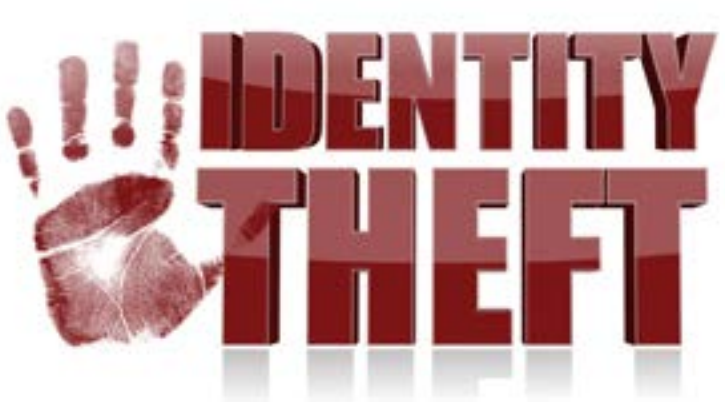
BankFirst
NATIONAL



Protecting Your Identity

Identity theft continues to be one of the fastest growing crimes in the United States. An American falls victim to identity fraud every two seconds. Bank First recommends following these tips to keep your information – and your money – safe.

- **Don't share your secrets.**
  Don't provide your Social Security number or account information to anyone who contacts you online or over the phone. Protect your PINs and passwords and do not share them with anyone. Use a combination of letters and numbers for your passwords and change them periodically. Do not reveal sensitive or personal information on social networking sites.
- **Shred sensitive papers.**
  Shred receipts, banks statements and unused credit card offers before throwing them away.
- **Keep an eye out for missing mail.**
  Fraudsters look for monthly bank or credit card statements or other mail containing your financial information. Consider enrolling in online banking and e-statements to reduce the likelihood of paper statements being stolen. Also, don't mail bills from your own mailbox with the flag up.
- **Use online banking to protect yourself.**
  Monitor your financial accounts regularly for fraudulent transactions. Sign up for text or email alerts from your bank for certain types of transactions, such as online purchases or transactions of more than $500.
- **Monitor your credit report.**
  Order a free copy of your credit report every four months from one of the three credit reporting agencies at annualcreditreport.com.
- **Protect your computer.**
  Make sure the virus protection software on your computer is active and up to date. When conducting business online, make sure your browser's padlock or key icon is active. Also look for an "s" after the "http" to be sure the website is secure.
- **Protect your mobile device.**
  Use the passcode lock on your smartphone and other devices. This will make it more difficult for thieves to access your information if your device is lost or stolen. Before you donate, sell or trade your mobile device, be sure to wipe it using specialized software or using the manufacturer's recommended technique. Some software allows you to wipe your device remotely if it is lost or stolen. Use caution when downloading apps, as they may contain malware and avoid opening links and attachments – especially for senders you don't know.
- **Report any suspected fraud to immediately to the appropriate company.**

What to do if you are a victim

- Call your bank and credit card issuers immediately so they can close your accounts.
- Contact the fraud unit of the three credit reporting agencies. Place a fraud alert on your credit report and consider placing a credit freeze so the criminal can't open new accounts. The fraud unit numbers are:

  Equifax: (800) 525-6285
  Experian: (888) 397-3742
  TransUnion: (800) 680-7289

- Report the fraud to the Federal Trade Commission at consumer.gov/idtheft or call 1-877-IDTHEFT (1-877-438-4338).
- File a police report.
- Make sure to maintain a log of all the contacts you make with authorities regarding the matter. Write down names, titles and phone numbers in case you need to re-contact them or refer to them in future correspondence.
- For more advice, visit the FTC's website at consumer.gov/idtheft

Source: American Bankers Association