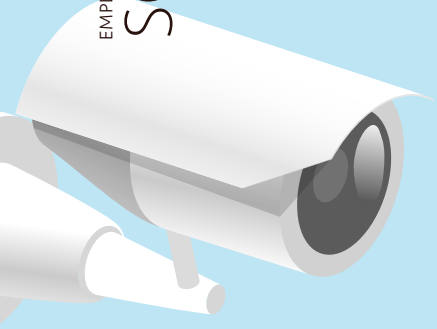
EMPLOYEE ASSISTANCE AND WORKLIFE SOLUTIONS

Safeguard

Your Personal Security



Being protective of your personal information is more important now than ever. As technology grows more sophisticated by the day, and as the number of ways we do business and exchange information with the world only increases, every one of us is increasingly vulnerable to fraud and identity theft. Keep reading to learn more about how to safeguard your personal and financial information, and the steps to take in the event your identity is compromised.

Avoid fraud and scams

According to the Federal Trade Commission (FTC), millions of people each year are defrauded by crooks using various schemes and tricks to get people to send money or offer up personal information. And, it can happen to anyone, regardless of a person's savvy, education, or experience. Here are a few tips from the FTC that can help you protect your personal information and avoid fraud:

- **Spot imposters.** Scammers often pretend to be someone you trust, like a government official, a relative, a charity, or a company you do business with. Don't send money or give out personal information in response to an unexpected request or pay upfront for promised services — whether it comes as a text, a phone call, or an email.
- **Do online searches.** Type a company or product name into your favorite search engine with words like "review," "complaint," or "scam." Or, search for a phrase that describes your situation, like "IRS call." You can even search for phone numbers to see if other people have reported them as scams.
- **Don't believe your caller ID.** Technology makes it easy for scammers to fake caller ID information, so the name and number you see aren't always real. If someone calls asking for money or personal information, hang up. If you think the caller might be telling the truth, call back using a number you know is genuine.
- **Hang up on robocalls.** If you answer the phone and hear a recorded sales pitch, hang up and report it to the FTC. These calls are illegal, and often the products are bogus. Don't press 1 to speak to a person or to be taken off the list. That could lead to more calls.
- **Sign up for free scam alerts.** Get the latest tips and advice about scams sent right to your inbox from the FTC. To sign up, go to FTC.gov/Scams and click on the *Get Email Updates* button.

To view the full list of tips, visit Consumer.FTC.gov – 10 Things You Can Do to Avoid Fraud.

Know the signs of stolen information

One of the more problematic aspects of identity theft and personal information fraud is not knowing you're a victim until it's too late. The most recent annual Aftermath Survey conducted by the Identity Theft Resource Center reports that while 42.5 percent of respondents learned of their stolen identity within three months of the theft, just over 16 percent said they didn't find out for at least three years. What's worse, many people don't

find out until they're denied for a loan or receive notices from a collection agency. Keep regular tabs on your credit report and account statements, and take note of these common signs that your personal information has been stolen:

- Unauthorized accounts on your credit report
- Unauthorized transactions or missing money from an account
- Unexpected drop in credit score
- Receiving a bill in your name for an account you didn't open or services you didn't use
- Sudden suspension in utility services
- Credit, housing application, or loan denial
- Receiving notification of a data breach at a company where you do business or have an account
- Merchants refuse your checks
- Calls from debt collectors about unpaid bills that aren't yours
- Legitimate notification from the IRS that multiple tax returns were filed in your name, or that you have income from an unknown employer

Report and recover from fraudulent activity

If you discover that someone has stolen your personal information, the FTC recommends that you immediately:

Call the companies for the affected accounts
Ask to speak with the fraud department and have them freeze all associated accounts.

Change account logins, passwords, and PINs
It's a good idea to do this for all accounts regardless of a confirmed breach. Once one account becomes compromised, it's safe to assume that others could be at increased vulnerability.

Place a fraud alert on your credit report
Set up a free, one-year fraud alert by contacting one of the three credit bureaus listed to the right; each bureau is required to inform the other two, so there's no need to reach out to all three.

Obtain a free copy of your credit reports
AnnualCreditReport.com
877-322-8228

Report identity theft to the FTC
IdentityTheft.gov
877-438-4338

Work with an identity theft specialist
Your EAP is available 24/7 to help with personal security and identity theft issues. Call any time to schedule a free consultation with a financial expert or attorney.

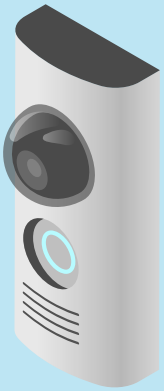
Much of this newsletter's content was compiled from online resources provided by the Federal Trade Commission. Visit FTC.gov and IdentityTheft.gov for a wealth of valuable information.

CREDIT BUREAU CONTACT INFORMATION

EQUIFAX
Equifax.com/personal/credit-report-services
800-685-1111

EXPERIAN
Experian.com/help
888-EXPERIAN (888-397-3742)

TRANS UNION
TransUnion.com/credit-help
888-909-8872



24 HOURS A DAY
(800) 222-0364
TTY: (888) 262-7848
FOH4YOU.COM

The EAP is a voluntary and confidential employee benefit available to federal employees and their family members at no cost.

EAP FOH4You.com
PSC Federal Occupational Health
U.S. Department of Health and Human Services