

Identity Theft involves criminals co-opting personally identifiable information – such as a person’s name, social security number or account number – for their own use. This is a crime which puts victims in the position of having to clear their credit reputation and credit records - in essence, to prove their innocence.

StellarOne takes every precaution to protect customer information. This includes refusing to give account information over the phone unless the customer can verify their identity.

## Consumer Tips to Avoid Becoming a Victim of Identity Theft

### Manage Your Mailbox and Internet Banking Access

- ◆ Do not leave bill payment envelopes clipped to your mailbox or inside with the flag up; criminals may steal your mail and change your address.
- ◆ Know your billing cycles and watch for any missing mail. Follow up with creditors if bills or new cards do not arrive on time. An identity thief may have filed a change of address request in your name with the creditor or the post office.
- ◆ Carefully review your monthly accounts, credit card statements and bills as soon as you receive them. If you suspect unauthorized use, contact the provider’s customer service and fraud departments immediately.
- ◆ When you order new checks, ask when you can expect delivery. If your mailbox is not secure, then ask to pick your checks up instead of having them delivered to your home.
- ◆ Although many consumers appreciate the convenience and customer service of general direct mail, some prefer not to receive offers of pre-approved financing or credit. To “opt-out” of receiving such offers, call (888) 5 OPT OUT sponsored by the credit bureaus.
- ◆ The Direct Marketing Association offers services to help reduce the number of mail and telephone solicitations. To join their mail preference service, mail your name, home address and signature to:  
Mail Preference Service  
Direct Marketing Association  
P.O. Box 9008  
Farmingdale, NY 11735-9008.
- ◆ Treat your Internet Banking password as carefully as you do your password for ATM/debit card transactions. Do not share your passwords with anyone and change your passwords on a regular basis (use 10-digit combinations of letters and numbers).
- ◆ Notify your financial institution immediately if you suspect your Internet Banking password has been compromised or lost.

### Check Your Purse or Wallet

- ◆ Never leave your purse or wallet unattended – even for a minute.
- ◆ Don’t carry your Social Security card or PINs (personal identification numbers) in your wallet.
- ◆ Carry only personal identification and credit cards you actually need. If your I.D. or credit cards are lost or stolen, notify the creditors immediately and ask the credit bureaus to place a “fraud alert” in your file.
- ◆ Keep a list of all your credit cards and bank accounts along with their account numbers, expiration dates and credit limits, as well as the telephone numbers of customer service and fraud departments. Store this list in a safe place.

### Keep Your Personal Numbers Safe and Secure

- ◆ When creating passwords and PINs do not use any part of your social security number, birth date, middle name, wife’s name, child’s name, pet’s name, mother’s maiden name, address, consecutive numbers or anything that a thief could easily deduce or discover.
- ◆ Ask businesses to substitute a secret alpha-numeric code as a password instead of your mother’s maiden name.
- ◆ Shield the keypad when using ATMs.
- ◆ If you choose to write down any passwords, keep them in a secure place and separate them from any identifying account numbers, etc.
- ◆ Get your Social Security number out of circulation and release only when necessary – for example, on tax forms and employment records, or for banking, stock and property transactions.
- ◆ Do not have your Social Security number printed on your checks, and do not allow merchants to write your Social Security number on your checks. If a business requests your Social Security number, ask to use an alternative number.

## Bank, Shop and Spend Wisely

- ♦ Don't give out personal information on the phone, through the mail, or over the Internet unless you are absolutely sure you know who you are dealing with. **EXERCISE EXTREME CAUTION.**
- ♦ Store personal information in a safe place and **SHRED** documents you don't need. Shred unused preapproved credit card offers, unused checks, charge receipts, copies of credit applications, insurance forms, statements, expired charge cards and credit offers you get in the mail. **DO NOT DISCARD IN THE TRASH.**
- ♦ Cancel your unused credit cards so that their account numbers will not appear on your credit report.
- ♦ When possible, watch your credit card as the merchant completes the transaction.
- ♦ Sign your credit cards immediately upon receipt.
- ♦ Carefully consider what information you want placed in the telephone book and ask yourself what it reveals about you.
- ♦ Ask businesses what their privacy policies are and how they will use your information: Can you choose to keep it confidential? Do they restrict access to data?
- ♦ Ask businesses: Do they keep confidential information in locked cabinets?
- ♦ Choose to do business with companies you know are reputable. **BE VERY CAREFUL ONLINE.**
- ♦ When conducting business online, use a secure browser that encrypts or scrambles purchase information and make sure your browser's padlock or key icon is active.
- ♦ Use firewalls, anti-spyware and anti-virus software. **KEEP THEM UP TO DATE.**
- ♦ Don't open email from unknown sources, never click on links sent in unsolicited emails; instead type in a web address you know.
- ♦ Log out of any Internet Banking System and close your web browser immediately upon completion of your banking business.

## Review Your Information

- ♦ Order a free copy of your credit report from the three credit reporting agencies every year and make sure all the information is correct, especially your name, address and Social Security number. Look for indications of fraud, such as unauthorized applications, unfamiliar credit accounts, credit inquiries and defaults and delinquencies that you did not cause.
- ♦ Check your Social Security Earnings and Benefits statement once a year to make sure that no one else is using your Social Security number for employment.

## Victims: Steps To Take

If you suspect misuse of your personal information to commit fraud, take action immediately. Keep a detailed chronological record of all conversations and correspondence when you take the following suggested steps:

1. Contact your bank(s) & credit card issuers immediately to ensure the following: protected access to your accounts; stop payments on missing checks; personal identification numbers (PINs) and online banking passwords changed; new accounts opened, if appropriate. Be sure to indicate to the bank or card issuer all of the accounts and/or cards potentially impacted. Customer service or fraud prevention telephone numbers can generally be found on your monthly statements. Contact the major check verification companies to request they notify retailers using their databases not to accept these stolen checks, or ask your bank to notify the check verification service with which it does business. Three of the check verification companies that accept reports of check fraud directly from consumers are: Telecheck 800.710.9898, International Check Services 800.631.9656 and Equifax 800.437.5120.
2. File a police report with your local police department. Obtain a police report number with the date, time, police department, location and police officer taking the report. The police report may initiate an investigation into the loss with the goal of identifying, arresting and prosecuting the offender and possibly recovering your lost items. The police report will be helpful when clarifying to creditors that you are a victim of identity theft.
3. Contact the three major credit bureaus and request a copy of your credit report. Review your reports to make sure additional fraudulent accounts have not been opened in your name or unauthorized changes made to your existing accounts. Check the section of your report that lists "inquiries." Request "inquiries" be removed from your report for the companies that opened the fraudulent accounts. In a few months, order new copies of your reports to verify your corrections and changes and to make sure no new fraudulent activity has occurred. Request a "fraud alert" for your file and a victim's statement asking creditors to call you before opening new accounts or changing your existing ones. This can help prevent an identity thief from opening additional accounts in your name. Here are the major credit bureaus and their phone numbers: Equifax 800.525.6285, Experian 888.397.3742 and Trans Union 800.680.7289.
4. Check your mailbox for stolen mail. Make sure no one has requested an unauthorized address change, title change, PIN change or ordered new cards or checks to be sent to another address. If a thief has stolen your mail to get credit cards, bank and credit statements, pre-screened credit offers or tax information, or if an identity thief has falsified change-of-address forms, that's a crime. Contact your local post office and police.