Virtual Card
TERMS AND CONDITIONS

Date document last updated: 01 June 2024

These Terms and Conditions must be read in conjunction with the relevant product specific terms and conditions, as well as the Remote Banking agreement, where applicable, which can be found on our website. The Global Account Virtual Card Terms and Conditions can be found in the Global Account Terms and Conditions on our website.

1. You may use the Virtual Card(s) for:

1.1. Digital Payments via any of the supported Digital Wallets (Apple Pay, Google Pay. etc.); or

1.2. Subscriptions and other recurring payments; or

1.3. eCommerce transactions:

1.3.1. In-App purchases; or

1.3.2. Scan to Pay transactions and any other type of transaction as determined by the Bank from time to time.

2. Your Virtual Card(s) are automatically activated when created.

3. **There is a limitation of up to ninety-nine Cards - a combination of Physical Card(s) and Virtual Card(s), that you may have/create on your account during the life span of your account.**

4. The above limitation includes additional, renewal, replacement, cancelled, removed, and deleted card(s) for both physical card(s) and Virtual Card(s).

5. You may have a physical card and Virtual Card(s) at the same time.

6. You may use one Virtual Card for multiple eCommerce transactions, In-App purchases, streaming services, subscription payments, QR payments via Scan to Pay on the RMB Private Banking App and contactless Tap to Pay transactions on supported Digital Wallets, without the need to create separate Virtual Card(s)

7. Your Virtual Card(s) has a dynamic CVV which changes **frequently.**

8. Should you cancel your physical card linked to your transactional account and/or credit facility on your RMB Private Banking App, you may replace it with a Virtual Card(s).

9. You will have the ability to block and unblock your Virtual Card(s) on the RMB Private Banking App and your Virtual Card(s) can be kept in a blocked state and only unblocked when required for use.

10. Your Virtual Card(s) can be permanently deleted on your RMB Private Banking App. It is your responsibility to ensure that you either block or delete your Virtual Card(s) should you no longer want to make use of it.

11. Your Virtual Card(s) is **valid for 5 years** from the month of its creation.

12. The spend threshold on your Virtual Card(s) is dependent on available funds in your corresponding transactional account and/or credit facility.

13. Virtual Card(s) maximum spend limits are pre-determined and cannot be customised. These maximum limits may be defined by the Bank from time to time. You can customize your Virtual Card(s) limits for different transactions below the maximum spend limit via the RMB Private Banking App. The maximum spend limit for the card and your customized limits per type of transaction on your Virtual Card(s) will not affect the limits set on your Physical Card, and vice versa.

14. Your use of your Virtual Card(s) must not in any way be a contravention of the Exchange Control Regulations or any similar regulations promulgated from time to time and you must comply with all relevant Exchange Control requirements.

15. To create a Virtual Card(s), you must have an FNB Easy Zero account, FNB Easy account, FNB Current account, FNB Global Account, FNB Fusion account, FNB Credit Card account, FNB Business Current account, RMB Private Bank Current account, RMB Private Bank Fusion account or RMB Private Bank Credit Card account as well as the latest version of the RMB Private Bank App loaded on your device(s).

You may be required to use a Personal Identification Number ("PIN") when performing a contactless transaction via a near-field communication/connectivity (NFC) enabled Device on RMB Pay.

16. The Virtual Card(s) can only be accessed by way of your RMB Private Banking App. You must take the necessary precautions to safeguard your device(s) and access credentials, accounts, cards, and banking channel access mechanisms, such as

passwords, Card PINs and One-Time-Pins(OTPs).

17. All Virtual Cards you create on your banking app linked to your accounts are for your personal use and their details should not be shared with anyone else.

18. YOUR OBLIGATIONS

18.1. All Virtual Cards you create on the RMB Private Banking App linked to your accounts are for your personal use and their details should not be shared with anyone else.

18.2. Any Third-Party digital wallet(s) and any other payment service(s) that you use and access on your Device(s) with your Bank card are not part of the Bank's services and are not controlled by the Bank.

18.3. If you are younger than 18, you must get your parent's or legal guardian's consent to use the Third-Party digital wallet(s) and any other payment service(s).

18.4. For security reasons, you must ensure that your Device is always kept in your possession, as the same caution needs to be taken with your Device as with your physical Bank card. You are personally responsible for the security of and access to your Device, including the safeguarding of your personal security code(s). It is therefore your responsibility to secure your Device and its contents through the security features made available to you by the Third Party. You will be liable for any Third-Party digital wallet(s) and any other payment service(s) transactions made with your Device even when you are not in possession of your Device, whether such transactions were made with or without your authorisation, by any person known to you or any Third-Party having possession of your Device.

18.5. If your Device is lost or stolen, you must notify the Bank immediately. Should you fail to do so the Bank will not be held liable for any losses you may incur before you notify us. You will be liable for any transactions made with your Device using Third-Party digital wallet(s) and any other payment service(s) when your Device is lost or stolen, and you have not notified the Bank.

18.6. **TAKE NOTE:** Your access information is the only way we can know you are who you say you are when you transact, you must keep your access information secret and safe and you must not allow anybody to use your access information. You must never give or show your Device Credentials and /or Sensitive Card Credentials to any person, including our employees or anyone claiming to work for or represent us in any way. You must never respond to requests to enter or "confirm" your Device Credentials and / or Sensitive Card Credentials sent to you via an email, SMS, or instant message. This is known as "phishing" where the sender tries to trick you into giving them your confidential information by pretending a communication was sent from us. We will never ask you to give us your sensitive secret information, including Device Credentials and/or Sensitive Card Credentials by email, SMS, instant message or even over the telephone. You must not respond to these "phishing" messages, as the Bank will not be held responsible for any loss you may suffer. Fraudsters will also attempt to call you to get your Device Credentials and/or Sensitive Card Credentials ("Vishing"). You can also receive an SMS, email or instant message with a link which will take you to a fraudulent website requesting the capture of your Sensitive Card Credentials ("Smishing"), and you should never interact with anyone who attempts to obtain information via "Vishing" or "Smishing".

18.6.1. You will not be liable for unauthorised and fraudulent transactions that occur on the corresponding Bank account, because of the loss or theft of your Device provided that you inform the Bank of the Device being lost or stolen immediately or as soon as is reasonably possible**.**

18.6.2. **You will be liable for PIN-based transactions or transactions approved by way of the Bank Application and/or the use of your Device(s), in any manner, including Devices/services you have authorised to make use of your Bank card for payment where applicable.**

18.6.3. Third-Party digital wallet(s) and any other payment service(s) (such as certain financial apps that help you track your spending across different financial institutions but not limited to) may ask you to enter your Device Credentials and/or Sensitive Card Credentials to use their service, and if you do so, you may put yourself at risk as the Third-Party may be able to access information about your accounts, instructions, transactions and other confidential information. If you are defrauded because you used a Third-Party digital wallet(s) and any other payment service(s), we will treat this as a voluntary compromise of your Device Credentials and/or Sensitive Card Credentials and confidential

information and will not be legally responsible to you or any other person for any loss or damage you or they suffer.

18.7. The same Device Credentials and/or Sensitive Card Credentials can be used to access different Third-Party digital wallet(s) and any other payment service(s). This means that if your Device Credentials and/or Sensitive Card Credentials are disclosed to a Third-Party you can be defrauded across many of the Third-Party digital wallet(s) and any other payment service(s). You must immediately contact us if you know or even suspect that your Device Credentials and/or Sensitive Card Credentials have been compromised to ensure that your profile is secured.

18.8. By allowing an Authorised User to access your profile with your Device Credentials and/or Sensitive Card Credentials, you give that person the authority to act as your agent. This means that anything the Authorised User does or does not do, will bind you or be attributed to you. In other words, we will treat anything they did or did not do, as if you personally did it or did not do it.

18.9. You must ensure that your Device which you use for instructions or transactions is always in your possession and protected with an additional access code, password or pattern lock.

18.10. You must not keep your Device Credentials together with your Sensitive Card Credentials and other documents. Do not store your Device Credentials and/or Sensitive Card Credentials on the equipment you use to access our interfaces or channels. For example, never store your Sensitive Card Credentials and/or Device Credentials with or near your mobile, computer, and Devices. For security purposes, we recommend that you memorise your Sensitive Card Credentials and/or Device Credentials.

18.11. If you do not notify us of an unauthorised transaction, you agree that we can treat the transaction as correct and hold you legally responsible for the transaction as if you had done or approved it.

18.12. You must report the suspicious or unauthorised transactions to us immediately when you become aware that a suspicious transaction has taken place and you must open a case at the nearest police service or law enforcement agency. We will investigate the suspicious or unauthorised transaction(s) that you report to us, and it may be necessary as part of our investigation, for you to supply us with certain information, including a police services or law enforcement agency case number. You must co-operate with us and the authorities in any investigation and provide us with accurate information. Based on the outcome of our investigation, we may refund you subject to these Terms and Conditions:

18.12.1. Note: This section does not apply if the fraud or suspected fraud was committed by Authorised Users.

19. THE BANK'S OBLIGATIONS

19.1. We reserve the right to block your access to our interfaces or channels at any time to maintain or restore security if we reasonably believe that your Device Credentials and/or Sensitive Card Credentials were or may be obtained or are being used or may be used by an unauthorised person.

19.2. The Bank reserves the right to cease supporting any Third-Party digital wallet(s) and any other payment service(s) without notice to you.

19.3. The Bank's General and Product Specific Terms and Conditions and Virtual Card Terms and Conditions apply (available on the Bank's website).

20. THIRD-PARTY DIGITAL WALLET(S) AND ANY OTHER PAYMENT SERVICE(S)

20.1. Payments may be effected via the use of Near-Field Communication (NFC) or ecommerce/in-app payment functionality on a Third-Party digital wallet(s) and any other payment service(s). Payments using NFC or ecommerce/in app payment functionality on a Third-Party digital wallet(s) and any other payment service(s) may only be available at selected contactless merchants.

20.2. Your use of a Third-Party digital wallet(s) and any other payment service(s) this means that you accept any Third-Party terms and conditions depending on the choice of Third-Party digital wallet(s) and any other payment service(s). You alone are responsible for obtaining the terms and conditions or rules that apply to you and the Third-Party digital wallet(s) and any other payment service(s). Make sure you read and understand these terms and conditions and ensure that you are comfortable before engaging in any transactions. You take sole responsibility and assume all risk arising from your interaction with or use of any Third-Party digital wallet(s) and any other payment service(s). You are responsible

for obtaining, reading and understanding the privacy policy that applies to your use of any Third-Party digital wallet(s) and any other payment service(s).

20.3. The Bank has no control over such Third-Party digital wallet(s) and any other payment service(s). We will not be a party to any disputes that may arise or occur between you and the Third-Party.

20.4. The Bank is not responsible for the accuracy, reliability, availability, effectiveness, or correct use of information you receive through the Third-Party digital wallet(s) and any other payment service(s). This may include you compromising your Device Credentials and/or Sensitive Card Credentials.

20.5. We provide this functionality only as a convenience. The Bank is not responsible for the products, services, or other content available on the Third-Party digital wallet(s) and any other payment service(s). The Bank will not be responsible for any loss or damage you may suffer, whether directly or indirectly, because of a Third-Party digital wallet(s) and any other payment service(s). You hereby agree to indemnify and hold the Bank harmless for any loss or damage you may suffer, or cause, in this regard**.**

21. Budget facility transactions are not currently supported on your Virtual Card(s).

22. You can earn eBucks on all qualifying transactions using your Virtual Card(s). For more information about eBucks rewards visit www.eBucks.com.

23. Not all merchants may accept a Virtual Card transaction. The Bank will not be held liable should a Virtual Card transaction not be accepted by a Merchant.

24. Subscription transactions will use the Virtual Card(s) CVV for the first transaction or registration activity to authenticate the card and account. Recurring subscription transactions will be validated using only the Virtual Card number and expiry date.

25. We are not liable for any direct or indirect loss suffered by you arising from any malfunctions, failure, delay or service channel and shared network that may occur in relation to the use of the Virtual Card(s).

26. Your Virtual Card(s) transaction history will be available on your Banking App as well as your Account Statement. There maybe a delay in your Virtual Card(s) transaction reflecting on your transaction history.

27. Any payment that we have made to a supplier for any transaction is final and irreversible, unless:

27.1. allowed by the VISA rules and regulations, as published by VISA from time to time on the VISA website "http://www.visa.co.za", or there was duplication in payment due to human and/or technical error by the supplier.

27.2. you can provide proof (e.g. written, call recording etc.) that you attempted to resolve the dispute with the supplier according to the agreement between you and the supplier.

28. You must report or log a dispute or fraud claim on your RMB Private Banking App or call the Fraud Help Desk at:

28.1. Inside South Africa: 087 575 9444; or

28.2. Outside South Africa +27 11 369 2924

29. INTERPRETATION

In this Terms and Conditions, the following words will have the following meanings:

29.1. The words, '**you**' or '**your**' means the Bank account holder and/or their Authorised User/s.

29.2. The words '**us**', '**we**' or '**our**' only means the Bank.

29.3. '**Days**' will mean calendar days unless qualified by the word '**business**'. A '**business day**' means any day other than a Saturday, Sunday, or official public holiday as gazetted or declared by the government of the Republic of South Africa.

30. Definitions

30.1. **"Authorised User"** means any person/s the account holder appoints to use the Third-Party digital wallet(s) and any other payment service(s) on their behalf (e.g., to do transactions).

30.2. "Bank" means "us," "we", "our" "FNB" (First National Bank, a division of FirstRand Bank Limited) or "RMB Private Bank" (Rand Merchant Bank, a division of FirstRand Bank Limited).

30.3. **"credit provider, the bank, we, us, our" means** FirstRand Bank Limited, a registered bank, registration number 1929/001225/06.

30.4. **"cardholder, you, your, I"** means the Primary cardholder to whom we have issued the Virtual Card(s).

30.5. **"CVV"** means the card verification value code which appears at the back of your Virtual Card(s).

30.6. **"Device(s)"** includes but is not limited to, a piece of mechanical or electronic equipment, associated firmware, applications, software, websites, APIs, wearables, products, and services.

30.7. "**Device credentials"** includes but is not limited to password, passcodes login details used as a method of accessing or authorizing a transaction through a device.

30.8. **"FNB"** means First National Bank, a division of FirstRand Bank Limited.

30.9. **"PIN"** means the personal identification number linked to the card and/or a One Time PIN ("OTP").

30.10. **"Sensitive Card Credentials"** means the card number, expire number, CVV, PIN and OTP's.

30.11. **"Virtual Card(s)" means** a digital card that can be used for eCommerce transactions, In-App purchases, streaming services, subscription payments, QR payments via Scan to Pay on the RMB Private Banking App and contactless Tap to Pay transactions on supported Digital Wallet. The use of the Virtual Card Terms and Conditions which must be read in conjunction with the product terms and conditions, as well as the Remote Banking agreements, where applicable, and may be viewed on the RMB Private Banking website.