Recognizing Credit Card Fraud

Author: Yoivy Guerra
Financial Analyst – Bank Customer Service Office
Superintendency of Banks of Panama

At some point, we have surely heard about credit card fraud, either in news broadcasts or because an acquaintance or family member has been a victim of it.

Usually, cards are lifted for the purpose of creating fake cards with the victim's account number and making unauthorized charges to the credit card itself.

Credit card fraud can occur when consumers give their credit card number to unknown individuals, when cards are lost or stolen, when the magnetic strip is copied, or when employees of a business copy the card or card numbers of a card owner.

It is worth noting that this task was easier with the magnetic strip, causing the Superintendency of Banks in our country to issue Rule 6-2011, a regulation directing the move from the magnetic strip to smart cards in our banking system. The smart cards (chip cards) best protect our information and, consequently, our bank accounts.

On the other hand, we must clarify that fraud can still occur on our accounts, through phishing and identity theft. Therefore, it is important to know more about the methods used for fraud against our banking accounts and tools, so that we can take the necessary preventive actions to avoid being a victim of criminals.

Below, we will describe the most common types of fraud in greater detail.

Identity theft is the fraudulent use of someone's personal information – such as their personal identification card, 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 the victims of identity theft are not held liable for the crimes, it takes a lot of work by the victim to prove fraud and clean up the financial chaos caused by the crimes.

Skimming (copying the magnetic strip) is making an illegal copy of a credit card or a bank card using a device that reads and duplicates the information on the original card.

Dishonest business employees use small machines called "skimmers" to read numbers and other information from credit cards and capture and resell them 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 phone emails 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.

The crime succeeds because the emails look legitimate, with realistic bank logos and website addresses (or URLs) that are very close to the real thing.

When accountholders respond, they are directed to a fake website 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 victim's bank accounts using the passwords to authorize the electronic transfer of funds to other accounts.

Consequently, we must bear in mind that banks never ask for personal information in this way. Don't respond to emails or phone calls asking you to provide your credit card numbers, social security number or other personal data.

Even when you have a legitimate request, banks ask that you never send detailed account information in an email, because emails are not secure and the information may be intercepted by criminals. Instead, visit in person, use the bank's secure website, call on the phone or write a letter when you are attempting to settle a dispute with a merchant or your bank.

Now that we know the most common methods of bank fraud and their characteristics, let's look at some security advice that will be very helpful in avoiding being a victim of crimes.

New cards

- 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. Many credit card issuers advise 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.

Protect your wallet or purse

- Keep a close eye on your belongings.
- Never carry all your cards – only bring the one or two that you might need.
- Carry your credit cards separate 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.

Internet safeguards

- If you bank online, don't use "automatic sign in" for bank or credit card sites.
- Some websites offer "free access" if you provide your credit card number. Stay away from these sites – 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 over 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.

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.
- Protect your security code. 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 after 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.

- Keep copies of your vouchers and ATM receipts, so that you can check them against your billing statements.
- 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 because you were using it in unusual places.
- If you are going to make any unusually large purchases, notify your card company so that your account is not be 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.
- It is important to keep your fraud insurance current, because this will guarantee the return of charges for the unauthorized use of the credit card. This insurance is optional for the cardholder.

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 as soon as you notice them. You have a set period, established in the signed contract and usually thirty days from the date the billing statement was issued, to dispute any mistaken or unrecognized charges.
- File claims in writing. You may call the bank or card issuer and send them the claim afterwards.
- 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. (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 trouble with your credit card

- Call the card issuer immediately when the card is lost or stolen.
- After making the call, send a letter to the card issuer. The letter should contain the card number, the date when you lost it and the date when you informed the issuer that the card was lost.
- Once you report the lost card, you are not responsible for any unauthorized charges.

You may lose protection if, due to negligence, you do not report the loss of the card or the unauthorized charges on your statement in a timely manner.

Remember, you are the first line of defense against fraud. Take precautions and implement the necessary safety standards and you may prevent greater complications in the future

Source: http://www.consumer-action.org/english/articles/recognizing_credit_card_fraud_english#Topic_01