YOU CAN HELP FIGHT PHONE FRAUD

A CONSUMER ACTION PUBLICATION

1

You can help Fight Phone Fraud

Your phone bill arrives, you glance at the total due and send your payment to the phone company without much thought.

What's wrong with this picture? Did you know that by not carefully reviewing your bill you may be a victim of phone fraud and not even realize it?

Phone fraud—the theft of a company's or individual's telecommunications service—is a multi-billion-dollar problem being addressed by local phone companies and gov-

ernment agencies. But if individuals do not look out for and report fraudulent charges, thieves and scam artists will continue to make money.

Because local phone companies are required to bill for other companies that provide telephone services, there is an increased possibility that fraudulent charges may appear on your phone bill. Consumers play an important role in fighting phone fraud because frequently the first step in detecting a scam or fraud is identifying and reporting unauthorized charges that appear on your phone bill.

So, let's start over: Your phone bill arrives, you pour a cup of tea, settle into a comfortable seat, and study the charges carefully, questioning any charge that is unknown to you. Taking adequate time to review your phone bill can save you money and help stop phone fraud.

Phone Frauds

Despite nationwide efforts to combat phone-related rip-offs, crooks are busy devising new ways to commit phone fraud. They seem to find new loopholes as fast as regulators and phone companies can close them.

You could be the victim of a telephone salesperson out to trick you into switching your long distance company. Or your phone bill could be hit with fake charges as a result of a contest entry you filled out.

Phone customers usually are not held responsible for financial losses from fraud. However, all phone users end up paying more for phone service in the long run because billions of dollars in industry losses result in higher rates for everyone.

If you find unauthorized charges or other evidence of fraud, report it to your local phone company, long distance carrier, state public service (or public utility) commission or U.S. government agencies, such as the Federal Communications Commission (FCC). (See page 13.)

3

SLAMMING

Josephine checks her phone statement every month to make sure that she has not been billed for any calls she didn't make. One month she notices she is being billed by a different company for her long distance calls—and the new rates are three times as high. Josephine is a victim of "slamming"—her long distance carrier was changed without her authorization.

ABOUT SLAMMING

You have the right to choose the phone company or companies that carry your calls. When you decide to use a certain company, you designate that company as your primary provider and your service cannot be switched without your permission. In most states, you have the right to choose a local phone company and a long distance carrier. You might also have the right to choose a different company to carry your "local toll" or "intraLATA" calls—calls you make to places that are outside your local calling area but do not qualify as long distance calls. If you are switched from the service provider or providers that you have chosen without your permission, it is called slamming.

What can you do to avoid slamming?

- Review your phone bill carefully.
- Don't fall for common tricks used by devious salespeople, including contest entries that authorize a switch in tiny print, or telemarketers who record people saying "yes" to an innocent question and use it as proof that the customer approved the new carrier.
- If you have been slammed, or are worried about it happening in the future, consider asking your local phone company not to make any changes to your account without your written or oral consent. This means your local, toll or long distance carrier can't be switched until you notify the local phone company.

Cramming

While reviewing his phone bill, David notices one page with an unfamiliar design and company name at the top, showing a $19.95 charge for "voice mail." He calls the company at the top of his bill to question the charge, but isn't able to get an explanation. He then calls his local phone company and learns he is a victim of "cramming"—being billed for unauthorized charges.

About cramming

When third parties add charges to your phone bill for goods or services you did not authorize or receive, it is called cramming. Local phone companies are required to bill for other phone companies, whose charges will appear on separate pages of your local phone bill. Sometimes charges look like ordinary phone numbers and have no explanation. Your bill can be crammed as a result of accepting a collect call from a stranger, filling out a sweepstakes or raffle ticket or responding to misleading voice prompts during a call.

Cramming can negatively affect your credit—often unfairly. Even if your local phone company removes the charges, you might be hounded for the money by a collection agency and you could end up with a blemished credit rating. If you believe you are being charged unfairly, document your claim of fraud by sending letters to your local district attorney's office, state attorney general or federal regulatory agency. Keep copies of all letters.

How can you avoid being crammed?

- Review your telephone bill carefully. If you have questions about a charge, call the service provider whose name and company emblem appear on that bill page.
- Notify your local telephone company about charges you don't recognize, and complain to it if you are unable to resolve a disputed bill with the company that charged it.
- Avoid filling out contest entries unless you read all the fine print.
- Keep a record of calls made or accepted on your home phone, especially for pay-per-use 1-900 and 976 numbers and collect calls.

Toll fraud

Mei Ling got a message asking her to call a number with an 809 area code. When she returned the call, she realized that she did not know the calling party and hung up. Her next phone bill has a charge of more than $30 for a call to the Caribbean. She had been tricked into making a costly international call. Mei Ling is a victim of one of the many types of "toll fraud."

About toll fraud

Toll fraud is the theft of phone time, accomplished by crooks who connect to your phone line, trick you into placing expensive pay-per-use (1-900 or 976) or costly international calls, or fool you into paying for long distance or collect calls.

Thieves make random calls to pagers and leave a phone number for a foreign country or a pay-per-use number in order to get you to place an expensive call in return. The first time the customer realizes what happened is when a bill arrives with unknown charges—often totaling thousands of dollars.

Sometimes crooks pretend to be phone company employees, and ask you to help them by agreeing to authorize collect or other calls billed to your phone.

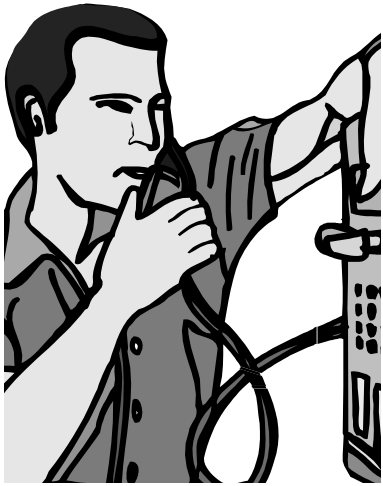
How can you avoid toll fraud?

• Don't accept collect calls from unfamiliar persons or return calls to unfamiliar telephone numbers. Beware of faxes, e-mail, voice mail and pager messages that ask you to call an unfamiliar number. Calling 1-900 numbers will result in charges to your phone bill.

• Although 1-800 and 1-888 numbers are toll-free, callers are sometimes instructed to dial another telephone number to continue the call or may be automatically forwarded to another line. In either case, the call will carry a charge. Pay close attention to recorded voices, as they may be asking you to accept charges for the call or other services.

• Find out where the area code is before you dial calls that indicate that long distance charges will apply. Calls to the Caribbean can be very expensive but do not require the telltale 0-1-1 prefix for an international call. Unscrupulous advertisers use pager or e-mail messages to trick you into making calls that turn out to be very expensive.

• If you see strangers in or around your telephone junction box or outside wiring, do not approach them because they may be dangerous. Report the situation to your local law enforcement agency.



CALLING CARD FRAUD

Paulo travels a lot on business and often uses his long distance calling card at airports and other public places. His latest phone bill lists thousands of dollars in charges for calls he didn't make. Paulo is a victim of calling card fraud—someone stole his calling card number and personal identification number (PIN) by watching him place a call.

HOW CAN YOU AVOID FRAUD INVOLVING YOUR CALLING CARD?

• Ask your calling card company to issue a card that does not have your PIN on it. Memorize the PIN and do not write it on the card.

• Don't reveal your calling card number and PIN to anyone who might use it to make calls without your permission.

• When you place calling card calls in public, cup your hand over the keypad of the phone while entering your number or speak softly when giving it to an operator. Be aware of anyone who might be trying to see or overhear your number and PIN.

• Never give your calling card number to a stranger who calls you.

• Consider using a "prepaid" or "debit" card to make calls when traveling.

• Ask your carrier for a "one-number" or "call-home" card, which provides your loved ones and friends with a number that can only be used to call your home.

Identity Theft

Julia, who lives in San Francisco, got a call from a phone company requesting that she pay an overdue phone bill. The bill was for a phone number in Los Angeles. Since she knew nothing about the phone number, Julia asked her phone company to investigate. It turned out that someone posing as Julia had gotten a phone in her name.

About identity theft

Crooks steal personal information and use it to set up accounts in the victims' names. While the victims usually are not liable in cases of identity theft, it can be a long and difficult process for victims to prove that the debts do not belong to them.

How can you avoid becoming a victim of identity theft?

- Limit the amount of personal information you carry in your wallet, in case you lose it or it gets stolen.
- Check your credit reports annually by contacting one or all of the three largest credit reporting bureaus (Equifax, Experian and Trans Union) in case debts that are not yours are being reported.
- Before you dispose of papers that contain sensitive personal information, such as bank account numbers, your Social Security number or your date of birth, tear them up.

Outside line scams

Lee is a receptionist at a busy office. A caller identifies himself as a phone company employee and asks Lee to dial a series of digits to test the switchboard. A few weeks later, Lee's employer finds thousands of dollars in fraudulent calls on the company's bill. Lee realizes she fell for a scam and gave a crook access to her employer's outside phone line.

About outside line scams

Callers may identify themselves as telephone company employees, such as service or security technicians, and say they are conducting service tests. They ask you to dial a series of numbers, and then ask you to hang up. This gives callers access to an outside line and they are able to make operator-assisted calls that are billed to your account.

What can you do to help avoid outside line scams?

- Be suspicious if anyone claiming to be an employee of your local phone company or long distance carrier asks you for an outside line, call forwarding or a calling card number, or if anyone asks you to dial a number for them. Phone company employees never make such requests.
- Ask for the caller's name and number so you can verify they are indeed a representative of the phone company.
- Report any suspicious calls to your phone company.

WIRELESS PHONE FRAUD

Carlton is a salesperson who often uses his wireless phone while traveling on busy highways, and sometimes forgets to turn it off when he stops off on sales visits. A recent billing statement showed thousands of dollars worth of calls made to and from places Carlton had never been. When he reported the information to his wireless carrier, the company called law enforcement authorities, who told Carlton that data had been stolen from his phone using a scanning device and "cloned" into other wireless phones that were sold on the street.

ABOUT WIRELESS PHONE FRAUD

From high-tech data theft to simple phone theft, wireless phone fraud cost the wireless industry approximately $182 million in 1998, according to the Cellular Telecommunications Industry Association.

How can you avoid wireless phone fraud?

• Protect sensitive documents such as customer service agreements, which include electronic serial numbers.
• If you receive wrong number calls or hang-ups frequently on your wireless phone, report it to your wireless carrier; it could indicate someone else is using your wireless number.

• Report unusual call activity or high calling volumes appearing on your monthly wireless bill to your wireless provider.

• If you have to leave your wireless phone in an unattended car, lock it up, out-of-sight, and use the keypad lock code.

• If you don't make international calls, ask your carrier to limit your account to calls placed within the U.S.

• Turn off the phone when it's not in use or if you are in slow-moving traffic. Identifying numbers cannot be stolen from a turned-off phone.

• Because wireless phone technology varies from company to company, ask your wireless carrier about added security measures that can help protect you from being a victim of wireless phone fraud.

How to complain when phone fraud happens to you

When you find a problem on your phone bill or suspect phone fraud, call your local phone company *and* the company that is billing you for the questionable charges. Ask your local phone company to advise you on which law enforcement or regulatory agencies you should contact.

Also report slamming or cramming complaints to:

• Your state public utilities commission, or public service commission. Look it up in the state government pages of your local phone directory or check out the National Association of Regulatory Utility Commissioners' Web site (http://www.naruc.org) for a listing of all state agencies.

• Your state attorney general's office. (You can look up the number in the state government pages of your local phone directory.)

• The Federal Communications Commission (FCC)
Informal Complaints/Public Inquiries
Mail Stop 1600A2
2025 M Street, N.W.
Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322)

FOR MORE INFORMATION ON PHONE FRAUD PREVENTION

• Ask if your local phone company or long distance carrier has any consumer information on phone fraud. In addition, many companies have Web sites that contain consumer education information.

• The Alliance to Outfox Phone Fraud® (www.gnat.net/~outfox/) offers tips and advice on fraud prevention for consumers and businesses.

• Consumer Action's Web site (www.consumer-action.org) and referral and advice switchboard (1-415-777-9635 and 1-213-624-8327) provide information and resources on preventing and dealing with phone fraud.

• The National Fraud Information Center, a project of the National Consumers League, assists people in recognizing and filing complaints about telephone solicitation and Internet fraud through its toll-free hotline at 1-800-876-7060. The center's Web site (www.fraud.org) features information to help consumers avoid becoming victims of fraud.

• The World of Wireless Communications (www.wow.com), the Web site of the Cellular Telecommunications Industry Association, features news and consumer tips on wireless phone fraud prevention.

CONSUMER ACTION

Web site: www.consumer-action.org

717 Market St., Suite 310
San Francisco, CA 94103
(415) 777-9635

523 West Sixth St., Suite 1105
Los Angeles, CA 90014
(213) 624-8327

Chinese, English and Spanish spoken.

Leave a TTY message anytime:
(415) 777-9456

E-mail: hotline@consumer-action.org
info@consumer-action.org

ABOUT THIS PUBLICATION

'You Can Help Fight Phone Fraud' was created by Consumer Action with funding from SBC Communications Inc., the parent company of Pacific Bell, Southwestern Bell, Nevada Bell and SNET. It is available in English, Spanish, Chinese, Korean and Vietnamese.