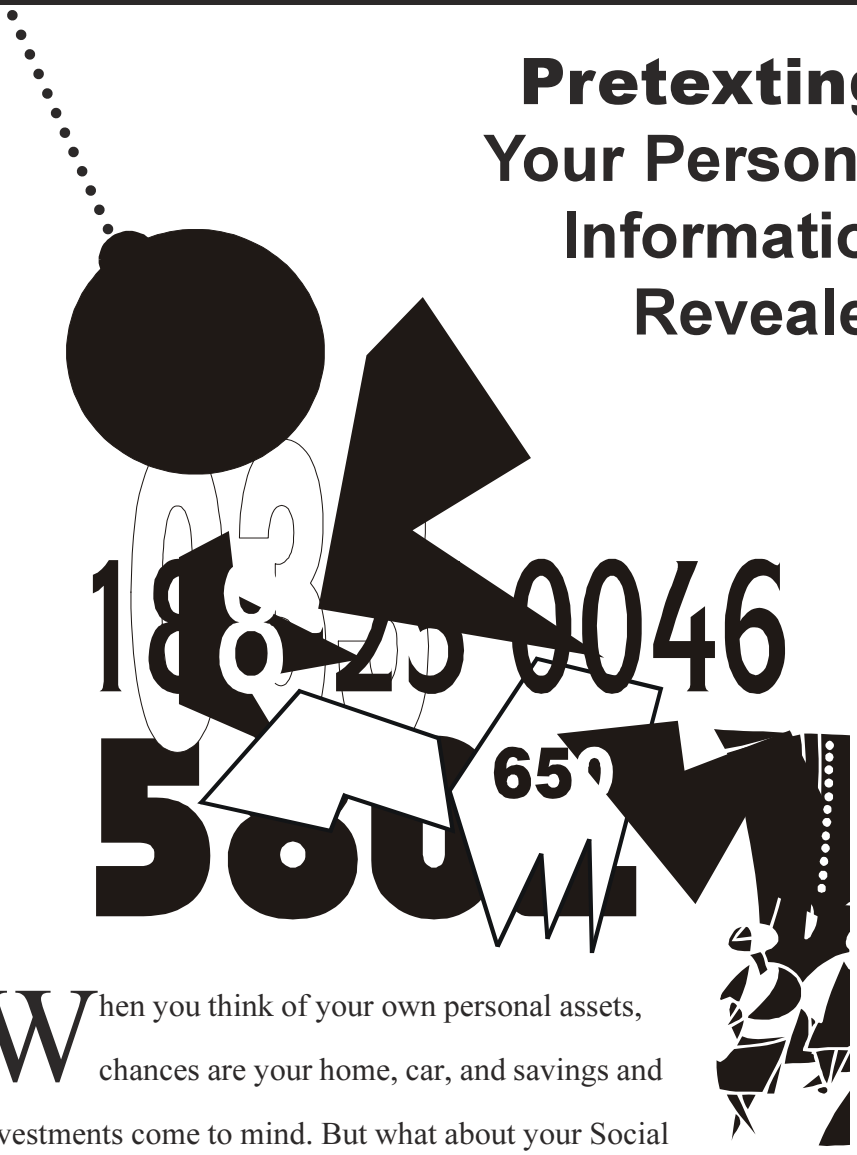
CREDIT

FOR THE CONSUMER www.ftc.gov

FEDERAL TRADE COMMISSION 1-877-FTC-HELP

FTC FACTS for Consumers

Pretexting: Your Personal Information Revealed



When you think of your own personal assets, chances are your home, car, and savings and investments come to mind. But what about your Social Security number and your bank and credit card account numbers? To people known as "pretexters," that information is a personal asset, too.

Pretexting is the practice of getting your personal information under false pretenses. Pretexters sell your information to people who may use it to get credit in your name, steal your assets, or to investigate or sue you. **Pretexting is against the law.**

How Pretexting Works

Pretexters use a variety of tactics to get your personal information. For example, a pretexter may call, claim he's from a survey firm, and ask you a few questions. When the pretexter has the information he wants, he uses it to call your financial institution. He pretends to be you or someone with authorized access to your

account. He might claim that he's forgotten his checkbook and needs information about his account. In this way, the pretexter may be able to obtain personal information about you such as your Social Security number (SSN), bank and credit card account numbers, information in your credit report, and the existence and size of your savings and investment portfolios.

Keep in mind that some information about you may be a matter of public record, such as whether you own a home, pay your real estate taxes, or have ever filed for bankruptcy. It is **not** pretexting for another person to collect this kind of information.

There Ought to Be a Law — There Is

Under a new federal law — the Gramm-Leach-Bliley Act — it's illegal for anyone to:

- use false, fictitious or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution.

- use forged, counterfeit, lost, or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution.

- ask another person to get someone else's customer information using false, fictitious or fraudulent statements or using false, fictitious or fraudulent documents or forged, counterfeit, lost, or stolen documents.

The Link to Identity Theft

Pretexting can lead to "identity theft." Identity theft occurs when someone hijacks your personal identifying information to open new charge accounts, order merchandise, or borrow money. Consumers targeted by identity thieves usually don't know they've been victimized until the hijackers fail to pay the bills or repay the loans, and collection agencies begin dunning the consumers for payment of accounts they didn't even know they had.

According to the Federal Trade Commission, the most common forms of identity theft are:

Credit Card Fraud — a credit card account is opened in a consumer's name or an existing credit card account is "taken over";

Communications Services Fraud — the identity thief opens telephone, cellular, or other utility service in the consumer's name;

Bank Fraud — a checking or savings account is opened in the consumer's name, and/or fraudulent checks are written; and

Fraudulent Loans — the identity thief gets a loan, such as a car loan, in the consumer's name.

The Identity Theft and Assumption Deterrence Act makes it a federal crime when someone: "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."

Under the Identity Theft Act, a name or SSN is considered a "means of identification." So is a credit card number, cellular telephone electronic serial number or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual.

Protect Yourself

Even though the laws are on your side, it's wise to take an active role in protecting your information.

- Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with. Pretexters may pose as representatives of survey firms, banks, Internet service providers and even government agencies to get you to reveal your SSN, mother's maiden name, financial account numbers and other identifying information. Legitimate organizations with which you do business have the information they need and will not ask you for it.

- Be informed. Ask your financial institutions for their policies about sharing your information. Ask them specifically about their policies to prevent pretexting.

- Pay attention to your statement cycles. Follow up with your financial institutions if your statements don't arrive on time.

- Review your statements carefully and promptly. Report any discrepancies to your institution immediately.

- Alert family members to the dangers of pretexting. Explain that only you, or someone you authorize, should provide personal information to others.

- Keep items with personal information in a safe place. Tear or shred your charge receipts, copies of credit applications, insurance forms, bank checks and other financial statements that you're discarding, expired charge cards and credit offers you get in the mail.

- Add passwords to your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.

- Be mindful about where you leave personal information in your home, especially if you have roommates or are having work done in your home by others.

- Find out who has access to your personal information at work and verify that the records are kept in a secure location.

- Order a copy of your credit report from each of the three major credit reporting agencies every year. Make sure it's accurate and includes only those activities you've authorized. The law allows credit bureaus to charge you up to $9.00 for a copy of your credit report.

  Equifax: call: 1-800-685-1111 or write: P.O. Box 740241, Atlanta, GA 30374-0241
  Experian: call: 1-888-EXPERIAN (397-3742) or write: P.O. Box 949, Allen TX 75013-0949
  Trans Union: call: 1-800-916-8800 or write: P.O. Box 1000, Chester, PA 19022

  Your credit report contains information on where you work and live, the credit accounts that have been opened in your name, how you pay your bills and whether you've been sued, arrested or have filed for bankruptcy. Checking your report periodically can help you catch mistakes and fraud before they wreak havoc on your personal finances.

If You Think You're a Victim

If you think you've been a victim of pretexting, the Federal Trade Commission recommends that you:

1. **Report it to your financial institution immediately.** Close accounts that have been tampered with and open new ones with new Personal Identification Numbers (PINs) and passwords.

2. **Contact the fraud departments of each of the three major credit bureaus immediately.** Tell them to flag your file with a fraud alert including a statement that creditors should get your permission before opening any new accounts in your name.

   Equifax: call: 1-800-525-6285 and write: P.O. Box 740241, Atlanta, GA 30374-0241
   Experian: call: 1-888-EXPERIAN (397-3742) and write: P.O. Box 949, Allen, TX 75013-0949
   Trans Union: call: 1-800-680-7289 and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834

3. **Contact your local police as soon as possible, and ask to file a report.** Even if the police can't catch the pretexter, having a police report can help you in clearing up your credit records later on.

4. **Contact the Federal Trade Commission as soon as possible.** The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint, or to get free information on any of 150 consumer topics, call toll-free, 1-877-FTC-HELP (1-877-382-4357), or use the complaint form at **www.ftc.gov**. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

If you've been a victim of identity theft, file a complaint with the FTC by contacting the FTC's Identity Theft Hotline by telephone: toll-free 1-877-IDTHEFT (438-4338); TDD: 202-326-2502; by mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; or online: www.consumer.gov/idtheft.

The FTC has published a free 21-page booklet, **Identity Theft: When Bad Things Happen to Your Good Name.** This comprehensive guide includes information on what consumers can do to reduce their risk of ID theft; how consumers can protect their personal information; the steps consumers can take if they do become victims of ID theft; and a directory of government resources available to ID theft victims. For your copy, call 1-877-IDTHEFT or visit www.consumer.gov/idtheft.

FEDERAL TRADE COMMISSION | FOR THE CONSUMER
1-877-FTC-HELP | www.ftc.gov

Federal Trade Commission
Bureau of Consumer Protection
Office of Consumer and Business Education

January 2001