USEFUL INFORMATION ON CREDIT CARDS

Information on Credit Information Bureau (CRIB)

The CRIB is an independent repository of credit information and credit history of borrowers. All authorised financial institutions are mandated to provide the bureau with factual information on credit granted to customers and how they service their debts.

Why your CRIB report is important:

- Your CRIB report is a record of your credit repayment history compiled from different credit providers. As most lenders check your credit information to assess your credit worthiness prior to making a decision, a good repayment history will make it easier for you to obtain credit faster and at concessionary terms.

- Reviewing your credit report regularly, makes aware of any incorrect information uploaded to your credit file and gives you the opportunity to correct same.

Tips on managing a good credit profile:

- Borrow only what you can repay from your income. If you are in financial distress, you can inform the Bank to reduce your credit limit of the credit card to control your spends.
- Maintain a good credit record to reflect positively on your 'credit worthiness'. Ensure that Monthly Minimum Payment is made on your credit card prior or on the Payment Due Date.
- Regularly review your credit report on CRIB and analyse your payment history and status. This would help you make important decisions such as consolidating your debts or reviewing your financial planning.

How to protect your Card and PIN

Here are some tips to help you protect or minimise your card being misused.

Things you should do:

- Update your contact records with the Bank so we can send you SMS alerts for your transactions or contact you if we detect any peculiarity on your credit card activities.
- Please place your signature on your card immediately as you receive it, with a ball point pen.
- Activate your credit card using our secured digital channels (Mobile app / iBanking) or by calling our Client Care hotline on 0112480480.
- When you login to the Mobile app / iBanking, create a PIN that is convenient for you to remember, but is not easily guessed (such as date or year of birth or telephone number etc.) by another party.
- Do not keep expired/replaced cards. Always destroy the old cards after activating the new cards, by cutting it into pieces and disposing with care.
- When using your card at any merchant establishment for a transaction, ensure that the card is visible and the transaction is processed in your presence. You should not let the card be taken to a different location away from your sight, as most frauds take place when the cardholder is not around.
- When using your card at any merchant establishment, ensure that all details have been entered correctly before signing the transaction receipt, or acknowledging the transaction receipt, or entering the PIN.
- You may check your transactions and the card balance anytime using Mobile app / iBanking. Please check the records frequently and inform the Bank of any disputes. This will help you reconcile when you receive your monthly statement.
- If you are traveling abroad, do inform us about your travel plans.
- Always keep your mobile phone with you as your phone has access to the One Time Password (OTP), Mobile app and stored card details.

To safeguard your card:

- After completing an ATM transaction, remember to take your credit card. Beware of anyone offering you help with the transactions or retained card, unless identified as Bank staff.
- If you notice your credit card is lost or stolen, immediately call the Bank to report, or you may block your card conveniently by logging into the Mobile app / iBanking.
- Request for a card replacement immediately if you come to be aware that your card details have been compromised.

Things you should not do:

- Do not share images of your credit card with friends and family to perform transactions on your behalf.
- Do not save your credit card information on commonly used devices, such as office computer, family laptop etc. when prompted to do so.
- Do not keep the credit card and PIN together. Memorise the PIN for your safety.
- Do not disclose your card details or PIN to anyone including any financial institute or any other officials. You are the only authorised person to have access to them.

Be aware of Internet misuse:

- Be aware of phony “lookalike” websites. Always ensure that you are using a secure website when submitting credit card details.

  Ways to identify a secure website:
  - Look for the “padlock” icon on your browser’s status bar. This signals your information is secure.
  - Check the beginning of the web address. It should read as https:// rather than just “http://.”
- Carefully read the terms and conditions of the online purchase. Specially look at ‘Refund policy’, ‘Delivery policy’, ‘Surcharges’, ‘Currency in use’ and buyer’s obligations.

Do you know the Regulatory guidelines for credit card usage?

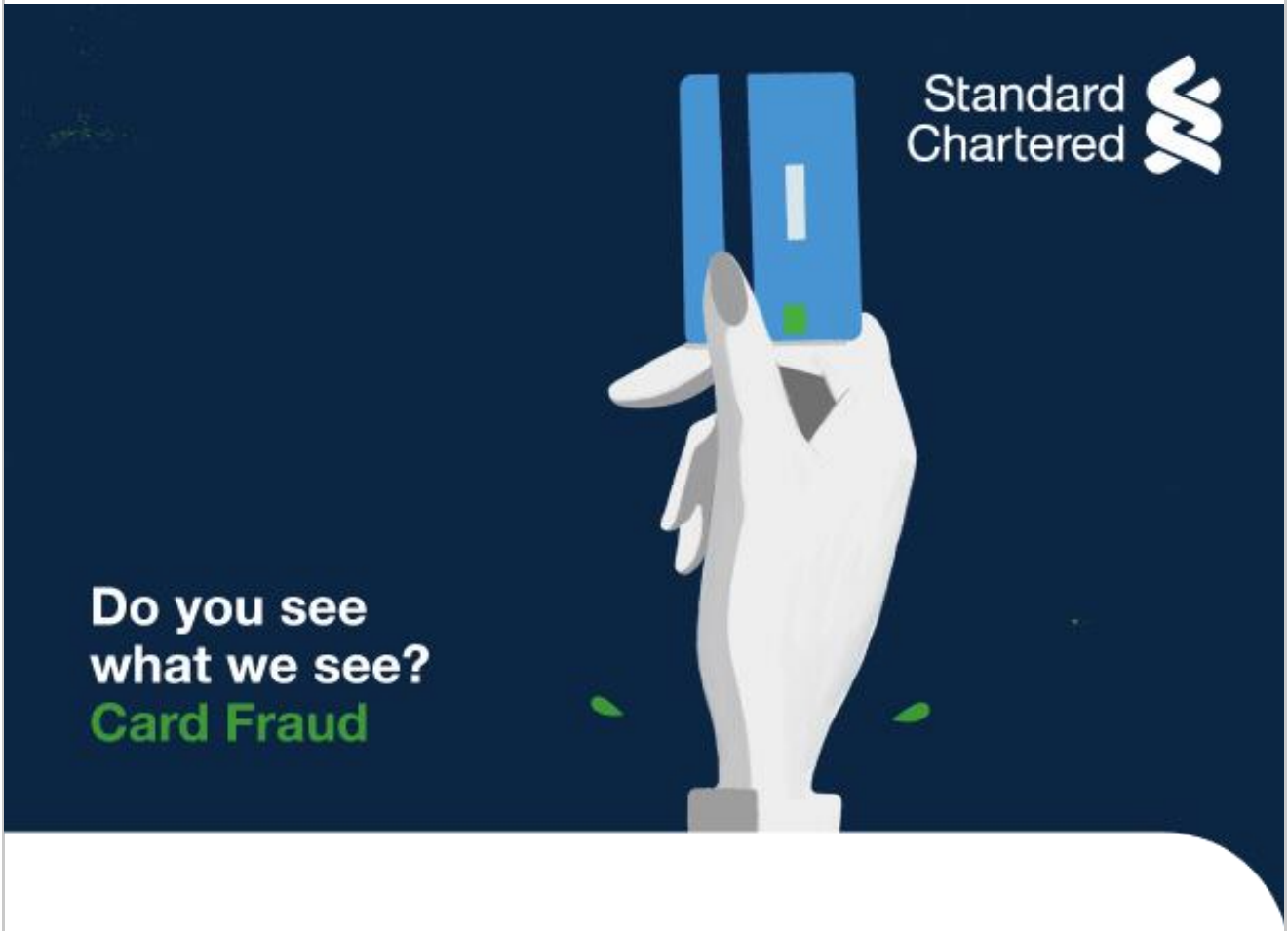
Electronic Fund Transfer Card (EFTC) usage must be in accordance to directions issued by the Central Bank of Sri Lanka on Electronic Fund Transfer Cards (EFTCs) and other guidelines: In summary, **refrain** from using your credit card for (unless otherwise payments are made via a foreign currency account);

- commercial purpose transactions other than for Imports of personal nature
- capital transactions including payments in relation to restricted foreign exchange transactions
- any type of purchase not permitted by the law of Sri Lanka

Remember

- to surrender your credit card during permanent migration or overseas employment (unless the card is issued against an FCY account)

- that you’ve agreed to abide by the Regulatory terms by signing the EFTC Declaration



Prevent card fraud before it happens to you

Did you know that fraudsters can misuse your credit/debit card and make purchases without your knowledge, even when your card is with you? All they need is your card information.

Examples of card fraud

Lost or Stolen Card Fraud

When fraudsters use your **lost or stolen card** to make unlawful purchases.

Card-Not-Present Fraud

When transactions are made **without the physical card** by using information like your card number, expiry date and CVV.

Counterfeit Card Fraud

When a **skimming device** is used to duplicate your card information to create a counterfeit card.

Phone Fraud

When fraudsters obtain your card information by **impersonating banks**, **phone companies**, etc.

Shop only on reputable online sites. Look out for the lock icon or 'secure and verified' badge at the bottom of the page.

Keep your card in sight when purchasing in-store and check that the correct card is returned to you.

Never share your card details like expiry date, CVV or PIN with anyone.

Check that the package is intact when you receive a new card. Report any lost or stolen cards to us immediately.

Always shred your card statements, receipts, and cut up expired or damaged cards before discarding them.

Stay vigilant

Fraudsters are getting more creative. Never let your guard down.

SPOT
THE WARNING SIGNS

Are there unauthorised transactions on your card statement?

STOP
SUSPICIOUS ACTIVITY

Never reveal your card details to anyone.

REPORT
THE INCIDENT

The sooner you report it to us, the better the chances of stopping the fraud.

For more fraud prevention tips, visit sc.com/fightingfraud/myaccount

To report a fraud, please call +94 112 480 480