Credit and Debit Card Security Tips

Many of these tips are just common sense and others are tips to keep in mind when doing a transaction, at ATMs, restaurants and merchants.

Be careful with your PIN

- Always cover the keyboard when entering your PIN.
- Never disclose your PIN.
- Don't write it down or record it on your cell phone, or on note paper in your wallet.
- Change your PIN frequently.
- Whenever you get a new card, sign it when received, check frequently to make sure you are carrying your own card.
- Never assign the same PIN to different products (Savings, Checking, Credit Card, etc.) or media (audio, internet, ATMs, etc.).

Never lose sight of your card

- Never hand over your card to strangers for no reason.
- Never let anyone swipe your card on devices other than those designated for that purpose. (ATM's or POS terminals or data phones)
- Whenever you use your card make sure it is swiped in your presence (do not lose sight of it, mostly in restaurants or bars) and make sure it is only swiped once.
- Always block your card, if it is stolen or lost or retained by the ATM.

Use a secure network for Internet transactions

- Do not use public networks (internet cafes, for example)
- Always type in the bank's website address.
- Always look for a secure exit from your bank's website.

ATMs

- Use ATMs you are familiar with, otherwise look for a well lighted ATM at a safe location.
- Look around the ATM location before approaching and don't use it if you see someone suspicious in the area.
- Don't open your bag or wallet while standing on line at the ATM.
- Be ready with your card when approaching the ATM.
- Check to see if there are any strange objects in the ATM slots or keyboard.
- Avoid help from strangers.

- Do not follow instructions or indications on notices affixed to the ATM, that tell you to enter your PIN several times.
- Only follow instructions on the ATM screen.
- Do not enter your PIN until the ATM asks for it.
- If you think the ATM is not working correctly, press the “Cancel” key, withdraw your card and go to another ATM.
- Never force your card into the card slot.
- If your card gets stuck, is retained or lost or if someone interferes with you at the ATM, report it immediately to the bank or to police using the help line provided or the nearest phone.
- Always make sure to finish the transaction by pressing the CANCEL key prior to leaving the ATM.
- Don’t rush while making your transaction and carefully put away your card and cash in your bag or pocket, before you leave the ATM.
- Always wait until the ATM tells you that your transaction has been completed.
- Monitor your account balance and account statement regularly and immediately report any discrepancy to the bank.

At bank offices

- Fully identify bank officials.
- Hand over your cash only at the teller window.
- If you observe anything abnormal in the bank, immediately inform a correctly identified bank official.
- If you withdraw cash, do not count it in the presence of other people and put it in a safe place.

After you leave the bank or ATM

- Avoid walking long distances, looking at shop windows for a long time or speaking on the street.
- If you have made transactions for large sums of money, ask someone you trust to accompany you or ask a competent authority to accompany you.

Internet

- Always make your bank transactions on personal equipment, do not use internet cafes, computer rooms or other public locations.
- Always type in your banks website: www.name of bank website. com.co directly on the browser.
- Never enter using a link sent by Email, even if the Email comes from someone you know. Do not believe those Email messages that suggest you enter your account number or provide them with information. This is called “phishing”, an illegal practice were delinquents set up a website similar to the bank’s website to steal your PIN and then empty your account.
- Email addresses that appear on the upper part of your screen that say https:// instead of the usual http:// and the browser displays a closed lock symbol at the bottom of it.
- Avoid processing formats included in Email messages that ask for your personal financial information.

Identity Theft or Phishing

- Constantly monitor the status of your accounts at risk centers to validate possible negative reports.
- Report loss or theft of your identification documents to risk centers.
- Do not give out your personal or business information for surveys conducted on the phone or other media.

Security Measures when you Receive your Credit Card at Home.

- **Sign your card:** Sign it as soon as possible. Remember that this will give you better security in case of loss or removal.
- If your card is renewed, remember that you can only use it when your current card expires. In this case, **always destroy the old card by cutting it in half**.

PIN Security Measures

- Memorize your secret code (PIN). **Never write your PIN down anywhere**.
- **Never give your PIN to anyone.**
- **Do not write your PIN on your card**
- Do not write your credit card account number on a post card or on the outside of an envelope you are mailing.
- **Do not store your PIN number in the same place you keep your credit card** or your ATM card.
- **Never give out your credit card number or other personal information over the phone,** unless you can confirm that you are speaking with a trusted financial institution or an honest merchant.

ATM Security Measures

- **If you notice anything suspicious** near the ATM or if the ATM retains your card for no apparent reason, **inform the bank immediately.** If this is not possible, at night for example, immediately call your credit card company and cancel your card.
- If you detect something wrong at the ATM, for example **a strange device, immediately inform the bank** and as a preventive measure, do not make any transactions at that ATM.
- **Act quickly if your card is blocked** at an ATM**.**
- Immediately request the presence of a financial entity professional at the ATM location and do not accept help from persons not belonging to that entity; they may be waiting for the chance to take your card or get your PIN number.

Security Measures in case of theft

- Watch your possessions well.
- **Never carry all of your cards, only carry one** or two at the most**.**
- **Carry your credit cards outside your wallet,** in a credit card holder or in a compartment in your bag.
- If your bag is stolen, call the issuing entity immediately.
- Be particularly alert at airports and other public places.

Security Measures for identity theft fraud.

- **Do not lend your card to anyone,** because you are responsible for all charges to it. You are not protected against unauthorized use, if the charges are made by someone to whom you gave the card knowingly and willingly, including family members and friends.
- Do not give your account number to anyone who calls on the phone or sends you an Email.

- **Always carefully check the payments listed on your account statement** and compare them to the copies of your purchase receipts.
- Keep a record of your credit and debit account numbers so that you can quickly inform your financial entity in case of card loss.
- Always take your receipts from ATM's, supermarkets and gas stations with you. Check to make sure that the amount on the copy of the receipt given to you by the merchant is the same as the one on the financial entity statement.
- Make sure you know who has access to your cards. If they are used without your knowledge, it's possible you may have to pay anyway.

Beware of Fraudulent Telephone Calles and Emails

At Banco Cathay security is first. We appreciate this opportunity to alert you regarding one type of telephone or Email scams currently run in our country.

How does it work?

Unknown persons contact you by phone or Email saying they work for the financial entity, trying to obtain confidential customer information such as identification, internet site user ID and password, card number, account numbers, address, telephones, Email address, claiming that they need it to update your information with the Entity or that it is needed to complete approved credit information.

Some advice to avoid this type of calls or Emails

- Do not respond to phone calls or Emails that ask you to enter the financial entity website using some pretext. These emails and phone calls may seem legitimate.
- Contacts between Banco Cathay and its customers are made through an assigned Executive. If you have any doubt as to the identity of the assigned Executive, you can inquire at any of our Branch Offices.
- Banco Cathay will **NEVER** ask for the following confidential information by phone or Email: user ID, passwords, account numbers, card numbers.
- Whenever you use our internet services, type in the corresponding address directly into the browser. Never enter using "links" received from any other media.
- Try not to use public locations (such as internet cafes) to make financial transactions of any kind, because your confidential information may be captured.

How to detect a phone call or Email scams?

Normally, fraudulent Emails have the name of the sender (From) that appear to be legitimate and with logos copied from the financial entity website.

Elements that identify them are:

- The Email is alarmist and requires quick action.
- It includes a link (access to a website) that tells you to click on it to confirm or update your personal information.
- They frequently have grammatical errors, not normal in your usual communications with the institution.
- The Email reaches your mailbox several times in one day (repeatedly).

Fraudulent phone calls are made by unknown persons passing for financial entity personnel, they may even use the real names of these officials.

Elements that identify them are:

- The call comes from a private number that cannot be identified.
- They ask the customer to answer questions to confirm their identification.
- Normally the call is short, does not provide details, and they rush the customer into answering.
- Fraudulent calls can be made several times a day, to the same number until they locate the customer.

How to report possible phone call or Email scams?

If you believe that you have received a fraudulent phone call or email from Cathay Bank, contact us immediately by calling telephone number 2527-7725, 24/7, 365 days a year.