

PUBLIC SAFETY BULLETIN: Identity Theft Protection

Safeguarding your personal and financial information requires ongoing diligence. In today's world, you cannot let your guard down. Identity thieves are constantly looking for new ways to obtain personal and financial information such as credit card or Social Security numbers. It is important to educate yourself about the risks and learn how to protect your personal data.



FULTON
INDUSTRIAL



BOULEVARD
IMPROVEMENT
DISTRICT

Take These 11 Steps to Guard Your Identity

You are unlikely to find a fail-safe way to prevent identity theft, and monitoring services only let you know after something has gone wrong. But there are 11 things you can do to make it much harder for identity thieves.

1. Freeze Your Credit

Freezing your credit with all three major credit bureaus – Equifax, Experian and TransUnion – restricts access to your records so new credit files cannot be opened. It's free to freeze your credit and to unfreeze it when you want to open an account, and it provides the best protection against an identity thief using your data to open a new account. Visit [NerdWallet](#) to learn how to freeze your credit.

2. Safeguard Your Social Security Number

Your Social Security number is the master key to your personal

data. Guard it as best you can.

When you are asked for your number, ask why it is needed and how it will be protected. Do not carry your Social Security card with you. Securely store or shred paperwork containing your Social Security number.

3. Be Alert to Phishing and Spoofing

Scammers can make phone calls appear to come from government entities or businesses, and emails that appear to be legitimate may be attempts to steal your information. Initiate a callback or return email yourself, working

from a known entity such as the official website, rather than responding to a call or email. And be wary of attachments as many contain malware. Visit [NerdWallet](#) to learn how to avoid financial scams.

4. Use Strong Passwords and Add an Authentication Step

Use a password manager to create and store complex, unique passwords for your accounts. Do not reuse passwords. Adding an authenticator app can reduce your risk. Do not rely on security questions to keep your accounts

safe; your mother's maiden name and your pet's name are not hard to find. Think carefully about what you post on social media so you do not give away key data or clues about how you answer security questions.

5. Use Alerts

Many financial institutions will text or email when transactions are made on your accounts. Sign up so that you know when and where your credit cards are used and when there are withdrawals or deposits to financial accounts and more.

6. Watch Your Mailbox

Stolen mail is one of the easiest paths to a stolen identity. Have your mail held if you are out of town. Consider a U.S. Postal Service-approved lockable mailbox. You can also sign up for Informed Delivery through the USPS, which gives you a preview of your mail so you can tell if anything is missing. Visit [USPS](https://usps.com) to enroll in Informed Delivery.

7. Shred, Shred, Shred

Any credit card, bank or investment statements that someone could fish out of your garbage should not be there in the first place. Shred junk mail, too, especially preapproved offers of credit.

8. Use a Digital Wallet

If you are paying online or in a store, use a digital wallet



which is an app containing secure, digital versions of credit and debit cards. You can use it to shop online or at a compatible checkout terminal. Transactions are tokenized and encrypted, which makes them safer. In addition, contactless transactions have fewer health risks. Visit [NerdWallet](https://nerdwallet.com) to learn about safe online shopping.

9. Protect Your Mobile Devices

Use passwords on your electronic devices. Use a banking app rather than a mobile browser for banking.

10. Check Your Credit Reports Regularly

The three major credit reporting bureaus give consumers access to free credit reports weekly, accessible by using [AnnualCreditReport.com](https://annualcreditreport.com). Check to be sure that accounts are being

reported properly and watch for signs of fraud, like accounts you do not recognize. To request your free credit reports, visit the [AnnualCreditReport.com](https://annualcreditreport.com) website. To sign up for a free credit report and score and to receive alerts when there are changes, visit the [NerdWallet](https://nerdwallet.com) website.

11. Monitor Financial and Medical Statements

Read financial statements. Make sure you recognize every transaction. Know payment due dates and call to investigate if you do not receive an expected bill. Review "explanation of benefits" statements to make sure you recognize the services provided to guard against healthcare fraud.

Remember, identity theft can happen to anyone! If you suspect you have been a victim, be sure to act quickly to minimize any damage.