

Protecting Financial Privacy in the New Millennium

Gramm – Leach – Bliley Privacy Act
(GLBA)



© Copyright 2002. Melissa Guenther, LLC. All rights reserved.

Objectives

Part 1

- Understand:
 - the driving forces behind privacy regulation
 - key privacy terms and concepts
 - obligations under the privacy regulations
- Perform your job functions in a manner consistent with the privacy requirements
- Properly distribute your institution's privacy and opt out notices in the course of customer interaction
- Accurately address customer questions and issues regarding privacy

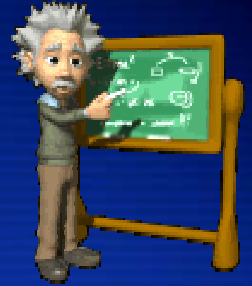
Part 2

- Global networks, global privacy
- GBLA Terms and Definitions



Practical Applications

Privacy training is about teaching employees the things they need to know about privacy



Privacy Awareness is about keeping employees mindful of the things they have learned about privacy and the responsibilities they have with respect to privacy



The Responsible Company

Information technology is a two
edged sword



The challenge for today's connected
Enterprise is to preserve the benefits
while minimizing the drawbacks

Why GLBA?

American public has shown strong concerns about the privacy of its personal information - buying habits, medical records and financial information.

One purpose of the GLBA is to help protect people against the *unwanted* sharing of personal information.

Privacy is a Major Business Issue

Companies require rich data to:

- ✓ personalize services
- ✓ build relationships
- ✓ drive sales.

Consumer and
company
benefits of direct
marketing

Consumers want merchants to:

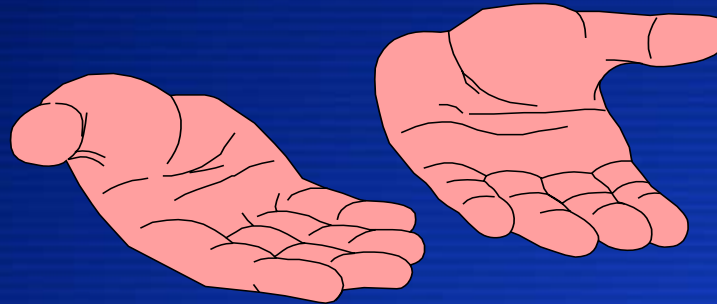
- ✓ know their needs
- ✓ personalize offers and services.

Company's
need to know
its customers

Lack of
trust and
privacy

The Privacy Paradox

More than regulatory compliancy



Without trust and privacy protection,
consumers will not entrust personal data to company

Privacy Rules are intended to ensure the
Confidentiality and **Security** of consumer
information.

GLBA



Since July 1, 2001, U.S. Financial institutions were required to meet vigorous new guidelines to protect confidential customer financial information

The intent of the safeguards is threefold

1. Insure the security and confidentiality of customer records;
2. Protect against any anticipated threats or hazards to the security or integrity of the records; and,
3. Protect against unauthorized access to or use of customer that could result in substantial harm or inconvenience to any customer.

Standards

Administrative, technical,
and physical safeguards for customer
records and information

- Written Security Program
- Board of Director Approval
- Risk Assessment
- **Manage and Control Risk**
- **Appropriate Measures**
- **Oversee Service Providers**
- **Monitoring of Program**

Protection - initial scope of Act is to safeguard Customer information

Detection - requires Security Awareness training to support the information security program in general, not just customer information

Reaction - special emphasis in the Security Awareness training should include component to train employees about what they need to do to protect customer information

GLBA in a Nutshell



- Notice
- Choice
- Access
- Security

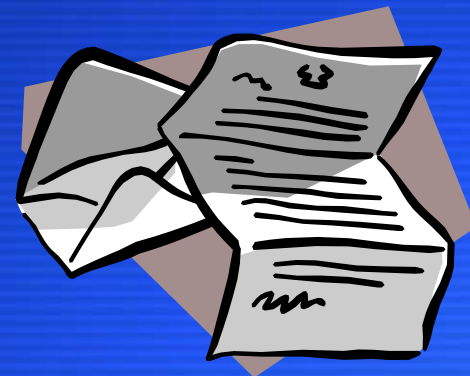
Confidentiality and Security of Clients

- Restrict access to client information to those that need to know.
- Ensure client information is not visible or accessible to others.
- Do not discuss client information in places where others may overhear
- Do not share existing passwords with anyone or give old passwords to new employees when contractor leaves.
- Discard old or used client information appropriately
- Only use

Notice

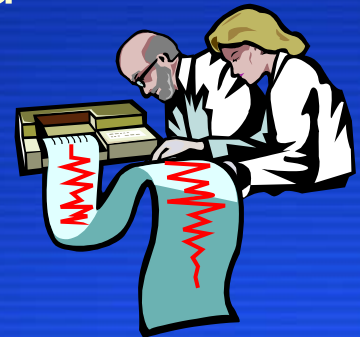
Refers to data collectors' disclosure of their information practices prior to collecting personal information from consumers

Privacy Policy: must tell customers what information it collects and how it is used



Choice

Refers to company providing consumers with options regarding whether and how personal information collected from them may be used for purposes other than those for which it was provided



Right to Opt-Out: must explain customers ability to prevent the sale of your customer data to third parties

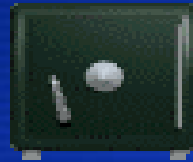
Access

Refers to the customer's ability to view the data collected about him or her, and challenge its accuracy and completeness



Security

Refers to data collectors' responsibility to take reasonable steps to ensure that information collected from consumers is accurate and secure from unauthorized use



Safeguards: required to develop policies to prevent fraudulent access to confidential financial information. Policies must be disclosed to all customers.

Penalties for Non Compliance



Adverse consequences include:

Cease and desist orders.

Civil money penalties may also be imposed.

Negative press and loss of public confidence

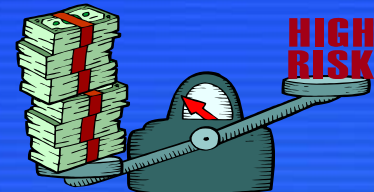
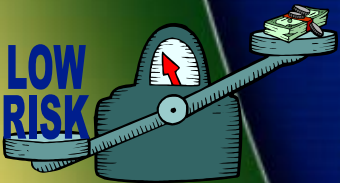
Potential Violations



- Failure to provide the customer with a Privacy Notice at the time of establishing an ongoing customer relationship.
- Failure to provide the customer with the right to "opt out" of information sharing at the time of establishing a customer relationship.
- Failure to track customer opt-outs and prevent information sharing on those accounts.

Potential Violations

- Failure to provide a Privacy Notice on an annual basis.
- Failure to provide a Privacy Notice when there is a change in the institution's privacy policy.
- Inadvertent breaches of customer privacy and confidentiality. This is perhaps the greatest risk you face as an employee.



Vulnerabilities

Whenever personally identifiable information is gathered, stored or processed, it is possible that the privacy of some individuals may be threatened.

- Company web site?
- Email marketing?
- Data collection and storage?
- Employee awareness and actions?

What Can You Do?

Top Eight List for an Aware
Enterprise

8. PROTECT YOUR EQUIPMENT

Keep it in a secure environment Keep food, drink, and cigarettes *AWAY* from it.

Know where the fire suppression equipment is located and know how to use it

7. PROTECT YOUR AREA

Keep unauthorized people *AWAY* from your equipment and data

Politely challenge strangers in your area

6. PROTECT YOUR PASSWORD

Never write it down or give it to anyone

Don't use names, numbers or dates which are personally identified with you

Change it often, but change it immediately if you think it has been compromised

5. PROTECT YOUR FILES

Don't allow unauthorized access to your files and data

NEVER leave your equipment unattended with your password activated - **SIGN OFF!**

4. PROTECT AGAINST VIRUSES

Don't use unauthorized software

Back up your files before implementing ANY new software

3. LOCK UP STORAGE MEDIA CONTAINING SENSITIVE DATA

If the data or information is sensitive or critical to your operation, lock it up!

Human leak – do not discuss confidential information of any customer inappropriately

2. BACK UP YOUR DATA

Keep duplicates of your sensitive data in a safe place, out of your immediate area
Back it up as often as necessary

AND...#1 on the list of things
to support security in your
company

REPORT SECURITY VIOLATIONS

Tell your manager or contact Security if you see any unauthorized changes to your data

Immediately report any loss of data or programs, whether automated or hard copy

Report all suspicious email

Immediately report any contact (face –to–face, phone, email) from someone you don't know asking for confidential information

Safeguard customer data at your Work station



Password Protected
Screen Saver

Password construction &
management

Shredding

Incident Reporting

Email Guidelines

Information Classification
Guidelines

ID Badges

Visitor Control

Clean Desk

Verify customer identity before
information is released



Social Engineering

Incident Reporting

Visitor Control

Identity Theft

Social Engineering- Fact or Fallacy?

From Nov. 12, 2001 Fortune Magazine
"Ask Annie" Column

Dear Annie,

I compile market research , including information about our competitors, for a small software company. Most of it comes from the WEB, news articles, legitimate industry contacts, or industry reports we purchase. Now my boss wants me to start calling our largest competitors, posing as a potential reseller, to try to get product information out of them that way. I don't feel this is ethical. Am I just being a Pollyanna? Does everyone do this?

- *Squeamish in Seattle*

Respect new access restrictions to customer information files



Password Construction and management

Email encryption

Keep customer information confidential,
refrain from sharing customer information
in conversations with other employees
and outside parties

Phone conversations

Social Engineers

Fax machines

Shredders

Email

Informal, social gatherings



In the Elevator

So, how was your day?

I spent hours trying to collect payment from a borrower! The Smyth's have had some hard times and may have to file bankruptcy.



Finally

Know and follow your institution's
Privacy Policy



Privacy Policy

A statement of:

- how and why a company collects information
- what it does with it
- what choices you have about how it is used
- whether you can access the information, and
- what is done to assure that the information is secure

Conditions under which we may share information

Conditions

Under certain **conditions** your institution may share information with non-affiliate third parties without a customer's permission. These situations are called **exceptions**

Exceptions include situations where a firm performs services for the institution (such as data and transaction processing firms)

Four Concepts of Privacy

Personal customer information that can be shared with other entities, and the conditions under which it can be shared

Intrusion Detection

G-L-B makes it illegal to obtain (or attempt to obtain) customer information from a financial institution relating to another person by false or fraudulent means.

This means companies have to make sure they can detect such attempts.

Broad Definition of Financial Institution

Includes any entity that engages in activities that are "financial in nature" and virtually any other "financial" activity that federal regulators may designate

Expressly included are insurers, agents, and brokers

Also affected:

- Mortgage lenders
- "pay day" lenders
- Finance companies
- Mortgage brokers
- Account services
- Check cashers
- Wire transferors
- Travel agencies operated in connection financial services
- Debt collectors
- Credit counselors
- Financial advisors
- Tax preparation firms, and more



Practical Applications

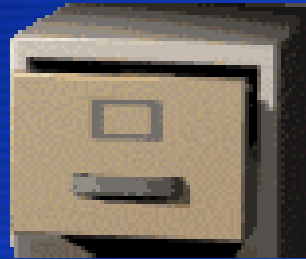
Practice Session 1

Case Study

Customer inquiring about Opt-Out
statement

Overview

As a part of your daily interactions with customers you may find yourself in a situation similar to the employee in the following scenarios



Overview

A lifelong customer of your institution has just received a Privacy Notice in the mail. The notice indicates that the institution retains certain "nonpublic personal information" about the customer; that is the institution's policy NOT to share this information with outside parties; and that nonetheless, the institution may share this information with certain parties.

The customer has stopped by your institution with questions concerning this letter. Your responses will assist him in gaining a better understanding of this letter, with whom and under what circumstances the institution may share nonpublic personal information, and your customer's rights to prevent such sharing.

Following is a scenario that addresses how you can answer question from a customer relating to GLBA.

Scenario 1



What's this Privacy Notice I received in the mail? I've been a customer here for years.



A new federal Privacy regulation requires financial institutions to send written notice to all customers explaining our policies of sharing nonpublic personal information. This is the Privacy Notice that you received.

**What exactly is
nonpublic personal
information?**



Nonpublic personal information is information that we have collected regarding you and your financial activities over the history of our relationship. It includes account, application and transaction information as well as data from others sources such as credit reports. You can choose whether or not you want us to share this information with nonaffiliated third parties.



I'm sorry, but I'm in the medical professional, not Finance. What is a nonaffiliated third party?



A nonaffiliated third party is anyone who is not one of our institution's affiliates. An affiliate is a business that is part of our corporate family. For example three banks and a mortgage company are owned by our parent corporation. These are our affiliates. Those parties not under common ownership with us are non-affiliates.

Your Privacy Notice says you can share data with nonaffiliated third parties. Do I have a choice about what you can share?



Yes. Under the privacy rules, you have the right to choose whether certain information is shared. You may "opt out" of this information sharing.

You mentioned affiliates, too. Do I have a choice about what you can share with them?



Yes a different law, the Fair Credit Reporting Act, gives you additional rights to opt out of certain information sharing with affiliates.

Opt out? What does that mean?



If you choose to opt out, we cannot share your information with nonaffiliated third parties. There are some exceptions however.

**Exceptions?
What do you
mean by that?**



There are times when we may share information with others. For example, in the course of marketing our products to you, processing your transactions, and other legal situations when permitted by law. In these special situations, your opting out does not prevent the sharing of information.

You should know that certain information, such as account numbers and PINS, as a general rule may not be shared.



Thanks. You've been quite helpful.

You're welcome. Please, don't hesitate to contact me with any additional questions you may have in the future.

Practice 2

Consumer Privacy Quiz

Question # 1

(True/False) Under the privacy regulation, an opt-out notice is required whether or not a financial institution shares information with nonaffiliated third parties.

- A) True
- B) False

Question # 2

(Multiple Choice) Regarding a third party service provider's use of information, a financial institution is required to:

- A) Monitor usage and address the usage in a contract with the third party service provider.
- B) Address the usage in a contract which may provide the basis for a cause of action against the third party service provider; however, the institution does not have to monitor usage.
- C) Monitor the usage.
- D) Do nothing and the institution has no basis for a cause of action against the third party service provider.

Question # 3

(Multiple Choice) Some customers do not wish to receive any communications from their financial institution. In that case, an institution:

- A) Does not need to provide any notices—either initial or annual.
- B) Must provide both initial and annual notices.
- C) Must have notices available and must have an explicit direction from the customer not to communicate with that customer, but then does not need to provide annual notices.

Question # 4

(True/False) In the privacy regulation, a customer is defined as an individual who obtains or has obtained a financial product or service from an institution which will primarily be used for personal, family, or household purposes.

- A) True
- B) False

Question # 5

(Multiple Choice) The following must be included on a privacy policy disclosure for an institution which shares information:

- A) A detailed description of security measures taken to protect a customer's privacy.
- B) Categories of nonpublic personal information that the financial institution collects.
- C) Categories of entities with which the institution shares information.
- D) b and c only.
- E) a and c only.

Question # 6

(True/False) A financial institution must disclose its privacy policy to all of its account holders.

- A) True
- B) False

Question # 7

(Multiple Choice) Under the regulation, an institution must:

- A) Provide a disclosure notice to each customer prior to establishing the customer relationship.
- B) Always provide an opt-out option.
- C) All of the above.
- D) None of the above.

Question # 8

(Multiple Choice) Nonpublic personal information about a customer may be provided to a nonaffiliated third party when:

- A) The institution has provided an opt-out notice to the customer and a reasonable period of time has passed from the time that notice was provided without receiving an opt-out instruction from the customer.
- B) The institution has provided an initial privacy disclosure to the customer only.
- C) The customer has never indicated in the past that he or she does not want his or her information shared.
- D) None of the above.

Question # 9

(Multiple Choice) The privacy regulation's definition of "consumer" would include:

- A) An individual who purchases traveler's checks once from an institution.
- B) An individual who has an account with an institution.
- C) Someone who uses an institution's ATM on a weekly basis.
- D) a, b, and c.
- E) b and c only.

Question # 10

(Multiple Choice) In addition to annual notices, a new privacy disclosure must be provided to a customer:

- A) Upon request.
- B) Monthly as a statement stuffer.
- C) When the current disclosure no longer accurately reflects the institution's policy.
- D) a and c only.
- E) All of the above.

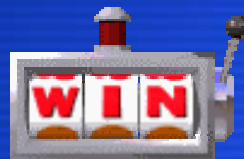
Consider the alternatives

The company that neglects privacy concerns runs serious risk of embarrassing and costly negative fall out from privacy incidents.



But the company that is proactive on privacy not only minimizes privacy risks, it is also better able to deflect criticism should a privacy incident occur.

Plus, it is in a position to win customers through its commitment to privacy.



Part 2

Global Networks, Global Privacy

(Optional)

"www" stands for World Wide Web

If your company's web site advertises a product for sale, it is advertising to the entire planet, whether you intend to sell in other countries or not

If your web site accepts input from visitors, it is accepting input from every country on earth

Some countries have different ideas about Privacy than you find in the US

European Union or EU

- consists of more than a dozen countries
- inhabited by more people than North America
- contains 10 of the world's richest nations
- exports more goods and services than the US



Some EU countries have had data privacy legislation in place since the 1980s

EU recently harmonized the privacy protections in member states under Data Protection Directive

The DPD:

- sets standards for protection of personal data
- limits data transfers to countries outside the EU, which might not have the same level of protection
- protects "the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data"

Under the DPD, personal data must be:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

- DPD also prohibits the transfer of data relating to individuals to any non-EU countries that are considered "unsafe" destinations for protection of personal data.
- It might surprise you to learn that the US is considered "unsafe."

- Potential to seriously impact the operations of companies which have dealings in both the US and the EU.
- US Department of Commerce, in consultation with the European Commission, developed a "safe harbor," a way for US organizations to comply with the DPD.
- US company certifying to the safe harbor satisfies EU organizations that the it provides "adequate" privacy protection, as defined by the Directive. To qualify, a US company agrees to seven safe harbor principles, which actually make good privacy policies as well:

1. Notice: Organizations must notify individuals about the purposes for which they collect and use information about them.
2. Choice: Organizations must give individuals the opportunity to choose (opt out).
3. Onward Transfer (Transfers to Third Parties): To disclose information to a third party, organizations must apply the notice and choice principles.
4. Access: Individuals must have access to personal information ...and be able to correct, amend, or delete that information where it is inaccurate.

5. **Security:** reasonable precautions must be taken to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.
6. **Data integrity:** data must be relevant for the purposes used...and reliable for its intended use, accurate, complete, and current.
7. **Enforcement:** to ensure compliance, there must be affordable, independent recourse mechanisms; procedures for verifying that the commitments to the safe harbor principles have been implemented; and obligations to remedy problems arising out of a failure to comply with the principles.

GLBA Privacy Terms

Consumer

Customer

Opt out

Nonpublic personal information

Personally identifiable financial information

Affiliate

Non-affiliated third party

Privacy Notice

Consumer

- A consumer is any one who has obtained a product or service from your institution. The individual need not establish a contractual or formal relationship with the institution. A consumer has a more temporary relationship with the institution than a customer. For example, a consumer is anyone who cashes a check, purchases travelers checks, or randomly uses an ATM.
- Note that all customers are consumers, but not every consumer is a customer. For example if an individual walks into a institution and cashes a check, that person is a consumer (assuming he has no formal relationship with the institution). However, if that same individual opens an account with the institution, he then becomes a customer.

Customer

A **customer** is anyone who, as an individual, has an account or any sort of continuing relationship with your institution, where that account is for personal, family or household purposes.

Anyone who has a consumer loan, deposit, credit, trust, or investment account with the institution; purchases an insurance product from the institution; maintains a safe deposit box; etc.

Any account opened for business purposes is not considered covered under these regulations.

Opt Out

Opt-out" is contrary to the "opt-in" approach preferred by most consumer and privacy advocates. Opt-in would prohibit a financial institution from sharing or selling your data if you did *not* give your affirmative consent.

With opt-out, you give your implied consent by failing to return the notice. The default for the opt-out approach is that your data is shared until and unless you notify the company otherwise.

Non-personally Identifiable Information

- Non-personally identifiable information is any data element or collection of data elements that, by itself, cannot be associated with a specific individual. There are two types of non-personally identifiable information usually collected on web sites.
 - The first type includes information provided during registration.
 - the state in which you live and your gender.
 - The second type of non-personally identifiable information which is routinely gathered from all site visitors focuses on website activity.
 - how many people visit the site
 - the pages they visit
 - what website they are coming from,
 - how long they stay, etc.
 - is collected on an aggregated, anonymous basis, which means personally identifiable information is not associated with this data.
 - is generally gathered through the use of web server logs and cookie technology.

Nonpublic Personal Information?

“Any information that a customer provides to you to obtain a financial product or service from you.”

Includes account balances, payment history, and credit or debit purchase information.

Aggregate information and blind data are not covered and can be disclosed without triggering any obligations under the Act.

Personally Identifiable Financial Information

Any information - financial or otherwise - that your institution has about its customers, that can be tied to a specific customer

Any data element or collection of data elements that directly identifies an individual or that individual's residence, including:
your name,
postal and e-mail addresses,
date of birth,
credit card information,
prescription number or
telephone number.

Includes:

Information provided by a customer to an institution to obtain a financial product or service,

Information resulting from a transaction between an institution and a customer,

Information from a credit bureau, etc.

Other Entities

- 1. Affiliates.** An affiliate is a firm owned by your institution, or a sister firm owned by the same company that owns your institution, or a firm that owns your institution.
- 2. Nonaffiliated Third Parties.** A Nonaffiliated Third Party is any firm that is not part of your corporate family (i.e., not owned by the institution or by the company that owns the institution).

Note that affiliates include both financial institutions and non-financial institutions.