

Protect Your Credit and Identity

Debra E. Schroeder, Extension Educator, and Rebecca L. Versch, Extension Educator

Take every step possible to protect your credit cards and all personal identity documents.

When and Where Identity Theft Occurs

Losing your credit card or your purse or billfold, whether through loss or theft, can lead to fraudulent use of not only your credit, but your identity.

Identity theft occurs when a thief steals your personal identification and uses that information to open credit card accounts, rob bank accounts, make withdrawals from ATMs and obtain employment opportunities or make down payments/deposits on a car or housing.

In addition, fraudulent use of your credit and your identity can result from someone who:

- gets your credit card information through a telephone call or an internet contact
- scavenges your credit card and personal information (like Social Security number, employee ID number, etc.) from papers in your trash
- listens to and records the credit card or other ID numbers you might say over the phone
- watches you key in your account number or Personal Identification Number (PIN) in checkout lines or at ATMs

A capable criminal needs to know only your credit numbers to fraudulently make numerous charges, including cash withdrawals, against your accounts. The following crime prevention tips will help you guard against someone illegally using your credit cards.

Protect Your Identity

Thieves can obtain your personal information by sorting through your trash and accessing public records. They may even steal from your mailbox. Take great care to protect and conceal the following information:

- name
- address

- date of birth
- Social Security number
- mother's maiden name
- credit card numbers
- driver's license number
- bank account numbers
- phone numbers

Security Precautions

- Do not carry your Social Security card, birth certificate or passport in your purse or wallet except when needed. Store these items in a safe deposit box.
- Never print your Social Security or driver's license numbers on your checks.
- You do not have to give out your Social Security and/or driver's license numbers or other personal information when asked, although a business may refuse your business if you do not furnish the requested information. If this information is requested, ask these questions before determining whether to release the information.
 - Why is the number needed?
 - How will it be used?
 - What law requires that I give you this number?
 - What will happen if I refuse to give the number?
- Lock your door *every time* you leave. Also, help protect your property by making a list of all serial numbers. File the list of serial numbers in a safe place. Landlords do not provide personal property insurance, but renters' policies are available for apartment dwellers or home renters.
- For security reasons, you should not loan your house or apartment key to others. Leave a duplicate key to your home or apartment with someone you trust, in case you are locked out or lose your key. Remember to return the key after you unlock your home. Do not leave your house or apartment unlocked just because you cannot locate the key or will be gone only a short while.

- Don't carry your credit cards and driver's license in the same carrier or wallet. If the carrier is stolen or lost, you still have some ID with you.

Protecting Your Credit Card/Debit Card

- Photocopy both the front and back of all your credit cards and keep the copies in a safe and secure location, i.e., lock boxes or a safety deposit box. This will enable you to cancel your credit card as soon as possible if it is stolen.
- Sign all credit cards as soon as they arrive.
- Do not leave credit card bills, credit card and ATM transaction receipts, store receipts or bank account statements lying out in the open where anyone can see the account numbers. Keep important papers out of sight. Pay bills before the due date and take all of the mail out of your mail box as soon as it arrives.

When disposing of any papers that might have account numbers on them, tear them up in small pieces before you put them in the trash. This includes any mailings that come indicating you have been preapproved for a credit card or offering you credit.

- Unless you are *absolutely confident* you are dealing with a reputable company, never give your credit card account number over the telephone or Internet.
- Don't be fooled by a scam where a con artist asks for your credit card number to "verify" a prize he or she says you have won.
- Never give information over the telephone to an *unknown caller*. If a caller tells you he represents your bank or financial institution, hang up. Be sure you have a *dial tone*, and call that institution to confirm that the caller is actually from your bank.
- Notify credit card companies in advance of a change in address.
- When you use a credit or debit card to make a purchase, maintain visual contact with the card. If possible, watch and make sure no extra imprints of your card are made and the transaction receipt is deposited in the cash register.
- Carry receipts in a safe place, separate from the purchase. Keep your credit/debit card receipts and check them against the monthly billing statement.
- Prepay gas pumps are another place to exercise caution. Turn your vehicle off and take the keys out, putting them in your pocket. Cover your hand when keying in account numbers and PIN numbers. Make sure to take your printed receipt and safely return your charge card to your billfold before leaving the station.

- When traveling, notify your credit card company of your travel plans, giving route, destination and timeline. Record all confirmation and cancellation numbers for reservations.

Make sure motel/hotel rooms are always locked when in and leaving the room. Use the safety latch when in the room. Deposit valuables in room or management safes. In case of an emergency evacuation, take billfold/purses with you.

When checking out of the room, turn in keys (if a key card, make sure they are cancelled out), ask the desk clerk to close your account and give you a receipt with a zero balance. Finally make sure you take with you all copies of your receipts and transactions, filing them to check against your bill.

- "Smart cards," such as prepaid phone cards and bank cards, provide protection against someone stealing your card and charging large amounts against your account. They are for a specific amount of money and when the amount is spent, no more money/credit is available. Carefully study the costs of transactions with such cards so that you get the most value for your money. Once the money on the card is spent, destroy the card if it is not renewable.

ATM Transactions

According to the Bank Administration Institute, the most dangerous hours for ATM crime are from 7 p.m. to midnight. Approximately 49 percent of the ATM-related crimes occur during these hours.

The following are ATM safety and security tips:

1. At drive-up ATMs, keep all windows closed, except the one you are using, and all vehicle doors locked. Keep the vehicle running and watch all other vehicles around you.
2. If you get out of your vehicle, lock all the doors after you exit. Keep your keys handy so you can re-enter the vehicle quickly.
3. When approaching the ATM, be alert for anything suspicious, especially two or more people in a nearby vehicle, particularly if no one else is at the ATM.
4. Never approach an ATM if the lights at the site are not working. Avoid using ATMs with obscuring bushes around them, especially at night.
5. Particularly after dark, take a companion along to the ATM and park close to the ATM in a well-lighted area.

Using the ATM:

1. When waiting in line to use the ATM, wait well behind the person or car ahead. Do not approach the ATM until he or she has completed the transaction.
2. When using the ATM and someone is closer than you would like them to be, politely ask him or her to move back a few steps. If he or she does not move, cancel your transaction immediately and wait in your locked vehicle or other safe location until that person leaves or choose another ATM.
3. Before you approach the ATM, have your card ready and know your code.
4. Familiarize yourself with the machine before using it so you can complete your transaction quickly.
5. Protect your Personal Identification Number (PIN). Memorize it. Do not write it on the card or carry it in your wallet or purse.
6. Select a PIN different from all other numbers noted in your wallet or purse, such as your address, date of birth, telephone number or Social Security number. Change your number periodically for additional security.
7. Never accept offers of assistance with the ATM from strangers. If you are having trouble, contact your financial institution.
8. When your ATM transaction is complete, immediately take your property — card, receipt, money, etc. — and put them in your pocket, wallet or purse and leave.

Never stand around and count your money. You can do that when you get to the safety of your locked car. If your transaction is not correct, you cannot discuss it with the machine anyway. Call the financial institution as soon as possible.

9. ATM robberies often occur after the patron has completed his or her transaction. Always have your head up and be aware of your surroundings when you leave the ATM. If you feel or sense someone is following you, walk or drive to the nearest business where there are a lot of people and call the police.

Make sure you carefully check your bank account and credit card statements every month. Make sure that you can identify every transaction as a transaction that you are responsible for making. If any transactions are in question, call the card issuer as soon as possible to get more details. Determine if you are responsible for the transaction, or if someone else is.

What To Do When Your Card And/Or Identity Is Stolen

If you lose or misplace or have your ATM card stolen, notify the card issuer *immediately*. If you report an ATM card missing before it is used without your permission, the Electronic Fund Transfer Act (EFTA) says the card issuer cannot hold you responsible for any unauthorized withdrawals. If unauthorized use occurs before you report it, the amount that you can be held responsible for depends on how quickly you report the loss to the card issuer.

For example, if you report the loss within two business days after you realize your card is missing, you will not be responsible for more than \$50 of unauthorized use. If you do not notify the card issuer within two business days, you could be held responsible for up to \$500 of unauthorized use. If within 60 days after your bank statement is mailed to you, you do not report an unauthorized transfer or withdrawal, you risk total loss of funds.

If you still have your card but the account number was used without your authorization, you owe nothing.

In cases involving identity theft, you must send the information in writing. Write that you are willing to cooperate to reclaim the loss. Be clear that you are not responsible for the charges in question and someone else used your card to steal. Keep copies of all your correspondence and document telephone calls you make.

Any other creditors affected by the theft of your identity should be notified immediately in writing. Contact your local police department, county sheriff or state patrol office to report the theft. The Nebraska State Patrol number is (402) 471-4545.

Immediately call the three national credit reporting organizations to place a fraud alert on your name and your Social Security number. You should follow up any verbal communications with a letter explaining your situation. The toll-free contact numbers and addresses of the major credit reporting agencies are:

Equifax, PO Box 740241, Atlanta, GA 30374-0241;
(800) 525-6285, www.equifax.com

Experian, PO Box 2002, Allen, TX 75013-0949
(888) 397-3742, www.creditexpert.com

Transunion, PO Box 2000, Chester PA 19022
(800) 916-8800, www.transunion.com

If you suspect that someone is using your Social Security number, alert the Social Security Administration office at (800) 269-0271 to that fact.

Resources

“AmEx Unveils ‘Disposable’ Credit Card Numbers,” <http://news.com.com/2100-1017-245428.html?legacy=cnet>

“Credit Card Security Precautions,” *The Complete Campus Crime Prevention Manual, Campus Crime Prevention Programs*, Goshen, K.T., 1996, p.338-343.

Federal Reserve Board, *Consumer Handbook to Credit Protection Laws: Electronic Fund Transfers*, retrieved April 2007, from <http://www.federalreserve.gov/pubs/consumerhdbk/electronic.htm>

“Identity Theft-Your Good Name Gone Bad! What is Identity Theft?,” *Call for Action*, 5272 River Road, Suite 300, Bethesda, MD. www.callforaction.org

National Security Institute, *How to be ATM "street-wise,"* retrieved April 2007, from http://www.lanl.gov/orgs/pa/newsbulletin/2004/03/10/safety_tip_atm.html

“Online Fraud: Protection Guarantee — Shop with Confidence,” http://home3.americanexpress.com/newzealand/cust_svce/onlinefg.asp

“Identity Theft,” Nebraska Department of Justice, Office of Attorney General, Consumer Protection Division, 2115 State Capitol Building Lincoln, NE. www.ago.state.ne.us

“The Librarian’s Guide To Cyberspace for Parents and Kids,” American Library Association.

“Your Money Hard Charging,” *Consumer Reports*, December, 2001, pages 58-59.

Acknowledgment

The authors would like to acknowledge the help of former UNL police officer Larry Kalkowski in the preparation of this guide.

UNL Extension publications are available online at <http://extension.unl.edu/publications>.

**Index: Financial Management
Credit and Debt**
Issued March 2008

Extension is a Division of the Institute of Agriculture and Natural Resources at the University of Nebraska–Lincoln cooperating with the Counties and the United States Department of Agriculture.

University of Nebraska–Lincoln Extension educational programs abide with the nondiscrimination policies of the University of Nebraska–Lincoln and the United States Department of Agriculture.