

## Terms and Conditions for the use of Virtual Cards and Mobile Cards

---

### 1. The Visa PayWave™ Facility and MasterCard® contactless Facility

- 1.1 Your contactless-enabled card may be used to carry out card transactions at all Visa or MasterCard point-of-sale terminals and at such other readers or systems as we may from time to time approve.
- 1.2 You may also use the contactless-enabled card to effect card transactions at Visa payWave or MasterCard contactless readers.
- 1.3 You may use the contactless-enabled card to effect any number of card transactions on contactless readers ("**Contactless Transactions**") so long as the value of each Contactless Transaction in Singapore does not exceed:
  - (a) for Visa payWave contactless-enabled cards, SGD200 or such other amount which we may specify from time to time; and
  - (b) for MasterCard contactless-enabled cards, SGD200 for retail purchases and SGD45 for transit related transactions (i.e., bus and train fares).The limit per Contactless Transaction may vary from country to country.
- 1.4 Any usage of the contactless-enabled card at any contactless reader, if permitted by us, shall be subject to such terms and conditions as we, Visa and MasterCard may agree from time to time.

### 2. Virtual Cards and Mobile Cards

#### 2.1 Virtual Cards

- (a) Virtual Cards are only issued to primary cardholders.
- (b) Your Virtual Card is ready for use immediately upon issuance.
- (c) You are required to register for Mobile Banking before you can access your Virtual Card.
- (d) Your Virtual Card details are masked by default in the Mobile Banking app. While the Virtual Card details are masked, you may add the Virtual Card to your Mobile Wallet by following the instructions in your Mobile Banking app.
- (e) To perform any other transaction, you are required to unmask your Virtual Card details by following the instructions in your Mobile Banking app. You will only need to do this once for each Virtual Card while your physical card remains inactive.
- (f) For your security, before your physical card is activated, you will only be able to perform the following types of transactions (as may be updated by us at any time) on your Virtual Card:
  - (i) Mobile wallet transactions that require provisioning from within the Mobile Banking app;
  - (ii) 3DS transactions that require additional security verification by card schemes such as VISA's Verified by VISA and MasterCard SecureCode; and
  - (iii) any other type of transaction that we may notify you of from time to time.

The above limits on transaction types will be lifted upon activation of your physical card.

#### 2.2 Registering, adding and activating Mobile Cards

- (a) You may add a Mobile Card in your Mobile Wallet if you hold a credit card (except HSBC Corporate cards and any other cards we may designate from time to time) issued by HSBC Bank (Singapore) Limited in Singapore, and your card account is in good standing.

- (b) You may add a Mobile Card in your Mobile Wallet by following the instructions of the Mobile Wallet provider (including installation of the latest operating system on your Eligible Device), and the registration and verification flow of your Mobile Wallet.
- (c) When you register a Mobile Card in your Mobile Wallet, you need to login to your Mobile Banking app for verification and activation purposes. For Supplementary Card registration, we will send an SMS message to the Supplementary Cardholder's mobile number registered with us for verification and activation purposes. If we do not have a record of the Supplementary Cardholder's mobile number, we will not be able to send an SMS message to them – they can update their mobile number by visiting one of our branches or by downloading a change of personal particulars form from [www.hsbc.com.sg](http://www.hsbc.com.sg) and submitting the completed form to us.
- (d) We may limit the number of Eligible Devices in which the same card can be added from time to time. Please refer to our latest communications regarding such limit.

### **2.3 Use of Virtual Cards and Mobile Cards**

- (a) You may make and authorise transactions with your Mobile Card where Mobile Wallet is accepted for payment. We will not be responsible if any retailer refuses to accept your Mobile Card.
- (b) To make and authorise a transaction, you may place your Eligible Device near Visa payWave or MasterCard contactless readers, and verify your identity as the Cardholder as determined by the Mobile Wallet provider.
- (c) You cannot use your Virtual Card or Mobile Card for cash withdrawals or cash advances at an ATM or over the counter. Your Virtual Card and Mobile Card cannot be linked to a bank account.
- (d) Transactions made with your Virtual Card and Mobile Card are subject to the credit limit on your card and any limits that certain merchants may specify from time to time. If you are using your Virtual Card or Mobile Card outside Singapore, certain countries may specify transaction limits.

### **2.4 Card Account and credit limit**

- (a) Your physical card, Virtual Card and Mobile Card constitute one and the same card and share the same card account and the credit limit of that card account.
- (b) All Virtual Card and Mobile Card transactions will be billed to the same card statement of the physical card. There will not be a separate statement for your Virtual Card or Mobile Card.

### **2.5 Security**

Wallet provider may recommend from time to time, including the following:

- (a) take reasonable precautions to keep card details and security details relating to your Virtual Card, Mobile Card, Mobile Wallet and Eligible Device (including your Device Passcode, fingerprint and/or any other biometric credentials stored in your Eligible Device and/or any cloud storage platform) safe and to prevent loss, theft or fraudulent use of them;
- (b) safeguard your Mobile Wallet and Eligible Device and keep them under your personal control at all times;
- (c) DO NOT allow anyone else to use or log on to your Eligible Device, Mobile Banking app and Mobile Wallet;
- (d) DO NOT store anyone else's fingerprint or biometric credentials in your Eligible Device;
- (e) DO NOT choose obvious numbers as your Device Passcode (such as Identity Card number, date of birth, telephone number, number with same digits or other that can be easily guessed or identified by shoulder surfing) or tell anyone else your Device Passcode or write down or keep your Device Passcode close to your Eligible Device;
- (f) DO NOT install or launch Mobile Banking app or Mobile Wallet in a smartphone or other device with any pirated, hacked, fake or unauthorised application or where the software lockdown has been overridden (such as a "jailbroken" or "rooted" smartphone or device);



- (g) change your Device Passcode regularly and use an alphanumeric code for your Device Passcode;
- (h) if you have already set up access to your Eligible Device by way of a Device Passcode or fingerprint or other biometric credentials, review this and ensure that you change any Device Passcode that can easily be guessed or that has already been shared with anyone else and delete any fingerprint or other biometric credentials that is not your own;
- (i) delete your Mobile Banking app as well as Mobile Card from the Mobile Wallet before you dispose of your Eligible Device or pass your Eligible Device to someone else (whether temporarily or otherwise); and
- (j) remove the Mobile Card from the Mobile Wallet upon cancellation of your Mobile Card.

## 2.6 Fees and charges

- (a) All applicable interest, fees and charges that apply to your card will also apply to the Virtual Card and Mobile Card.
- (b) Your mobile phone service provider, telecommunications provider, retailer and/or the Mobile Wallet provider may impose fees and charges in relation to your adding, activating or using the Virtual Card or Mobile Card or for making transactions using your Mobile Wallet and the Mobile Card. Please refer to them for further details.

## 2.7 General matters

If you have any questions or complaints about your card, please contact us at 1800-HSBC NOW (4722 669) from Singapore, or (65) 64722 669 from overseas. If your question or complaint is about the Mobile Wallet, please contact your Mobile Wallet provider.

## 2.8 Definitions

- (a) “**contactless reader**” means a point-of sale device at which contactless-enabled cards may be used to execute card transactions, either by tapping the contactless-enabled card against the reader or by waving the contactless-enabled card on a contactless basis over or against such reader, without requiring any signature, PIN or other authentication on your part as the cardholder
- (b) “**Device Passcode**” means the access passcode of your Eligible Device.
- (c) “**Eligible Device**” means such model of smartphone, tablet or other device (such as watch) with Mobile Wallet function in which a Mobile Card can be registered and added, as designated by us from time to time.
- (d) “**Mobile Card**” means a digital version of your HSBC Credit Card which you add in the Mobile Wallet of your Eligible Device.
- (e) “**Mobile Wallet**” means a wallet application installed in an Eligible Device in which your Mobile Card is added.
- (f) “**Virtual Card**” means a digital version of your HSBC Credit Card which you can access in the Mobile Banking app.

## 3. Changes to these terms

3.1 We live in a rapidly changing world. Sometimes this means we need to update these terms and conditions. These updates include amendments to the terms and features applicable to Contactless Transactions, Virtual Cards and/or Mobile Cards.

3.2 We may amend or supplement these terms and conditions, if it is reasonably necessary to:

- (i) reflect changes to our operational costs, business operations or systems and processes, or our arrangements with third parties;
- (ii) give effect to:
  - (a) applicable law, rule, regulation;
  - (b) a change, recommendation, order, requirement, notice, direction, code, circular or guidance issued by any regulatory, supervisory, governmental, statutory authority, stock exchange, self-regulatory, or resolution body having jurisdiction over us or a court of competent jurisdiction;
- (iii) reflect changes to industry or market conditions or practice;



(iv) align with standards or expectations including in respect of:

- (a) banking and financial services practices;
- (b) environmental, social and governance practices;
- (c) consumer and investor protection practices;
- (d) cyber, digital, technology (including financial technology (FinTech)) practices e.g., those relating to crypto-assets, digital assets, virtual assets, asset tokenisation and artificial intelligence (including generative artificial intelligence and machine learning);
- (e) operational resilience and data management practices; or
- (f) taxation and transfer pricing practices; or
- (g) otherwise protect our legitimate interests.

3.3 To the extent reasonably practicable, we'll give you reasonable notice of any changes to these terms and conditions before such terms and conditions take effect.

3.4 We can choose how to give this notice to you. This may include:

- (i) contacting you directly (through mail, email, post or via mobile);
- (ii) placing signs or notices at our branches;
- (iii) publishing the change on our website; and/or
- (iv) using any other method we think is reasonably appropriate.

3.5 If you don't agree with a change, you can cancel your existing credit card, after paying all amounts you may owe us.

**4** These terms and conditions are governed by the laws of the Republic of Singapore and the parties submit to the non-exclusive jurisdiction of the courts of Singapore.

**5** All information is correct at the time of publishing or posting online.