Fraud Awareness Guide

How you can Help

قطـر مصـدر إلهامنـا
Inspired by Qatar

البَنك التّجَاريّ
Commercial bank

www.cbq.com.qa

A bank's best line of defense is its customers, who play a vital role in preventing and detecting fraud.

"**Security is Shared Responsibility**" and customers, need to safeguard themselves by securing and protecting their Card(s) and PIN(s) at all times when transacting through various channels. The following best practice, TIPs and guidelines will assist in achieving this shared responsibility:

PIN Security - Best Practices

- Never share or disclose your PIN with anyone (including family members, a waiter/waitress, cashiers, sales staff or helpful bystanders at an ATM.
- Memorize your PIN and do not write or store it anywhere else.
- Enter the PIN in a way that other bystanders, sales staff or overhead cameras cannot observe. Use your other hand or body to shield your PIN entry during every transaction conducted at a POS terminal or ATM.
- Refrain from changing your PIN to identical (such as 1111, 2222) or consecutive (i.e. 1234, 5678) numbers or information, such as your telephone number, date of birth or P.O. Box number which are easily guessed.
- Routinely change your PIN at any Commercialbank ATM.
- Maintain different PIN's for different cards.

Card Security - Best Practices

- Never share your card with anyone.
- Make sure that you sign your card(s) on the back of the card's signature panel on receipt of a new/renewed/reissued card.
- Keep your cards in a folder or wallet in an organized way so that if one is missing, it will be noticed immediately.
- Never leave your cards unattended in a vehicle, office or in an unsecured area, where they are susceptible to opportunistic thieves.
- Make sure your card is returned to you after each purchase and ensure that it is your own by reviewing the name embossed on the card and your signature.
- Always see that the card is visible to you when completing a transaction.

ATM Security Best Practices

- Stand close to the ATM and shield the screen and PIN pad by using your body and other hand to ensure nobody sees you entering your PIN.
- Never hurry when using an ATM. Make sure you are not distracted, intimidated or rushed into your transaction by bystanders.
- Never accept help from well meaning strangers when using an ATM. Always be on alert of strangers asking for or offering to help. While one distracts you, the other may be stealing your card and money.
- If your card gets jammed or retained at the ATM report it immediately by calling our 24/7 Call Center +974-44490000, while you are still in front of the ATM.
- Before leaving the ATM always check if you got your card back and do not forget to collect cash from the cash dispenser.
- Please refer to "Card" and "PIN" security best practice for further guidance.

Deterring Online Fraud

Devising ways to deter fraud in all its forms will go a long way toward mitigating your risks.

- Ensure that your firewall, spam filter, anti-virus and anti-spyware protection is active and up to date.
- Create strong passwords but do not use the same password for multiple applications and do not share or divulge your passwords with anyone.
- Ignore emails and attachments from senders you don't know.
- Use your pop-up blocker.
- Download files and transact only from Trusted & Secure (https://) sites.
- Only give your card details when you initiate a purchase yourself and never the other way around.

Anti-Phishing Emails

Phishing is an email scam that attempts to trick you into revealing card numbers, PIN's and account login passwords or other financial information. Most phishing attacks start as an email that links to a fake internet site that looks legitimate with familiar logos and graphics, but is not.

- Be cautious of emails requesting personal or financial information.
- Do not respond to emails that make urgent request for information, aren't personalised and are of a threatening or exciting nature. Remember if it sounds like it is too good to be true, then it usually is.
- Do not click on links, download files or open attachments in emails from unknown senders.
- Always check the legitimacy of the inquiry by calling Commercialbank.
- Report suspicious emails or websites to Commercialbank by calling us at +974-44490000.

Smart Travel – TIP's

Don't let fraud ruin your vacation. Take these easy measures before you travel

- Habitually keep Commercialbank informed of when and where you'll be traveling.
- Travel with only the Credit and Debit cards that you plan to use.
- Travel with more than one type (Diners Club, Visa and MasterCard) of card which leaves you with a wider choice for transacting.
- Do not pack your cards in unaccompanied luggage and refrain from leaving your cards in your hotel room, while you are out.
- Make sure you take along our 24/7 customer service help line number +974-44490000 for assistance in case of need or to make Lost/stolen card reports.
- Retain your transaction receipts, it will assist you in reconciling your statement. Do not throw receipts in the rubbish without destroying them first.

General Guidelines

- Enroll yourself for Commercialbank's "FREE" SMS banking service, so you can be alerted on all transactions made using your Credit and Debit cards.
- Ensure that Commercialbank has your up-to-date contact details, including mobile, office, home and email address details, so that we can contact you to authenticate unusual spend patterns on your cards

- Ensure that you not lose sight of your card at all times and be observant of the transaction being performed.
- Keep us informed, in advance, if you are going to make any unusually large purchases by calling our 24/7 Call Center on +974-44490000.
- Regularly reconcile your transaction receipts against your monthly statements through internet banking, E-statements or hardcopy statements.
- Advise Commercialbank if you have not received your E-statement or hardcopy statement, as a matter of urgency.

If you become a victim of Fraud

If you detect unauthorised transaction(s) from your statement or receive unknown debit advices through SMS Alerts.

- Immediately notify our 24/7 Call Center on +974-44490000, without delay.
- Register your complaint by filing up a "Dispute Form" provided by the Bank.
- Immediately return the card/plastic of which transactions are being disputed to the Bank as evidence of having same in possession, whilst being a victim of fraud.
- Provide as much evidence as you have including a copy of passport with recent travel stamps, transaction receipts and supporting correspondence with the merchant.
- If you are residing in a country where you have been a victim of fraud also report such incidents to law enforcement authorities by filing a Police report.
- If you are not registered for SMS or Internet Banking services register for same whilst requesting your replacement card.

Taking all of the above precautions will minimise your chances of becoming a victim of fraud. At Commercialbank – we are committed to safeguarding the interest of our customers at all times, so stay safe, stay secure.