IDENTITY THEFT PROTECTION

VisionBank®
See what we can do for you.™

VISIONBANK

GREAT PEOPLE + STRONG COMMUNITIES + QUALITY SERVICE

VISION

VisionBank is committed to being the bank of choice.

In the communities we serve by being the:

BEST BANK	BEST COMPANY	BEST INVESTMENT
Customers do business with.	***Employees*** ever work for.	***Shareholders*** make.

VALUES

We are committed to delivering professional services to our customers and teammates by:

- Doing what is right, doing what we say, and doing it now.
- Creating lasting first impressions by being engaged.
- Building long lasting relationships.
- Responding to phone calls, emails, and requests the same business day.
- Making active contributions to a positive team environment and valuing your teammate's contributions.
- Realizing attitudes are contagious. Smile, have fun, work hard and celebrate.

Identity theft and fraud may not seem like a topic you would expect to happen to yourself, but it can. This booklet covers what you should do if you were ever put in that situation and how to handle it. It also highlights ways to avoid fraud and gives you the different types of identity theft used today.

Identity theft covers a range of fraudulent acts. Some common types of identity theft include credit card fraud, phone and utility fraud, insurance fraud, bank fraud, government benefits fraud, and medical fraud. An identity thief might open an account in someone's name, file taxes on their behalf to receive the refund, or use their credit card number to make online purchases.

Stolen bank account information might be used to pay utilities, phone bills, or accessories. An identity thief could also use stolen insurance information to access medical care. In very rare cases, an identity thief might use someone else's name in a criminal proceeding.

No matter the situation, identity theft can happen to anyone at anytime and it is very important to know how to handle these situations.

Visit IdentityTheft.gov to report identity theft and get a personal recovery plan. The site provides detailed advice to help you fix problems caused by identity theft, along with the ability to:

- ✓ Get a personal recovery plan that walks you through each step
- ✓ Update your plan and track your progress
- ✓ Print pre-filled letters and forms to send to credit bureaus, businesses, and debt collectors

At identityTheft.gov, there's detailed advice for tax, medical, and child identity theft – plus over thirty other types of identity theft. No matter what type of identity theft you've experienced, below tells you what to do right away.

WHAT TO DO RIGHT AWAY

STEP 1 Call the companies where you know fraud occurred.

Call the fraud department. Explain that someone stole your identity. Ask them to close or freeze the accounts. Then, no one can add new charges unless you agree.

Change logins, passwords, and PINs for your accounts.

STEP 2 Place a fraud alert and get your credit reports.

To place a free fraud alert, contact one of the three credit bureaus.

That company must tell the other two.

Experian.com/help | 888-397-3742

TransUnion.com/credit-help | 888-909-8872

Equifax.com/personal/credit-report-services | 1-800-685-1111

Get updates at IdentityTheft.gov/creditbureaucontacts.

Get your free credit reports from Equifax, Experian, and TransUnion. Go to annualcreditreport.com or call 1-877-322-8228.

Review your reports. Make note of any account or transaction you don't recognize. This will help you report the theft to the FTC and the police.

STEP 3 Report identity theft to the FTC.

Go to IdentityTheft.gov, and include as many details as possible.

Based on the information you enter, IdentityTheft.gov will create your Identity Theft Report and recovery plan.

A fraud alert lasts one year. It will make it harder for someone to open new accounts in your name.

STEP 4 Go to IdentityTheft.gov for next steps.

Your next step might be closing accounts opened in your name, or reporting fraudulent charges to your credit card company.

1 SPOT IMPOSTERS.

Scammers often pretend to be someone you trust, like a government official, a family member, a charity, or a company you do business with. Don't send money or give out personal information in response to an unexpected request – whether it comes as a text, a phone call or an email.

2 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.

3 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 to a number you know is genuine.

4 DON'T PAY UPFRONT FOR A PROMISE.

Someone might ask you to pay in advance for things like debt relief, credit and loan offers, mortgage assistance, or a job. They might even say you've won a prize, but first you have to pay taxes or fees. If you do, they will probably take the money and disappear. Learn where to get real help with these issues at consumer.ftc.gov.

5 CONSIDER HOW YOU PAY.

Credit cards have significant fraud protection built in, but some payment methods don't. Wiring money through services like Western Union or MoneyGram is risky because it's nearly impossible to get your money back. That's also true for reloadable cards (like MoneyPak or Reloadit) and gift cards (like iTunes or Google Play). Government offices and honest companies won't require you to use these payment methods.

6 TALK TO SOMEONE.

Before you give up your money or personal information, talk to someone you trust. Con artists want you to make decisions in a hurry. They might even threaten you. Slow down, check out the story, do an online search, consult an expert — or just tell a friend.

7 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.

8 BE SKEPTICAL ABOUT FREE TRIAL OFFERS.

Some companies use free trials to sign you up for products and bill you every month until you cancel. Before you agree to a free trial, research the company and read the cancellation policy. And always review your monthly statements for charges you don't recognize.

9 DON'T DEPOSIT A CHECK AND WIRE MONEY BACK.

By law, banks must make funds from deposited checks available within days, but uncovering a fake check can take weeks. If a check you deposit turns out to be a fake, you're responsible for repaying the bank.

10 SIGN UP FOR FREE SCAM ALERTS FROM THE FTC AT FTC.GOV/SCAMS.

Get the latest tips and advice about scams sent right to your inbox.

ACCOUNT TAKEOVER IDENTITY THEFT

Account takeover fraud occurs when criminals gain or have access to your bank or credit card accounts—usually because of a data breach, phishing scam, or malware attack—and start making charges to those accounts. Account takeover identity theft can happen with small businesses, commercial businesses, or even corporate account takeovers.

AUTO LEDNING FRAUD

This occurs when a consumer, a dealer or auto lender submits or accepts a fraudulent consumer application for credit. Auto dealers can be more concerned about getting customers into a vehicle versus doing a thorough identity verification process. At the same time, the borrower may be falsifying information on the loan application in order to get approved for the car. If approved and the loan goes unpaid, the lender takes a loss.

BIOMETRIC IDENTITY THEFT

Biometric ID theft is when the physical or behavioral characteristics used to verify a person's identity through a device are stolen. These characteristics are measurable, such as a fingerprint or voice recognition "Hey, Alexa", that can be copied and recorded.

BUST-OUT FRAUD

This occurs when a consumer applies for credit and uses their own name or a synthetic identity with the intent of maxing out all available credit and eventually disappearing. Lenders are left assuming all the risk as a result and bust-out fraud can happen from people using synthetic IDs or loan stacking methods.

CHILD IDENTITY THEFT

Scammers sometimes use children's Social Security numbers and other information to open new accounts, apply for government benefits, take out loans, and more. They do this because children usually don't have credit. The child may not know their credit has been used to run up debt in their name until it's time to apply for school or car loans.

CRIMINAL IDENTITY THEFT

Criminal identity theft is when a criminal gives your information to a police officer or law enforcement. This can happen when your ID is lost or stolen and in the possession of a criminal. They provide your name and information if arrested, which could show up on a background check for you or result in a warrant issued under your name.

DEBIT/CREDIT CARD FRAUD

Credit card fraud or debit card fraud is when someone uses your credit card or credit account to make a purchase you didn't authorize. Fraudsters can also steal your credit card account number, PIN and security code to make unauthorized transactions, without needing your physical credit card.

DRIVER'S LICENSE IDENTITY THEFT

Driver's license theft is the most common form of ID theft. The person who stole your ID may try to buy items under your name and get other forms of identification with their picture which can lead to criminal identity theft. You may want to consider adding an initial security alert to your credit file if your driver's license is stolen.

EMPLOYMENT IDENTITY THEFT

Employment identity theft is when a criminal applies for a job using your Social Security number or ID. Employers report income to the IRS under your name, and the government expects you to pay taxes on all income earned in your name. The best way to spot this is to review your credit report to find anything that you don't recognize.

INTERNET OF THINGS IDENTITY THEFT

Internet of Things (IoT) identity theft is when your smartphones or tablets are paired with consumer products such as cars, heart monitors and household appliances that are connected to the Internet, creating an opportunity for hackers to steal your data. Sometimes these connected products can have security flaws, creating a point of weakness around the victim's personal data that leads to the IoT fraud.

LOAN STACKING FRAUD

Loan stacking fraud occurs when multiple loans are taken out by borrowers who slide through today's automated approval process. Consumers love the ease of access to these online loans and so do fraudsters. Loopholes in online lending marketplaces can result in multiple lenders making loans to the same, fake borrowers.

MAIL IDENTITY THEFT

Mail identity theft is one of the oldest ways for a criminal to steal your personal information. If your mail has been stolen a thief may be able to retrieve your financial account information to make purchases or open up new credit cards. They could also change your address on your statements or bills.

MEDICAL IDENTITY THEFT

This happens when someone steals another person's identity to obtain medical services. As a result, no one may notice for awhile or until the victim receives a statement for care that they never received. By reading your claims received in the mail, reviewing in detail any statement of benefits, or going online to check existing claims you can monitor all medical activity done in your name.

MORTGAGE FRAUD

Mortgage fraud occurs when a borrower, broker or an appraiser lies about information on the application for a mortgage loan. They may do this in order to get approved for a bigger loan or just to get the loan approved.

NEW ACCOUNT TAKEOVER

New account takeover or new account identity theft is when a criminal creates a new account under your name using personal information they received from stealing your data, either directly or via a data breach. It is a combination of both synthetic identity theft and account takeover theft.

ONLINE SHOPPING FRAUD

Online shopping fraud or ecommerce fraud occurs when a criminal leverages stolen payment information or fraudulently acquired bank or credit card accounts to attempt retail transactions without the account owner's knowledge. The items purchased are then shipped to an address other than victim's where the stolen items are sold or shipped overseas.

SENIOR SCAMS

Senior identity theft or senior scams are very common as older Americans may not be checking their accounts or financial reports often since they're typically not opening as many new accounts or seeking new credit.

SOCIAL SECURITY NUMBER IDENTITY THEFT

Social security number (SSN) identity theft can usually happen from data breaches or Tax ID theft. If you start to notice mail that lists the wrong last four digits of your SSN or the wrong name or address this may be a sign of fraud or ID theft.

SYNTHETIC IDENTITY THEFT

Synthetic ID theft merges real and fake personal consumer data to create a new identity using information such as Social Security numbers, names, addresses, and birthdays that can be bought on the dark web. If you start to receive mail or phone calls asking about new credit accounts or get mail addressed to a different name this could be a sign of synthetic ID theft.

TAX IDENTITY THEFT

Tax identity theft happens when fraudsters have your name and Social Security number and file a tax return in your name before you file yours. In some cases, the fraudsters use fake income and withholding numbers so they can get a bigger refund check sent to their address.

AMES
515-956-4343
104 Chestnut Street
107 Main Street
4510 Mortensen Road

BOONE
515-433-4499
1704 S Marshall Street
504 Story Street

HUXLEY
515-597-4477
100 Centennial Drive

GRIMES
515-986-5746
925 SE Gateway Drive

OGDEN
515-275-2420
217 W Mulberry Street

www.VisionBank.com
800-574-8123

VisionBank®
See what we can do for you.™

Member FDIC