Protecting Your Credit Cards

- **AVOID** providing card and account information to anyone over the telephone.
- Only give your credit card account number to make a purchase or reservation you have initiated. And **NEVER GIVE THIS INFORMATION OVER A CELLULAR PHONE.**
- **NEVER** give your credit card to someone else to use on your behalf.
- **WATCH** your credit card after giving it to store clerks to protect against extra imprints being made.
- **DESTROY** any carbons. DO NOT discard into the trashcan at the purchase counter. Keep charge slips in a safe place.
- **SAVE** all receipts, and compare them to your monthly statement. **REPORT ANY DISCREPANCIES IMMEDIATELY!**
- **KEEP** a master list in a secure place at home with all account numbers and phone numbers for reporting stolen or lost cards.
- **DESTROY** solicitations for new credit cards by shredding them. Don't just throw them in the trash or recycling container. These mailings often contain pre-approval letters with your name and an account number already assigned. Thieves can easily establish credit in your name.

Lost or Stolen Cards

ALWAYS report lost or stolen cards to the issuing company **IMMEDIATELY**. This limits any unauthorized use of your card and permits the company to begin the process of issuing a new card.

Get Involved!

No one individual or agency working alone can prevent crime. It takes police and citizens working in partnership. The District of Columbia's community policing strategy provides many ways for police and communities to work together to prevent crime and build safer neighborhoods. These include regular PSA (Police Service Area) meetings in your community, problem-solving groups, citizen patrols and more. To learn more about community policing activities in your neighborhood, call your local police district:

1st District Station Desk:	698-0555	TTY: 863-4032
2nd District Station Desk:	715-7300	TTY: 364-3961
3rd District Station Desk:	673-6815	TTY: 518-0008
4th District Station Desk:	715-7400	TTY: 722-1791
5th District Station Desk:	698-0150	TTY: 727-5437
6th District Station Desk:	698-0880	TTY: 398-5397
7th District Station Desk:	698-1500	TTY: 889-3574

For more crime prevention information, or to schedule a crime prevention presentation, call the Metropolitan Police Department's Community Outreach Section at 727-0783. Or visit our Web site at: **mpdc.dc.gov**.

Information in this brochure comes from the:

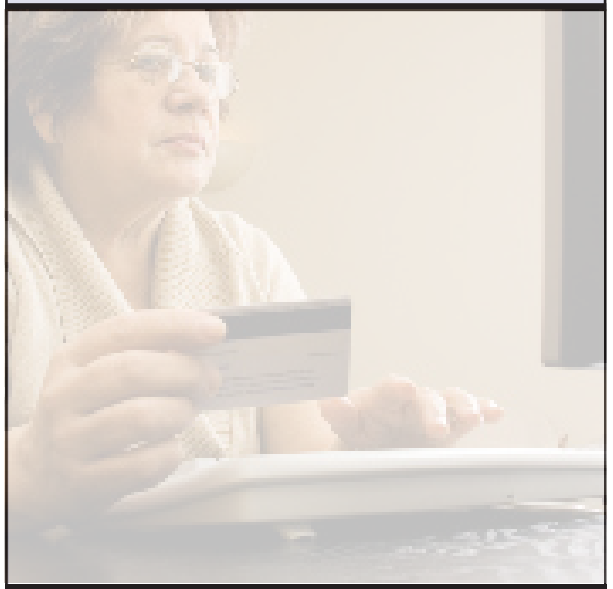
National Crime Prevention Council
1000 Connecticut Avenue, N.W.
13th Floor
Washington, D.C. 20036
Tel: 202-466-6272
Fax: 202-296-1356
www.ncpc.org

NATIONAL CRIME PREVENTION COUNCIL

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Metropolitan Police Department
300 Indiana Avenue, NW
Washington, DC 20001

Revised May 2007

Protecting Your Private Information



FOR YOUR SAFETY

Information on Protecting Your Identity and Credit Card Information from Thieves and Scam Artists

METROPOLITAN POLICE WASHINGTON D.C.

Don't share your credit with thieves.

Take precautions when conducting your business online, using electronic tellers, or paying with credit cards at merchants.

As our lives become more integrated with technology, keeping our private information confidential becomes more and more difficult. Electronic transactions can leave you vulnerable to fraud and other crimes.

What About Those Passwords?

Whether on the Internet or using an online banking program, you are often required to use a password. The WORST ones to use are the ones that you think of first—your own or your spouse's name, maiden name, pets' and children's names, etc. The BEST passwords mix numbers with upper and lowercase letters. A password not found in the dictionary is even better. There are programs that will try every word in the dictionary in an effort to crack your security. Avoid breaks in your security by doing the following:

- Change your password regularly.
- Memorize your password. If you have several, develop a system for remembering them. If you do write down the password, keep it at home or hidden at work. Don't write your password on a post-it note and stick it on your monitor or hard drive.
- Set up a special account or set aside a different computer at work for temporary help and other unauthorized users.
- If you have the option of letting your computer or a web site remember a password for you, DON'T USE IT! Anyone who uses your machine will have automatic access to information that is password protected.

Using ATMs and Long Distance Phone Cards

It is extremely important for you to protect your Personal Identification Number (PIN). A PIN is a confidential code that is issued to the cardholder to permit access to that account. Your PIN should be memorized, secured and not given out to anyone—even family members or bank employees. The fewer people who have access to your PIN, the better.

- **NEVER** write your PIN on ATM or long-distance calling cards.
- **DON'T** write your PIN on a piece of paper and place it in your wallet. If your wallet and card are lost or stolen, someone will have everything they need to remove funds from your account, make unauthorized debit purchases, or run up your long-distance phone bill.
- **BE SURE** to take your ATM receipt to record transactions and match them against monthly statements. Dishonest people can use your receipt to get your account number.
- **NEVER** leave the ATM receipt at the site.

When You Shop in Cyberspace

You can prevent problems **BEFORE** they occur by:

- Doing business with companies you know and trust. If you haven't heard of the company, research it or ask for a paper catalog before you decide to order electronically. Check with your state consumer protection agency on whether the company is licensed or registered. Fraudulent companies can appear and disappear very quickly in cyberspace.
- Check to see if your computer connection is secure. In Internet Explorer, for example, you should see a small yellow lock in the lower right corner of the screen. In Netscape, a secure connection is shown by a small lock highlighted in yellow in the lower left corner of the screen.
- Using a secure internet browser that will encrypt or scramble purchase information. If there is no encryption software, consider calling the company's 800 number, faxing your order, or paying with a check.
- Never give a bank account or credit card number or other personal information such as your Social Security number and date of birth to anyone you don't know or haven't checked out. And DON'T provide information that is unnecessary to make a purchase. Even with partial information, con artists can make unauthorized charges or take money from your account. If you have an even choice between using your credit card and mailing cash, check or money order, use a credit card. You can always dispute fraudulent credit card charges, but you can't get cash back.