

CONSUMER ACTION

www.consumer-action.org

221 Main Street, Suite 480
San Francisco, CA 94105
415-777-9635
TTY: 415-777-9456

523 W. Sixth Street, Suite 1105
Los Angeles, CA 90014
213-624-8327

PO Box 70037
Washington, DC 20024
202-544-3088

hotline@consumer-action.org

Chinese, English and Spanish spoken

Consumer Action created this publication
in partnership with WaMu.



© Consumer Action 2007

TRAINING MANUAL

QUESTIONS AND ANSWERS



ABOUT CREDIT CARD FRAUD

A Consumer Action Publication

Table of contents

1

CREDIT CARD FRAUD

3

IDENTITY THEFT

4

SKIMMING, PHISHING & ONLINE FRAUD

7

PROTECTING YOURSELF

12

YOUR BILLING STATEMENT

15

REPORTING CREDIT CARD FRAUD

18

WHEN FRAUD STRIKES

19

HELPFUL RESOURCES



CREDIT CARD FRAUD

How does credit card fraud occur?

Credit card fraud happens when consumers give their credit card number to unfamiliar individuals, when cards are lost or stolen, when mail is diverted from the intended recipient and taken by criminals, or when employees of a business copy the cards or card numbers of a cardholder.

What is an unauthorized charge on my credit card?

An unauthorized charge is a purchase on your credit card that you did not make or permit anyone else to make. When your card is lost or stolen, the person who finds it or steals it may use it to make purchases. Criminals can use the card by forging your name, or order goods and services by phone or on the Internet.

For more information about free educational publications from Consumer Action, visit www.consumer-action.org.

My brother stole my credit card and personal identification number (PIN) and took out a cash advance using the card. Can I still dispute the transaction?

Yes, if you did not allow your brother to use your card. You may have to sign a sworn statement that your brother took the card and PIN without your permission.

What is a counterfeit credit card?

Counterfeit credit cards are fakes that have real account information stolen from victims. Often, the victims still have their real cards, so they don't know a crime has occurred. The cards appear legitimate, with issuers' logos and encoded magnetic strips. Criminals use stolen account information to create counterfeit cards or to charge items over the phone or the Internet. Counterfeit cards often are used just a few times and abandoned before the victim becomes aware and reports their misuse.

IDENTITY THEFT

What is identity theft?

Identity theft, or ID theft, is the fraudulent use of an individual's personal information—such as Social Security number or date of birth—to commit financial fraud.

What happens to victims of identity theft?

Identity thieves harm and inconvenience victims by using their names and other personal information to open new credit accounts or access existing credit and bank accounts, and by placing fraudulent charges on these accounts. Victims of identity theft have to dispute these charges as fraudulent, and locate and close down all bogus accounts opened in their names.

Are victims of ID theft held liable for the losses?

No. But while victims of identity theft are not held liable for the losses, it may take years for victims to clean up the financial and credit problems caused by the crime.

SKIMMING, PHISHING & ONLINE FRAUD

What is credit card “skimming”?

Credit card skimming refers to thieves making an illegal copy of a credit card or a bank card using a device that reads and duplicates the information from the original card. Dishonest business employees use small machines called “skimmers” to read numbers and other information from credit cards and capture and resell it to criminals, who create counterfeit cards or charge items over the phone or the Internet.

What is “phishing”?

Phishing is a crime that starts with deceptive e-mails being sent to consumers. These messages are made to look as if they come from the person’s bank, in an effort to get the intended victim to reveal personal information, such as bank account numbers and online passwords. Phishing has become a widespread practice of criminals, who have succeeded in stealing personal information from many people. The crime succeeds because the e-mails look legitimate, with realistic bank logos and web site addresses (URLs) that are very similar to the bank URLs.

What could happen if I respond to a phishing e-mail?

Account holders who respond to such e-mail messages are directed to a fake web site where they are asked to type in account numbers, passwords and other personal banking or credit card information. Then, in a matter of hours, the criminals can drain your bank accounts, using your passwords to authorize the electronic transfer of funds to accounts they control.

How can I tell the difference between a scammer’s e-mail and a legitimate attempt by my bank to contact me?

Banks don’t use e-mail communications to ask for personal information because e-mail is not secure. Hit the delete button and never respond to such an e-mail. Don’t respond to e-mails—or phone calls—asking you to provide your credit card numbers, Social Security number or your mother’s maiden name. Even when you have a legitimate request, banks ask that you never send detailed account information in an e-mail. This is because criminals might intercept your e-mails. When you wish to address an issue that requires personal account information, visit your bank in person, use its secure web site, place a phone call or write a letter.

How can I protect the bank and credit card accounts I access online?

Change your user name and password several times per year. Never use variations of your name, children’s names, birth date, address, etc., that might be guessed by criminals. Examine your bank’s web site home page and log-in screens carefully. If the look of the site changes, contact the bank by phone before logging in to ask if they have made site changes and to let them know you have concerns.

What is a credit card “security code” and what purpose does it serve?

Many credit cards have a special numerical code used by many merchants to verify that the card is in your possession when you make purchases by phone or on the Internet. These 3- or 4-digit numbers are found at the top right corner of the

card or on the back, following the credit card number, near the space where you sign the card. If your card number and expiration date were stolen, but not the card itself, the thief would not have access to this security code.

What should I do when I receive a new credit card?

As a protection, most card issuers now suggest that you call from your home phone to activate a new card before you use it. Sign the back of the card as soon as you receive it. Some people suggest writing “ask for ID” in the signature space. This is not a good idea. Many credit card issuers have advised merchants not to let purchases go through if the cardholder hasn’t signed the card.

PROTECTING YOURSELF

How can I prepare myself in case my card is lost or stolen?

Record all your account numbers and company contact information and keep this list in a safe and secure place. Do not keep it in your wallet or purse.

How can I protect myself against unauthorized charges?

Keep copies of your vouchers and ATM receipts, so that you can check them against your billing statements. Notify your card issuer immediately if you suspect unauthorized use or fraudulent use of your card.

How can I avoid becoming a victim of credit card fraud?

It might not be possible to guarantee that you won’t become a victim of fraud, but you can take these steps to cut down on your chances:

- Safeguard your wallet or purse at all times.
- Never leave your purse or wallet unattended in public.
- Never carry all your cards—only the one or two that you might need.
- Carry your credit cards separately from your wallet in a credit card case or in another compartment in your purse.
- If your credit card is lost or stolen, call your credit card issuers immediately.

What is mail fraud and how can I avoid it?

Mail fraud is the illegal use of the postal service to commit a crime, such as the theft of mail. To avoid mail fraud:

- Notify the post office immediately if you change your address.

- Make sure your mailbox is secure and always locked. Never leave outgoing bill payments in your mailbox or apartment building lobby. Instead drop them off at the post office or postal service mailboxes.
- Call your credit card and banking companies to change your billing address when you move.
- Always put your return address on the envelope.
- Shred before discarding all unwanted credit card solicitations.
- Be aware of when your credit card and other bills are due to arrive each month, and call the companies if you fail to receive them.

What is “zero liability” on a credit card?

Credit card payments processed by Visa, MasterCard, American Express and Discover are subject to a “zero liability” policy—a guarantee that you will not be held responsible for any fraudulent charges.



What are some ways I can protect my credit card when I use it online?

Payment card networks, such as Visa, MasterCard and American Express, offer services to help you avoid fraud, such as special verification passwords. Make sure you are using a secure merchant site by dealing only with well-known reputable stores and checking that your browser is in the

secure mode before making a purchase. (Look for a padlock or other security symbol in the lower right corner of your browser window.) Avoid websites that offer “free access” if you provide your credit card number. If you give them the number, your card is likely to be charged by the company you give it to, and maybe by companies unknown to you as well.

I bank online—is there anything I can do to protect my personal information?

If you bank online, don’t use your Internet browser to automatically fill in your user name and password when you log in to bank or credit card sites, or to any merchant site that keeps your card number on file. Anyone using your computer would be able to sign on automatically and access your accounts. You can deactivate this function in your Internet browser’s “preferences” menu under “security.”

How can I make sure that my personal identification number (PIN) is safe?

With your PIN number and your card, a thief can make cash advance withdrawals from your account at an ATM machine. Keep your PIN secure by following these tips:

- Never write down your PIN—memorize it.
- Never give your PIN to anyone.
- Don’t write your PIN number on your credit card.
- Don’t write your credit card number on a post card or on the outside of an envelope you are going to mail.
- Don’t keep your PIN number in the same place as your credit card or ATM card.

How can I protect my credit cards?

Never provide your credit card number or other personal information on the phone, unless you are able to verify that you are speaking with your financial institution or a merchant you trust. When you lend your card, you are responsible for all charges. You will not be protected against unauthorized use if someone to whom you knowingly and willingly gave the card, including family and friends, makes the charges. Don't give your account number to anyone who calls you on the phone.

How can I protect myself from credit card skimming or any other attempt to steal my credit card number?

Watch closely as store and restaurant employees handle your card to make sure they are not copying or skimming your credit card number. The devices used for skimming are sometimes disguised as cell phones. After you make a purchase and your card is handed back to you, make sure it is your card and not a dummy card or another person's card.

I plan to take a trip and to use my credit card while I am away. Should I notify my credit card company?

If you are going to be traveling and plan to use your card away from home, notify your credit card company. This may prevent your account from being flagged for possible fraud and any inconvenience you might suffer if your issuer blocks your account.

We are going to renovate our bathroom and pay for the materials with our credit card. Should we let our credit card company know about our plans?

If you are going to make any unusually large purchases, notify your card company so that your account is not flagged for possible fraud. For instance, if you are renovating your home and plan to purchase materials, fixtures or appliances, let your issuer know in advance.

Why should I care about fraud when my credit card company has to pay for it, not me?

Consumers are not financially responsible for unauthorized charges if they behave responsibly and report lost or stolen cards, but credit card companies experience losses of close to \$50 billion dollars per year because of credit card fraud. These costs "trickle down" in the form of higher interest rates and fees that are paid for by all consumers.

What are credit card companies doing to fight fraud?

Most credit card companies have developed the technology to help identify fraudulent activity and they will act quickly to stop misuse once they discover it. Your card company may contact you because it notices an especially large purchase or a charge made in a town that is not near your home or in another country. Occasionally, your card may be blocked or suspended until you call the company back. To avoid any inconvenience, notify your card company if you plan to be out of town or to make any large purchases.

YOUR BILLING STATEMENT

Is there any way that I can monitor my credit card between statements?

Yes. If you have Internet access, consider enrolling at the bank's web site so you can access your credit card account online. You can monitor your account online for unauthorized charges between statements.

Why is it important to review my credit card statement when it arrives?

To protect yourself against unauthorized credit card charges, report fraud as soon as you become aware of it. Review credit card statements the day you receive them and report any questionable charges to your card issuer immediately.

What should I do if my credit card statement does not arrive?

If one of your credit card bills is late, call the card issuer right away. A missing statement may indicate that your statement has been stolen. Call your issuer if you don't receive your statement at the usual time. (You are responsible for paying your bills on time even when you didn't receive the statement.)

What should I do with old statements after I have paid them?

Store old statements and receipts in a secure place and shred them before you discard them.

What will happen if I move and forget to change my mailing address with my credit card company?

If you don't update your address, you may not receive the billing statement in time to avoid a late payment charge. Make sure to update your records with your credit card company when you move. Many merchants verify your address and ZIP code to make sure they match the bank's records.

I got a phone call from someone selling "credit card loss protection insurance." Is this a good thing to buy?

No. Be wary of credit card protection offers. This type of insurance is unnecessary because federal law limits your credit card fraud liability. But scam artists try to sell \$200-\$300 credit card insurance by falsely claiming that cardholders face significant financial risk if their cards are misused. According to recent Federal Trade Commission estimates, 3.3 million consumers have purchased unnecessary insurance to prevent unauthorized use of their credit cards. To make sure you are fully protected against unauthorized use, report missing cards right away, before they are used. This way you are not responsible for any fraudulent charges. If a thief uses your card before you report it missing, the most you will owe under federal law for unauthorized charges is \$50. If your card has a zero liability policy, you will owe nothing.

Should I pay for a service that will notify all my card issuers if my cards are lost or stolen?

Save money by doing it yourself. Keep credit card account numbers and toll-free numbers in a separate place from your credit cards so that you can easily find the information when you need it.

REPORTING CREDIT CARD FRAUD

What should I do when my card is lost or stolen?

If you lose your credit cards or realize that they have been lost or stolen, call the issuers immediately. Most credit card companies have 24-hour customer service lines to deal with emergencies. Ask your issuer if it recommends that you follow up with a letter, and if so, ask what information you need to include in the letter. Report the loss of your card as soon you can. If someone has used your card without your permission, your maximum liability under federal law is \$50 per card.

What law protects my credit history from being damaged if I am a victim of identity theft or credit card fraud?

The federal Fair Credit Reporting Act (FCRA) gives you the right to get a free credit report if you are the victim of identify theft. It also gives you the right to place a fraud alert in your file. Many states have their own consumer reporting laws that may give you additional rights. Contact your state or local consumer protection agency or your state attorney general for more information. You can find these agencies in the government pages of the phone book.

What law protects me from unauthorized charges made by a credit card thief?

Regulation Z, which implements the Fair Credit Billing Act and the Truth in Lending Act, protects you against unauthorized purchases. To be fully protected, report the problem to the credit card issuer, preferably in writing.

Include your name and account number and an explanation of why you believe the charge is incorrect. Include a copy of your billing statement with the questionable charge highlighted. Send your letter to the address designated by the creditor for handling billing errors or claims of unauthorized use. Do not send it in the same envelope with your payment. You must pay the portion of your bill that is not in dispute.

What is a credit card “billing error”?

Under federal law, a billing error is defined as:

- A credit card charge for something you did not agree to buy.
- A purchase made by a person who is not authorized to use your account.
- A charge that is not properly identified, that is for a different amount than the actual purchase, or that was charged more than once.
- A charge for something that was not delivered or not accepted by you when delivered.
- A mathematical error on your billing statement.
- A failure to properly credit a payment or other credit to your account.
- A failure to mail the bill to your current address, provided you told the creditor about any address change at least 20 days before the end of the billing period.
- Any charge which you cannot identify without more information.

What is my liability for charges made without my permission by someone who found or stole my credit card?

You’ll owe nothing if you report the lost card before unauthorized charges are made. When unauthorized purchases or cash advances were made, federal law restricts your liability to \$50 per card. However, if your card has a “zero liability” policy, you will not be liable for fraudulent charges.

When I checked my account online, I saw a charge I didn’t make on my credit card. What should I do?

With online access, you can monitor posted transactions on a daily basis. This can help you monitor your account for fraud. If you look at your account online and see a charge that you didn’t make, contact your credit card company immediately. Notify the company even if the card is still in your possession. You may be told that you must wait because you can’t dispute “unbilled activity” until it shows up on a monthly statement. Tell the company that this is more than just a dispute—you suspect fraud.

WHEN FRAUD STRIKES

I looked for my credit card and found it was missing.

What should I do?

Call the card issuer immediately if your card is lost or stolen. Follow up your phone call with a letter to the card issuer. The letter should contain your card number, the date the card was discovered missing, and the date you reported the loss. Once you report the lost card, you are not responsible for any unauthorized charges.

A credit card that I don't use very often was stolen. I don't know when it was taken, but when I contacted the bank, it said that charges had been made on the card recently.

Will I have to pay for the unauthorized charges?

When you are late in reporting a lost or stolen credit card, or do not become aware of unauthorized use until you receive a billing statement, your liability is limited to \$50 per card by federal law. Federal law allows the issuer to ask you to pay up to \$50. However, many card issuers have "zero liability" policies—this means that cardholders aren't liable for unauthorized charges.

What is a fraud affidavit?

If you report that a charge is fraudulent, you may be asked by your card issuer to sign an affidavit that you did not make the purchases in question. An affidavit is a written statement you sign under oath, swearing that the contents are true to the best of your knowledge. Sign, date and return the fraud affidavit promptly.

HELPFUL RESOURCES

How can I get a free annual copy of my credit report?

A new law has given consumers the right to request a free copy of their credit report from each of the three major national credit reporting agencies. You can get your free credit reports on the Internet at www.annualcreditreport.com. To request your free reports by phone, call 877-322-8228. Your reports will be mailed to you.

Can I request my free credit reports by mail?

Yes, but you must use a special form that you can download from the site mentioned above. Mail the completed form to:

Annual Credit Report
Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

Why should I check my credit report?

Checking your credit report at least once a year may help prevent identity theft and gives you a chance to make sure that all items and credit accounts listed in the report are accurate.



What is “Verified by Visa”?

When you enroll in the “Verified by Visa” program you can protect your Visa card online with a personal password. Visit the Visa web site (www.visa.com) for more information.

Which federal agencies can help me with credit card fraud?

The Federal Trade Commission (FTC) (www.ftc.gov/ftc/consumer.htm) offers free publications on credit cards, billing rights and how to avoid credit card fraud.

The federal agencies that regulate banks are also responsible for helping consumers deal with bank and credit card fraud.

Different agencies regulate different types of banks:

- National banks (the word “National” or the initials N.A. appear in or after the bank’s name) and federal branches of foreign banks are regulated by the Office of the Comptroller of the Currency (OCC), Customer Assistance Group, 1301 McKinney Street, Suite 3450, Houston, TX 77010; fax: 713-336-4301. (Your letter or fax should provide the bank’s full name and address.)
- Federal Reserve System member banks are regulated by the Federal Reserve Board, Division of Consumer & Community Affairs, Washington, DC 20551; 202-452-3693; www.federalreserve.gov.
- Savings associations and federally chartered savings banks whose names have the word “Federal” or the initials F.S.B. are regulated by the Office of Thrift Supervision, Consumer Complaints, Washington, DC 20552; 800-842-6929; www.ots.treas.gov.

- Federal credit unions are regulated by the National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314; 703-519-4600. www.ncua.gov.

- State-chartered banks that are not members of the Federal Reserve System are regulated by the Federal Deposit Insurance Corporation, Consumer Response Center, 2345 Grand Ave., Suite 100 Kansas City, MO 64108; 877-275-3342; www.fdic.gov.

As a credit card fraud victim, how can I protect my credit?

By monitoring your credit report on a regular basis, you can check for fraudulent accounts and inaccurate information. (See page 19.) As a credit card fraud victim, you have the option to place a fraud alert on your credit report. Fraud alerts will ensure that creditors contact you before any new accounts are opened in your name or when changes are made to your existing accounts.

Contact the fraud departments at any of the three major credit bureaus to place a fraud alert on your credit file:

- Equifax: www.equifax.com; 800-525-6285
- Experian: www.experian.com; 888-397-3742
- TransUnion: www.transunion.com; 800-680-7289

The credit bureau you contact will place alerts with the other two bureaus. After placing an alert, you are entitled to ask for a free copy of your credit report from all three major credit bureaus.