Code of Conduct for Card Operations

Contents

---

1. Preamble

This is a mandatory code of conduct (hereinafter referred to as 'Code') prepared in terms of the Credit Card operational guidelines No. 01/2010 issued by the Central Bank of Sri Lanka for adoption by Credit Card issuing member banks/ institutions (hereinafter referred to as 'Issuer') and/or their associates. It is expected that this code will act as a benchmark service standard in dealings with individual customers. The Code details the obligations the issuers undertake when issuing credit cards and other card products. This code will guide issuer's staff in dealing with customers. The Code is expected to help the credit card users understand their rights and measures they should take to protect their interests. The issuers who adopt this Code will place it on their websites and make copies available to customers on request.

About this Code

As a mandatory document, the Code promotes competition and encourages market forces to achieve higher operating standards for the benefit of the customers. In the Code, `we/our' denotes the issuer. The standards of the Code are governed by the key commitments detailed in section 2.

Unless stated otherwise, all parts of this Code apply to all the credit card products and services, whether we provide them across the counter, over the phone, on the internet and/or by any other method.

Commitments outlined in this Code are applicable under normal operating business environment. In the event of force majeure, it should be clearly understood that we may not be able to fulfil the commitments under this Code.

2. Key Commitments

We commit to:

act fairly and reasonably in all our dealings by;

a. meeting the standards in this Code, for the products and services we offer, and in the procedures and practices our staff/agents will follow.
b. making sure our products and services comply with relevant laws, regulations, guidelines, directions and circulars.
c. ensuring that our dealings with customers rest on ethical principles of integrity and transparency.
d. engaging in lawful and ethical consumer practices.

help the customer understand how our credit card products and services operate by offering the following information in a simple language;

a. what are the benefits to the customer.
b. how the customers can avail of the benefits.
c. what are the costs, fees and charges.
d. whom/how the customer can contact to address their queries.

deal quickly and effectively with customer queries and complaints by;

a. offering channels to route their queries.
b. listening to them patiently.
c. communicating responses to the customers within 5 working days of receipt of complaint/ query.
d. informing the customers how to take their complaint forward, if they are not satisfied with our response.

publicise this Code, by making it available for public access on our website and make copies available to customers on request in English, Sinhala and Tamil.

3. Information (Enabling the customers to choose products and services, which meet their needs)

Prior to issuing a credit card, we will;

a. provide information explaining the key features of our credit card products including;
    - relevant terms and conditions;
    - applicable fees and interest rates;
    - method of calculating minimum amount due and interest;
    - how to avoid or minimize the interest charges and penalty charges;
    - billing and payment procedures;
    - renewal and termination procedures; and
    - any other important information that may be required to operate the card;
b. make the customer aware of the minimum information/ documentation required from the customer to enable us to issue a credit card including the documentation with respect to their identity, address, employment etc., and any other document that may be stipulated by statutory authorities in order to comply with legal and regulatory requirements.
c. verify the details provided by the customer on the credit card application by contacting via telephone and/or visiting through agencies appointed by us for this purpose, if deemed necessary.

We will inform our targeted turnaround times when the customers apply for a product/ service.

We will provide a service guide detailing the terms and conditions, interest and charges applicable, rights and liabilities of the customer if the credit card is lost / misused and other relevant information with respect to usage of the credit card, along with the first credit card.

We will provide our contact details such as telephone numbers, postal address, website/ email address to enable the customers to contact us whenever they need to.We advise the customer to collect all payment receipts to reconcile their monthly statements. If the customer does not recognize a transaction, which appears on the credit card statement, more details will be provided, if requested. In some cases, we may need the customer to provide us confirmation or evidence to prove that they have not authorised a transaction.

4. Tariffs (Interest/ Fees/ Charges)

We will provide our schedule of fees and charges (including interest rates);

a. with the application form,
b. in the welcome pack,
c. when the customer calls on the customer service numbers,
d. on our website, or
e. through our designated staff.

We will clearly explain how we apply interest and/or charges to customer's account using examples, on request, in addition to the information in the credit card statement and the publication available on the website.

Changes in our tariffs

When we change our tariffs (interest rate and/or other fees/charges) on our credit card products, we will update the information on our telephone messages, website, and on the credit card statement, in order to notify the customers at least 10 days prior to implementation of such changes.

5. Sales and Marketing Ethics

Field Personnel

a. Our sales representatives will identify themselves when they approach customers and potential customers for selling card products.
b. In the event of receipt of any complaint from customers, that our representative has engaged in any improper conduct, we shall take appropriate steps for readdress of complaint.

Telemarketing

a. If our telemarketing staff/agents contact the customers over the phone for selling any of our credit card products or with any cross sell offer, the caller will identify himself/herself and advise the customer that he/she is calling on our behalf.
b. It is ensured that customers will be contacted only when the call is not expected to inconvenience the customer. Generally between 0900 hrs and 1900 hrs.
c. Calls earlier or later than the prescribed time period may be placed only when the customer has authorised to do so either in writing or orally.

Telemarketing Etiquette

Our telemarketing staff will follow acceptable tele-calling etiquette as follows;

Pre Call

Calling only on lists that have been cleared by the bank or the bank appointed Direct Sales Agent.

During a Call

a) Identify themselves and our bank, and state reason for the call.
b) Request permission to proceed, if denied permission, apologise and politely disconnect.
c) Always offer to call back on landline, if call is made to a mobile phone.
d) To the extent possible, talk in the language which the customer is most comfortable.
e) Keep the conversation limited to business matters. Never interrupt or argue.
f) Check for the customer's understanding of the 'Most Important Terms and Conditions' if the customer plans to buy the product.
g) Provide their telephone no., their supervisor's name or our bank contact details if requested by the customer.
h) Thank the customer for their time.

Post Call

a) If the customer has expressed lack of interest for the offering, we will endeavour not to call the customer for the next 6 months with the same offer.
b) In the event a customer calls regarding products already sold, the sales staff will direct the

customer to the relevant department/ unit of the bank to handle such queries.

Confidentiality of Customer Information

The sales representatives will respect the customer's privacy at all times. The customer's interest may generally be discussed only with the customer and any other individual/family member such as the customer's accountant/secretary/spouse, if authorised by the customer in writing, by e-mail, by recorded telephone line, by fax or sms.

Training

The sales representatives are provided with the required training and guidance in order to perform their task effectively.

6. Issuance of Credit Card / PIN

We will generally dispatch the customer's credit card to the mailing address mentioned by the customer through courier/ registered post. Alternatively, we shall deliver the customer's credit card to an address under the customer's specific instructions.

If the credit card received by the customer is not activated, the customer can activate the card as prescribed by the Bank.

PIN (Personal Identification Number) whenever allotted, will be sent to the customer separately.

7. Account Operations and Credit Card Statements

To help the customer manage the credit card account and check details of purchases/cash drawings using the credit card, we will offer the customer the facility to receive credit card transaction details either via mail or eStatements. Credit card statement will be generated on a predetermined date of every month which will be notified to the customer.

In the event of non-receipt of credit card statement, we advise the customer to inform us to obtain a copy of the statement, which will be sent within 10 calender days to enable the customer to make the payment in a timely manner.

We will inform the customer of any new services and value additions, that we may introduce from time to time with the option to accept/decline and will indicate the fees/ charges applicable for such new services in advance.

In the event of a cheque deposited to the customer's card account being returned, we will inform the customer of such return within 7 calendar days from the receipt of such unpaid cheques.

We will not unduly penalize the customer if cheques are deposited prior to the payment due date within the time frame prescribed by us, but realized after the due date due to errors/ delays on our part.

We will inform the customer of any proposed upgrade and/or limit enhancement on the customer's account. The customer would be given the option to accept or decline the proposed upgrade and/or limit enhancement within a stipulated time period therein. We expect the customers will carefully read such notifications and respond accordingly.

8. We will advise the customer what can be done to protect the customer's credit card from misuse.In the event the customer's credit card has been lost or stolen, or the customer's PIN or other security information becomes known to a third party, we will, on the customer notifying us, take immediate steps to deactivate the customer's card and take action in accordance with the terms and conditions of the cardholder agreement.

9. Confidentiality of Account Details

We will treat the customer's personal information as private and confidential (even when the individual is no longer a customer). We will not reveal transaction details of the customer's accounts to a third party, other than in the following exceptional cases;

a. if required by law.
b. if requested by the customer in writing, by e-mail, by recorded telephone call, by fax or sms (These requests will be archived for future reference).

c. in order to comply with the law.
d. if in our interests, it requires us to give the information to prevent fraud, for audit etc.

10. Collection of dues

Customer confidence and long-term relationship. In some instances calls would be placed earlier or later than the Our bank's dues collection policy is built on courtesy, fair treatment and persuasion. We believe in fostering prescribed time period of 0900 hrs and 1900 hrs in order to contact the customer regarding payment dues, to ensure smooth operation of the customer's credit card.

Our staff or any person authorized to represent us in collection of dues and/or security repossession will identify himself/herself and interact with the customer in a civil manner.

We will provide the customer with all the information regarding dues and will give sufficient notice for payment of dues.

We will respond to any queries made or clarifications requested by the customer with regard to the customer's dues and recovery letters within 05 working days of receiving such request.

11. Handling of Complaints

Handling of customer complaints internally

- We will have a Complaints Handling Procedure within the organization.
- Our complaints handling procedure including the targeted response times to customer complaints and escalation process, will be displayed on our website.

Making a complaint to the Financial Ombudsman, Sri Lanka

If the customer does not get a satisfactory response to the customer's complaint from us within 30 days and the customer wishes to pursue other avenues for redress, the customer may approach The Financial Ombudsman, Sri Lanka .

Address; No. 143A, Vajira Road, Colombo – 05. Telephone: +94 11 259 5624 Fax : +94 11 259 5626 Email : fosril@sltnet.lk Website : www.financialombudsman.lk

11. Termination of Credit Card

The customer may terminate the credit card by giving notice to us and by following the procedure laid down by us in our terms and conditions of the cardholder agreement after clearing all outstanding dues, if any.

We may terminate the customer's credit card, if the customer is in breach of the cardholder agreement and take necessary action to settle unresolved issues, if any, according to the dispute resolution procedure.

12 . Card Security Awareness

What is on-line Fraud?

When someone poses as a legitimate company to obtain personal data and fraudulently conducts transactions on your existing accounts is online fraud. This is often called "phishing" or "pharming" the most common methods of online fraud are fraudulent emails, websites, and pop-up windows, or any combination of these.

No reputable business will ever email you requesting that you update your personal information, including account or credit card numbers, system passwords or customer identification numbers via a link to their site.

What is Phishing?

Phishing is a scam where Internet fraudsters request personal information from users online. These requests are most commonly in the form of an email from an organization with which you may or may not do business. In many cases, the email has been made to look exactly like a legitimate organization's email would appear complete with

company logos and other convincing information. The email usually states that the company needs you to update your personal information or that your account is about to become inactive, all in an effort to get you to click the link to a site that only looks like the real thing. If you click on the link to go to the phony website and enter all of your information, you've just been the victim of a phishing attack. The fraudsters have just captured all the necessary information to access your accounts online.

What is Pharming?

Pharming is an activity criminals use to redirect users from legitimate websites to fraudulent ones where confidential information such as credit card and bank account numbers are requested.

What is Pretexting?

You receive a phone call from someone who claims to be contacting you from your financial institution. They speak to you about your accounts and personal information in a way that suggests they must be legitimate. However, this person is actually an identity thief who has uncovered some information about you and is looking for more.

Browser Security

Turn Off Auto-Complete

Make sure that the browser is set so that it does not remember your passwords. You can set that option in the settings from one of the menus. The exact location of those settings is different for each browser.

Type Your Banking Site's Address Directly

Don't visit your banking web site from links. Always type the web address into the browser's address bar yourself. This will help reduce the chance of phishing scams where people are redirected to sophisticated fake banking web sites that can look exactly like the real thing. Bookmark your Bank's website address and use this to access the website.

Closing Your Banking Session

Always log out of your account when you are done, and also be sure to close the browser to remove additional information that may be stored in the browser

Check security symbols

When sharing personal information on a website, always look for the padlock symbol in the browser status bar. If this is not present the transmission will occur over a less secure connection.

Check the website URL

Normally the URL begins with the letters "http". However over a secure connection the address should begin with "https".

E-mail Security

Avoid opening any suspicious emails requesting your account information and/or password or mails from unknown senders. If you have opened any suspicious email, do not open any attachment or link it may contain, delete it.

General

After successfully logging into Online Banking, be sure to check the time-stamp for the last successful login & the last login date. Ensure you protect your system by having a Firewall, which protects your PC against intrusion, an Antivirus and Adware/Spyware software program with an auto update feature. Review your account transactions regularly.

Protecting Your Credit / Debit Card

- Never let anyone else use your credit card / debit card
- Immediately sign the back of the new card as soon as it is received
- Always destroy your old, expired cards by cutting them up
- Keep your card in a safe place and treat it as carefully as you treat cash and/or any other financial instrument
- Carefully discard receipts from card transactions and ATMs once you have checked these against your account statement. This will help prevent others acquiring information about you and your cards.
- Make sure you get your card back every time you use it
- Never send your credit card number via e-mail

- Keep your personal information, including mobile phone number, up-to-date so we can contact you if an unusual transaction is detected
- Obtain SMS alert facility, so that you can keep a track on all yours as well as your add-on card holder's transactions then and there
- Check your statements regularly, it is easy to do with Online Services
- Let us know immediately on +94 11 2350000 if you've lost your Card, or think it may be stolen. We will then be able to cancel the Card and prevent fraudulent transactions.

Protecting Your Card PIN / Passwords

- Never keep your PIN in your wallet, purse or diary, or record it in a way that others could understand
- Do not tell anyone else your PIN, password or security information
- Always try to cover your hand when entering your PIN at an ATM to prevent others seeing your number
- Do not choose a PIN that is easily associated with you, ex: – your birth date, phone number or parts of your card number
- If you become aware of, or suspect your card or your PIN has been lost, stolen or disclosed, you should notify us immediately on +94 11 2350000

Tips on Password Security

- Create strong passwords
- Don't use words that can be found in a dictionary
- Don't use the same password for every site
- Do use a mix of upper- and lower-case letters, numbers, and at least one symbol
- Use Different Passwords
- Do not write down Passwords
- Do not store Passwords on Storage Devices
- Do Not Send Passwords through Email

Tips to Shop Wisely Online

Using your Card online is safe and convenient as long as you follow a simple rule. When shopping online, only use "secure" web pages when you enter your Card details. A web page is secure if there is a locked padlock in the lower right-hand corner of your browser or if the address starts with 'https', where the 's' stands for secure. Also, it is your responsibility to practice safe computing (e.g. encryption, virus scanning software, firewall, anti-spy-ware software and other similar safeguards)

- When using your card to purchase on-line, look for reputable Internet stores.
- Check that the on-line merchant or store has a return and refunds policy
- If you have to use a password to access a service, make sure this isn't easily identifiable and don't disclose it to anyone
- If you make an on-line purchase, print out a copy of the transaction for your records. This will make it easier to check against your credit card statement
- Contact DFCC Bank call center on +94 11 2350000 as soon as possible if an unrecognized charge or charges appear on one of your statements

Tips for using Online Banking

- DFCC Bank will never ask Card members to supply personal information or card account details via email / phone.
- Never accept or transfer money if you don't know its source.
- Beware of people/organizations who are asking you to receive funds on their behalf and then transfer it to a named address.
- Beware of phone applications that can steal your personal information from the phone and disrupt your SMS messages.
- Do not install or download applications on your mobile phone from unauthentic websites. Always download from the relevant play store and look for the publisher name.
- Always keep an updated antivirus on your phone and computer to protect your information.

Tips for Using ATM's

- Observe your surroundings before using an ATM

- Do not allow a stranger to assist you while using an ATM.
- Have your card out and ready to use
- Shield the screen and keyboard so anyone waiting to use the ATM cannot see you enter your PIN or transaction amount
- Put your cash, card and receipt away immediately. Count your money later, and always keep your receipt
- If you see anyone or anything suspicious, cancel your transaction and leave immediately
- If anyone follows you after making a transaction, go to a crowded well-lit area and call the Police
- When using a drive-up ATM, make sure all passenger car doors are locked and windows are up
- Do not leave your car unlocked or engine running when you get out to use an ATM
- While many ATM's are available 24 hours a day, some may be open only during local business hours. To be on the safe side, plan your withdrawals ahead of time
- Look out for unfamiliar fixtures on ATM s. These fixtures will not appear to be part of the normal ATM, or are attached to the slot where you insert your card. If you notice something suspicious don't use it and report it to the Bank immediately

Tips for when using the cards overseas

- When you are planning a holiday make sure, you inform your bank on your travel plan along with the updated contact details.
- Obtain SMS alert facility so that you are aware about all transactions made from your card.
- Keep receipts of all transactions performed during your overseas stay, so that you can verify your transactions upon receiving the statement
- Do not keep card and pin together
- Always carry some spare cash with you, in case of an emergency
- Make sure you have the emergency 24-hour telephone numbers for your cards with you, so you can report any theft or loss immediately

How to Dispute a transaction on your Credit / Debit Card

- If you notice any unidentified or unauthorized transaction on your Credit or Debit Card, you may call the bank customer service hot-line for further information on the transaction. If you are still not convinced, you may request to dispute the transaction.
- Any transaction that you disagree with, must be communicated to the bank within 30 days of the transaction date. Any transaction notified to you by the bank via SMS alert is deemed as a transaction acknowledged by you.
- Resolving your dispute may involve a charge-back with the respective merchant and the Acquiring Institute. Such charge-back is bound by the rules and time frames set by respective card scheme network organization.
- If you agree to have performed the transaction, but you require the transaction to be cancelled, or believe that a credit is due to you from the merchant, obtain all supporting documents that would support your dispute case. Always attempt to directly resolve the transaction dispute with the merchant you transacted with, prior to complaining the same to the bank.

13 Feedback and Suggestions

Customers can provide feedback on our services and their suggestions will help us to improve our services. Call on 0112350000 or email to info@dfccbank.com or by mail to Manager Customer Service ,DFCC Bank PLC No 73/5 Galle road Colombo 3