

Protect your phone records

Your phone records are private because they contain a lot of sensitive personal information about you, your family and your activities. People who get your calling and billing records without your permission could use that information to hurt you or steal from you.

Telling lies or pretending to be the account holder in order to get another person's calling records and telephone account information is called "pretexting." It is a crime under federal law and in virtually every state to use lies or pretend to be someone you're not to get another person's phone records.

Who wants your phone records?

There are many reasons why people might want your phone records. These people might include:

- **Jealous spouses or stalkers.**
- **People involved in messy divorces or lawsuits who are looking for dirt.**
- **Corporate spies or political campaigns digging for scandals.**

Your phone records could be valuable to people who want to steal from you. Identity thieves can use personal information to set up credit or phone service billed in your name. Con artists who want to steal your assets might be able to discover where you bank or which financial services companies you use. Information in your phone records might also allow someone to impersonate you in order to commit crimes.

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 officers' phone records illegally.

How pretexting happens

Pretexting is done in a variety of ways. In order to get enough information to pretend to be you and get access to your phone records, pretexters might speak with your neighbors or coworkers, falsely claim to be conducting phone surveys, or find information about you that is available to the public from sources such as deeds and court records.

Armed with your personal information, a pretexter could try to access your telephone records by logging in to your account through the company's web site or calling customer service.

Your 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 online phone accounts may also include:

Here are some made-up examples of what could happen if phone records fall into the wrong hands:

Tamika is going through a tough divorce. Her husband is trying to gain custody of their children. He alleges that Tamika spends long hours with a co-worker. A friend of the husband pretends to be Tamika in order to get a copy of her wireless phone bill. The phone bill shows late-night calls to the co-worker. The husband's lawyer charges in court that Tamika is an unfit mother because she is having an affair with a co-worker.

Jonah has a chronic disease and does not want his workplace to know about his illness. A jealous co-worker hired a private investigator to get copies of Jonah's cell phone bills. On the bills, the co-worker noticed that Jonah often called a certain number. The co-worker dialed the number and discovered that Jonah had been calling a doctor's office. He searched for the doctor online and found that the physician is an AIDS specialist. The co-worker told people at work that Jonah has AIDS.

Peter is a police officer who has an unlisted home phone number to protect his family. One day a man called the unlisted number and talked to Peter's six-year-old son. The caller warned the boy, "Tell your father to back off." The caller also asked Peter's son where he went to school. Peter learned later that the caller had bought his phone number from an illegal web site. Peter had to move to keep his family safe.

- **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.**
 - **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 a person who has the phone.**

Consumer protections

A federal law makes it illegal to use pretexting to buy, sell or obtain phone records without the customer's permission. (Law enforcement officers are exempted.) The punishment for lying to a phone company in order to get someone else's phone records includes prison sentences and fines. The law is enforced by the U.S. Department

of Justice. It also prohibits the sale or transfer of confidential phone records.

Stronger pretexting rules will take effect in late 2007. The consumer protections were passed by the Federal Communications Commission (FCC), which oversees telephone companies. The new rules will require:

- **Phone companies to implement password protection for certain types of access to your account information.**
- **That you are informed if your personal information is accessed or inadvertently released to a third party without your consent.**

Complaints should go to the FCC and the Federal Trade Commission (FTC). The Federal Trade Commission Act makes it illegal for anyone to use deceit or other unfair practices in order to obtain non-public personal information about another person.

Protecting yourself

Get an unlisted number. Fewer people will be able to call your phone number. Your number and address will not be listed in phone directories, on Internet search engines or with directory assistance. Remember, if you give your unlisted number to businesses or other people, it may be sold or shared for marketing. If you are asked for your unlisted phone number, ask why it is needed and if you are required to provide it.

Set up strong passwords. The new FCC rules require password protection for online account access. Also, customers must provide a password when they request call detail information by phone. Make passwords (and password reminders) impossible for a stranger to guess. Never use your mother's maiden name or your birth date, phone number, street address, pet's name or any part of your Social Security number as a password.

Limit the information you share. Don't give out any personal or financial information unless you trust the person you are dealing with. Ask why the information is needed. The companies you do business with already have the information they need about you.

Talk to your phone company. As of late 2007, telephone carriers must obtain explicit, opt-in consent from customers before releasing account information to joint venture partners or outside contractors for marketing purposes. Carriers are required to notify customers when passwords, online accounts or addresses are changed. Notice is also required if there is an unauthorized disclosure of your confidential information.

Ask your phone company these questions about the security of your phone records:

- **How do you prevent illegal access to my phone records?**
- **Can you remove the numbers I call from my wireless phone bill?**

- **Is it possible to deactivate online access to my phone accounts if I don't need it? (If not, set up a password before a pretexter or hacker beats you to it.)**
- **How and when will I be notified if my account information is changed or disclosed without my permission?**

Keep your information secure. Store phone bills and other paperwork containing personal information in a safe place under lock and key. Call the company if your statements don't arrive when they are supposed to. Shred or tear up billing statements before throwing them away. Speak to family members about the dangers of providing information to strangers. If anyone calls asking for personal information, tell family members not to reveal anything and to pass the call to you.

Advice for victims

If you are a victim of phone records pretexting, consider closing your phone accounts and opening new ones. Use passwords to protect access to your phone records on your new accounts. Ask your local police if you can file an incident report. Having a police report may help prove that someone stole your phone records in case you have to prove your innocence in a civil or criminal case.

How to complain

Call your phone company if you think your customer information has been disclosed without your permission. The pretexting rules apply to all types of phone service: local, long distance, wireless and Voice over Internet Protocol (VoIP).

If you are not satisfied with the company's response, file a complaint with the FCC. If the agency finds a violation, it can issue citations and propose fines.

Send a copy of your complaint to the Federal Trade Commission (FTC). The FTC works with the Federal Communications Commission (FCC) to prevent unlawful sale of phone records by marketers, data collectors or web sites.

Assistance and information

Government agencies

Federal Communications Commission

445 12th Street, S.W.
Washington, DC 20554
Phone: 888-225-5322
Web site: www.fcc.gov/cgb
Email: fccinfo@fcc.gov

Federal Trade Commission

Consumer Response Center, FTC
600 Pennsylvania Ave., N.W.
Washington, DC 20580
Phone: 877-382-4357
Web site: www.ftc.gov

Non-profit consumer organizations

Consumer Action

221 Main Street, Suite 480
San Francisco, CA 94105
Phone: 415-777-9635
Web site: www.consumer-action.org
Email: hotline@consumer-action.org

National Consumers League (NCL)

1701 K Street, N.W., Suite 1200
Washington DC 20006
Phone: 202-835-3323
Web site: www.nclnet.org
Email: questions@nclnet.org

About this publication

Consumer Action and the National Consumers League created this publication with funding from Verizon. For more about the partnership, visit the Consumer Action web site. © 2007



**PROTECT
YOUR
PHONE
RECORDS**