

# Protecting Against Identity Theft

Identity theft occurs when someone wrongfully obtains and uses another person's personal information (name, date of birth, Social Security number, etc.) to take on that person's identity. It involves stealing money, obtaining goods, or getting other benefits by pretending to be someone else. It is a crime to use another person's identity.

## How can you protect your personal information?

There are several basic steps you can take to reduce or minimize your risk of becoming a victim of identity theft or fraud:

- Protect your Social Security number (SSN), credit card and debit card numbers, personal identification numbers (PINs), passwords, and other personal information.
- Provide your SSN only when absolutely necessary. Ask to use another type of identification as an alternative.
- Create a unique Customer ID to use (instead of your SSN) when accessing account information wherever possible, including on Diversified's website.
- Protect your incoming and outgoing mail. Do not leave mail in your unlocked mail box for an extended period of time.
- Don't give out personal information over the phone, through the mail, or online unless you've initiated the contact or you are sure you know who you're dealing with.
- Destroy any materials containing your financial information before placing in the trash. Tear or shred receipts, copies of credit applications, insurance forms, checks and bank statements, expired credit cards, and credit offers.
- Keep a close watch on your bank account statements and credit card bills for any irregularities.
- Update your computer's virus protection software regularly and install any necessary security patches.
- Don't open files sent to you by strangers or click on hyperlinks in email messages (always type in the website address yourself).
- Use a firewall program, especially when using a high-speed Internet connection.
- Don't use an automatic sign-in feature that saves your user name and password. Always sign off when you're finished.
- Look for the website privacy policy and read it, such as the Internet Privacy Policy posted on Diversified website. A company's policy should answer questions about maintaining accuracy, access, security and control of personal information collected by the site. It should also answer how the information will be used and whether it will be provided to third parties. If you don't see a privacy policy, or if you can't understand it, consider not doing business with that company.
- If you need to provide your personal or financial information through an organization's website, look for an indicator that the site is secure. For example, a lock icon on the browser's status bar or a website address that begins with "https" (the "s" means it is a secure connection).

### What are the warning signs of identity theft?

Signs may include:

- Your monthly credit card and bank statements suddenly stop arriving.
- Unauthorized charges or withdrawals appear on your statements.
- You are denied credit for no apparent reason.
- You start receiving bills from companies you do not recognize.
- Collection agencies try to collect on debts that do not belong to you.
- You receive credit cards you did not apply for.
- The last sign-in date shown by a site that has your personal information is wrong.

### What can you do if you suspect identity theft?

If you suspect that your personal information has been wrongfully used:

- Put a fraud alert on your credit reports by calling one of the three credit bureaus – Equifax (888-766-0008), Experian (888-397-3742), and TransUnion (800-680-7289). An initial fraud alert stays on your credit report for at least 90 days.

- Request an updated credit report at [annualcreditreport.com](http://annualcreditreport.com) and check it for any new loans (e.g., home, car, school, etc.) taken out in your name or any new credit card accounts you didn't open. Close these accounts immediately.
- Place a credit freeze on your credit file by calling all three credit bureaus. The freeze prevents lenders from seeing your credit report unless you grant them access and can prevent others from taking out new credit in your name, even if they have your SSN and other personal information.
- File a fraud report with your local police department.
- File a complaint with the U.S. Federal Trade Commission at [ftc.gov/idtheft](http://ftc.gov/idtheft) and click on "Report ID Theft."
- Call Diversified and any other financial institutions to start the process of securing your accounts.

For more information about protecting against identity theft, visit the Federal Trade Commission's website at [ftc.gov/idtheft](http://ftc.gov/idtheft).

For information about your retirement account at Diversified, visit [divinvest.com](http://divinvest.com) or call **800-755-5801**.