Protecting yourself from ID theft and fraud

Identity theft was among the top three fraud types reported to the Federal Trade Commission.

—Consumer Sentinel Network FTC February 2021

Identity theft occurs when someone steals your personal information and pretends to be you to open bank and credit accounts, make purchases, or conduct criminal activity.

Once your information is compromised, thieves can drain your bank account, establish credit in your name, get medical treatment posing as you, or file a tax return in your name and get your refund.

In this guide, you will learn what you can do to protect yourself from identity theft—and how to respond if your identity has been stolen.

How ID theft happens

Thieves can steal your personal information and assume your identity easily by:

- Taking your credit cards, driver's license, checks, or pre-approved credit card offers from your mailbox.
- Rummaging through your garbage, the trash of businesses, or public dumps.
- Calling you for personal information to supposedly verify an account or award a prize.
- Phishing/SMiShing—sending you a bogus email or text message (SMS), asking you for personal information to make a payment, or directing you to fake websites.

Keep in mind, criminals often prey on people's fears to lure their victims into clicking on links and providing personal information.

(continued)

UnionBank®

Simple steps you can take to protect yourself

- **Shred documents** and destroy hardware (old CDs, hard drives, etc.) containing personal information, including pre-approved credit offers, old statements, cancelled checks, and ATM receipts.
- **Clean out your wallet** and store Social Security cards, unused credit cards, checks, and personal documents in a safe place.
- **Pay attention** to who may be listening when you make purchases by phone or give your Social Security number for identification.
- **Never give out personal information** like your Social Security number, account numbers, passwords, or PINs in emails, text messages, or during phone calls unless you personally initiated the contact. If you did not, visit the company website or call to verify their identity. Thieves can hack into your email contact list and pose as trusted contacts to get information.
- **Memorize your PINs** and change them regularly so you do not have to carry them in your purse or wallet.
- **Check your credit report** at least once a year to be sure it is accurate. If you find new accounts you did not open, a high number of inquiries from creditors, or negative items, take action immediately.

Important things to remember online

- **Bank online using a computer or mobile device that you know is secure** and protected with security software.
- **Ensure that your devices have software** including a firewall, spam filter, and virus, malware, and spyware detection. Make sure the security software is up to date to protect yourself from computer viruses and malware that can log your keystrokes or steal your data.
- **Be wary of WiFi hot spots** at cafés, libraries, and airports that require you to enter personal or account information.
- **Never reveal personal information on social media sites** like Facebook, LinkedIn, Twitter, or blogs. Change your privacy settings to conceal personal information, such as your date of birth.
- **Do not fall for "too good to be true" offers** that require a fee for promises of future payoffs.
- **Shop on secure websites** displaying the padlock icon, green address bar, or HTTPS on the address bar that indicate the website is secure.
- **Create strong, unique passwords** and change them if you think your accounts have been compromised. Passwords should consist of numbers, symbols, and uppercase and lowercase letters. Don't reuse passwords across accounts.
- **Monitor your bank and credit card accounts** frequently for unusual activity. Most banks and credit card issuers offer alerting services for transaction and balance thresholds, which can help you identify unauthorized activity.
- **Enable two-step verification to access your accounts**, when offered. Two-step verification provides an extra layer of protection. In addition to your regular password, you type in a numeric code to access your account. The code is sent to you via a different channel (e.g., text message, email, etc.) every time.
- **Be mindful of the latest fraudulent schemes.** Romance and IT scams are on the rise. Question any request to transfer money, make payments, verify credentials, or check on account balances even if these requests come from perceived trusted sources like a software company or someone with whom you may have initiated a personal relationship.

Review your credit report regularly

By law, you can request a free credit report annually from the three consumer credit reporting bureaus: Equifax, Experian, and TransUnion. Request all three reports for free at annualcreditreport.com. Check your report carefully for any evidence of fraud. If you find any incorrect items, contact both the credit reporting bureau and the company that sent the information.

(continued)

Recovering from identity theft

Identity theft can happen fast, so it is important to take action immediately. Here is a checklist of things to do as soon as you suspect you might be a victim:

1. Contact the credit reporting bureaus and authorities

- ☐ **Request a fraud alert** on your credit report to inform creditors that your credit history may not be accurate. Also request a statement in your file asking creditors to call you directly before opening new accounts in your name or making changes to your existing accounts.
- ☐ **Notify all three major credit bureaus** of the fraud in writing. If fraudulent new accounts were opened in your name, include copies of your FTC Identity Theft Report.
- ☐ **File a police report** detailing the theft with your local police department or in the community where the fraud occurred. Make photocopies of the report, as you may need to provide copies to help resolve your case.
- ☐ **Contact the Federal Trade Commission (FTC)** at 877-ID THEFT (877-438-4338) or online at identitytheft.gov. Based on the information you enter, IdentityTheft.gov will create an Identity Theft Report and recovery plan.
- ☐ **Alert other applicable authorities**, such as the Social Security Administration (SSA), the United States Postal Inspection Service (USPIS), or the Securities and Exchange Commission (SEC), as needed.

See the **Resources** section at the end of this guide for key contact information.

2. Notify your banks and credit card issuers immediately

- ☐ **Review all your accounts**—including checking, savings, credit cards, home equity, brokerage, and phone service—for signs of fraud.
- ☐ **Put a stop payment order on checks** that are missing or close the account and open a new one.
- ☐ **Request a "hold" on impacted accounts** or close fraudulent new accounts. Write down the names of the representatives you speak with and document calls for future reference.
- ☐ **Follow up your calls in writing,** detailing any unauthorized activity. Attach copies of your account statements with fraudulent items circled to support your claim. Send these documents via certified mail with a mailing receipt and keep copies for your records.

Receive an ID theft recovery plan and access other useful resources when you report ID theft to the FTC at identitytheft.gov.

3. Protect your credit

- ☐ **Open new accounts** to replace any accounts you had to close.
- ☐ **Change all your PINs and passwords**—even on accounts that were not impacted. Do not forget email accounts, frequent-flyer accounts, and online merchants—anywhere you use a password.
- ☐ **Continue to monitor** your bank, credit card, and brokerage accounts frequently for any new activity that may be unauthorized.

(continued)

Resources

Union Bank®

- Get the information and tools you need to protect your identity and report fraud at unionbank.com/privacy.
- Monitor your account activity by setting up Account Alerts in Online and Mobile Banking.

Federal Trade Commission

If you are a victim of identity theft, visit identitytheft.gov, the Federal Trade Commission's website, as soon as possible. This comprehensive resource center includes checklists, sample letters, and directions on how to:

- **Prevent** more damage
- **Repair** damage
- **Move forward** depending on situation

Credit bureaus

Request your credit report or report a problem:

- **Equifax**, equifax.com, 800-525-6285
- **Experian**, experian.com, 888-397-3742
- **TransUnion**, transunion.com, 800-680-7289

To request a free annual credit report, go to annualcreditreport.com.

Government agencies

Report identity theft and fraud:

- **U.S. Department of Justice**, justice.gov/criminal/fraud/websites/idtheft.html
- **Social Security Administration**, socialsecurity.gov/antifraudfacts