



Securing Sensitive Data and Guarding Against Identity Theft

Joanna P. Crane
Federal Trade Commission
June 17, 2009

The views expressed are those of the speaker and not necessarily those of the FTC or any other person.

Why is information security important to your business?

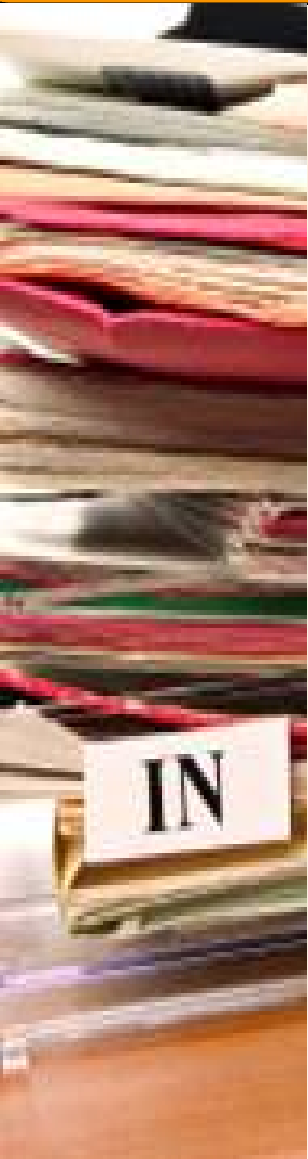
- According to *Information Week*, the amount of data captured and stored by businesses doubles every 12-18 months.
- Failure to protect sensitive data can lead to identity theft or other harm to consumers – and also can harm your company.

The views expressed are mine and don't reflect the official position of the FTC.



Why is information security important to your business?

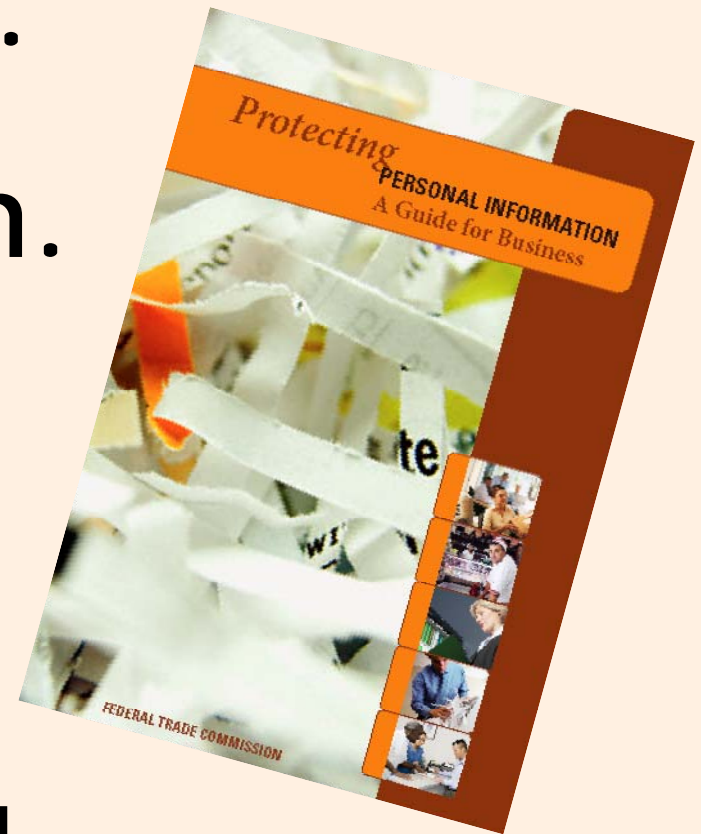
- Existing laws require many businesses to:
 - Implement measures that are reasonable and appropriate under the circumstances to protect sensitive consumer information.
 - Notify consumers if there's a data breach.
 - Protected information includes, for example, Social Security numbers, account information, and information derived from credit reports.



Five Key Principles


From "Protecting PERSONAL INFORMATION:
A Guide for Business"

1. Take stock.
2. Scale down.
3. Lock it.
4. Pitch it.
5. Plan ahead.




1) *Take Stock.*

Know what you have
and who has access to it.

- 
- Check files and computers for:
 - What information you have; and
 - Where it's stored. Don't forget portable devices and offsite locations.
 - Trace the flow of data from entry to disposal. At every stage, determine who has access — and who should have access.

2) *Scale down.*

Keep only what you need for your business and streamline storage.

- 
- Collect only what you need and keep it only for the time you need it.
 - Scale down what you store on devices connected to the Internet.
 - Slip Showing? For receipts you give to customers, properly truncate credit card number and delete the expiration date.

2) Scale down.

Limit your use of Social Security numbers.

- Social Security numbers can be used by identity thieves to commit fraud.

Don't collect Social Security numbers out of habit or convenience. Only collect them when needed, such as to report wages to the government or to seek a credit report.



3) *Lock it.*

Protect the information you keep.

TRAINING & OVERSIGHT

- Train your employees and oversee contractors and service providers.
- Use good hiring procedures and build information security training into orientation.
- Get handouts, tutorials, quizzes, and tips at www.OnGuardOnline.gov.



3) *Lock it.*

Protect the information you keep.

COMPUTER SECURITY

- Effective security covers data on your network and all devices, including laptops and PDAs.
- Remember the basics: firewalls, strong passwords, antivirus software.
- Check vendors and expert websites like www.sans.org for alerts and updates.
- Work with your Tech Team to detect unauthorized entry into your system.



3) *Lock it.*

Protect the information you keep.

PHYSICAL SECURITY

- Lock offices, store rooms, desks and drawers and train employees to keep them that way.
- Limit access to areas and databases with sensitive files.
- Secure data that's shipped or stored offsite.



4) *Pitch it.*


Properly dispose of what you no longer need.



- Shred, burn, or pulverize paper records you don't need.
- Use wipe utility programs on computers and portable storage devices.
- Place shredders around the office.
- If you use credit reports, you may be subject to the FTC's Disposal Rule.


5) *Plan ahead.*

Create a plan to respond to security incidents and be ready to help consumers.

- 
- A red pushpin is pinned to a white document with a green line. The pushpin is in the foreground, and the document is slightly blurred in the background.
- Put together a “What if?” plan to detect and respond to a security incident.
 - Designate a senior staff member to coordinate your response.
 - Investigate right away and preserve evidence, such as computer logs.
 - Take steps to close off vulnerabilities, e.g., disconnect compromised computers from the Internet.
 - Consider whom to notify if a breach occurs.

5) *Plan ahead.*

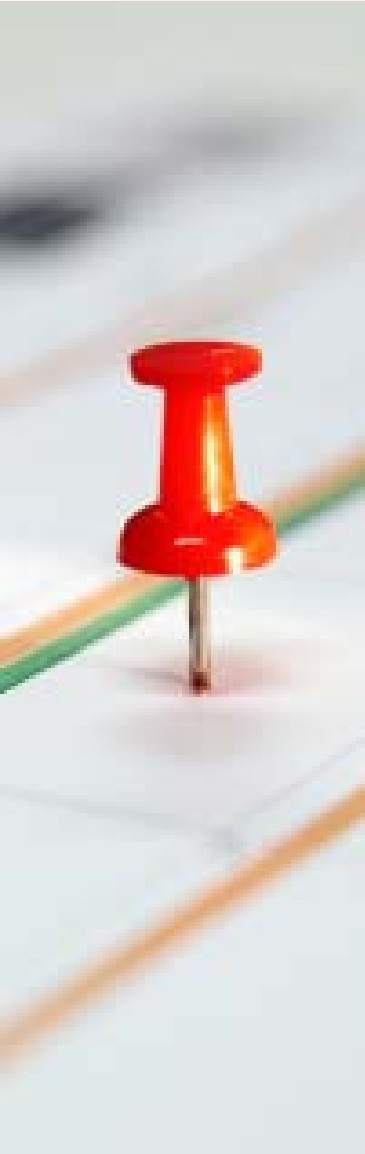
Know whom to notify and when.

- 
- A red pushpin is pinned to a document with a green line and a blue line. The pushpin is in the foreground, and the document is slightly blurred in the background.
- If sensitive personal information is compromised, consumers may be at risk of identity theft.
 - Plan to notify, as appropriate, law enforcement, other businesses and consumers. *Remember:* state law may require notice to consumers.
 - Visit [ftc.gov/infosecurity](https://www.ftc.gov/infosecurity).

Help for Consumers

We suggest you:

- give victims information about how to recover from identity theft and refer them to FTC for more help: www.ftc.gov/idtheft or 877-ID-THEFT.
- give them information on the documents you will require from them to resolve fraudulent debts.
- give them closure letters absolving them of fraudulent debts once an incident is resolved.



What you can do now

- **READ THE GUIDE.** “*Protecting Personal Information: A Guide for Business*” is available at www.ftc.gov/infosecurity.
- **ORDER COPIES.** Get free guides for your staff at www.ftc.gov/bulkorder.
- **LINK TO THE GUIDE.** Link to the Guide from your webpage. Get buttons at www.ftc.gov/infosecurity.
- **PUBLISH THE ARTICLES.** The website also has columns you can “drop in” to newsletters or websites.



The screenshot shows the FTC website page for "Protecting Personal Information: A Guide for Business". The page features a navigation menu with the following options: "Read the guide", "Publish the articles", "Present the slides", "Link to us", "Order copies", "View related topics", and "En español". The main content area is titled "Is your company keeping information secure?" and includes a paragraph of text and a list of five key principles: "Take stock", "Scale down", "Lock it", "Pitch it", and "Plan ahead". A "Read the guide >>" link is located below the text. The footer of the page contains the text "Home | For Consumers | For Business | News Room".

Federal Trade Commission | File a Complaint | Order Publications | Privacy Policy | FTC Search

Protecting PERSONAL INFORMATION A Guide for Business

[Read the guide](#)

[Publish the articles](#)

[Present the slides](#)

[Link to us](#)

[Order copies](#)

[View related topics](#)

[En español](#)

Is your company keeping information secure?

Most companies keep sensitive personal information in their files and on their computers—names, Social Security numbers, account data—that identifies customers or employees. You'll need information like that to fill orders, meet payroll, or perform other necessary business functions. But if sensitive data falls into the wrong hands, it can lead to fraud or identity theft.

Safeguarding sensitive data is just plain good business. Are you taking steps to protect personal information? A sound data security plan is built on five key principles:

- ▶ **Take stock.** Know what personal information you have in your files and on your computers.
- ▶ **Scale down.** Keep only what you need for your business.
- ▶ **Lock it.** Protect the information you keep.
- ▶ **Pitch it.** Properly dispose of what you no longer need.
- ▶ **Plan ahead.** Create a plan to respond to security incidents.

[Read the guide >>](#)

Home | For Consumers | For Business | News Room

*Guarding Against Identity Theft:
The Red Flags Rule*

*Red Flags Rule on Duties
Regarding the Detection,
Prevention, and Mitigation
of Identity Theft*

RED FLAGS RULE

- A “red flag” is a pattern, practice, or specific activity that could indicate identity theft

PURPOSE OF THE RED FLAGS RULE

- To ensure that your business or organization is on the lookout for the signs that a crook is using someone else's information, typically to get your products or services with no intention of paying.
- It's not just another data security regulation.

WHO IS COVERED BY THE RED FLAGS RULE?

- Financial institutions and creditors are covered
- They must conduct a periodic risk assessment to determine if they have “covered accounts.”
- If they do, they must develop, implement, and administer a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with:
 - the opening of a covered account, or
 - any existing covered account.

WHAT IS A COVERED ACCOUNT?

An "account" is:

- A continuing relationship established by a person with an FI or creditor to obtain a product or service for personal, household, or business purposes.

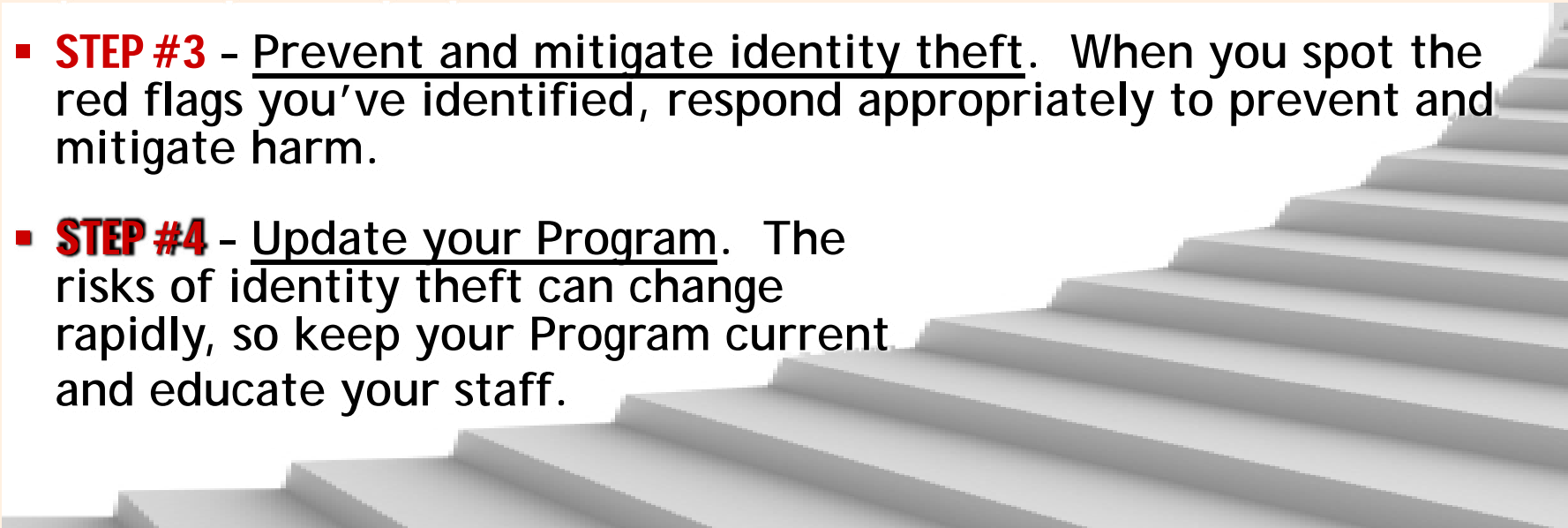
A "covered account" is:

- A consumer account designed to permit multiple payments or transactions, or
- Any other account for which there is a reasonably foreseeable risk from identity theft

HOW DO WE DESIGN AN IDENTITY THEFT PREVENTION PROGRAM?



DESIGNING YOUR PROGRAM

- **STEP #1** - Identify relevant red flags. Identify the red flags you're likely to come across in your business that indicate a crook is using someone else's information to get your products or services with no intention of paying.
 - **STEP #2** - Detect red flags. Set up procedures to detect them in your day-to-day operations.
 - **STEP #3** - Prevent and mitigate identity theft. When you spot the red flags you've identified, respond appropriately to prevent and mitigate harm.
 - **STEP #4** - Update your Program. The risks of identity theft can change rapidly, so keep your Program current and educate your staff.
- 

DESIGNING YOUR PROGRAM

The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of activities.

Identify relevant red flags

- Risk factors:
 - Types of covered accounts you offer or maintain
 - Methods for opening or accessing covered accounts
 - Previous experience with identity theft
- Sources of red flags:
 - Episodes of identity theft that have already happened
 - Changes in how crooks are committing identity theft
 - Applicable supervisory guidance

Identify relevant red flags

- Five categories of red flags:
 - Alerts, notifications, or other warnings received from credit reporting agencies or service providers
 - Suspicious documents
 - Suspicious personal identifying information
 - Unusual use of or other suspicious activity related to a covered account
 - Notice from customers, victims of identity theft, or law enforcement authorities

Set up procedures to detect red flags

- Verify identity
- Authenticate customers
- Monitor transactions
- Verify validity of address changes

Respond appropriately to red flags to prevent and mitigate Identity Theft

- Monitor accounts
- Contact customer
- Change passwords
- Close and reopen account
- Refuse to open account
- Don't sell the account or collect on it against the identity theft victim
- Notify law enforcement
- In some cases, no response may be warranted

**Update your program periodically
in light of:**

- Your experience with identity theft
- Changes in methods of identity theft
- Changes in methods to detect, prevent, and mitigate identity theft
- Changes in types of accounts offered
- Changes in business arrangements

EXAMPLES OF RED FLAGS

- Warning from credit reporting agencies

 **Fraud or active duty alert included in consumer report**

- Suspicious documents

 **Documents provided for identification appear to be altered**

- Suspicious personal information

 **Inconsistent with external information sources**

EXAMPLES OF RED FLAGS

- Unusual use of account

 **Account used in a way inconsistent with historical patterns of activity**

- Notice from customers

 **Customer notifies you about identity theft**

For More Information

- ftc.gov/infosecurity
- ftc.gov/idtheft
- ftc.gov/privacy
- idtheft.gov





Questions?

Joanna Crane

jcrane@ftc.gov

The views expressed are those of the speaker and not necessarily those of the FTC or any other person.