by reading the privacy notice provided by your bank, credit card issuer, insurance company, or investment firm. Look for the section explaining whether you can limit information sharing, and follow the instructions if you wish to exercise those rights.

Review account statements regularly, use strong passwords, enable multifactor authentication, and avoid responding to unsolicited messages requesting account credentials. It is also wise to examine your credit reports periodically and investigate unfamiliar accounts or transactions.

If you believe a financial institution has improperly disclosed your information, raise the issue with the institution and, when appropriate, submit a complaint to the Consumer Financial Protection Bureau or the regulator responsible for that institution.

Financial Privacy Is a Right Worth Exercising

The modern financial system depends on information sharing. Banks, insurers, lenders, credit bureaus, and service providers must communicate to process transactions, evaluate credit, detect fraud, and serve their customers.

But necessary information sharing does not mean consumers must surrender all control over their financial lives. The Gramm–Leach–Bliley Act, the Fair Credit Reporting Act, and related regulations establish meaningful protections while recognizing the legitimate operational needs of financial institutions.

Financial privacy is neither absolute nor nonexistent. Consumers have rights, financial institutions have responsibilities, and knowing the difference can help protect information that is far too valuable to ignore.

See Also: Federal Financial Privacy Resources

- [Consumer Financial Protection Bureau — Model Financial Privacy Forms](#)

- [Federal Trade Commission — Understanding the GLBA Privacy Rule](#)
- [Federal Trade Commission — Safeguards Rule](#)
- [Consumer Financial Protection Bureau — Submit a Complaint](#)
- [AnnualCreditReport.com](#)

Legal Information Notice: This article provides general educational information about federal financial privacy laws. It is not legal advice. Specific rights and obligations may vary according to the institution, information involved, applicable federal regulations, and state law.