

A Consumer Action Training Guide



PROTECT YOUR PHONE RECORDS

PURPOSE OF THE TRAINING

The purpose of the training is to help participants learn how important it is to safeguard sensitive personal information in their telephone account. Many people today have two or more phones, including cell phones and landlines. We receive billing statements in the mail that list detailed calling records and are able to access our phone records online.

But many people do not understand phone records are a central source of private information that criminals sometimes try to access without consent for illegal or harmful purposes. The privacy of phone records can be compromised by “pretexting”—a criminal act that identity thieves practice to access consumers’ personal information under false pretenses. Armed with confidential data detailing consumers’ identity, employment, bank accounts and calling activity, identity thieves and other scammers do serious, sometimes irreparable damage to consumers’ finances.

TRAINING OBJECTIVES

You will learn:

- Why someone would try to access your phone records
- Who would try to access your phone records
- How they try to access private information
- How to protect yourself from becoming a victim

Materials

Participants’ folders, which include:

- PowerPoint Presentation slides
- Protect Your Phone Records Leader Manual
- Worksheets and Activities (make copies as needed)

For the trainer:

- “Protect Your Phone Records” Training Manual Q&A
- “Protect Your Phone Records” PowerPoint Presentation
- Flip chart pad, markers and pens

SEMINAR DURATION

The training is approximately 1 hour and 45 minutes. One 10-minute break is included.

TRAINING OUTLINE

PART ONE (50 MINUTES)

- Protect Your Phone Records overview- (5 minutes)
- Phone Record Information- (5 minutes)
- Uses of Phone Records- (5 minutes)
How Can I Use It? - Activity (10 minutes)
- Access to Your Phone Records - (5 minutes)
- Participant Introductions-
Who are you? - Activity (10 minutes)
- Pretexting- (10 minutes)

BREAK (10 MINUTES)

PART TWO (50 MINUTES)

- Pretexting & The Law (5 minutes)
- Protecting Your Phone Records (10 minutes)
- Phone Company Responsibility (5 minutes)
- CPNI & Marketing (5 minutes)
Scenarios-Activity (5 minutes)
- Information & Assistance for Victims (5 minutes)
- Questions and answers (10 minutes)
- Wrap Up and evaluation (5 minutes)

TRAINING DESIGN

Before conducting the training, become familiar with:

- The Training Guide and Activities
- The Protect Your Phone Records Leader's Manual
- The accompanying PowerPoint Presentation

PROTECT YOUR RECORDS TRAINING OVERVIEW

Trainer Script:

Welcome. I am _____ and I will be your trainer today.

The purpose of the training is to help participants learn how important it is to guard sensitive personal information in their telephone accounts. Many people today have two or more phones, including their cell phones and landlines. It is common to access phone accounts online and to receive billing statements in the mail that list detailed calling records.

But many people do not understand phone records are a central source of private information that criminals sometimes try to access without consent for illegal or harmful purposes. The privacy of phone records can be breached by “pretexting”—a criminal act that identity thieves practice to access consumers’ personal information under false pretenses. Sometimes it may be people close to you who use your phone records to manipulate you or harm you.

Keeping your phone records private is much more important than most people realize. *Can anyone think how unauthorized access to a person’s phone records might be harmful?*

Unprotected phone records can:

- Be used against you in a dispute
- Provide confidential information exposing you to identity theft
- Expose information about you and your lifestyle that you would like to keep private

Review the Topics to be Covered:

- Phone Record Information
- Uses of Phone Records
- Access to Your Phone Records
- Pretexting
- Pretexting and the Law
- Protecting Your Phone Records
- Phone Company Responsibility
- CPNI (customer proprietary network information) and Marketing
- Information & Assistance for Victims

PART ONE (55 minutes)

PHONE RECORD INFORMATION (5 MINUTES)

Learning Objective:

- Know what information is on your phone records

Ask the class, “What information is contained in phone records?”

Resource: Direct attention to the “Protect Your Phone Records” brochure in the participant folder. The brochure serves as a condensed version of the materials provided in the training. Please review it to see how it may enhance your training.

Background: Various laws and information are in place to keep your phone records private, but you must take an active role in protecting your personal data. For each type of phone access there is different information available. For instance

Your **landline** phone record contains:

- Billing address and/or home address
- Long distance or local telephone numbers dialed from your phone
- Calls billed to a calling card or credit card
- Numbers from which collect calls were accepted
- Dates and lengths of calls outside your calling area.

Your **cellular** phone records:

- The number of all phone calls made or received by you and other family plan members

Your **online phone account** record:

- Alternate contact information you provided, such as home or office phone numbers
- Bank or credit information; i.e., credit or debit card numbers and bank account numbers

Your **phone company** may also keep:

- Birth date
- Social Security number
- All telephone and Internet services for which you subscribe
- Information about the phone that could be used to track the location of the person who has it

USES OF PHONE RECORDS (5 MINUTES)

Learning Overview:

- Learn who would want to access your phone records, and why

Background: You may be surprised to learn that people have an interest in your phone records. Any guesses as to who may have an interest in your phone records?

There are many people who may want to have access to your phone records. They include:

- Con artists and identity thieves
- Data brokers /salespeople
- Estranged spouses or former partners
- Someone involved in a lawsuit with you
- Stalkers
- Investigators, spies, bail bondsmen
- Criminals for retaliation purposes

Ask the class, “What are some possible uses for phone records?”

- A divorce custody battle. How could the phone records be used against the divorcee?
- Workplace jealousy. How can phone records negatively impact someone in the workplace?

TEACHING AID: *How Would I Use It? - Activity Sheet 1 (10 minutes)*

You will see a list of names of people who could potentially use your phone records. As a group, I would like you to formulate ways in which these predators might want to access people’s phone records. We’ll take 10 minutes to complete the exercise. Then each table will share their ideas with the class.

**ACCESS TO YOUR PHONE RECORDS
(5 MINUTES)**

Learning Overview:

- Identify how someone could gain access to your phone records.

Background: Can anyone share ways phone records could be accessed without permission?

Some common ways to access phone records:

- Viewing phone accounts online
- Pretexting
- Gaining access to your billing statement

**PRETEXTING
(10 MINUTES)**

What is pretexting?

- **Pretexting**, otherwise known as social engineering, is a method of obtaining someone else’s personal information under false pretenses. It is done by impersonating the victim or telling lies that will convince a company employee, organization member or other individual to divulge confidential data.

- Pretexting became front-page news in 2006 when Hewlett-Packard admitted that its investigators had obtained the phone records of journalists and its own board members under false pretenses in order to uncover the source of boardroom leaks.

Pretexters **obtain your information** by using:

- You and your neighbors, family, co-workers.
- People who are paid to track you down often use tricks to obtain phone records, sometimes without legal authority such as a court order or subpoena. These people include private investigators, bail bondsmen, debt collectors and others who gain financially by obtaining your records for resale to interested parties. Criminals who want to intimidate witnesses or harm police officers or their families might try to access their phone records illegally.
- Public records, **which are a legal source for** accessing information about you such as: home purchases, filed bankruptcy, business start up and marital status.

Family and friends could often be the source of “leaking” information to predators. Let me show you how. I promised to allow you to share a little about yourselves. Instead of introducing yourself, I want you to introduce your neighbor.

PARTICIPANT INTRODUCTIONS (10 MINUTES)

TEACHING AID - *“Who Are You?” Activity Sheet 2 (10 minutes)*

This exercise that allows for participants to introduce each other and gather information beyond what strangers would normally ask each other. There will be one person at each table who will receive a sheet of paper that says that the participant must gather some piece of private information about their partner. For example: your children’s names, pet’s name, mother’s maiden name, etc. ***The exercise will demonstrate how freely we give out information about ourselves.*** Without meaning to, you may have divulged information to someone who is trying to access information about you that may cause you harm.

Allow participants to introduce each other. Point out when sensitive personal information such as a family name, pet’s name, children’s names, ages and birth dates is mentioned in the introduction.

Let the class know that con artists and those trying to obtain information know that these facts are often used as passwords or as a security questions on your accounts. ***Alert your family and friends about revealing personal information to strangers.***

10 MINUTE BREAK

Announce a break. Let participants know where they can find the restrooms. Ask everyone to reconvene promptly so that the training can continue on schedule.

PART TWO (50 minutes)

PRETEXTING & THE LAW (5 MINUTES)

Learning Objective:

- Know about the laws and consumer rights that protect your phone records

Background: Often people are victims of crimes, fraud or deceptive practices and they don't realize it or are too busy to fight for their rights. It is critical to understand your rights and the importance of fighting for them. *Pretexting is a crime*. These are laws that have been put in place to protect you:

Pretexting Laws

- *1999 Gramm-Leach-Bliley Act*: The law makes it illegal to use pretexting to obtain financial records.
- *2006 Telephone Records & Privacy Protection Act* made pretexting to buy, sell or obtain phone records a federal crime punishable by up to \$500,000 and up to 10 years in prison
- *2007 The Federal Communications Commission (FCC)* requires telephone companies to put in place more stringent authentication measures. (It will be effective at the end of 2007.)

Legal access by law enforcement

- Law enforcement agencies, such as the police or the FBI, can lawfully obtain your phone records. Phone companies will also turn over customer phone records to someone with a subpoena or a court order.
- **Phone companies are required to notify customers** in the event their confidential data is released without permission (a “breach”). The timing of the notification depends on the circumstances of the breach and law enforcement agency decisions.

According to FCC guidelines:

- The company must first notify law enforcement within seven days of the breach.
- The company may notify the customer directly or disclose the breach publicly after seven business days following notification of law enforcement, unless the Federal Bureau of Investigation (FBI) or U.S. Secret Service request that notification be delayed. An FBI or U.S. Secret Service request can delay the disclosure indefinitely.

- The company may immediately disclose the breach if, after consulting the relevant law enforcement agency, the company believes there is an urgent need to do so in order to avoid immediate and irreparable harm to consumers.

PROTECTING YOUR PHONE RECORDS (10 MINUTES)

Learning Objective:

- How to protect yourself from pretexting and other forms of unauthorized access to your phone records.

Background: Prevention is often the key to not becoming a victim. *Know your rights and how to avoid situations that make you vulnerable to pretexting.*

Ways to keep your phone records private:

- **Get a non-published number.** Your number and address will not be listed in phone directories, on Internet search engines or with directory assistance. However, if you give your number to businesses or other entities, it may be sold or shared for marketing. If you are asked for your phone number, ask why it is needed and if you are required to provide it.
- **Set up strong passwords.** Place strong passwords on your phone accounts. Don't use easily guessed passwords. Never use your mother's maiden name, birth date, pet's name, phone number, street address or any part of your Social Security number as a password. Don't use obvious consecutive numbers, such as 1-2-3-4. Choose password reminders that are impossible for a stranger to guess.
- **Limit the information you share.** Don't give out any personal or financial information unless you trust the person you are dealing with. The companies you do business with already have the information they need about you.
- **Inquire about information needed.** You have the right to question why stores or other companies request your phone number.
- **Enlist family members.** Speak to those close to you about the dangers of providing information to strangers. Tell family members not to reveal anything to callers asking for personal information. When in doubt, children should pass the call to you or another adult.
- **Store phone bills and other paperwork** containing personal info in a safe place under lock and key.

Trainer: Maybe you question the need to take such extreme measures. But most victims wish they'd done things differently. There are even more ways you can limit the risk of unauthorized access to your phone records. Call your phone company and ask how it is complying with new FCC security measures effective in late 2007. **All phone companies must comply with the following minimum requirements:**

- Password protection on accounts before information is provided
 - *There are some exceptions to the password rule.* You won't need a password to call your phone company and get help with specific charges or service issues. Your company will also be allowed to provide the records to you without a password by mailing the information to your address on the account; calling you back at the number on the account; or requiring you to show a photo ID at one of its stores. For online access to your account, a password will be mandatory.

- Notification on password changes
- Customer consent before releasing data
- Notification when information is released without your permission (breach)

Your phone company may have even stronger protections for guarding customer information. Contact your phone company for specifics about what additional measures it takes to prevent pretexting and other illegal access.

You can ask your phone company to:

- Deactivate the online access feature if you don't manage your account online.
- Ask the company if it is possible to remove call details from your phone bills.

PHONE COMPANY RESPONSIBILITY (5 MINUTES)

Learning Objective:

What phone companies do to protect customer records.

Background: Phone companies must follow certain laws and abide by FCC rules:

- Keep records customer permission to use account information for marketing purposes.
- Monitor and record events in which customer information was disclosed to third parties.
- Train employees in the appropriate use of customer information.
- Review marketing efforts to ensure privacy requirements.
- Prepare and make publicly available annual certificates that the company has established operating procedures to comply with FCC rules.
- Inform the FCC of any actions taken against data brokers.
- Provide a summary of the customer complaints about unauthorized disclosure of customer information.

CPNI & MARKETING (5 MINUTES)

Learning Objective:

Learn what CPNI or “customer proprietary network information” is, and review customer options for restricting the use of CPNI for marketing purposes.

What is CPNI?

- Customer proprietary network information (CPNI) is all of your phone calling data, including the services you subscribe to, whom you call, when you call, how long your calls are, etc.
- CPNI applies to personal accounts and some business accounts.
- If your telephone company uses your customer information for other marketing, it must obtain your approval to do so. The company may request your approval orally, in writing or electronically. The company can request your approval using:

Opt-Out – Your telephone company sends you a notice saying it will consider you to have given your approval to use your customer information for marketing unless you tell it not to do so (usually within 30 days.)

Opt-In – Your telephone company sends you a notice asking that you expressly give it permission to use your customer information for marketing.

Your phone company is allowed to use your customer info without your approval to:

- Offer you service enhancements.
- Gather and publish aggregate customer data or use customer information for creating directories.

Phone companies are however prohibited from using CPNI to lure back customers who have switched to another service provider.

TEACHING AID: “Can you trust me?” - Activity Sheet 3 (10 minutes)

This is an exercise that allows participants to determine whether they are victims and to learn when it is safe to provide information. Have each participant study the scenarios for 5 minutes. Allow 10 minutes to discuss each situation, focusing on why information should or should not be revealed.

INFORMATION & ASSISTANCE FOR VICTIMS (5 MINUTES)

Learning Overview:

How to respond if you feel your records have been accessed without your permission.

Background: You have options to protect your phone records. If you feel that information has been released without your permission, consider turning your phone off and opening one under a new number. You can also set up passwords to prevent unauthorized access to your new account.

What can I do if my phone records have been stolen?

Ask your local police if you can file an incident report. Having a police report may support your claim that someone stole your phone records in case you have to prove your innocence in a civil or criminal case.

Who should I complain to if my phone information is disclosed without my permission?

If you think your customer information has been disclosed without your permission, start by calling your phone company. If you are unsatisfied with the company’s response, file a complaint with the FCC. If the agency finds that the company violated consumer protection rules, it can fine the company or issue a citation.

File a complaint with the FCC: Email: fccinfo@fcc.gov; Online: www.fcc.gov/cgb/complaints.html; Phone (voice): 888-CALL-FCC (888-225-5322); Phone (TTY): 888-TELL-FCC (888-835-5322); Fax: 866-418-0232; Mail: Federal Communications Commission, Consumer & Governmental Affairs Bureau, Consumer Complaints, 445 12th Street, SW, Washington, DC 20554.

TRAINING AID #1
HOW WOULD I USE IT?
(10 MINUTES)

Identity thieves:

Salesperson:

Estranged spouse:

Someone involved in a lawsuit with you:

Stalkers:

Police:

TRAINING AID 3
SCENARIOS
10 MINUTES

1. I call you. I am representing a company from which you receive services. I ask to speak with you because I would like to offer you greater service for a lower price. You agree, but while you're on the phone, your children are making noise in the background. The caller says, "Awe how cute. What's your son's name?" How do you respond?

- a. Why do you ask? Oh okay—my son's name is Jimmy (fake name)
- b. Sorry, I don't give that information to strangers
- c. Corey—I can't believe he just had his first birthday!

WHY: _____

2. I am a phone company representative. You called me to request some information about your account. You comment on how fast I picked up the phone and thanked me for the timely service. Ask for the last five phone calls that were made from your landline phone. I say sure, but our system is down so I have to look it up manually so it takes a little longer. I ask your name, but do not ask you Social Security number or your passcode. What would you do?

- a. Ask why I didn't go through the security screening before giving me that information?
- b. Said, "Thank you, I'm so glad you found it so fast." By the way, how do you verify customers?
- c. Leave it alone and pray that it doesn't happen again.

WHY: _____

3. I call you. I am with a phone survey company. I have called you before to conduct a 5-minute phone survey. At the completion of this call I ask, "Can I share your contact information with my partners so that they may also call you?" You respond:

- a. No, I do not want my information shared with other companies. Please remove me from your list.
- b. I do enjoy surveys, so please forward my information.
- c. By hanging up.

WHY: _____