

# JANUARY

## PRIVACY AND IDENTITY THEFT

Your personal information is a valuable resource for identity thieves, scammers, and even to corporations. Data breaches of customer databases and payment processing systems at retailers highlight the importance of protecting your privacy, while making sure companies with which you do business do the same.

Identity thieves steal your personal information to commit fraud. They can damage your credit status and cost you time and money to restore your good name. You may not know that you are the victim of ID theft until you experience a financial consequence (mystery bills, credit collections, denied loans) down the road from actions that the thief has taken with your ID. Follow these tips to protect yourself:

- **Secure your Social Security card.** Don't carry it in your wallet or write your number on your checks. Only give out your social security number (SSN) when absolutely necessary.
- **Protect your PIN.** Never write a PIN on a credit or debit card or on a slip of paper kept in your wallet.
- **Watch out for "shoulder surfers."** Shield the keypad when typing your passwords on computers and at ATMs.
- **Be skeptical.** Don't respond to unsolicited requests for personal information (your name, birthdate, social security number, or bank account number) by phone, mail, or online.
- **Collect mail promptly.** Ask the post office to put your mail on hold when you are away from home for more than a day or two.
- **Pay attention to your billing cycles.** If bills or financial statements are late, contact the sender.
- **Keep your receipts.** Ask for carbons and incorrect charge slips as well. Promptly compare receipts with account statements. Watch for unauthorized transactions.
- **Tear up or shred** unwanted receipts, credit offers, account statements, and expired cards, to prevent "dumpster divers" from getting your personal information.
- **Store personal information in a safe place** at home and at work.
- **Install firewalls** and virus-detection software on your home computer.
- **Create complex passwords** that identity thieves cannot guess easily.
- **Order your credit report once a year.** Check it more frequently if you suspect someone has gained access to your account information. See "Order Your Free Credit Reports"

## PROTECT YOUR PRIVACY

Your personal data is always being shared. Companies, known as data brokers, compile information about your income, family size, email addresses, stores and websites you visit, the brands you buy, credit cards used, hobbies, and your demographic information to create a profile about you and your lifestyle.

Some of the information you give willingly, but other bits of your personal information are collected in ways you may not realize. Data brokers often collect location-based data from your mobile phone, wearables like fitness trackers or sleep monitors, or from certain apps. Your information is analyzed by brokers to develop scoring and models to help them understand your behavior, and sell your consumer profiles to retailers and marketers.

There is also the “Internet of Things”, with sensors in household appliances, cars, and thermostats that monitor your behavior and communicate between each other and across networks.

Retailers use your information to offer targeted special promotions, customize the online ads you see, and even the prices you are charged for items. While this can be a bonus and help you get good deals, it all comes at the cost of your personal privacy. Unlike credit reports or scores, you cannot access or review the data files that have been created about you, or even know the data brokerage companies you should contact to correct inaccuracies. These data reports can also result in discrimination, where some consumers are only targeted with high interest loans or inferior financial products. Take these steps to protect your privacy:

- If you apply for a store loyalty card, do not include your full name so that it, and your purchase behavior, cannot be connected to your other consumer profiles.
- If you want to keep your purchase behavior private, consider using cash rather than electronic payment options.
- Maintain a separate email address for coupons and promotions from retailers.
- Be careful about what you post on social media. Data brokers may scrape information you post to enhance the information that they have in your consumer profile.
- Disable cookies when shopping online, to prevent companies from tracking your online browsing behavior.
- Beware of using cell phones in stores or using the public Wi-Fi in a store. By using these networks, stores may know which items you looked at and which aisles you visited.
- Look for privacy statements on websites, sales materials, and forms you fill out. If a website claims to follow a set of established voluntary standards, read the standards. Don't assume it provides the level of privacy you want.
- Ask how your personal information will be stored and used.
- Only provide the purchase date, model and serial numbers, and your contact information on warranty registration forms.
- Opt-out if you do not want the company to share your email address with other companies.

Check with your state or local consumer agency to find out whether any state laws help protect your privacy. Some companies and industry groups have also adopted voluntary policies that address privacy concerns.

## EDUCATION PRIVACY

Education privacy deals with the storage, control, sharing, and destruction of students' educational records. The Federal Education Rights and Privacy Act (FERPA) gives parents of school aged children (kindergarten through 12th grade) access to their education records. This act also restricts who the school can share the information with, such as other schools, without needing permission from a student's parent. Take action:

- Opt out of having your child's personal information used for directories that can be shared with third parties.
- Ask for documentation about the purpose of the data collection, if a school says that data collection is required. Find out how the data will be used, stored, and destroyed.

For more information call 1-800-872-5327.

Another education privacy issue involves data breaches, especially at colleges and universities. When these happen, social security numbers, birthdates, grades, addresses and other personal information are compromised. These breaches can impact students' academic records and financial aid, while making them vulnerable to identity theft. If your college has experienced a data breach find out what protections the school has put in place. The Privacy Rights Clearinghouse offers more information about your education privacy rights [www.privacyrights.org/topics/120](http://www.privacyrights.org/topics/120).

## WHAT TO DO AFTER A DATA BREACH

Data breaches of large organizations, such as retailers, schools, and employers have become common. These events can make your identity prone to identity theft. If you've been affected by a breach, have a plan of action:

- Sign up for a free credit monitoring service, if it is offered by the organization that experienced the breach. This service can alert you if credit accounts are opened with your information. If you have been involved in breaches from several companies, sign up for all the monitoring services. The services may be provided through different credit reporting agencies, and may detect different activities.
- Change passwords on any accounts connected to your compromised information.
- Contact the credit reporting agencies (Equifax, Experian, and TransUnion) to place freezes on your credit reports. This makes it difficult for someone to apply for credit in your name.
- If the breach involved a credit or debit card, your issuer may send you a new card with a new number. Update any accounts where the old card number was stored for easy payment or automatic recurring charges.

- Check your bank or credit card statements closely. Report suspicious charges to the fraud department.

## BEWARE: SYNTHETIC IDENTITY THEFT

Synthetic identity theft is a version of identity theft. In traditional ID theft, the thief steals all of the personal information of one person to create a new identity. However, with synthetic ID theft, a thief steals pieces of information from different people to create a new identity. For example, the thief may steal one person's social security number, combine it with another person's name, and use someone else's address to create a brand new identity. The thief can then use this fraudulent identity to apply for credit, rent an apartment, or make major purchases.

While you cannot prevent synthetic ID theft, you should still get copies of your credit report to check for accounts you did not open. Also, contact the credit reporting agencies to ask if there is a fragmented file (a sub-account that uses your social security number but not your name) attached to your main credit file. If this is the case, you may be the victim of synthetic identity theft. Report all cases of identity theft to the Federal Trade Commission.

## COMMON SCHEMES

Here are some common schemes that ID thieves use to steal your identity.

- **Telemarketing.** An ID thief may call you, making fraudulent offers for products, benefits or medical services. The caller will require you to provide personal information, such as your social security number, birth date, or Medicare ID number.
- **Tax ID theft.** In some cases, phony tax preparers steal your social security number and sell it to scammers. In others, someone files a tax return, using your social security number. For more information contact the IRS' Taxpayer Advocate Service at 1-877-275-8271 or visit [www.irs.gov/uac/Taxpayer-Advocate-Service-6](http://www.irs.gov/uac/Taxpayer-Advocate-Service-6).
- **Medical ID theft.** Medical service providers can take advantage of access to your insurance information to get medical services in your name, or to issue fraudulent billing to you and your health insurer.
- **Child ID theft.** Children's IDs are vulnerable because children don't need to file taxes or use their social security numbers to apply for loans for many years. By the time they are adults, the damage has already been

done. Follow the steps listed on [www.IdentityTheft.gov](http://www.IdentityTheft.gov) for a full guide on how to limit the impact of identity theft.

## REPORT IDENTITY THEFT

If you are a victim of identity theft, report it immediately. Visit [www.Identitytheft.gov](http://www.Identitytheft.gov) for a guide on what to do to limit the damage. Follow these steps:

- **Report it to your financial institutions.** Call the phone number on your account statement or on the back of your credit or debit card.
- **File a report with the Federal Trade Commission.** This detailed report is also called an ID theft affidavit.
- **Report the fraud to your local police.** Keep a copy of the police report, which will make it easier to prove your case to creditors and retailers. Together, your ID theft affidavit and your police report make up your ID theft report.
- **Contact the credit reporting agencies** and ask them to flag your account with a fraud alert, which asks merchants not to grant new credit without your approval.

An ID theft report will help you deal with the credit reporting agencies and companies that extended credit to the identity thief using your name.

Visit [www.identitytheft.gov/#what-to-do-right-away](http://www.identitytheft.gov/#what-to-do-right-away) for more information about creating an ID theft report. You can file your complaint with the FTC at [www.ftccomplaintassistant.gov](http://www.ftccomplaintassistant.gov) or by calling toll free 1-877-438-4338.

## ORDER YOUR FREE CREDIT REPORTS

You can request a free credit report once a year from each of the three major credit reporting agencies—Equifax, Experian, and TransUnion. If you ask the credit bureaus directly, they will charge you a fee to obtain your report. You may want to request your credit reports one at a time, every four months, so you can monitor your credit throughout the year without having to pay for a report. Order your free report, through [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228.

Check the accuracy of your credit report when you get it.

- Is your full name, social security number, birthdate, and address correct?
- Are employers, creditors, or home addresses listed that don't belong to you?
- Are account statuses correctly reported as open, closed, or delinquent?
- Do judgements, such as liens or bankruptcies, appear correctly?

If there are any inaccuracies, contact the credit reporting agency and creditor that furnished that information to get it corrected. If they don't fix your report, you can file a complaint with the Consumer Financial Protection Bureau.