Identity Theft

1ST FIRST NATIONAL BANK
AMES • ANKENY

Thieves are always designing new ways to steal personal information, but there are precautions you can take to help keep your identity secure. The following tips can help you protect yourself from Identity Theft.

Monitor Your Records

- Review your financial statements. Report unauthorized transactions promptly.
- Use online banking to monitor your account between statements.
- Know your billing cycles. Contact your financial institution if your statement is ever late.
- Obtain your FREE credit report at least annually:
  - www.annualcreditreport.com is the only official site to offer the report with no strings attached.
  - Review your credit report for unknown accounts or late payments.
  - Dispute any inaccurate information.

Protect Your Information at Home

- Keep personal information, such as financial or medical records, secure and organized. Consider using a locking file cabinet. Use an organization system that will help you detect missing documents.
- Destroy sensitive material before throwing it in the trash. Consider purchasing a personal shredder. Some thieves are willing to dig through dumpsters for identity information. In addition to personal documents, make sure unwanted credit mailings, old credit cards, and checkbooks are also destroyed.
- Ignore unsolicited phone calls asking for personal information. Scammers often impersonate businesses or fabricate other believable stories to get information from individuals. Legitimate businesses will not call you to verify personal information, but if the call claims to be a business you work with, call the business back at a verified number. Do not trust "Caller ID" information, which can be spoofed using internet devices.
- To reduce unwanted telemarketing phone calls, register your phone number on the National Do Not Call Registry at www.donotcall.gov or 888-382-1222.

Protect Your Mail

- Empty your mailbox promptly. Don't leave mail available for thieves overnight or while you're away.
- Sign up for electronic statements, to keep paper copies out of your mailbox.
- Opt out from unwanted "pre-approved" credit offers at www.optoutprescreen.com or 1-888-567-8688. Thieves could steal these offers and accept the cards on your behalf.
- Opt out from unwanted credit card checks. Contact your credit card company for details.
- If you regularly receive sensitive mail, consider opening a PO Box.

Protect Your Information When Traveling

- Keep your wallet thin. Only take information and credit cards you will need for the trip.
- Don't take your checkbook, since thieves can easily use check information for other fraudulent purposes. Use cash where possible. Only use credit or debit cards at trustworthy businesses, as cards can easily be copied for fraudulent use.
- Keep sensitive personal items (such as travel documents, credit cards, and prescription medications) secure. Consider locking these items in the hotel safe.
- Keep photocopies of important identification and travel documents, in case the originals are lost or stolen. Keep the copies separate from the originals.

Protect Your Wallet

- Only carry your Social Security card when necessary.
- If you must carry a Medicare card or other card showing your Social Security Number, carry a photocopy of the card with the SSN cut out. Only carry the original when necessary.
- Don't carry passwords or PINs.
- Sign the back of debit and credit cards. Unsigned cards may be easier for thieves to use.
- Keep a separate record of items in your wallet, along with contact information for any card issuers. This will remind you who to contact if your wallet is ever stolen.

Protect Your Computer

- Ignore unsolicited emails asking for personal information. Scammers often impersonate businesses or fabricate believable stories to get information from individuals. Legitimate businesses should not email you to verify personal information. If the email claims to be from a business you work with, call the business at a verified number.
- Be cautious when clicking links or opening attachments received in email. Scammers often disguise viruses in email attachments.
- Use strong passwords and create different passwords for different sites. Scammers are often able to crack sites with weak security and then use the passwords to access other sites.
- Use anti-virus software and keep it up to date. Out of date software may not detect new viruses.

Third Party Programs (Do Your Research):

- **Identity Theft Insurance** –Insurance terms vary, but many policies only cover costs incurred during the restoration process (phone calls, notary fees, lost wages, etc.). However, financial institutions typically reimburse for fraud losses.
- **Prevention Programs** – These are highly advertised and often expensive. However, no program can provide 100% protection. Consumers can typically achieve the same protection through free services.
- **Restoration Programs** – The biggest headache for Identity Theft victims is the time and effort spent cleaning up records. Some restoration programs counsel the customer through the process, while others will complete the work for the customer.

Other Resources:

Federal Trade Commission: 1-877-IDTHEFT (1-877-438-4338) or www.ftc.gov/bcp/edu/microsites/idtheft/

Three Major Credit Bureaus:

Equifax
Consumer Fraud Division
PO Box 740250
Atlanta, GA 30374

www.equifax.com
800-525-6285

Experian
Consumer Fraud Division
PO Box 1017
Allen, TX 75013

www.experian.com
888-397-3742

TransUnion
Fraud Victim Assistance Division
PO Box 6790
Fullerton, CA 92634

www.transunion.com
800-680-72