Identity Theft

What is Identity Theft?

Identity theft is the deliberate use of someone else's identity and occurs when someone uses your personal information, such as your name, Social Security number, or bank account number without your permission to commit fraud or other crimes. Some examples include the use of your name and Personal Identifying Information to open new bank accounts, establish new credit card accounts, forge checks, and even apply for loans. Some clues that could indicate your identity may have been stolen include failing to receive bills or other expected mail, receiving credit cards for which you did not apply, denial of credit for reasons that are not apparent, or receiving calls from debt collectors or companies about merchandise or services you did not purchase. While you can't entirely control whether you will become a victim, there are steps you can take to minimize your risk.

How Does Identity Theft Happen?

Identity thieves use a variety of methods to steal your Personal Identifying Information (PII), including:

- Dumpster Diving - Thieves rummage through trash looking for bills or other documents containing personal information;
- Mail Theft - Thieves dig through mail in search of bank and credit card statements, pre-approved credit card offers, tax information, and other documents that may have your personal information;
- Skimming - A credit/debit card number is stolen when processing your card using a special storage device;
- Phishing - This is a form of social engineering that often uses email to deceive you into disclosing personal information;
- Address Changes - Thieves frequently divert billing statements to another location by completing a false "change of address" form;
- Physical Theft - This is committed by stealing wallets, purses, and mail, such as pre-approved credit card offers, bank statements, or new check orders;
- Pretexting - This is a form of social engineering in which a thief lies about his identity or purpose to obtain an individual's personal information; and
- Data Breach - Steal electronic records through a data breach.

Protecting My Personal Identifying Information

Third Coast Bank SSB has procedures for protecting and monitoring our customers' accounts and personal identifying information. The following are a few tips you can use to reduce the risk of identity theft:

- Protect Your Social Security Number - Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give it out only when necessary;
- Shred Documents - Shred financial documents\information and personal information before discarding;
- Review Your Credit Report - Federal law requires the major nationwide credit reporting companies (Equifax, Experian, and TransUnion) to provide you with a free copy of your credit report every 12 months upon your request. Visit www.AnnualCreditReport.com to request your free copy;
- Never Click on Links in Unsolicited E-Mails - E-mails requesting account or personal identifying information and passwords should be deleted. These may be phishing scams;
- Protect Your Passwords - Use passwords that are hard to guess and memorize them. Avoid using predictable codes such as your birth date, mother's maiden name, or Social Security number. Do not share your passwords with anyone;
- Monitor Financial Statements - Carefully monitor bank, financial and credit card accounts regularly for unauthorized charges by checking account information through online banking. Immediately report any suspicious activity to your bank\financial institution; and
- Keep Personal Identifying Information Secure - Personal information not secured can be at risk:
    - Do not give out personal identifying information on the phone, texting, through the mail, or over the internet unless you initiated the contact and know who you are dealing with;
    - Avoid using public wireless connections, WIFI;
    - Safely store and dispose of personal identifying information; and
    - Don't "Overshare" information on social networking sites.

What Should You Do If You Are a Victim of Identity Theft?

It is recommended that you follow these steps where necessary as soon as you become aware of identity theft:

- Contact Financial Institutions - Contact Third Coast Bank SSB immediately if the fraudulent activity is related to your bank account(s). Review the activity on all your accounts, including checking and savings accounts, debit cards, loans, and other banking accounts and look for changed addresses, changed Personal Identification Numbers (PINs), or new cards ordered. Notify the fraud departments of credit card companies, as well as other banks and lenders, of the potential fraud. Close the accounts that you know or believe have been tampered with or opened fraudulently. Change your Online Banking username and password immediately;
- Contact the Police - Immediately call the local police or the police in the community where the identity theft occurred and file a report. The police can initiate an investigation and you can obtain information from the police report, which you will likely need to address credit report and account issues;
- Complete an Affidavit Form - Financial institutions and law enforcement agencies may require you to complete an "Identity Theft Victim's Complaint and Affidavit" form. The Federal Trade Commission (FTC) developed the Affidavit form for use by victims of identity theft, you can go to https://www.identitytheft.gov/ to report identity theft and get a recovery plan;
- Contact Credit Bureaus - Contact the toll-free number of any of the three consumer reporting agencies below to place a "fraud alert" on your credit report. You only need to contact one of the three agencies, because the first agency you contact will report the alert to the others;

Equifax:	1.800.525.6285	www.equifax.com
Experian:	1.888.397.3742	www.experian.com
TransUnion:	1.800.680.7289	www.transunion.com

- Request a statement be shown on the report whereby creditors contact you to verify future credit applications. Once a fraud alert is placed, you are entitled to one free copy of your credit report from each of the agencies. Review each credit report carefully once received. Look for inquiries from companies you have not contacted, accounts you did not open, and debts on your accounts that you cannot explain. Continue to check your credit reports periodically to ensure no new fraudulent activity has occurred;
- Contact the Federal Trade Commission - Report the criminal activity to the FTC by filing a complaint using the FTC's online complaint form or by calling the Identity Theft Hotline at 1-877-ID-THEFT (438-4338) and speaking with a trained identity theft counselor;
- Notify Check Verification Companies - Many retailers use major check verification companies so contact your bank and ask that your account information be reported to the Texas Closed Account Notification System (CANS). By doing so, all the major check verification entities will have access to the information and report the crime to any retailer who uses their services. To access the form which is required by your financial institution to enter the information on the database, please visit the following website - https://www.dob.texas.gov/public/uploads/files/Applications-Forms-Publications/Applications-Forms/cve_ssfininst.pdf;
- Keep Records - Document the names, phone numbers, and dates for each person you speak to regarding the incident. You can download and print a Chart Your Curse of Action form to record the steps you have taken to report the fraudulent use of your identity. Follow up on your phone calls with letters and keep copies of all correspondence; and
- Continue to Review All Accounts - Since identity theft can take time to completely resolve, carefully review all charges and transactions appearing on your account statements and online. Report any discrepancies immediately.

If you feel that you may be a victim of identity theft, please contact a bank representative as soon as possible so that we may take the proper precautions to help you.

Please note: Hyperlinks have been removed from this document. You will need to copy and paste any link into a new browser window to visit another website.