



Law enforcement and banks in the Willmar area have been receiving a higher-than-usual number of reports of identity theft and debit card fraud since the beginning of this year. While the source of the data being used hasn't been positively identified, some patterns have been emerging. We all need to be vigilant about preventing debit card fraud and identity theft. Here are some tips to combat having your card information stolen:

Never let your debit or credit cards leave your sight.

Many cardholders think nothing of letting wait staff in a restaurant take their card to another room for billing. Restaurants are a common location where "skimmers" will be recruited or planted by organized crime to record your card information on a small, easily-concealed electronic device carried by the skimmer. The skimmer is paid in cash or drugs, per good account, when they turn over the recording device to their "supervisor". The supervisor loads the information into a computer for later use or transmission farther up the line. The account information may be used that night or weeks later.

Guard your identity and account information with the same care you give your home and family.

- Carry only the minimum number of cards you will need.
- Keep your purse or wallet close to your body and closed - never leave it unattended unless it is in a securely locked desk, cabinet, locker, etc. Several local cases involved wallets stolen from employee break rooms or work stations, as well as those stolen from shopping carts.
- Look closely before inserting your card into an ATM or other reader. Anything which appears loose or fastened onto the card slot could indicate tampering, or that an information skimmer has been added by someone other than the merchant or bank to record your data.
- Do not let others see your PIN when you key it into a terminal. Shield the pad with your free hand or body.
- Do not give your card information over the phone unless you have placed the call expecting to be charged for a purchase. Never "confirm" your account number when called.
- Never hit "reply" if you receive an e-mail asking you to update an online account. Go to your regular account web site to confirm whether an update is needed.
- Notify your card's issuing financial institution if you will be traveling. Many card companies have tightened their fraud-detection software, and unusual activity will key an alert. If charges are made in multiple locations during one day, for things you don't normally purchase, or in a foreign nation, the company will try to contact you. If unable to reach you, they may shut your card down for their own protection – not what you want to have happen if you are really on vacation!

Check your accounts frequently. If anything appears odd, call your financial institution as soon as possible or sign up for On-line Banking and check your accounts whenever you want.

51 Main Street
PO Box 450
New London, MN 56273
320 354 2011

PO Box 62
Sunburg, MN 56289
320 366 3885

1690 1st Street South
PO Box 1740
Willmar, MN 56201
320 235 5900

www.lakeregion.com

If you are a victim, report as soon as possible.

Immediately notify the issuing financial institution to shut down your credit, debit, or checking account. You will probably need to close the account and start a new one (yes, this means changing all your auto-payments and auto-deposits). If you are contacted by your card company about possible fraudulent activity, confirm first that it is a legitimate call and not a “phishing” expedition. Then obtain as much detail as possible from the company about the activity.

You may contact law enforcement where you live or where a transaction was made. If reporting theft of an item (wallet or purse), you will need to report to the agency which has jurisdiction where the actual theft happened. When notifying law enforcement, you will be asked:

1. When the breach or transaction was made, or when the loss occurred
 2. The account number(s) and issuing financial institution(s)
 3. Where the transaction or theft was done
 4. The dollar amounts of any transactions
 5. A history of your general card use habits, and anything you noticed which might have been unusual when using it.
 6. Any contact information for those agencies you have notified of the loss.
- Identity theft can be reported to the Federal Trade Commission using their online complaint form at www.ftc.gov/idtheft or by calling 1-877-IDTHEFT (438-4338).
 - You may want to place a fraud alert on your credit files by contacting one of the three major credit reporting services: TransUnion, Equifax, or Experian.
 - Get a copy of your credit history to date. Get another one in several months.