ABA course content does not provide, nor is it intended to substitute for, professional legal advice.
Menu
Course Introduction
Overview of Privacy Related Laws
Privacy and the GLBA
Benefits of Information Sharing
Course Conclusion
Privacy for Customer Contact Personnel

Course Introduction

Overview

This course explores the everyday privacy issues that customer contact staff is faced with on a regular basis. It provides a broad overview of privacy laws impacting consumers, including the Right to Financial Privacy Act and the Fair Credit Reporting Act, with a deeper look at Regulation P: consumer privacy guidelines resulting from the passage of the Gramm-Leach-Bliley Act. This course defines the terminology used to discuss the privacy issue, including opt out, consumer vs. customer and how to answer consumer questions about their privacy rights.

Current Version: 7.0

Last Update: April 2019. Added summaries of Health Insurance Portability and Accountability Act (HIPAA), Children’s Online Privacy Protection Act (COPPA) and the General Data Protection Regulation (GDPR).

ABA course content does not provide, nor is it intended to substitute for, professional legal advice.

Page 1 of 50
Privacy for Customer Contact Personnel

Course Introduction

Overview

Protecting the privacy of consumer information held by "financial institutions" is at the heart of all privacy-related rules. The Right to Financial Privacy Act protects customers from unreasonable requests for information from the federal government. The Fair Credit Reporting Act protects customers from unauthorized sharing and use of their personal information by affiliates and explains what a bank must do if a breach occurs that impacts customer information. The Gramm-Leach-Bliley Act (GLBA) 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.

Course objectives

By the end of Privacy for Customer Contact Personnel, you will be able to:

- Define privacy
- Explain the purpose and function of six key consumer privacy laws
- Describe the privacy rules for financial institutions
Overview of Privacy Related Laws

Introduction

In this module, you will learn the purpose of privacy safeguards in the financial services industry.

Objectives

By the end of this module, you will be able to

- Explain the purpose and function of six key consumer privacy laws
Privacy for Customer Contact Personnel

Overview of Privacy Related Laws

Privacy Related Laws

Financial privacy is a blanket term for a multitude of privacy laws and issues. You are probably most familiar with privacy as the term is used to describe the issue of financial institutions selling customer information to other companies so that those companies may use that information for marketing. Other privacy laws exist, however, which apply to the sharing of information between bank affiliates and the sharing of information with the federal government.

There is no single law that governs privacy and security. Instead, there is a collection of federal laws and regulations governing specific industries and practices as well as a variety of state laws. Some of these laws prohibit sharing of customer information unless specific conditions are met while others allow sharing as long as the customer is given a choice whether the bank shares his or her information, how much is shared, and with whom.

Discussions on privacy often focus on the rules under the Gramm-Leach-Bliley Act, but there are other regulations relating to privacy that may impact your job.

These federal laws have been enacted to help safeguard the privacy of personal financial information.

- Fair Credit Reporting Act (FCRA)
- Right to Financial Privacy Act (RFPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Children’s Online Privacy Protection Act (COPPA)
- General Data Protection Regulation (GDPR)
- Gramm-Leach-Bliley Act (GLBA)

**TIP**
Because many states also have privacy laws that protect consumer information, you should check with your supervisor to see if any of those laws impact your bank.

Page 4 of 50
Privacy for Customer Contact Personnel

Overview of Privacy Related Laws

Privacy Related Laws

Fair Credit Reporting Act (FCRA)
The Fair Credit Reporting Act (FCRA), amended by the Fair and Accurate Credit Transactions Act (FACTA), is a law that protects the use and accuracy of consumer credit information. In part, the FCRA stipulates the rights consumers have regarding the sharing of their personal information between affiliated entities for example, a bank; a bank owned insurance agency and a bank-owned mortgage company. The FCRA does not prohibit this sharing but allows a consumer to direct what type of information may be shared and for what purpose.

Roll over the buttons below to see the information about FCRA.

Became effective
Fair Credit Reporting Act (FCRA) became effective 1971 and was further amended by the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

Privacy purpose
Stipulates disclosures required to inform consumers regarding the sharing of information between affiliated entities for advertising and other purposes.

Function
Financial institutions are subject to certain requirements outlined under the FCRA. Institutions must disclose how and for what purpose a consumer’s information may be shared with an affiliate and whether or not the consumer has a right to “opt out” of such sharing.

Note: For more information, see the Frontline Compliance course: FCRA: Sharing with Affiliates and Others.
Overview of Privacy Related Laws

**Privacy Related Laws**

**The Right to Financial Privacy Act (RFPA)**

The Right to Financial Privacy Act (RFPA) of 1978 applies to requests for bank records made by the federal government for individuals or partnerships of five or fewer individuals.

Corporations, trusts, estates, unincorporated associations such as unions, and large partnerships are not subject to the protections of the RFPA. The Act only governs disclosures to the federal government, its officers, agents, agencies, and departments. **It does not govern private businesses or state or local government.**

> Roll over the buttons below to see the information about RFPA.

**Became effective**

The Right to Financial Privacy Act (RFPA) was passed 1978.

**Privacy purpose**

Protects the financial records of individuals from unwarranted access by the federal government.

**Function**

Financial institutions may not release customer information to a federal government agency unless certain requirements are met, such as authorization from the customer, a subpoena, or search warrant. The law also ensures financial institutions may be reimbursed by the government for providing financial records.
Privacy for Customer Contact Personnel

Overview of Privacy Related Laws

Privacy Related Laws

Right to Financial Privacy Act (RFPA)
The Act only governs disclosures to the federal government, its officers, agents, agencies, and departments.

It does not apply to private businesses or state or local governments.

The RFPA contains specific notice and disclosure requirements and RFPA requests should be handled by someone in your bank familiar with these requirements. What is important to remember is that you, as a front-line employee, must never disclose customer information or hand customer records over to anyone—no matter how shiny their badge is!

Generally, banks process and respond to these requests through a central area. Always direct any requests for customer information to the designated individual at your bank for proper handling.

Note: For more in-depth information on the RFPA, see the Frontline Compliance course: Right to Financial Privacy Act.
Overview of Privacy Related Laws

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA), is United States legislation that provides data privacy and security provisions for safeguarding medical information. HIPAA can and does apply to banks—particularly if the bank engages in services on behalf of certain health care entities.

For example, banks that provide clearinghouse services for their health care clients may be a covered entity themselves. A health care clearinghouse converts health information from a non-standard format into a standard data format (i.e., a physician sends a paper claim to a health care clearinghouse where it is converted into a standard electronic format for submission to a health insurer for claims payment).

> Roll over the buttons below to see the information about HIPAA.

Became effective

Health Insurance Portability and Accountability Act (HIPAA) became effective on August 21, 1996.

Privacy purpose

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

Function

Financial institutions have a special relationship with HIPAA, wherein their mandate to comply is entirely dependent on what they do with information rather than what information they receive, disclose, use or maintain.

The law is particular about the specific scope of activities that financial institutions can engage in and still enjoy the exemption from the HIPAA rules. There are many activities that most banks, merchant service providers, and other financial institutions engage in that do not apply.
Privacy for Customer Contact Personnel

Overview of Privacy Related Laws

Privacy Related Laws

Health Insurance Portability and Accountability Act (HIPAA)

If a bank process "protected health information" (PHI) from a non-standard format into a standard electronic format for purposes of billing and claims payment, the bank is acting as a health care clearinghouse under HIPAA.

Banks can be considered “business associates” of covered entities—businesses such as financial institutions that perform services on behalf of covered entities are subject to HIPAA through contracts with covered entities. Business associates are defined as entities performing a service on behalf of a covered entity.

Some examples of business associate services set forth in the federal regulations are claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; and billing.

A bank or financial institution performing collection services, or any other type of services for a covered entity involving the transmission of protected health information, is a business associate and must comply with certain HIPAA requirements.
Privacy Related Laws

Children’s Online Privacy Protection Act (COPPA)

The Children’s Online Privacy Protection Act (COPPA) is a law created to protect the privacy of children under 13.

COPPA requires that site operators allow parents to review any information collected from their children. In practice, this means that any relevant site must provide full access to all user records, profiles and log-in information to a parent when requested. The FTC has stipulated that parents may delete certain information, but may not otherwise alter it.

Any website—including a bank website—that collects information from children under the age of 13 must abide by COPPA. This Act affects many popular sites like Facebook and other social networking sites.

> Roll over the buttons below to see the information about COPPA.

Became effective

The Act was passed by the U.S. Congress in 1998 and took effect in April 2000. COPPA is managed by the Federal Trade Commission (FTC).

Privacy purpose

COPPA was passed to address the rapid growth of online marketing techniques in the 1990s that targeted children. Various websites were collecting personal data from children without parental knowledge or consent.

Function

Although COPPA does not specifically define how website operators should obtain parental consent, the FTC has established guidelines to help website operators ensure compliance. Suggestions for compliance include:

- Clear display of downloadable consent forms that may be mailed or faxed to the operator
- Require that a parent use a credit card to authenticate age and identity
- Require that a parent call a toll-free phone number
- Acceptance of an email from a parent that includes a digital signature
Overview of Privacy Related Laws

Privacy Related Laws

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is the European Union’s (EU) regulation governing the use of personal data. It remains unclear what effect the rule will have on U.S. based banks offering banking products and services to European customers through internet banking websites, and U.S. regulators have not yet issued any formal guidance on the GDPR for banks based in the U.S. Banks should talk to their regulators to see how they plan to approach it.

> Click the buttons below to see the information about GDPR.

Became effective

The GDPR became effective May 25, 2018, and applies to companies with operations in the EU, or that collect the personal data of people in the EU.

Privacy purpose

According to the European Commission, the GDPR applies to “a company or entity which processes the personal data as part of activities of one of its branches established in the EU, regardless of where the data is processed; or a company established outside the EU offering goods/services (paid for or for free) or monitoring the behavior of individuals in the EU.”

The regulation defines “personal data” as anything that could identify an individual (referred to as a “data subject” by the regulation), either on its own or when combined with other pieces of data. IP addresses, social media handles and many other pieces of information that an organization might collect fall under the scope of the rule.

The premise is that the individual should have control over their data, such as the right to erasure—also known as the ‘right to be forgotten.’ Another important individual right under GDPR is the right to data portability, which refers to a data subject’s right to request their data from a company and have that data transmitted to another data controller.

In addition, the GDPR grants individuals the right to access their data in a free, electronic format, and expands the notion of “privacy-by-design,” which calls for companies to include data protection measures when designing their systems.

Function
Privacy for Customer Contact Personnel
How do banks determine if the GDPR applies? Larger, internationally active global banks already know that this applies to them, but smaller U.S. based institutions may not realize it applies.

For banks that are uncertain, a good first step is to conduct a privacy risk assessment to review the data they have for their customers, determine how many customers are in the EU, and if they regularly do business or marketing with them. Community banks may find additional clarity from the EU’s dedicated GDPR website, https://eugdpr.org/

To assist domestic U.S. banks with their assessment of whether GDPR may apply, ABA has developed a GDPR checklist that ABA member banks may access. https://www.abacom/Tools/Function/RiskMgmt/Pages/gdpr.aspx
Overview of Privacy Related Laws

Privacy Related Laws

Gramm-Leach-Bliley Act (GLBA)
Preserving the privacy of customer information is a core directive of Title V of the Gramm-Leach-Bliley Act (GLBA). Financial service providers' need, and customers expect, strong privacy programs. This is essential to keeping a customer's trust and to complying with privacy and information security laws and regulations.

» Roll over the buttons below to see the information about GLBA.

<table>
<thead>
<tr>
<th>Became effective</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Privacy purpose</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Function</th>
</tr>
</thead>
</table>

Became effective
Gramm-Leach-Bliley Act (GLBA) became effective 2000.

Privacy purpose
Title V of the GLBA requires financial institutions to safeguard the security and confidentiality of customers' nonpublic personal information.

Function
All financial institutions must provide initial disclosures to their customers describing policies for collecting and disclosing nonpublic customer information. Annual notices must be provided unless certain conditions are met.
Military Banking

Overview of Privacy Related Laws

Privacy Related Laws

Protection of customer information is not a new concept for the financial services industry. In fact, safeguarding customer information is one of the hallmarks of banking and goes back centuries. Federal laws have been in place for decades to ensure the accuracy and prevent the misuse of personal financial information.

Consumers must provide their confidential personal information to businesses, such as banks, to obtain financial products and services. Privacy rules regulate how financial companies may share the personal information they receive, and federal law requires financial entities to tell customers how their information is collected, shared, and protected. Basically, though, these codify good banking practices.
Overview of Privacy Related Laws

Privacy Related Laws

It is important to understand that the Gramm-Leach-Bliley Act (GLBA) is more than a consumer privacy law. For instance, the primary goal of the statute was to let banks, securities brokerages, and insurance companies combine as one company.

Because the statute was adopted just as the Internet was making information easy to share, Congress included provisions to protect customer information. Title V of the GLBA requires certain disclosures and safeguards for the protection of personal financial information.

Title V, the Privacy Rule, requires banks to take the following action:

- Have a written privacy policy
- Ensure that the bank’s privacy policy is communicated throughout the organization
- Give customers a written notice of the bank’s privacy policy both when the customer establishes a relationship with the bank, and annually thereafter unless certain conditions are met
- Give customers the right to prevent a financial institution from disclosing nonpublic personal information about them to nonaffiliated third parties by opting out from that disclosure after notice and a reasonable opportunity to exercise the option

You now know the key points of the three privacy laws that help safeguard the privacy of personal financial information.
Overview of Privacy Related Laws

Self Check Quiz

The left column lists privacy law acronyms. The right column lists the definition of each law.

Drag each term on the left up or down to align it with its corresponding definition on the right. When finished, click View Answer to see if you matched them correctly.

<table>
<thead>
<tr>
<th>Privacy Law</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLBA</td>
<td>Requires financial institutions to safeguard the security and confidentiality of customers' nonpublic personal information</td>
</tr>
<tr>
<td>COPPA</td>
<td>A law created to protect the privacy of children under 13</td>
</tr>
<tr>
<td>GDPR</td>
<td>Primary law regulating how companies protect EU citizens' personal data</td>
</tr>
<tr>
<td>FCRA</td>
<td>Stipulates disclosures required to inform consumers regarding the sharing of information between affiliated entities for advertising and other purposes</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Establishes national standards to protect individuals' medical records and other personal health information</td>
</tr>
</tbody>
</table>
Privacy for Customer Contact Personnel

Overview of Privacy Related Laws

Wrap Up

In this module you learned the purpose of privacy safeguards in the financial services industry. You can also describe key requirements under the FCRA, RFPA, HIPAA, COPPA, GDPR and GLBA privacy rules.
Privacy for Customer Contact Personnel

Overview

Federal legislation enacted by Congress in November 1999, known as the Financial Services Modernization Act, also known as the Gramm-Leach-Bliley Act (GLBA), made sweeping changes to the financial industry. Title V of the act requires compliance with broad financial privacy regulations. These regulations became effective on November 13, 2000, with compliance required as of July 1, 2001.

Gramm-Leach-Bliley Act (GLBA)

It is important to understand that the Gramm-Leach-Bliley Act (GLBA) is more than a consumer privacy law. For instance, the primary goal of the statute was to let banks, securities brokerages, and insurance companies combine as one company.

Because the statute was adopted just as the Internet was making information easy to share, Congress included provisions to protect customer information. Title V of the GLBA requires certain disclosures and safeguards for the protection of personal financial information.

Title V, the Privacy Rule, requires banks to take the following actions:

- Have a written privacy policy
- Ensure that the bank’s privacy policy is communicated throughout the organization
- Give customers a written notice of the bank’s privacy policy both when the customer establishes a relationship with the bank, and annually thereafter unless certain conditions are met
- Give customers the right to prevent a financial institution from disclosing nonpublic personal information about them to nonaffiliated third parties by opting out from that disclosure after notice and a reasonable opportunity to exercise the option

Sidebar

Nonpublic personal information

Title V of the GLBA generally prohibits any financial institution, directly or through its affiliates, from sharing nonpublic personal information with a nonaffiliated third party unless the institution provides the individual with a notice of its privacy
Privacy for Customer Contact Personnel

policies and practices, such as the type of information that it collects about the individual and the categories of persons or entities to whom it may be disclosed. Title V of the Act specifically mandates that financial institutions follow certain procedures with respect to disclosing nonpublic personal information to a nonaffiliated third party.
Privacy and the GLBA

Overview

Regardless of the position you hold in your bank, it is important to understand the issues surrounding the privacy of consumer information, so you are prepared to adequately protect that information as well as discuss customer questions and concerns. In this module you will learn how personal information is used by your financial institution and how to answer some common customer questions.

On June 1, 2000, the four federal bank and thrift regulators published virtually identical rules implementing provisions of the GLBA governing the privacy of consumer financial information. These rules establish the duties of financial institutions regarding the disclosure of customer information. Similar requirements apply to credit unions, securities broker-dealers, commodity traders, and nonbank financial companies. In 2010, rule-writing authority for Regulation P, the Privacy regulation, was transferred to the Consumer Financial Protection Bureau (the Bureau) which is now responsible for ensuring compliance.

Objectives
By the end of this module, you will be able to

- Define privacy under GLBA
- Describe the GLBA privacy rules for financial institutions
- Describe what information can be shared and when a customer must consent to information sharing
Privacy and the GLBA

Defining Privacy

**GLBA defines financial institution**
A financial institution is defined as a company that offers financial products or services to individuals such as loans, checking accounts, safe deposit boxes, insurance, and investments. Banks are examined for compliance with this law by their federal regulators.

Financial institutions are not the only entities that must comply with the Privacy Rule. The Federal Trade Commission (FTC) has jurisdiction over nonbank entities that are not regulated by the CFPB.

Generally, the Privacy Rule applies to consumers and protects information collected about individuals; it does not protect information collected about business entities.

Page 19 of 50
Privacy for Customer Contact Personnel

Privacy and the GLBA

Defining Privacy

The term “privacy” is often used as a short-hand reference to customer information and when that information may be shared with others. Although banks and other financial institutions are mindful of protecting the privacy and confidentiality of their customers’ financial information, most privacy laws are really information sharing laws, regulating with whom and how a financial institution may share a customer’s information.

Page 20 of 50
Privacy for Customer Contact Personnel

Privacy and the GLBA

Defining Privacy

Terminology
To have a general understanding of the requirements outlined under the Privacy Rule, it is important that you understand the terminology contained within the rule.

> Roll over the terms below to see the definitions.

Nonaffiliated third party
Any entity that is not an affiliate of, related by common ownership to, or affiliated by corporate control with, the financial institution; does not include a joint employee of such institution.

Customer
A consumer with whom a financial institution has a continuing relationship.

Opt out
A consumer’s right to deny a financial institution the ability to disclose any nonpublic personal information to certain nonaffiliated third parties.

Public information
Any information in which there is a reasonable basis to believe is lawfully made available to the general public from widely distributed media or federal, state, or local government records.

Consumer
An individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes. It also means the legal representative of such an individual.

Affiliate
Any company that controls, is controlled by, or is under common control with another company.

Nonpublic personal information
Personally identifiable financial information, including account balances, payment history, and debit card purchases.
Privacy for Customer Contact Personnel

- Provided by a consumer to a financial institution
- Resulting from any transaction with the consumer or any service performed for the consumer
- Obtained by the financial institution through any other means
Privacy for Customer Contact Personnel

Privacy and the GLBA

Defining Privacy

Self Check Quiz

The right column lists Regulation P terminology. The left column lists their corresponding definitions.

> Select the correct term for each definition, then click Submit.

Nonpublic personal information
Personally identifiable financial information provided by a consumer to a financial institution or obtained by a financial institution

Opt out
A consumer's right to deny a financial institution the ability to disclose any nonpublic personal information to certain nonaffiliated third parties

Affiliate
Any company that controls, is controlled by, or is under common control with another company

Nonaffiliated third party
Any entity that is not an affiliate of, or related by common ownership to, or affiliated by corporate control with, the financial institution; does not include a joint employee of such institution

Page 22 of 50
Privacy and the GLBA

Privacy Rule

GLBA defines customer and consumer
There is one key distinction in the Privacy Rule which is very important to understand—the difference between a customer and a consumer.

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. The difference is important because it tells us which rules apply.

A consumer is an individual who obtains or has obtained a financial product or service from a financial institution for personal, family, or household purposes.

Example
Margie is an individual. If she opens a checking account with your bank, she is also your customer.

If Margie just comes into the bank occasionally to cash her paycheck that is drawn on your bank, but she never opens an account, she is a consumer.
Privacy and the GLBA

Privacy Rule

Why is the difference between customers and consumers so important?

Customers
Only customers receive a financial institution's privacy notice automatically. Customers must receive the notice when the customer establishes a relationship with the bank and every year thereafter for as long as the customer relationship lasts if the bank is required to provide an annual notice.

Consumers
Consumers, on the other hand, are only entitled to receive your notice if your bank shares consumer information with unaffiliated third parties.

Example
Hometown Bank keeps a list of all individuals who apply for a loan but are denied credit. A third party wants to purchase the list so that it can contact the consumers in a marketing effort for some special loan products. In this scenario, even though Hometown Bank did not establish an ongoing relationship with the consumer (the loan was denied) it must give the consumer a privacy notice and allow that consumer to opt out of the sharing of his or her information with the third party. Most banks do not do this, as it is extremely cumbersome to manage this process.

Keep in mind that anyone can request a copy of the bank's privacy notice and bank personnel must be prepared to provide a copy. If the consumer agrees, it may be provided electronically.
Privacy for Customer Contact Personnel

Privacy and the GLBA

Privacy Rule

Privacy notice

The privacy notice must be given to individual customers or consumers at two important times during the customer relationship. It must be provided at account opening, and it must be provided annually as long as the individual is a customer of the bank and if certain conditions are met. (It also must be provided upon request.)

The bank regulatory agencies issued a Model Notice that banks may use. Although use of the Model is not mandatory, its use has become more important due to the revised annual notice requirements finalized in 2014. (This will be discussed further in the next section on the annual notice.) The Model replaces Sample Clauses that were used when the Privacy Rule was first adopted. It is based on consumer testing and banks that use it are granted certain protection, sometimes called a “safe harbor.” In order to be eligible for that safe harbor, the Model Notice must be of a specific font and paper size, and must be formatted to comply with the Model standards. The privacy notice must be in a clear and conspicuous format.

> Click the EZ Reference button to download and print a guide to using Privacy Notice Model Forms, which includes links to each form.
Privacy and the GLBA

Privacy Rule

The Privacy Rule requires financial institutions to disclose the institution’s policies and practices with respect to the following information:

- The categories of nonpublic personal information the bank collects
- The categories of nonpublic personal information the bank discloses
- The categories of affiliates and nonaffiliated third parties to whom the bank discloses information (there are some exceptions that do not have to be included)
- Under what circumstances and how a consumer can limit sharing of information (opt out)
- How the bank protects nonpublic personal information

NOTE
The rules pertaining to the sharing of information with affiliates, and the use of that information by affiliates for marketing purposes, fall under the Fair Credit Reporting Act and not the GLBA privacy rules. However, the privacy regulations require that this information be included in the privacy notice.

Glossary term

Nonaffiliated third parties
Any entity that is not an affiliate of, or related by common ownership to, or affiliated by corporate control with, the financial institution; does not include a joint employee of such institution.

Opt out
A consumer’s right to deny a financial institution the ability to disclose any nonpublic personal information to certain nonaffiliated third parties.
Privacy for Customer Contact Personnel

Privacy and the GLBA

Privacy Rule

Initial notice
The initial notice must be provided by mail or in-person and it must be in a form the customer can keep to refer to later. If a bank has a website, it may also be posted there, but a bank may not just refer a new customer to a website to obtain the privacy notice. It is not sufficient to post the bank’s privacy notice in the bank’s lobby, although a bank may do so as long as it is also provided by mail or in person. A bank may not provide either the initial notice solely by orally explaining the notice, either in person, or over the telephone.

When an existing customer obtains a new financial product or service from the bank and that product or service is to be used primarily for personal, family, or household purposes, the bank may provide a revised privacy notice that covers the customer's new financial product or service; or if the initial, revised, or annual notice that the bank most recently provided to that customer was accurate with respect to the new financial product or service, the bank does not need to provide a new privacy notice.

Special rule for loans: A bank establishes a customer relationship with a consumer when it originates or acquires the servicing rights to a loan for personal, family, or household purposes. If the bank subsequently transfers the servicing rights to that loan to another financial institution, the customer relationship transfers with the servicing rights.
Privacy and the GLBA

Privacy Rule

There are times when providing the initial privacy notice at account opening is not practical. A bank may provide the initial notice within a reasonable time after it establishes a customer relationship if establishing the customer relationship is not at the customer's election. For example, establishing a customer relationship is not at the customer's election if the bank acquires a customer relationship or the servicing rights to a customer's loan from another financial institution and the customer does not have a choice about the acquisition.

A bank may also delay providing the notice after establishing a customer relationship if it would substantially delay the customer's transaction, and the customer agrees to receive the notice at a later time. For example, if a customer opens an account over the phone, the bank may send the notice to the customer and not delay the opening of the account.

NOTE
Providing notice not later than when the bank establishes a customer relationship would not substantially delay the customer's transaction when the relationship is initiated in person at the bank office or through other means by which the customer may view the notice, such as on a website.
Privacy Rule

Annual notice
The Gramm-Leach-Bliley Act (GLBA) generally requires that banks send annual privacy notices to customers. These notices must describe whether and how the financial institution shares consumers’ nonpublic personal information. If the institution does share this information with an unaffiliated third party, it typically must notify consumers. Banks found that the cost of mailing a privacy notice each year was very expensive and caused information overload for consumers.

› Click the image to view an exception to the annual privacy notice requirement.

The Fixing America’s Surface Transportation Act (FAST Act) included legislation—now Public Law No: 114-94, Title 75—for a new exception to the annual privacy notice requirement under the Gramm-Leach-Bliley Act of 1999. The change took effect December 4, 2015. In August 2018, the Bureau updated Regulation P to conform with FAST Act provisions.

No Annual Privacy Notice Required
If a financial institution has not changed its policies and practices with respect to the disclosure of nonpublic personal information since its most recent privacy notice to customers and the financial institution only shares information under one of the existing statutory or regulatory exceptions for sharing information, it will no longer be required to send the annual privacy notice to consumers. (These exceptions are discussed later in this course.)
Privacy for Customer Contact Personnel

Privacy and the GLBA

Privacy Rule

Changes requiring annual notice

Because banking is a dynamic industry, changes in policies and procedures might require a bank that was exempt from sending an annual notice to begin sending it again. The Bureau’s 2018 changes create two different expectations to address situations when the exception from the annual notice is no longer available.

If the bank changes its policies with respect to the type of information it shares with third party service providers or for joint marketing, it is not required to offer an opt out, but advance notice must be provided. And so, when a bank changes how it shares information with a service provider or for joint marketing that is different from what was disclosed in its privacy notice, it has to provide notice before that information can be shared.

On the other hand, when a bank no longer qualifies for the exception because it changes its information sharing under one of the other exceptions, as discussed later in this course, it is not required to provide advance notice or an opt out. However, when the bank does begin to share under one of these exceptions and that sharing is inconsistent with the privacy notice it had previously sent the customer, it does need to notify the customer about the change to ensure that its privacy notice is consistent with its practices. The updated rule requires the bank to send a new privacy notice about this type of change within 100 days after the change.

According to the Bureau, these revised notices can be considered as the first annual notice and the next annual notice could be sent following the schedules set forth in Regulation P.
Privacy and the GLBA

Privacy Rule

If a customer requests the notice by telephone, the bank must provide it within ten days of the request. As a general rule, banks must provide this notice not less than annually during the continuation of the customer relationship. Annually means at least once in any period of 12 consecutive months during which that relationship exists. A bank may define the 12-consecutive-month period, but it must be applied on a consistent basis.

Example
Really Safe Bank provides its privacy notice annually and has defined their 12-month period as a calendar year. If a customer opens an account on any day of year one, the bank must provide an annual notice to that customer by December 31 of year two.

Banks are not required to provide an annual notice to a former customer. If a customer closes an account or the bank sells a loan and the servicing rights to another entity, that individual is no longer a customer of the bank for the purposes of receiving the annual privacy notice. (However, the information the bank obtained during the customer relationship must continue to be protected in accordance with your privacy policy.)
Privacy and the GLBA

Privacy Rule

Self Check Quiz

Which statement is true concerning the availability of the privacy notice?

Select the correct answer and click Submit.

A) It must be given to individual customers in-person
B) It must be in a form the customer can keep
C) It must be posted on the bank website
D) It must be posted in your bank lobby

B is correct.

A is incorrect because the privacy notice must be given to individual customers by mail or in-person. C is incorrect because the privacy notice does not need to be posted on the website. D is incorrect because the privacy notice does not need to be posted in the lobby.

Page 32 of 50
Privacy Rule

Self Check Quiz

In order for a bank to forego sending the annual privacy notice, which two requirements must a bank meet?

» Select the correct answers and click Submit.

A) The bank must not have any affiliates
B) The bank must not have changed its privacy notice since its most recent privacy notice to customers
C) The bank must send a notice weekly to remind customers to review the notice
D) The bank must not share customer information in a manner that provides the customer with opt out rights

B and D are correct.

A is incorrect because having affiliates does not impact the ability to take advantage of the annual notice exception. C is incorrect because the bank may forego the notice if it meets the statutory requirements.

Page 33 of 50
Privacy for Customer Contact Personnel

Privacy and the GLBA

Information Sharing

Opting out
Information sharing under the GLBA allows customers and consumers to “opt out” if the bank shares nonpublic personal information (NPPI) with nonaffiliated third parties and customers do not want their information shared with those nonaffiliated third parties. The GLBA gives consumers and customers the right to opt out or prohibit the bank from sharing their information with third parties. If your bank allows customers to opt out of sharing information with third parties, your privacy notice must explain how a consumer or customer may opt out.

Some banks allow customers to opt out online. The rules stipulate that requiring a customer to write a letter and mail it to the bank is not a reasonable way to opt out. If a bank does share, the bank must provide an opt out notice, with the initial notice or separately, prior to that sharing. The financial institution must provide consumers with a “reasonable opportunity” to opt out before disclosing nonpublic personal information about them to nonaffiliated third parties, such as 30 days from the date the notice is mailed. A “reasonable means” by which the consumer can opt out, includes, for example:

- Toll-free telephone number
- Detachable form with mailing information
- If the consumer has agreed to receive notices electronically, an electronic means such as a form that can be sent via e-mail or through the financial institution’s website

A bank may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer. For example, a customer who does not own a computer should not be required to opt out online as an only option.

NOTE
It is NOT a reasonable means if the only means of opting out is for the consumer to write his or her own letter to exercise that opt out right.

A bank may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer. For example, a customer who does not own a computer should not be required to opt out online as an only option.

Page 34 of 50
Privacy for Customer Contact Personnel

Privacy and the GLBA

Information Sharing

Opting out and joint relationships
If two or more consumers jointly obtain a financial product or service from a bank, the bank may provide a single opt out notice. Any of the joint consumers may exercise the right to opt out.

The bank may either:

(i) Treat an opt out direction by a joint consumer as applying to all of the associated joint consumers; or (ii) Permit each joint consumer to opt out separately.

If the bank permits joint consumer to opt out separately, the bank must permit one of the joint consumers to opt out on behalf of all of the joint consumers. A bank may not require all joint consumers to opt out before the bank implements any opt out direction.
Privacy for Customer Contact Personnel

Privacy and the GLBA

Information Sharing

Opt out exceptions
Consumers must be given the right to “opt out” of, or prevent, a financial institution from disclosing nonpublic personal information about them to a nonaffiliated third party, unless an exception to that right applies. The GLB Act provides specific exceptions under which a financial institution may share customer information with a third party and the consumer may not opt out.

When Congress adopted the Gramm-Leach-Bliley Act, it understood that there are times when information must be shared. Because of this, the law ensures banks can share NPPI about consumers and customers even though they have opted out.

Page 36 of 50
Privacy and the GLBA

Information Sharing

Exceptions permitting sharing without notice
The current exceptions that permit a financial institution to share information without notice or without notice and opt out rights are found in three separate sections of the GLBA.

The first exception allows a financial institution to share nonpublic personal information with a non-affiliated third party to perform services for the financial institution or to jointly market financial products and services, such as credit cards, annuities and insurance products. While this exception from the general requirements does not require the bank to offer the customer an opportunity to opt out, it does require the bank to notify the customer that their information will be shared.

The other two sections also create exceptions from the general prohibition against information sharing. For these exceptions, the bank is not required to provide notice and is not required to give the customer an opportunity to opt out.

Click the image to view the exceptions permitting nonpublic personal information to be shared.

- To process transactions requested by the consumer
- To effect, administer or enforce a transaction
- With the consent of the consumer
- To protect the confidentiality of records, to protect against fraud, to resolve customer disputes, or to persons holding a beneficial interest relating to the consumer or to persons acting on behalf of the consumer
- To provide information to insurance rate advisory organizations, rating agencies, persons assessing the financial institution’s compliance with industry standards or the financial institution’s attorneys, accountants and auditors
- To the extent specifically permitted by law
- To a consumer reporting agency (credit bureau)
- In connection with a proposed or actual sale or merger of the financial institution
- To comply with federal, state or local laws, properly authorized subpoenas or other official agencies with authority over the institution, such as regulatory examiners
Privacy for Customer Contact Personnel

Privacy and the GLBA

Information Sharing

Exceptions permitting sharing without notice, continued

> Roll over exceptions for sharing and disclosing information below to learn more.

Exception 1: Exception to opt out requirements for service providers and joint marketing

Banks can share information with outside service providers that perform services for the financial institution or function on its behalf, including marketing the institution’s own products or services or those offered jointly by the institution and another financial institution. The exception is permitted only if the financial institution provides notice of these arrangements and by contract prohibits the third party from disclosing or using the information for other than the specified purposes. The contract for a joint marketing agreement must provide that the parties to the agreement are jointly offering, sponsoring, or endorsing a financial product or service. Disclosure under this exception could include the outsourcing of marketing to an advertising company or to a third party marketer who sends a bank newsletter to customers of the bank. (Banks are prohibited, however, from sharing account numbers.)

Exception 2: Exceptions to notice and opt out requirements for processing and servicing transactions

Banks can share information with outside companies that provide essential services to the bank, such as processing transactions or ordering checks. This exception allows banks to share customer information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or under certain other circumstances relating to existing relationships with customers. Disclosures under this exception could be in connection with the audit of credit information, administration of a rewards program, or to provide an account statement.

Exception 3: Other exceptions to notice and opt out requirements

Banks may disclose information that is legally required, such as reporting interest to the IRS or responding to a subpoena or court order. Under this exception, banks can also disclose information to the bank's regulator for examination purposes. Banks may share under this exception to protect the confidentiality or security of customer records; protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; and for resolving consumer disputes or inquiries.
Privacy for Customer Contact Personnel

Banks may also share information under this exception with persons holding a legal or beneficial interest relating to the consumer; or to persons acting in a fiduciary or representative capacity on behalf of the consumer, such as a person with a power of attorney.

A customer may not opt out of sharing of information when the bank must comply with the Right to Financial Privacy Act or provide information to law enforcement agencies. (Law enforcement agencies include the CFPB or a Federal functional regulator, the Secretary of the Treasury, to a consumer reporting agency in accordance with the Fair Credit Reporting Act or to comply with the reporting requirements under the Bank Secrecy Act.)

NOTE
Banks may share information at the direction of the customer. It is always a good idea to get that authorization from the customer in writing.
Privacy and the GLBA

Information Sharing

Sharing information with affiliates
When the privacy rule was initially adopted in June 2000, it included an opt out right for certain information sharing under GLBA. At the same time, for convenience, the federal banking agencies determined that it made sense to include the notice and opt out rights for information sharing with affiliates, which is governed by FCRA, even though the FCRA notice and opt out does not require annual notice.

In updating the privacy rule, the Bureau has determined that information sharing under FCRA does not impact the ability of the bank to take advantage of the exception from sending annual privacy notices.
Not opting out
If the customer does not opt out—either for Privacy Rule or for FCRA information sharing or marketing rules—the bank may share nonpublic personal information with third parties and affiliates. The customer, however, may opt out at any time and that choice must be honored once it is made.

Under the GLBA, a customer's decision to opt out lasts indefinitely or until it is revoked by the customer. If, on the other hand, a customer opts out from information sharing with affiliates under FCRA, that opt out is only good for five years (the bank may extend the five years as a matter of policy).
Privacy and the GLBA

Information Sharing

Relation to state laws
There are some states that have passed privacy laws that are more protective than the federal law. Customers and consumers living in those states are protected by the applicable state law when it provides better protection.

For example, some states enacted an "opt-in" standard, which requires affirmative customer consent for sharing customer data in certain instances. The state laws impacting customers in those states must be disclosed in the "other important information" section on page 2 of the Model notice.

One such example is the California Consumer Privacy Act (CCPA), enacted in 2018. The CCPA was enacted very quickly and without adequate discussion or time to fully understand the consequences. This law is very broad and will be subject to interpretation in implementing regulations; therefore, its full impact is uncertain. In addition, other states are already considering adopting privacy laws similar to—if not modeled on—the CCPA, and this will exacerbate the existing patchwork of different, and often inconsistent, state privacy and data breach laws.
Privacy and the GLBA

Information Sharing

Self Check Quiz

The right column lists each exception for sharing and disclosing information. The left column lists the explanation for each exception.

> **Select the correct exception on the right that matches the explanation on the left, then click submit.**

<table>
<thead>
<tr>
<th>Service providers that perform services for the financial institution or function on its behalf, including marketing the institution's own products or services</th>
<th>Service providers and joint marketing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outside companies that provide essential services to the bank, such as processing transactions or ordering checks</td>
<td>Processing and servicing transactions</td>
</tr>
<tr>
<td>Disclosure of information such as reporting interest to the IRS or responding to a subpoena or court order</td>
<td>Other exceptions to meet legal or regulatory requirements</td>
</tr>
<tr>
<td>Disclosure of information authorized by the customer such as providing a verification of deposit (VOE) form to a mortgage company</td>
<td>At the customer's request</td>
</tr>
</tbody>
</table>
Privacy and the GLBA

Wrap Up

In this module you learned the privacy rules for financial institutions contained in the Gramm-Leach-Bliley Act. You know that the rules describe the type of information that can and cannot be shared.

Page 43 of 50
Privacy for Customer Contact Personnel

Benefits of Information Sharing

Communicating Benefits to Customers

It is important for customers to understand there are benefits and positive aspects to information sharing. The more customers know about these benefits, the more likely they will accept the practice.

It is important, then, for financial institutions to educate their customers about how information is managed to deliver better customer service and products.

Objectives

By the end of this module, you will be able to

- Identify the benefits of information sharing and how to communicate those benefits to customers

Page 44 of 50
Communicating Benefits to Customers

**Educating customers**

Sometimes it is appropriate for financial institutions to share personal financial information among affiliates as well as with certain third parties. Part of your job is to understand how and why consumer information is shared so you can educate your customers and address any concerns they may have.

Research shows that the more consumers know about the benefits of information sharing, the more accepting they are of the practice. In addition, the language you use to communicate your institution's privacy policies will affect your customer's comfort level. For example, consumers may be more receptive to sharing when you use *family of companies* rather than the term *affiliates*.
Privacy for Customer Contact Personnel

Benefits of Information Sharing

Communicating Benefits to Customers

Consumers also appear most receptive to the notion that privacy is a partnership, and that there are steps they can and should take to protect their financial information. Communicating customer benefits and choices can also be effective.

Consider the following phrases:

- “Banks use a combination of safeguards to protect your personal information”
- “You can help to maintain your privacy by taking these steps....”
- “We are partners with you in protecting your privacy”
- “In order to serve you better, we....”
- “Internal use of information saves you time and money”

› Click the EZ Reference button to download and print the Privacy Policy Notice Q & A document that shares some common customer questions and sample responses.

Page 46 of 50
Benefits of Information Sharing

Communicating Benefits to Customers

> Roll over the benefits of information sharing below to learn how to use them when communicating with your customers.

- **Fraud detection**
  "We use customer information to recognize unusual behavior that may signal unauthorized use of your account. By helping to spot and prevent fraud, we help you protect yourself against identity theft."

- **Availability and affordability of credit**
  "The free flow of credit information in the United States gives you more choices, allows you to be more mobile, and can help bring down your cost of credit."

- **Streamlined customer service**
  "Information sharing within our family of companies or with trusted business partners allows you, for example, to call a single toll free number to get information on or perform transactions involving any of your accounts at our institution. It also means less paperwork when opening new accounts because we can access information already on file."

- **Tailored products and services**
  "By analyzing your experience and transaction information, we can suggest a more appropriate account or package of accounts. We might suggest, for example, a higher-yielding CD, overdraft protection, or a home equity line of credit that works best for you and your needs."

- **Discounts**
  "Customers expect their financial institutions to recognize their total relationship. By sharing account information, we are able to offer products or discounts based on the breadth of your relationship with us. As a mortgage customer, for example, you might be offered free checking. Or, if you had a certain amount of deposits, you might be eligible for a discount on a home equity line of credit."

- **Innovation**
  "By examining our customer’s experience and transactions, we are better able to develop new products that suit customers’ needs. Sweep accounts and overdraft protection, for example, were developed in response to customers’"
Privacy for Customer Contact Personnel
preferences and habits.”

Efficiency
"By using outside vendors, which operate under strict confidentiality agreements, we can keep costs down by outsourcing functions such as check printing, credit card processing, or marketing.”
Benefits of Information Sharing

Communicating Benefits to Customers

Question
What benefit of information sharing helps to address a customer’s concern about identity theft?

Answer
Fraud detection. “We use customer information to recognize unusual behavior that may signal unauthorized use of your account. By helping to spot and prevent fraud, we help you protect yourself against identity theft.”

Page 48 of 50
Benefits of Information Sharing

Wrap Up

In this module you learned the benefits of information sharing and how to communicate those benefits to customers. By understanding how and why consumer information is shared, you can educate your customers and address any concerns they may have.
Wrap Up

By completing Privacy for Customer Contact Personnel, you can define privacy and explain the purpose and function of three key consumer privacy laws. You can also describe the privacy rules for financial institutions and what information can be shared and when a customer must consent to information sharing. In addition, you can communicate the benefits of information sharing to your customers.

» Click Exit to close this course.