PREVENTION OF CARD FRAUD GUIDELINES

ONLINE AND TELEPHONE SHOPPING

Shopping on the internet and telephone is easy and convenient, but it can also provide the ideal opportunity for fraud to be committed using your Card details. This is what you can do to help prevent card fraud.

Keep your PC protected against malware

Malware refers to computer programmes that perform harmful functions to your detriment. These programmes usually run silently in the background, and until the damage is done, they will go unnoticed. Malware can take the form of viruses, worms, Trojan horses, and spyware.

Therefore make sure that your PC is secure and fully protected from malware by:

- Always using the latest version of your operating system.
- Never running and/or installing programmes from unknown sources.
- Using a suitable auto-update anti-virus and anti-spyware.
- Using a personal firewall.
- Preventing the browser from storing (caching) the pages that you view by using the enhanced security features of the browser. If you allow the browser to cache to improve performance, erase this cache when you complete your session on Internet Banking.

You should always be very cautious when surfing the Internet. Some malware can infect your system from the websites that you visit.

Other things to remember:

- *Do not shop online from publicly accessible computers, such as those found in Internet cafes, as there is no way for you to know whether the operating system that you are using is secure enough. Be aware that some computers used in public are not properly protected against malware and there is no way for you to know this. Such malware is capable of recording information from your purchase without your knowledge, and this information will then be used fraudulently to gain access to your card account/s.*

- *Before using WI FI (wireless connections) to shop online, ensure that you have adequate security on your computer, especially if you are using a WI FI hotspot in a public area. Your personal data and Card details may be compromised unless adequate safeguards are in place.*

Look out for hoax email / telephone calls

Fraudsters send you an email purporting to be from your bank, a company you had visited or a social networking site pretending that there's a problem with your account/s, purchase or something similar. This is intended to get you to divulge your Card and personal details. Some may also try to reach you by telephone for the same fraudulent purpose. Therefore:

- Do not open any emails that you are not expecting and where the sender is not known to you.
- Do not click on any email links which are supposed to connect you to an online shop.
- Be careful with all email attachments that you receive.
- Delete any unsolicited emails immediately and clear these emails from the 'Deleted' folder afterwards.
- Do not respond with personal Card details to telephone calls you do not expect.

Other things to remember:

- *Do not record or divulge your PIN.*
- *Do not give your Card details in an email even for what may be a genuine transaction.*
- *Give Card details on the telephone only if you have made the call personally yourself and you have phoned a company known to you.*
- *Prior to making an order by telephone, know what information the company will need from you on the telephone to take your purchase order. The company will never need your Card PIN.*

Look out for the padlock

Check that the web merchant you are visiting handles your personal information in a secure manner. You can make sure of this by:

- Checking that the address (URL) on the browser address bar starts with ***https:***
- You can tell that the website is secure by looking out for the small **locked** padlock. If you are using Internet Explorer 10, the top of the browser displays a green address bar and a yellow padlock on the top right side of the address bar. When using Firefox the colour highlighting the security certificate will display in green next to the address bar.

Other things to remember:

- *Check that the web merchant is a reputable one. Search for and read feedback from other users. Other users may have suffered from fraudulent behaviour by the merchant. Typical behaviour by an apparent reputable merchant is to charge your Card account/s small amounts after you make a legitimate purchase. Such merchants play with small amounts as they know it will be uneconomical for the bank to start chargeback procedures.*
- *If the website you are using has a 'Logout option' or similar, use it.*
- *Print your online order to assist you remember the purchase when checking your Card account/s statement and may also be useful in the event of a dispute. We may need and ask you for a copy of these orders to assist the Bank recover money wrongly taken from your account/s.*
- *3D Secure is an authenticated payment system to improve on line transaction security. This Card is supported by this system but has to be registered. Registration is free of charge. It is highly recommended to make use of this service.*

Report to us

If you suspect that your details have been compromised report the matter to us immediately, currently on +356 2558 1789.