ID THEFT - TIPS & TOOLS

PROTECTING YOUR IDENTITY AND THE RECOVERY PROCESS

PROVIDENT Bank

myprovident.com | (800) 442-5201

Access Plus Direct Talk™ (800) 442-5201
24 Hours/7 Days A Week

Select or change your
Provident Bank Debit Card PIN (800) 567-3451
Report a lost debit card (800) 442-5201

REV 0417
©2017 Provident Bank. All Rights Reserved.

Member FDIC
Equal Housing Lender

PROVIDENT Bank

PROTECTING YOUR IDENTITY

- Do not give out personal or account information over the phone, by mail, emails or through the internet unless you initiated the contact or you are sure you know who you are dealing with.
  - If you do send your information by email or internet ensure you are sending it securely.
- Never respond to unsolicited requests for your social security number, account number, user names and passwords, or requests to verify your financial information.
- Secure your personal information at home, especially if you have roommates, utilize outside help or are having work done in your home.
- Guard your mail and trash from theft. Always shred all documents containing personal information.
- Check your bank and credit card accounts or statements regularly to ensure all charges are accurate.
- Obtain a copy of your credit report every year and check it for accuracy. You can obtain a free copy of your credit report annually from the three major credit bureaus by one of the following methods:
  - Telephone: (877) 322-8228
  - Website: www.AnnualCreditReport.com

OTHER HELPFUL TIPS

- Password-protect and encrypt your laptop, tablet, or smartphone.
- Use an Internet Security Suite and ensure it is updated automatically.
- Lock down your social media accounts, limit access to your family and friends, never say where you are currently; it's safer to post it afterwards. Also, don't post too much information about yourself, an identity thief can use this information to get into your accounts.
- Delete all emails containing sensitive data; inbox, sent items, and deleted folders.
- Mail can easily be stolen out of mailboxes. Receive all your bills and statements electronically, whenever possible.
- Use only well-known wireless networks when away from home. Fake networks can be setup anywhere to obtain your sensitive information.
- Always use strong passwords, especially for any of your bank, credit card or retail shopping sites.
- Never store your debit card PIN # with your card in your wallet or purse.
- Always use a credit card for online purchases, preferably the same one every time with a low limit.
- Never use a public computer or public Wi-Fi to do your online banking.
- On your phone or GPS, never store "home" with your actual address, use an address close by. If your car is stolen, they can use your GPS along with your garage door opener to get into your house.
- Limit what you carry. When you go out, take only the identification and cards you need.
- Take a picture of everything in your wallet and save it at home, so you know exactly what you are missing should your wallet be misplaced.

RECOVERY PROCESS – IF YOU BECOME A VICTIM

Is someone using your personal information to open new accounts, make purchases, or get a tax refund? Follow these steps to take back control of your identity:

Step 1: Notify the companies where you know fraud occurred.

- Call the fraud department. Explain that someone stole your identity.
- Ask them to close and reissue new cards / accounts or freeze the accounts so no one can initiate any new charges without your knowledge.
- Change logins, passwords and PINS for your accounts.

Step 2: Place a fraud alert and get your credit report.

- Placing a fraud alert is free and an important step in protecting your identity; it will make it harder for someone to open new accounts in your name.
- Contact one of the following three credit bureaus. The credit bureau you notify is required to notify the other two bureaus.
  - **Equifax.com/CreditReportAssistance (888) 766-0008**
  - **Experian.com/fraudalert (888) 397-3742**
  - **TransUnion.com/fraud (800) 680-7289**
- You should receive a letter from each credit bureau, confirming that they placed a fraud alert on your file.
- Obtain your free credit report immediately.
  Go to annualcreditreport.com or call (877) 322-8228.
- Review your report. Make note of any account or transaction you don't recognize. This will help you report the theft to the Federal Trade Commission and the police.

Step 3: Report identity theft to the Federal Trade Commission (FTC).

- Complete the FTC's online complaint form at ftc.gov/complaint. Give as many details as you can. The complaint form is not available on mobile devices, but you can call (877) 438-4338 to make your report.
- Be sure to print and save your FTC Identity Theft Affidavit immediately. Once you leave the page, you won't have access to your affidavit.

Step 4: File a report with your local police department.

- Go to your local police office with:
  - a copy of your FTC Identity Theft Affidavit
  - a government-issued ID with a photo
  - proof of your address (mortgage statement, rental agreement, or utilities bill)
  - any other proof you have of the theft (bills, IRS notices, etc.)
  - the FTC's Memo to Law Enforcement (available at IdentityTheft.gov)
- Inform the police someone stole your identity and you need to file a report. If they are reluctant, show them the FTC's Memo to Law Enforcement.
- Request a copy of the police report. You'll need this to complete other steps.
- Create your Identity Theft Report by combining your FTC Identity Theft Affidavit with your police report. Your identity theft report proves to businesses that someone stole your identity. It also guarantees you certain rights.
- Access **IdentityTheft.gov**. This is a federal government one-stop resource for identity theft victims. The website provides valuable tools you may need to guide you through the recovery process.