



LEADER'S GUIDE

PROTECT YOUR PHONE RECORDS

A Consumer Action Publication

Contents

Introduction — Page 2

About Your Phone Records — Page 3

How Phone Records Are Accessed Illegally — Page 5

Protecting Your Phone Records — Page 8

Information and Assistance for Victims — Page 14

Introduction

Keeping your doors and windows locked is no longer enough to protect yourself from thieves. A certain type of crook is not interested in your jewelry, stereo equipment, car or other personal property. These criminals are after something even more valuable—your personal information. Armed with what is supposed to be confidential data about your identity, employment, accounts and activities, identity thieves and other scammers are able to do serious, sometimes irreparable, damage.

Phone records are an important source of private information that someone might try to access without your consent for illegal or harmful purposes. Various laws and regulations are in place to keep your phone records private, but you must take an active role to protect your personal data. This guide can help you understand:

- ***Who would want to access your phone records;***
- ***Why they might want to do it;***
- ***How they try to access your private information, and***
- ***What you can do to reduce the chances of becoming a victim.***

Consumer Action has also created these free companion pieces to this background guide:

- ***A multilingual consumer brochure explaining how to protect your phone records. This brochure is available in***

bulk in Chinese, English, Korean, Spanish and Vietnamese.

- *A training curriculum with exercises and activities.*
- *PowerPoint training slides.*

For more information about these materials, contact Consumer Action:

- *Web site: www.consumer-action.org*
- *Email: info@consumer-action.org*
- *Phone: 800-999-7981*

About Your Phone Records

Why is it important to keep my phone records private?

You might not realize it, but your phone records contain all sorts of personal information that someone could use to hurt you, steal from you, or commit some other crime using your identity.

What information could someone get from my phone records?

Your landline telephone records may include:

- *Your billing address and, if different, your home address.*
- *Long distance and local toll numbers that were dialed from the phone.*
- *Calls billed to a calling card or credit card.*
- *Numbers from which collect calls were accepted.*
- *Dates and lengths of calls outside your local calling area.*

In addition, your wireless phone records may include:

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

Your phone account online may also include:

- *Alternate contact information you provided, such as home or office phone numbers.*
- *Bank or credit information you provided to pay your bills automatically, such as credit or debit card numbers and checking account numbers.*

Information the company keeps about you may also include:

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

Who would want my phone records?

Any number of people might want your phone records:

- *Con artists trying to steal your assets.*
- *An estranged spouse, a jealous boyfriend or girlfriend, or a stalker.*
- *Identity thieves, who look for opportunities to steal personal information (such as a Social Security number) that enables them to open credit accounts, buy cars, set up phone and other services, and commit crimes using someone else's identity.*
- *Someone involved in a lawsuit with you.*
- *Spies, who use phone records to uncover scandals that can ruin private and political careers.*
- *A private investigator, bail bondsman, debt collector and anyone else who is paid to track you.*
- *Data brokers, who gather data on people with the purpose of selling it to anyone willing to pay for it.*
- *Criminals who want to intimidate or harm witnesses or law enforcement officers.*

How could someone use the information from my phone records?

There are many ways that people who take your personal information without your knowledge or permission can use it to harm you. Here are some fictional examples of how phone account data could be used:

A husband going through a messy divorce asks a female friend to call the phone company and pretend to be his wife. She requests copies of the wife's wireless phone bill, which the husband then uses in court to allege that his wife often called home late at night while he was out of town—proof that she was frequently out rather than home with the children.

A coworker in competition for a big promotion hires a private investigator to get copies of her competitor's phone bills. On the bills are a number of calls to a local health facility that treats people with AIDS, a chronic and sometimes debilitating illness. This information is leaked to the hiring manager.

A would-be identity thief hacks into your online phone account records and obtains your Social Security number, birth date, and checking account number (used for automatic bill payment) along with call records showing frequent calls to a particular bank. He uses this information to make a large withdrawal from your account.

A witness testifying against the defendant in a trial gets a threatening phone call, even though her phone number is unlisted. After entering a witness protection program, she learns her number was purchased from an illegal "data broker"—someone who sells information about others.

How Phone Records Are Accessed Illegally

How could someone access my phone records?

There are numerous ways to access phone records illegally. These are two methods commonly used by data brokers and others:

First, they could try to view phone accounts online. If, for example, you have not yet activated your online account access, someone could use personal information they already have about you to establish an online account. By pretending to be you, they can log on and set up a password before you do.

Second, the most common method for obtaining someone's private phone records and call detail information is "pretexting."

What is pretexting?

Pretexting (sometimes also referred to as "social engineering") is a method of obtaining someone else's personal information under false pretenses. Pretexting is done by impersonating the victim or telling lies that will convince a company employee,

organization member or other individual to divulge confidential data.

When pretexters try to access another person's calling records and other account information, they might pretend to be the telephone service customer. In some cases, the pretexter already has the personal information needed to pretend to be you and access your records. For example, an ex-spouse or an employer may already have or know the required information used to establish your account.

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. Though the HP scandal was extremely well publicized, most cases of phone records pretexting occur without any media attention.

If a pretexter doesn't already have my personal information, how could he get it?

In some cases, the person trying to access your phone records might first need to get some key information before he or she can convincingly pose as you.

Pretexters have been known to try to trick neighbors or coworkers into revealing information about their intended victim. They also sometimes try to fool the intended victim into revealing personal information. For example, while falsely claiming to be conducting a phone survey, the pretexter might ask seemingly innocent questions about such things as who your phone company is or what your pet's name is. (Consumers often use a pet's name as the password for online accounts).

Public records are a legal source of certain types of personal information. If you have ever owned a home, filed bankruptcy, opened a business, or gotten married or divorced, there are public records about you. Many states make court records available to the public at government archives or online databases and pretexters might use them to seek information about you.

Is pretexting legal?

Using pretexting to obtain personal financial data from institutions or their customers has been illegal since 1999, when Congress passed the Gramm-Leach-Bliley Act. While this legislation was a step in the right direction, the law's language—and reach—was somewhat unclear, allowing room for lawyers to debate its application to pretexters who have obtained non-financial data, such as phone records.

In early 2007, the Telephone Records and Privacy Protection Act of 2006 became law, making pretexting to buy, sell or obtain phone records a federal crime punishable by fines of up to \$500,000 and prison sentences of up to 10 years. (Law enforcement officers and intelligence agents are, in most cases, exempt from punishment.) The law, which is enforced by the U.S. Department of Justice, also prohibits the sale or transfer of confidential phone records. Before the passage of this legislation, dozens of websites openly advertised personal phone records for sale for less than \$100.

Prior to 2007, some states had already outlawed telephone pretexting. Since the federal law does not preempt state standards, some states are considering strengthening their own measures against pretexting.

In 2007, the Federal Communications Commission (FCC), which is responsible for regulating interstate and international radio, television, wire, satellite and cable communications, took action to provide further protection from pretexters. The Commission's new rules require telephone companies to put in place more stringent authentication measures (such as mandatory password protection to online accounts and mandatory passwords prior to the release of call detail records over the phone) and impose clearer customer notification guidelines in case of a breach. The FCC rules do not preempt stronger state laws.

Protecting Your Phone Records

What can I do to keep my phone records private?

Though the following measures are not a guarantee of privacy, they do make it more difficult for prying eyes to see your private data.

- **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 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.*
- **Ask why information is 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.*

What should I do with my phone bills so they don't fall into the wrong hands?

Store phone bills and other paperwork containing personal information in a safe place under lock and key. Shred or tear up billing statements before throwing them away. Dumpster div-

ing—searching through garbage to find statements and other documents that reveal personal information—is a favorite trick of identity thieves and other crooks.

In what specific ways can my phone company help protect my information?

All phone companies must meet certain minimum requirements for protecting customer information, but some may place even stronger protections on accounts. For specifics about how your phone company protects your information, ask what measures it takes to prevent pretexting and other illegal access to customers' phone records.

In accordance with new security regulations imposed by the FCC in 2007, all telephone companies must:

- ***Require password protection for online account access. Also, customers must now provide a password when they request call detail information by phone. Without a password, the company can only release phone records by sending the information to the address of record or by calling the customer at the telephone number of record. Phone companies are allowed to provide account information to customers who show a valid photo ID in one of their stores or offices.***
- ***Notify customers when a password, back-up password, online account, or address of record is created or changed.***
- ***Obtain explicit consent from their customers before releasing customer data to joint venture partners, independent contractors or other third parties for the purpose of marketing communications-related services.***
- ***Notify customers in the event of a breach of their confidential data. (This requirement includes some exceptions for law enforcement officers and agencies.)***

To ensure that your personal information is as well-protected as possible, you:

- ***Should ask your phone company to deactivate the online access feature if you don't manage your account online. (If this is not possible, set up a password before a pretexter or hacker beats you to it.)***

- ***Should call the company immediately if your statements don't arrive when they are supposed to.***
- ***Might consider asking the company if it is possible to remove call details from your phone bills.***

Telephone companies take pretexting very seriously. To thwart impostors, some have changed internal procedures. For example, one company has stopped asking customers for their Social Security numbers as a chief way to establish identity, requesting instead a piece of information that is on their phone bill. This company is also training customer service representatives how to identify possible pretexters.

Telephone companies have sued dozens of people who have allegedly obtained phone records without authorization using deceptive and fraudulent access methods.

What duty does my phone company have to protect my records?

Phone companies must operate within any and all applicable laws and abide by all rules set forth by the FCC. This includes fulfilling FCC requirements to:

- ***Keep a record of whether or not individual customers have granted permission to use their account information for marketing purposes.***
- ***Keep accurate records of all instances when customer information was disclosed to third parties.***
- ***Train employees in the appropriate use of customer information.***
- ***Review marketing campaigns to ensure they meet customer information privacy requirements.***
- ***Prepare and make publicly available annual compliance certificates certifying that the company has established operating procedures to ensure compliance with FCC rules.***
- ***Inform the FCC of any actions taken against data brokers.***
- ***Provide a summary of the complaints the company receives about the unauthorized disclosure of customer information.***

What is CPNI?

Customer proprietary network information (CPNI) is all your phone calling data, including the services you subscribe to, whom you call, when you call, how long your calls are, etc.

Can my CPNI be used for marketing purposes without my permission?

The Telecommunications Act of 1996, together with FCC regulations and rulings, generally prohibited the use of CPNI without customer permission. Until recently, however, customers who wanted to keep their information out of the hands of marketers were given the opportunity to use the “opt-out” process. The “opt-out” process gave the customer 30 days to contact the company as to whether or not to share their CPNI data with joint venture partners and outside contactors.

The FCC now requires companies to obtain affirmative, or “opt in,” consumer consent before they are allowed to share CPNI with joint venture partners or independent contractors for the purpose of marketing communications-related services. The company must require third parties that have legitimate business reasons to access your phone records to keep shared customer information confidential.

Your phone company is still allowed to use your customer information, without your approval, to market the same type or higher grade of service than you already subscribe to. These are called “service enhancements.” For example, if you purchase basic local telephone service from a company, it does not need your permission to use your customer information to try to sell you voice mail or caller ID services. However, if you only subscribe to local services, the company cannot try to market long distance or wireless services to you without your prior consent.

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

The CPNI rules do not prohibit companies from gathering and publishing aggregate customer data or using customer information for creating directories.

Customer information rules apply to all types of telephone companies: local, long distance, wireless and, now, voice over Internet Protocol (VoIP).

To ensure you are taking advantage of all opportunities to keep your phone records private, ask your phone company if there is anything further you can do to limit the sharing or selling of your data.

Do CPNI regulations apply to business phone customers?

CPNI regulations for personal customer accounts do not necessarily apply to all business accounts. Individually negotiated CPNI protections may be placed on business accounts that are serviced by a dedicated account representative and based on a contract that specifically addresses the issue of CPNI protection.

Who can obtain my phone records legally?

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.

Will I be informed if my personal account information is disclosed or accessed without my permission?

Phone companies are required to notify customers in the event of a breach of their confidential data, but the timing of the notification depends on the circumstances of the breach and the instructions of law enforcement.

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 FBI or U.S. Secret Service request that the notification be delayed. An FBI or U.S. Secret Service request can delay the disclosure even longer, perhaps 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.

While some argue that the built-in notification delays are necessary for law enforcement to conduct an effective investigation, many counter that the rule is needlessly overbroad, and that timely notification of a breach may be essential for certain victims to protect themselves.

Information & Assistance for Victims

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

If you believe that you have been a victim of phone records pretexting or that your personal account information has been obtained in some other way without your permission, consider closing your phone account and opening a new one. Set up passwords to prevent unauthorized access to your new account.

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 has been disclosed without my permission?

If you think your customer information has been disclosed without your permission, start by calling your phone company to report your concern.

If you are unsatisfied with the company's response, file a complaint with the FCC. If the agency finds that your company violated regulations aimed at protecting consumer information, it can fine the company or issue a citation.

- **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

Also submit a copy of your complaint to the Federal Trade Commission (FTC). (See contact information on page 15.) The FTC works with the FCC to prevent the unlawful sale of phone records by marketers, data collectors or websites. The agency has filed suits against several pretexters under laws barring unfair and deceptive practices.

Are there plans for additional legislation to protect the privacy of telephone service customers?

Along with the new rules established in 2007, the FCC adopted a Further Notice of Proposed Rulemaking, soliciting input on what additional steps, if any, the commission should take to further protect the privacy of consumers. Some areas of protection that may warrant further attention are data encryption, data retention limits and audit trails.

Where can I get more information about protecting my phone records?

Government agencies

Federal Communications Commission

445 12th Street, SW

Washington, DC 20554

Phone: 888-225-5322

Website: www.fcc.gov/cgb

E-mail: fccinfo@fcc.gov

Federal Trade Commission

Consumer Response Center, FTC

600 Pennsylvania Ave., NW

Washington, DC 20580

Phone: 877-382-4357

Website: www.ftc.gov

Non-profit consumer organizations

Consumer Action

221 Main Street, Suite 480

San Francisco, CA 94105

Phone: 415-777-9635

(English, Spanish and Chinese spoken)

Website: www.consumer-action.org

Email: info@consumer-action.org

National Consumers League (NCL)

1701 K Street, NW, Suite 1200

Washington DC 20006

Phone: 202-835-3323

Website: www.nclnet.org

Email: answers@nclnet.org

Consumer Action

www.consumer-action.org

221 Main Street, Suite 480

San Francisco, CA 94105

Phone: 800-999-7981

Email: info@consumer-action.org

English, Spanish and Chinese spoken

*Consumer Action and the National Consumers League
created this publication with funding from Verizon. © 2007*