MAURITIUS BANKERS ASSOCIATION LIMITED

CARD FRAUD AND SKIMMING

What is Card Fraud?

The fraud occurs when a bank card is stolen, lost or the bank card/card data is obtained by illegal means and without the permission or knowledge of the legitimate cardholder. The bank card or the card data may then be used to make unauthorized purchases and fraudulent transactions. Cardholders are required to be vigilant and take a number of precautionary measures to mitigate the risks against card fraud.

What is Card Skimming?

Card Skimming is the copying of encoded information stored on the magnetic stripe of a card by fraudsters, to create counterfeit cards to make illegal purchases and cash withdrawals, to the detriment of the legitimate cardholders. Card skimming usually happens at the ATM or Point of Sale (POS) where the fraudsters conceal sophisticated devices on the card slot or use hand held devices to copy the card information. A small camera is often used to obtain your PIN or a person may be watching you enter your PIN.

Important tips to avoid becoming a victim of Card Fraud and Skimming:

- Always keep your contact details updated. Notify your bank about your travel plan. If not on roaming, advise your bank about any new contact numbers while being abroad to facilitate transaction verifications.
- Report immediately the loss or theft of your card to your bank. Store your bank's hotline number on your cell phone so that you have it handy should you need to stop your card.
- Be aware of your surroundings, particularly while using an ATM at night, early in the morning or when there are few people around.
- Never use an ATM that is tampered with or visibly damaged and be vigilant while using another ATM.
- Stand close to the ATM and use your body as a shield as extra security to protect your card and PIN.
- While transacting, always keep an eye on the ATM card slot to ensure that your card is not taken out, skimmed and replaced without your knowledge.
- Do not accept assistance from anybody at ATMs, even from security staff.
- Memorize your PIN and never write it down or store it electronically on your cell phone, tablet, laptop or any other portable/wireless devices.

- Do not keep your PIN and card together if you are unable to memorize the PIN.
- Do not choose the same PIN for your debit and credit cards, so that if you lose one, the other one will still be safe.
- Do not let other people use your cards and gain access to your pin.
- Never throw away your ATM receipts, credit statements, credit cards or bank statements in paper baskets or garbage bins; shred or burn them instead.
- Remember to take back your card when you complete your transaction at any Merchant or ATM.
- In case your card is retained without any specific reason at a local or overseas ATM, inform your bank immediately.
- Destroy old cards by cutting part of the magnetic stripe.
- Sign your card with permanent ink as soon as you receive it.
- Do not lose sight of your card when you pay at a restaurant – request for the machine to be brought to your table or else accompany your card to the POS machine.
- If a merchant swipes or inserts your card in two different POS machines, write down his name and inform your bank as soon as possible.
- Always verify transaction slips for correct purchase amounts before you sign them.
- Keep your transaction slips and verify them against your statement or your account activity through internet banking to spot any suspicious transactions and query them immediately.
- Do not send nor reply to e-mails that include or request card details such as your card number, expiry date or other details like the security code on the back of your card. Your bank will never ask you such information.
- Use only secure websites when shopping online. Identify a secure website by looking for 'https' in the web address.
- Never disclose credit cards or other personal information on a website that is not secure.

What to do if you are a victim of Card Fraud and Skimming?

- Never assume your card has been retained by an ATM. Always contact the bank and request the card to be blocked immediately – a skimmed card can be replicated in minutes and be used immediately.
- If you notice any suspicious foreign objects or people loitering around the ATM, call the Police and your respective Banks immediately.
- Review your account statements on a regular basis and report any irregular transactions to your bank immediately.
- Subscribe to your Banks' SMS notification services where available; this will inform you of any transactional activity on your account.

Caution:

The contents of this insert are made available for information purposes and guidance only and on the understanding that the MBA is not providing professional advice.

October 2016