



Digital Wallet Third-Party Applications or Services Terms and Conditions

Last amended: September 2026

These Terms and Conditions are applicable when you register to use or access a Third-Party digital wallet(s) and any other payment service(s).

1. INTERPRETATION

In this agreement, the following words will have the following meanings:

- 1.1. The words, '**you**' or '**your**' means the Bank account holder and/or their Authorised User/s.
- 1.2. The words '**us**', '**we**' or '**our**' only means the Bank.
- 1.3. '**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 Botswana.

2. DEFINITIONS:

- 2.1. "**Authorised User**" means any person(s) the account holder appoints, in accordance with the Digital Wallet Third Party Terms and Conditions, to use third-party digital wallets and other payment services on the cardholder's account (e.g. to do transactions).
- 2.2. "**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).
- 2.3. "**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."
- 2.4. "**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.
- 2.5. "**Digital wallet**" means is an electronic platform that securely stores a user's payment credentials such as bank cards (debit/Credit) and enables them to make fast, seamless, and cashless transactions across multiple channels, including online, in-app, and in-store (POS/Swiping machines).
- 2.6. "**Sensitive Card Credentials**" means the card number, expire number, card verification value (CVV), personal identification number (PIN) and one-time passwords (OTP's).
- 2.7. "**Third-Party**" means any individual or entity other than the Bank (Swoo Pay and Google Pay).
- 2.8. "**Phishing**" is where the sender tries to trick you into giving them your confidential information by pretending a communication was sent from us.
- 2.9. "**Vishing**" is a scam where someone calls you, pretending to be from a trusted company (like your bank), to trick you into sharing your personal or banking information.
- 2.10. "**Smishing**" is a scam where someone sends you a fake text message pretending to be from a trusted company to trick you into sharing your personal or banking information.



3. TERMS:

- 3.1. Make sure you read and understand these terms and conditions and ensure that you are comfortable before engaging in any transactions.
- 3.2. You must have a physical card and Digital Card(s) at the same time.
- 3.3. To link your Card(s) to a Digital Wallet(s), you must have either one of the following accounts: an FNB Future Save Account, FNB Future Forward, FNB Poloko account FNB Smart account, FNB Gold account, FNB Youth Account(FNBY & FNBY Next), FNB Islamic account, FNB Staff account, FNB student Account, FNB Premier account, FNB Private account, FNB Global Account, FNB Credit Card account, FNB Business Current account, and new bank account products approved and introduced by FNB Botswana in the future, as well as the latest version of the FNB Banking App loaded on your Device(s).
- 3.4. You may be required to use a Personal device ("PIN")/ Personal Device Passcode/Biometrics when performing a contactless transaction via a near-field communication/connectivity (NFC) enabled Device.
- 3.5. You will also be required to capture your Bank Card PIN on the terminal/POS if exceed certain payment threshold in addition to the above.
- 3.6. Digital 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 customise your Digital Card(s) limits for different transactions below the maximum spend limit via the FNB App.
- 3.7. Should you cancel your physical card linked to your transactional account and/or credit facility on your FNB Banking App, it will be cancelled on the digital wallet as well.
- 3.8. You will have the ability to block and unblock your Digital Card(s) on the FNB Banking App, and your Digital Card(s) can be kept in a blocked state and only unblocked when required for use.
- 3.9. Your Digital Card(s) can be permanently deleted on your FNB Banking App. It is your responsibility to ensure that you either block or delete your Digital Card(s) should you no longer want to make use of it.
- 3.10. Your Digital Card(s) will remain valid under the following conditions:
 - 3.10.1. From the date of creation until the expiry date of the linked physical debit or credit card (old card), if the re-issued physical debit or credit card has not been activated before expiration date of the old card.
 - 3.10.2. From the date of creation until the expiry date of the re-issued physical debit or credit card, if the re-issued physical debit or credit card was activated before the previous card expired.



- 3.10.3. From the date of creation until the expiry date of the replacement of the physical debit or credit card that was created due to initial/previous card being damaged.
- 3.10.4. From the date of creation until the date of the linked physical debit or credit card was reported as lost, stolen, or compromised due to fraudulent activity, resulting in the cancellation of the physical debit or credit card.
- 3.11. The spend threshold on your Digital Card(s) is dependent on available funds in your corresponding transactional account and/or credit facility.

YOUR OBLIGATIONS

- 3.12. You agree that by accepting these terms, you are authorising your Sensitive Card Credentials to be added and used on a Third-Party digital wallet(s) and any other payment service(s), to a new Device to make payments and it is your responsibility to ensure that you are not authorizing an unknown Device, service, or individuals to use your Sensitive Card Credentials.
- 3.13. You acknowledge that 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.
- 3.14. Where the card is linked to a Youth Account, authorisation to link the card to Third-Party digital wallet(s) must lie with the parent or legal guardian associated with the account.
- 3.15. 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.
- 3.16. 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.
- 3.17. 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, pattern lock and security biometrics (face id , fingerprint reader).
- 3.18. 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.
- 3.19. 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.

3.20. 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 when you have not notified the Bank.

3.21. **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.

3.22. **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.**

3.22.1. 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.

3.22.2. You must not respond to these “phishing” messages, as the Bank will not be held responsible for any loss you may suffer.

3.22.3. Fraudsters will also attempt to call you to get your Device Credentials and/or Sensitive Card Credentials (“Vishing”).

3.11.4 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 and you should never interact with anyone who attempts to obtain information via “Vishing” or “Smishing”.

3.23. 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 have informed the Bank of the Device being lost or stolen immediately or as soon as is reasonably possible.

3.23.1. **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.**

3.23.2. **SECURITY OF ACCESS INFORMATION**

3.23.2.1. 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.

3.23.2.2. 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.

3.23.3. BREACH OF INFORMATION

3.23.3.1. 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.

3.23.4. REPORTING TRANSACTIONS

3.23.4.1. 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.

3.23.4.2. You must log all disputes within 90 days from the day of the suspected transaction. 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.

3.23.4.3. If you do not notify us of an unauthorised transaction within 90 days, 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. **Note: This section does not apply if the fraud or suspected fraud was committed by Authorised Users.**

4. THE BANK'S OBLIGATIONS

- 4.1. 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.
- 4.2. The Bank reserves the right to cease supporting any Third-Party digital wallet(s) and any other payment service(s) without notice to you.
- 4.3. The Bank's General and Product Specific Terms and Conditions and These Terms and Conditions apply (available on the Bank's website).

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

- 5.1. 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.
- 5.2. 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). 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).
- 5.3. 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.
- 5.4. 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.



5.5. 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.

END