PINNACLE BANK

How to Protect Yourself and Your Finances from Identity Theft

Identity theft can often lead to financial loss, damage to your credit score, and legal problems.

This publication will cover steps on how to stay vigilant, preventive tactics, and, if you or someone you know has become a victim of identity theft, what actions you can take to recover.

What is Identity Theft?

Identity theft is a form of fraud that involves stolen information and/or impersonation; where the bad actor obtains your personal data, such as financial information, or identifying information (Tax ID Number, Date of Birth, and more) to pose as you and conduct fraudulent transactions.

There are several ways that bad actors can steal your identity, including in person, and digitally; examples include:

Lost or stolen belongings:

- Bank statements or tax documents that have been discarded but not destroyed properly;
- Mail;
- Personal belongings, such as driver's license, credit/debit cards or social security card.

Data Breaches, as a cause of:

- Digital laxity, such as conducting confidential transactions over public Wi-Fi;
- Digital fraud tactics, such as phishing, fraudulent email, texts, or phone calls;
- Digital footprint, including the misuse of social media, or visiting deep-fake sites and proving personal information.

Preventing Identity Theft

Keep Your Personal Information Secure

Store documents that contain identifying information, such as but not limited to, bank statements and medical records in a safe and secure area in your home. When documents are no longer needed, ensure that they are properly destroyed, such as shredding.

Try to avoid carrying your social security card or other confidential documentation, unless needed for a specific purpose.

If you store your documents electronically, ensure your anti-virus system is up to date. Take advantage of password protection options or encryption methods when storing documents digitally.

When your devices reach their end of life, ensure that they are completely wiped, before selling or donating.

Monitor Your Bank Accounts

Ensure that you are reviewing your financial activity on a regular basis. Take advantage of digital banking, including alerts to notify you of any suspicious or out of trend activity.

If you suspect any unusual or unauthorized activity, contact your bank right away to report the incident.

Collect Your Mail

Bad actors often target uncollected mail as it can contain confidential, financial, or medical information. Establish collecting your mail as part of your daily routine.

Take advantage of the additional United States Postal Service options available, such as, placing a hold on your mail when on vacation, or forwarding mail when you are moving.

You may monitor your mail by signing up for USPS' Informed Delivery service, to gather a preview of your incoming mail, and track any expected sensitive mail.

Visit USPS Informed Delivery

Take Advantage of Monitoring Services

Financial monitoring applications, such as those offered by the credit bureaus, can provide a holistic view of your financial accounts. Monitoring the status of financial accounts under your tax identification number (TIN) can help you protect yourself against identity theft, as well as reporting it and taking action before the impact of an incident escalates.

Take advantage of the available free credit reports from **AnnualCreditReport.com**. Review the reports for unknown accounts or debt, if a bad actor has used your information to open an account, **report it**.

You may request a fraud alert be placed on your credit, at no cost, by contacting one of the three credit bureaus, **click here** to learn more about the types of fraud alerts available.

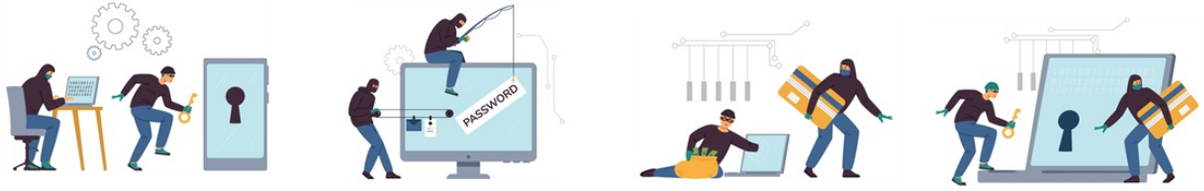
Know the Warning Signs

It is important to understand the most common warning signs to recognize an identity theft attack.

- Receiving unexpected bills, including bills for accounts that you did not apply for
- Receiving unexpected debt collection notices
- Unfamiliar credit inquiries
- Missing communication, such as mail

If you receive phone calls or emails regarding updating personal or financial information, or unpaid debt, remember to remain aware of phishing schemes, and do not provide any personal identifying-information or payment before ensuring the request is valid. Contact the requestor at a known phone number to validate the authenticity of the request.

Business Preventative Practices - Identity Theft Doesn't Only Happen To Individuals!



Employee Training

Your employees are the frontline defense of your business, ensure that employees know how to properly handle confidential data, and what protocols to follow when it comes to the destruction of sensitive documentation/information.

Employees should know what scams and fraud tactics to be vigilant of, as well as how to report suspicious activity. Educating your employees on detecting fraud attempts, such as phishing, is the first step to protect your business from encountering a malicious attack.

Access Control

It is advised that employee access is granted based on their job function. When handling sensitive tasks and information, assign dual custody or other control protocols, to maintain confidentiality and data integrity.

Have a Data Breach Response Policy

Having a data breach response policy documented allows you or your employees to take immediate action to minimize losses and maintain your business's reputation. Data breach response policies should consider various types of attacks, such as ransomware and phishing.

To mitigate a data breach, ensure that employees receive frequent training, to ensure they are aware of the most common fraud tactics, and how to report suspicious activity.

Additional Steps Based on Lost/Stolen Information

There are signs and action steps you can take, if you believe you or someone you know has become victim of a fraudulent attack. Below is a list of action steps, based on the information that has been stolen.

Social Security Number

1. Report the incident to the **Federal Trade Commission**

2. Create a my **Social Security account** to review your social security's use history, or contact your local office

3. Consider setting up an **E-Verify account** so you can lock your Social Security number and protect yourself from employment-related identity fraud

4. If applicable, learn more about the circumstances when you might be eligible for a **new Social Security number**.

5. Complete IRS Form 14039, identity theft affidavit. Submit **Form 14039 online** or mail **Form 14039**

Banking Information

1. Contact your bank to report the incident, and if applicable report any suspicious activity on your account statement(s).

2. Request to close your accounts and open a new one.

3. Update your online banking credentials.

4. Ask your bank about fraud detection or mitigation services available.

5. If you have automatic payments set up, update them with your new bank account information.

Personal Identification Documents

- Drivers License: Contact the **nearest DMV branch** to report it.
- Passport: Report a lost or stolen passport to the U.S. State Department:

  Online at **travel.state.gov**. or by telephone at 1-877-487-2778
- Medical Insurance Information: Contact your medical insurance provider using the number on your insurance statements.

Resources

(Linked)

Know Your Rights (IdentityTheft.Gov)

Know your rights when recovering from identity theft

Report It (IdentityTheft.Gov)

Report identity theft to the Federal Trade Commission

A Security Guide for Businesses

A Federal Trade Commission publication for small businesses

IRS Identity Theft Information

An IRS publication with information on tax-related identity theft

Contact us right away if there's a problem!

If you believe you are the victim of a scam, had fraudulent activity, or something just doesn't seem right - contact us immediately.

We will work with you to review your transactions and understand the extent of the issue.

Online Banking Fraud Prevention Best Practices

Navigate to our Fraud Prevention Best Practices to learn more about how to protect you and your accounts

Pinnacle Bank

(888) 485-7050

Get in Touch

PINNACLE BANK