Credit card fraud can occur 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 the company's customers. Then,

- Unauthorized charges are made to the victim's credit card.

- Counterfeit cards are made with the victim's account number.

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

- Identity thieves can harm and inconvenience victims by using their names and other personal information to commit crimes, open new credit accounts and access existing credit and bank accounts.

- While victims of identity theft are not held liable for the crimes, it takes a lot of work by victims to prove fraud and clean up the financial chaos caused by the crimes.

Skimming is 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.

- Criminals use the information to create counterfeit cards or to charge items over the phone or the Internet.

Phishing is sending massive numbers of phony e-mails to consumers, pretending that the messages come from the person's bank, in an effort to get the intended victim to reveal personal information, such as bank account numbers.

- Phishing has become a widespread practice of criminals, who have succeeded in stealing personal information via e-mail from many people. The crime succeeds because the e-mails look legitimate, with realistic bank logos and web site addresses, or URLs, that are very close to the real thing.

- When account holders respond, they 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 drain the victims' bank accounts, using the passwords to authorize the electronic transfer of funds to other accounts.

- Banks never ask for personal information in this way. 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, because e-mails are not secure and the information may be intercepted by criminals. Instead, visit in person, use the bank's secure web site, call on the phone or write a letter when you are attempting to settle a dispute with a merchant or your bank.

Security codes are three- or four-digit numbers found on the back of credit cards that are used by some merchants to verify that the card is in your possession when you make purchases by phone or on the Internet.

- The numbers are found at the top right corner of the card on Visa and MasterCard credit cards, or on the back, following the printed 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 the security code required by many merchants when you make online purchases.

New cards

- 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 with a permanent black ink pen as soon as you receive it.

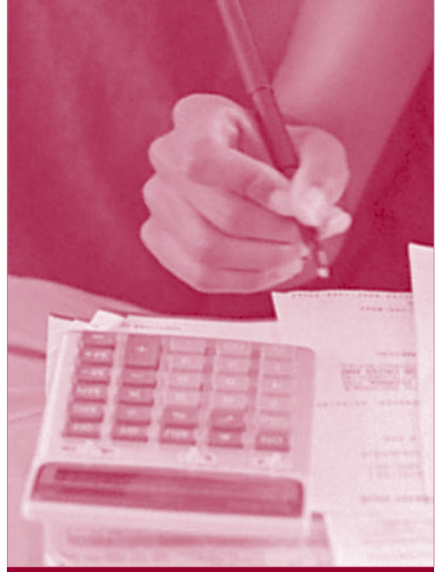
- Some people suggest writing "ask for ID" in the signature space. This is not a good idea. Consider signing your cards instead of writing "ask for ID." Many credit card issuers have advised merchants not to let purchases go through if the card isn't signed.

- Record all your account numbers and company contact information and keep the record in a safe, secure place.

- Keep copies of your vouchers and ATM receipts, so that you can check them against your billing statements.

Protect your wallet or purse

- Keep a close eye on your belongings.



When fraud strikes

- 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 missing, and the date you reported the loss.

- Once you report the lost card, you are not responsible for any unauthorized charges.

- Even if you are late in reporting the loss, or were not aware of the unauthorized use until your next statement arrives, your liability is limited to $50 per card by federal law. However, you may lose your protections under the law if you negligently fail to report the loss of the card or the unauthorized charges on your statement in a timely manner.

- When you report credit card fraud to your issuer, you will be sent a fraud affidavit for you to fill out, sign and return.

- Return the fraud affidavit promptly.

- Never carry all your cards – only bring 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 wallet or purse is stolen, call your credit card issuers immediately.

Avoid mail fraud

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

- Make sure your mailbox is secure and always locked. Never leave your outgoing bill payments in an unlocked mail box or apartment building lobby.

- Call your credit card and banking companies to change your billing address when you move.

- Always put your complete return address on the envelope.

- Shred all your unwanted credit card solicitations before you discard them.

- Know when your credit card and other bills are due to arrive, and call the companies if you fail to receive them.

Internet safeguards

- If you bank online, don't use "automatic sign on" for bank or credit card sites.

- Some websites offer "free access" if you provide your credit card number. Stay away—it is likely that your card will be charged by the company you give it to, and maybe even by companies you have never heard of.

Protect your information

- Never write down your personal identification number (PIN)—memorize it.

- Never give your PIN to anyone.

- Don't write your PIN number on your card.

- Don't write your credit card account number on a post card or on the outside of an envelope you are going to deposit in the mail.

- Don't keep your PIN number in the same place as your credit card or ATM card.

- 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 trusted financial institution or a reputable merchant.

- Don't lend your card to anyone, because you are responsible for all charges. You will not be protected against unauthorized use if the charges are made by someone to whom you knowingly and willingly gave the card, including family and friends.

- Don't give your account number to anyone who calls you on the phone or sends you an e-mail.

Using your card

- 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 to look like cell phones.

- After you make a purchase and your card is handed back to you, make sure it is your card.

- 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 blocked your account because you were using it in new places.

- 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.

Your credit card company

- Consumers are not financially responsible for unauthorized charges (if they behave responsibly and report lost or stolen cards), but credit card companies report losses of close to $50 billion dollars per year because of credit card fraud.

- Most credit card companies have developed technology tools to help identify fraudulent activity and 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 or country that is not near your home. Occasionally, your card may be blocked or suspended until you call the company back. This is done to protect you and the issuer.

- 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.

- 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

- Review credit card statements closely on the day they arrive.

- If you have Internet access, consider using a credit card issued by a bank that allows you to access your account online. You can monitor your account online for unauthorized charges between statements.

- Report any questionable charges to your card issuer immediately.

- 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 even when you didn't receive the statement.)

- Store old statements and receipts in a secure place and shred them in a shredder or tear them up before you discard them.

Reporting credit card fraud

- The Fair Credit Billing Act is a federal law that gives you the right to resolve credit card billing errors, including unauthorized charges.

- When you purchase goods or services using a credit card and something goes wrong with the purchase, you have the right to dispute the charge and ask for a "chargeback" — a refund from your credit card company.

- To dispute charges on your statement, contact your card issuer within 60 days of the statement date or you lose your right to do so.

- You cannot dispute a transaction that has not been posted to your account, but with online access you can monitor posted transactions on a daily basis and be more in control of your account.

- Always dispute charges in writing. You can call your card company and follow up with a letter. In some cases, the card company will send you a form to fill out about your dispute. Include a full description of the disputed item—including the merchant's name, transaction date, amount of the charge and the posting date. Describe the reason for the dispute in a few sentences. Make sure you send your letter and the form, if required, to the correct address for billing disputes.

- Do not include your dispute letter with your bill payment.

Helpful resources

Free credit reports

www.annualcreditreport.com

Checking your credit report at least once a year can help prevent identity theft. You have the right to get one free copy of your credit report every year from each of the three major credit reporting companies, Equifax, Experian and Trans Union. Get free credit reports online or, to request your free reports by phone, call 877-322-8228. Your reports will be mailed to you.

You can request your free credit report by mail, too. Download an order form online at www.annualcreditreport.com. Mail the completed form to:

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

Visa

http://usa.visa.com/personal

If you have a card with a Visa logo on it, these free protections apply to your card:

- Verified by Visa. Visa allows you to create a personal password to use when you provide your Visa credit card number on the Internet. The password program assures safer online shopping. (Don't share your password with anyone else.)

- Visa's "zero liability policy" covers all Visa credit and debit card transactions processed over the Visa network. The only transactions not covered under the policy are ATM and point-of-sale transactions in which you use your personal identification number and transactions that are not carried over Visa's networks. *(Cards bearing a MasterCard logo also have zero liability coverage similar to Visa's. Visit the MasterCard web site at www.mastercard.com for more information.)*

Federal Trade Commission (FTC)

www.ftc.gov/bcp/consumer.shtm; 877-FTC-HELP

The FTC offers free publications on credit cards, billing rights and how to avoid credit card fraud.

The National Fraud Information Center

www.fraud.org

The National Fraud Information Center, a project of the National Consumers League, offers advice and prevention tips to help you avoid becoming a victim of fraud.

State Attorney General's Office

To find your state office, check the phone directory or visit the National Association of Attorneys General web site (www.naag.org) for a free look-up.

Consumer Action
www.consumer-action.org
221 Main Street, Suite 480
San Francisco, CA 94105
415-777-9635
TTY: 415-777-9456
hotline@consumer-action.org

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

Chinese, English and Spanish spoken

CHASE

This publication was created by Consumer Action in partnership with Chase.

Recognizing Credit Card Fraud

A Consumer Action Publication