TERMS AND CONDITIONS (TERMS) FOR THE USE OF YOUR CARD ON A STANDARD BANK-APPROVED DIGITAL WALLET

1. **General**

1.1 Important clauses that may limit our responsibility or involve some risk for you are in bold. Please read them carefully.

1.2 The Terms are between you and us, **the Standard Bank of South Africa Limited** (**Standard Bank, we, us** or **our**). When we mention **you** or **your**, we refer to the person we have approved as the authorised holder of a qualifying Standard Bank card (**Card**).

1.3 A **wallet** is a mobile application incorporating a digital wallet, as approved by us, that allows you to make payments to any merchant that supports and accepts the wallet, using a Card/s enrolled (registered) in your name and activated on the wallet. **You will know that a wallet is approved by us as you will be requested to accept the Terms before you can enrol your Card on the wallet.**

1.4 You will only be able to use the wallet if your smartphone, tablet, wearable or other device (**device**) is compatible with your wallet.

1.5 **The Card terms apply to and must be read together with the Terms. You must comply with both the Terms and the Card terms.**

1.6 **Unless the Terms state otherwise, your Card terms will continue to apply to the enrolment or use of any Card through the wallet.**

2. **Your card on the wallet is separate from your plastic card**

2.1 Once you have enrolled and activated a Card on your wallet (which is then referred to as a **Token**), it exists independently and separately from your plastic Card. This Token can then be used to pay for transactions wherever your wallet is accepted.

2.2 **This also means that if your plastic Card is reported as lost, stolen or compromised (you suspect that someone may have unauthorised access to or use of your Card details), or if it expires, your corresponding Token will not be deleted. To delete the Token yourself you must use the wallet. If you cannot, you can ask us to do it for you, for example in the instances set out in clause 5.1 below.**

2.3 **For certain wallets, such as Apple Pay or Google Pay, we will automatically update your existing Token with the new Card details as soon as these are generated. This process could happen before your new Card has even been delivered to you. For other wallets, such as Samsung Pay, Garmin Pay and Fitbit Pay, you will have to update your Token with the new Card details once you have received them.**

3. **Using a token to pay for a transaction**

3.1 Once you have enrolled and activated your Card on your wallet (this is called **provisioning**) and the Token has been created, authentication is managed within the wallet. This means we will not take additional steps to authenticate you as we do when you pay with a Card, such as asking for a card PIN and/or a signature (when you use your Card in person) or a one-time PIN or similar code (when you use your Card at a website or through a mobile app).

3.2 We therefore assume that you have authorised all transactions where your Token is used as a method of payment, **even if the transaction took place without your knowledge or consent or was not authorised by you**.

3.3 **This means that, unless you notified us beforehand that your Token is being used or is about to be used without your knowledge or consent, or that your device, wallet and/or security codes (as set out in clause 4.1 below) have been compromised, or unless you took proactive steps to delete the Token yourself immediately, you are liable for all losses related to that transaction, even if another wallet was used. (If your Card details and security codes have been compromised, a fraudster could use this information to enrol and activate your Token in their wallet and then use the Token to make payments to any merchant that accepts it.)**

3.4 We may stop supporting the use of the Token on specific wallets at any time.

4. **Keeping your device, token and other information secure**

4.1 You must take all necessary steps to prevent the unauthorised or fraudulent use of your device, wallet, Token/s and any confidential code, username and password, card PIN, security token, access code, pattern and other information that you use when you pay with your Token or when you access your wallet (collectively called **security codes**).

4.2 You must comply with all security guidelines provided to you. For example:

4.2.1 **Protect and keep your security codes confidential – there is no reason for any person, including our staff, to use or know them.**

4.2.2 **Immediately let us know if you suspect that your security codes have been compromised (through the call centre or at a branch near you) and either delete the Token yourself or ask us to do it.** This also applies where you have inadvertently shared your security codes with a third party, through "**vishing**" (when a fraudster pretending to be a bank or your mobile network operator convinces you to share your security codes with them), "**phishing**" (when you receive an email requesting you to click on a link to a fraudulent website) or "**smishing**" (when you receive an SMS purporting to be from a bank and requesting your personal information or security codes).

4.2.3 Check your Card and wallet statement regularly for any suspicious or unauthorised transactions and let us know immediately if there is an issue.

4.2.4 Always delete your Token/s from your old device if you plan to change, replace or destroy it, or send it in for repair.

4.2.5 Keep your device or wallet security software up to date.

4.2.6 Take reasonable precautions to keep your device safe and secure. **We strongly recommend that you keep the device in your possession and protected with an access code or biometrics (Face ID or Touch ID).**

4.2.7 Keep your contact details up to date and let us know immediately if they change.

4.2.8 Immediately let us and your mobile network operator know if your device is lost or stolen or if you believe you have been a victim of a SIM swap (in other words the SIM card connected to your mobile phone number is changed without your knowledge or consent). You must also report the incident to the police as soon as possible.

4.2.9 Immediately change your security codes if you suspect that your email address, mobile number or other personal information has been compromised or if your device has been stolen. If this impacts the contact details we have for you, you must also let us know immediately about the compromise or theft. (This would impact the products or services that you have with us, including our Mobile Banking App, Internet Banking, and MyUpdates as well as the contact details we use to contact you for fraud prevention and information purposes.)

4.3 **If you fail to keep your device/s, Token, security codes or other information secure, this may result in the unauthorised use of the wallet, your Token/s, your Card account, any other card/s (digital or plastic) or bank accounts linked to the Card account or other information and you could suffer losses because of this.**

5. Deleting the token

5.1 You can only stop your Token from working in the wallet if you remove the Token from the wallet or if you ask us to do so on your behalf. For Apple Pay and Google Pay, you can also switch off the functionality through the Standard Bank Mobile Banking App.

5.2 You should delete the Token if you no longer wish to use it or the wallet, or if you suspect that the Token has been or could be compromised, for example because your device has been lost or stolen, or your Card details and/or security codes have been compromised. If you cannot delete the Token yourself, you can ask us

to do it for you. **It is very important to delete the Token when it has been compromised, because if a fraudster has already managed to enrol and activate your Token in their wallet, they will continue to use your Token when it is updated automatically with the new Card details, as in the case of Apple Pay and Google Pay (see clause 2.3 above).**

5.3 **Except where your Card account is closed, we will only delete the Token in the wallet if you ask us to do it.**

5.4 **If you want us to delete the Token for you, you must phone our call centre or go to any branch. (When you cancel your Card through a Standard Bank ATM, Internet Banking or our Mobile App, it does not mean that the Token is also cancelled.)**

6. Fees and costs relating to the wallet

We will not charge you extra fees when you use your Token through the wallet (all the usual Card fees still apply). However, other parties (including the wallet provider and any mobile network service provider) may charge you for the use of the wallet.

7. The wallet provider is solely responsible for the wallet

7.1 When you register for a wallet, you accept the wallet provider's terms and conditions as well as their data security and privacy policies. **We are not responsible for the security, function, content or any other aspect of a wallet. The wallet provider's terms and conditions are separate from these Terms. It is your responsibility to read the wallet provider's terms and ensure that you are comfortable accepting them before enrolling and activating your Card/s on or using a Token/s through the wallet.**

7.2 Any information collected by a wallet provider through your registration and use of the wallet, including personal information, is subject to the wallet provider's terms and conditions and their data security and privacy policies. Such information is not governed by our data protection policy, our general terms and conditions or these Terms. **We are not responsible for any loss you suffer in connection with a wallet provider's use of your information.**

7.3 A wallet provider is solely responsible for the operation of the wallet. However, if you have any questions about how to use a wallet or any problems with a wallet, you can contact our Client Contact Centre for help.

8. Sharing information with third parties

For you to use your Token through the wallet we may need to share your personal information with the wallet provider and any third party that provides services to the wallet provider and to us in respect of the wallet services. **By using your Token through the wallet, you are giving consent for us to share your information with these parties.**

9. **Where we are not liable**

9.1 **We do not give any guarantee that a wallet will be accepted by all merchants or that it will work as a payment method.**

9.2 **In addition to any limitation of our liability as set out in the Card terms and except as provided for in law, we are also not liable for any loss or inconvenience you suffer if:**

9.2.1 **you breach these Terms;**

9.2.2 **the loss is caused by circumstances beyond our control or is indirect or consequential;**

9.2.3 **the wallet provider is unavailable or does not work for any reason;**

9.2.4 **you are unable to enrol or activate your Card on the wallet or experience any other technical issue;**

9.2.5 **a merchant refuses to accept wallet payments; or**

9.2.6 **there is a security breach affecting any information stored in the wallet or sent from your wallet provider, or information on your Token (this is the wallet provider's responsibility).**