Plastic Fraud

Created by Federal Reserve Bank of San Francisco

Getting a Handle on Debit and Credit Cards

State-of-the-art thieves are concentrating on plastic cards. In the past, this type of fraud was not very common. Today, it is a big business for criminals. Plastic cards bring new convenience to your shopping and banking, but they can turn into nightmares in the wrong hands. This pamphlet describes credit and debit cards and some common schemes involving card fraud with tips to help you avoid them.

Credit and Debit Cards

Although they may look the same, all plastic cards do not work the same. In fact, there are two very different kinds of cards in use today: credit cards and debit cards. As the names imply, *credit* cards allow the extension of credit and the delay of payment while *debit* cards charge or debit your account at the moment of the transaction.

Credit Cards

Many credit cards work as follows: You charge goods or services and the merchant who accepts your credit card sends the transaction information to the card-issuing institution. The institution then bills you, usually on a monthly basis. In many cases, payment may be made by the due date with no interest assessed. If the total bill is not paid by the due date, you often can pay off your debt in monthly payments that include finance charges.

Debit Cards

Debit cards, unlike credit cards, automatically withdraw funds from your account at the time you make a transaction. Debit cards are used most commonly at automated teller machines (ATMs) and for purchasing goods directly in stores. The machine-readable plastic card contains a magnetic strip indicating your account number, bank number, and type of account. Debit card users gain access to the issuing institution's computer by using a secret code, their personal identification number (PIN). The PIN should only be known to the card holder.

Avoiding Card Fraud

Although credit and debit card fraud can take many forms, the following examples explain some situations to watch for.

Stolen Cards at the Office

Over the lunch hour when you leave your office for lunch, you could be the target of a credit card thief. Credit card thieves often gain illegal access to the offices of employees who are away in order to search unattended. Most times, they leave the offices and immediately go on a shopping spree, charge credit cards to their limits, and withdraw cash on debit cards.
Protect your credit cards as you would cash. Never write your PIN number on your debit card. Instead, always commit your PIN number to memory.

Extra Copies of Charge Slips

When processing your credit card, a dishonest merchant may decide to imprint a few extra copies of the charge slip. Later, the merchant can submit these copies to the issuing institution for payment on phony charges.

Keep your eye on your credit card whenever it is in use. Watch clerks process your credit payments. Open your credit card bills promptly each month. Make sure that you made the listed purchases. Also, report any charges that you did not make to the credit card company.

Discarded Charge Slips

Sometimes, people may collect copies of your discarded charge slips from the wastebasket. Dishonest people could use the information from the copies to order merchandise by mail and ship it to a phony address. In addition, they could also sell the copies to counterfeiters who would take the account numbers and use them to alter cards or make new ones.

After signing a credit card slip, ask for your receipt or duplicates. After you have compared them to the charges listed on your monthly credit card statement, tear them up and throw them away.

Unsigned Credit Cards

Stealing and using credit cards that have not been signed is another potential fraud. In other words, credit card thieves could steal your unsigned credit cards and then sign your name on the card in their handwriting. By doing so, they take your name as an alias and they will never have a problem writing and verifying their own signature.

Protect your credit cards. When you receive a new or replacement card, sign the back of it as soon as it is activated. Always be sure to store it in a safe place. Cut up expired cards before disposing of them.

Loss of Multiple Cards

While shopping, you can easily be targeted by pickpockets. If your purse or wallet is stolen, you may lose all your credit cards at one time.

Separate your cards. Only carry those cards with you that you plan to use. Also, check your cards from time to time and put aside those cards you don't use very often.

Strange Requests for Your PIN Numbers

This form of fraud involves thieves who find creative ways to steal your credit or debit cards when you don't know about it. For example, sometimes people crawl behind rows in movie theaters and steal pocketbooks while you are watching a movie. When you return home they call you, identify themselves as bank security agents, and ask for your PIN numbers. If you hesitate, they simply ask you to phone their supervisor and give you an accomplice's phone number to call. By doing so, they are able to get your PIN numbers and use the stolen debit cards to withdraw cash and make purchases.

Again, never reveal your PIN number to anyone. Also, never keep your PIN number in your purse or wallet. Don't write your PIN on your card either. Always try to memorize it.

Recognizing Counterfeit Cards

Legitimate Cards

Legitimate cards follow standard specifications as to color, tint, quality, and style. Stamped letters and numbers are spaced evenly and sized equally. The signature panel is uniform in size and is almost impossible to scrape off.

Altered Cards

Altered cards are made from actual cards. The original stamped data is melted down or pressed out. Then, the card is re-stamped with legitimate account numbers, names, and expiration dates, which have been illegally

obtained. On altered cards, the letters do not line up well and are usually irregular in size. Some credit card companies help merchants identify altered cards by making an authenticator machine available to merchants. The machine authenticates or verifies certain information that is encoded on the back stripe on the back of the card.

Counterfeit Cards

Counterfeiters make most counterfeit cards by silkscreening or painting the card logo and issuing institution's name onto a blank piece of card plastic. Because they are silkscreened, the cards don't look exactly like the real thing. Real credit cards are printed. Also, the signature panel on silkscreened cards may be glued or painted on and can be easily lifted or chipped. This panel may also appear uneven in size or placement.

New Technology

New technology is making it more difficult for criminals to use, alter, or counterfeit credit and debit cards. Some of the innovations are already in use .These security features have been added to major credit cards: 1. Holograph – a three-dimensional, laser produced optical device that changes its color and image as the card is tilted. 2. Fine-line printing – a repeated pattern of the card company name positioned as background for the company logo. 3. Ultra-violet ink – special ink that is visible only under ultra-violet light, which will display the credit card company's logo.

On the Internet

While using the Internet, you can learn about any number of topics and buy almost anything. Be aware, though, that Internet shopping, like traditional shopping, may carry some risk. Software to protect you and your privacy is often a part of most web sites. In fact, when ordering online, it would be wise to check if you are on a secure server by looking for a security symbol such as an unbroken key or padlock symbol at the bottom of your Internet browser window. These symbols indicate that any information you may send to the web site, including your credit card numbers, is encrypted or put into computer code prior to transmission.

Consumer Liability

It is important to keep a personal list of your credit and debit card numbers, the issuing banks, and their phone numbers so that you can contact them in case of loss or theft.

Credit Cards

If your credit card is lost or stolen, contact your bank or issuing institution immediately. Your monthly statement should list the phone number of whom to contact. You do not have to pay for any unauthorized charges made after you have notified the issuing bank or institution. The most you will have to pay for unauthorized charges is $50 on each account. But this can add up if several cards are lost or stolen at the same time. If you think that you did not make some or all of the purchases listed on your statement, you can take action. The Fair Credit Billing Act, an addition to the Truth-in-Lending law, requires prompt correction of billing mistakes. Within 60 days after the bill was mailed, you must notify the creditor in writing. You do not have to pay the amount in question while you are waiting for an answer.

Debit Cards

If your debit card is lost or stolen, notify the issuing bank or institution immediately. According to the Electronic Funds Transfer Act, if notification is given within two business days of discovery of the loss or theft, you may only be liable for $50. If you do not notify them within the

two-day limit, you could lose up to $500. Finally, if notification is not given within 60 days after receiving a statement showing unauthorized withdrawals, you could be liable for everything.

What is the Law?

The Credit Card Fraud Act imposes prison sentences and stiff fines on persons convicted of unauthorized or counterfeit use of credit cards and debit cards. Also, the law makes it a federal crime to use any unauthorized card, plate, code, or account number to obtain money, goods, or services. The Secret Service is authorized to investigate violations under this act.

For More Information

You can file a complaint with the Federal Trade Commission (FTC). Although the FTC cannot resolve individual problems for consumers, it can act against a company if it sees a pattern of possible law violations. The FTC's web site also includes a series of articles that provide guidance on e-commerce and the Internet.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
http://www.ftc.gov
(877) FTC-HELP

For help with a specific consumer problem or to learn more about protecting your privacy on the Internet, contact Call for Action (CFA), an international non-profit network of consumer hotlines.

Call for Action
5272 River Road, Suite 300
Bethesda, MD 20816
http://www.callforaction.org
(301) 657-7490

For additional information, contact you local Financial Institution.