FNB Zambia Remote Banking Terms and Conditions

Date last amended: September 2023

This important document sets out the rights and duties between you and First National Bank Zambia Limited (FNB) division of FirstRand Bank Limited, with registration number 2008/72041 ("the Bank") in relation to the use of the Bank's self-service interfaces which may be branded as interfaces from FNB. This agreement applies to you if you use any of the following self-service Banking interfaces: Online Banking, Cellphone Banking, .mobi, the Banking App. Read this document carefully. You must seek independent advise if you do not understand any part of this document.

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

The words, "you" or "your" means the account holder and their authorised user/s. An authorised user is any person/s the account holder appoints to use the self service interfaces on their behalf (e.g. to do transactions).

The words "us," "we" or "our" means the Bank. Before you can use the self- service interfaces which include Online Banking, Cellphone Banking, the Banking App and .mobi (collectively called "self- service" interfaces)

If you are younger than 18, you must get your parent's or legal guardian's consent to use the self service interfaces.

When does this agreement start?

This agreement starts as soon you do any of the following:

- register to use any of the service interfaces;
- get access to be able to use any of the service interfaces; • actually use any of the service interfaces;

1. THIRD PARTY RELATIONSHIPS AND ADDITIONAL TERMS AND CONDITIONS

(a) Other terms & conditions that also apply to you

This agreement applies along with the other terms & conditions of the Bank that govern your accounts, our services and our relationship with you. Certain of the products and services that we make available to you on the service interfaces, including those provided by third parties, may have their own terms & conditions. These third party services providers may include prepaid service providers; Lottery service providers; Broadcaster and streaming services; Retail service providers; Technology and Smart device providers etc. if applicable. You must read this agreement together with all these other relevant terms & conditions if applicable. The Bank will not be liable for any delays in respect of third party providers. Your use of the third party service means that you accept and will be subject to the terms and conditions associated with it. If you do not accept those terms and conditions you are advised not to make use of the service.

(b) **Which agreement applies in instances of conflict**

If there is a conflict (difference) between this agreement and any other product terms & conditions, the provisions of this agreement will apply; unless the conflict relates to the use of the third party products or services, in which case, their terms and conditions will apply.

(c) We are not responsible for links to third party sites, its content or for the third party's actions or omissions, or its goods or services

For your convenience only, the service interfaces may allow you to view or access third party websites or content or purchase content, products or services provided by third parties. Even though we may make third party websites, content or products or services available to you, we do not endorse or recommend the third party or its products or services. You alone are responsible for deciding whether the third party or its products or services meet your requirements. Terms and conditions and rules may apply to those products and form an agreement between you and the third party.

You alone are responsible for obtaining the terms and conditions or rules that apply to you and the products or services offered by the third party. The categories/ types of third parties whose products, services or offerings may be available from or associated to the service interfaces may vary from time to time. They may include lotto service providers; coupon providers; voucher catalogue providers and other subscription providers. We have no control over such third parties or their products or services. We are not a party to any disputes between you and the third party. You alone are responsible for ensuring that any transactions you make on these third party sites are lawful. Some services are only available to persons who are 18 years old or older.

We are not responsible to you for any loss or damage you suffer, whether directly or indirectly, because of a third party or its products or services or your use of the products or services. You alone take the risk of using or purchasing third party products or services. You hereby agree to indemnify us and hold us harmless for any loss or damage you may suffer, or cause, in this regard.

2. ELECTRONIC VOUCHERS AND REDEMPTION OF DISCOUNT BENEFITS

Certain third parties offer electronic discounts on certain products via their computer system from time to time for redemption against products purchased. The Bank offers qualifying Bank customers the opportunity to receive these discounts when paying with their qualifying cheque, debit or credit cards. The qualifying cards may change from time to time and you are encouraged to ensure that you check these terms and conditions periodically for updates.You are advised to read these terms and conditions carefully.

The Bank does not distribute nor endorse any products or services to which the discounts apply. Should you have any issues either with the service or product purchased you need to liaise with the relevant third party store at which the purchase was made.The Bank does not have any control over the products that the discounts are offered for and cannot be held liable for the unavailability of these products in any way. Complaints regarding quality or quantity of the merchandise purchased must be directed to the third party concerned. Whilst we make every endeavor to ensure the accuracy of the discount offered, changes may be implemented from time to time. The Bank does not accept any responsibility for any loss which may arise from accessing or reliance on the information from the a third party and to the fullest extent permitted by Zambia law, we exclude all liability for loss or damages direct or indirect arising from use of this service.
The service is a value added service and no fees are charged for the redemption of the coupons.

3. ACCESS TO THE INTERFACES AND SECURITY

(a) Steps you must take to protect yourself

***NOTE**: Information that is sent over an unsecured link or communication system can be unlawfully monitored, intercepted, or accessed. While we take all reasonable steps to prevent this from happening, you need to understand that this risk exists.*

You play an important role in protecting yourself against fraud. For your safety you must follow the security tips/recommendations we give you on the service interfaces from time to time. You must also read the tips published at the Bank's Security Centre on the Banking App and the online Banking Communications Page. You must (where applicable) log off from the service interface when you have finished transacting. The Bank recommends that you do not use public communication facilities such as internet café's, but when you do, you must take special care. It is your responsibility to ensure that you have the necessary anti virus or anti-malware software on your device

If you are a cellphone Banking or inContact customer and you notice anything suspicious you must also contact your service provider/network operator to report the suspicious activity e.g. SIM Swaps (a sudden loss of service can be an indication of a SIM SWAP). Please take note of the following contact details for SIM Swop

- MTN Toll freeline 111
- Zamtel - +260 (211) 333 152
- Airtel Zambia Limited – 111

(b) For your protection and security you must enter the correct access information to identify yourself whenever you log onto the service interfaces. Since we deal with each other in a non-face to face environment, for your security you will need to enter the correct access information or take any other steps acceptable to us for us to verify your identity and the electronic communications you send us using the service interfaces each time you logon to the service interfaces. This is known as "authentication". Access information includes access credentials, or Cellphone Banking personal identification number ("mobile pin" or "MOPIN"). To protect you, we can refuse to act on any instructions you send us or can cancel your access (temporarily or permanently) if you don't meet the authentication requirements. This includes where you enter the wrong access information. We may require of an additional layer authenctication for certain transactions this may include transactions where a unique number (OTP or one time PIN) is sent to your device before the transaction can be completed. Similarly, when an instant message sent to your Banking App to request authorisation for the transaction or activity. Take note: You can have the OTP sent to your inContact number or a separate mobile number of your choice. **A loss of signal to your OTP or inContact number can indicate a SIM SWAP and notify the Bank immediately as a precaution and to minimise any loss**.

Customers who have a linked Banking App will not receive an OTP via sms but a notification via IM (instant messaging) via the Banking App requesting you to approve or decline the transaction. We cannot guarantee receipt or delivery of an SMS and/or e-mail as the Bank is dependent on third parties such as your chosen Mobile Network operator, for relaying of SMS and/or email.

The *inContact* Service is a messaging system which provides you with notifications of certain account activity by sending a message to your selected Mobile number and/or email to your email address and/or, IM (Instant Message) to linked Banking App. Please be advised that we will initially attempt to deliver an IM to your linked Banking App, failing which we will send through an SMS and finally if those are unsuccessful we will send through e-mail notification(if applicable). This is due to the relative safety of the IM communication mechanism, as these are delivered directly to a single user's App. IM is also not susceptible to the risk of a sim swop.

(c) You are responsible for making sure you have the necessary equipment and software to use the service interfaces

To be able to access the service interface/s you must have the necessary hardware, software and access to third-party communication services. You will be responsible for paying the cost of this and the cost of any upgrades that you require. To access online banking you need to have access to a computer that has an active account with an Internet Service Provider (ISP) and an Internet browser software program. To access cellphone banking you need to be activated via your cellphone and cellphone network service provider. In order to use the FNB Banking App you must ensure that you have a compatible smartphone and access to data. You will be responsible for paying the relevant cellphone and/or network service provider charges that you incur when using the service channel. You are responsible for the equipment you use to access the service interfaces. We have no control over the equipment, software or service providers. We are not responsible for any error or delay that may arise as a result and are also not responsible if you are unable to access the service interfaces because of your equipment, software or services provided to you by third parties. It is your responsibility to ensure all inactive devices are delinked from your profile. It is your responsibility to ensure that you have the necessary anti virus or anti-malware software on your device.

(d) We are entitled to act on and accept all transactions done after your access credentials have been entered or applied

All electronic communications that are sent to us during a logged in session will be treated as valid and authentic (i.e. after you have met our authentication requirements and are logged in to an interface). This means that these electronic communications will have the same legal effect as written and signed paper communications from you. Since we deal with you non-face-to-face we will act on and accept all instructions or transactions done after your correct access credentials have been entered and you meet the verification requirements set by us. We will assume that all such transactions have been authorised by you, even if such transactions took place without your knowledge or consent or were not authorised by you. This will not apply to transactions that occur after you have requested that we cancel your access credentials.

You must never reveal your access credentials to anyone under any circumstances. This includes when you use third party applications (apps) and sites. Certain financial aggregation apps (such as apps that help you track your spending across different financial institutions) may ask you to enter your access details to use their service. Take note that if you do so you put yourself at risk. In addition third parties will be able to access information about your accounts, banking history and other confidential information. You use such sites and apps at your own risk. If you are defrauded because you used a third party app or site the Bank will treat this as a voluntary compromise of your access details and confidential information and will not be legally responsible to you or any other person for any loss or damage you or they suffer.

(e) Authorised Users act on your behalf as your agent

By allowing an authorised user to access your account using the service channel, you give that person the authority to act as your agent. This means that anything the authorised user does or doesn't do will be attributed to you. In other words their actions or failure to act (omission) will be considered by us as your actions or failure to act (omission).

(f) Steps you must take to protect your access information (access credentials, cards and equipment)

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 access information to any person, including any person who is an employee of the Bank or claiming to work for or represent us in any way. You must never respond to requests to enter or "confirm" your access 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. The Bank will NEVER ask you to give us your sensitive secret information, including access credentials by email, SMS, instant message or even over the telephone. If you respond to these "phishing" messages and lose money as a result of doing so, the Bank will not refund you.**

Take note: For your convenience, the same login or access credentials can be used to access different electronic interfaces, this is the case for Online Banking and the Banking App. This means that if your access credentials are disclosed to someone else you can be defrauded across all the electronic interfaces which can expose you to greater losses. **You must immediately contact the Bank if you know or even suspect that your access credentials have been compromised to ensure that your loss is minimised.**

(g) **Additionally if you suffer a sudden loss of service on your mobile device contact the Bank immediately.**

You must ensure that your device/s which you use for transacting is always in your possession and protected with an additional access code, password or pattern lock. Should your device to which your Banking App is linked is no longer in your possession either permanently (for eg. due to theft, loss or in the event that you have sold it) or temporarily (your device is being repaired) you must contact the Bank immediately and or delink your Banking App immediately.

If you receive suspicious communications (including emails, SMSs) call the Bank's on **260 211 366800 or 362 or report via the FNB App/Online Banking.** For immediate action and assistance, we recommend that you call the Fraud Team. Please include your name and number in your email in case we need more information from you.Standard rates apply

You must not keep your access credentials together with your access cards or other Banking documents. Do not store your access credentials on the equipment you use to access the Bank service interfaces. For example, never store your PIN or Cellphone Banking PIN on, with or near your cellphone, computer, and telephone or with your e-Reg Card or Telephone Banking Card. For security purposes, we recommend that you memorise your access credentials. You must also follow the tips published on the Bank's Security Centre or Online Banking Communications Page. You are not allowed to register for the service or access the service channel using someone else's access information or personal information.

(g)You must IMMEDIATELY ask us to cancel your access code(s) if you suspect or know that your access code(s) have been lost, stolen or may be used without your permission.

Prompt notification is the best way of keeping your losses to a minimum, you must tell us immediately if you suspect or know that your access information has been lost, stolen or compromised (might be used without your permission).

In instances whereby you suspect or know that your access code(s) have been lost, stolen or may be used without your permission, call the Bank's Fraud Team on 3. .

If there is a dispute about whether or when you told us to cancel your access code(s), it will be your responsibility to prove how and when you told us to cancel your access code(s). For this reason you must keep any reference numbers we give you when you call us to cancel your access code(s). We advise you to request a reference number and store it for every call you make to us.

After we have cancelled your access code(s) we will reject all transactions done from the date on which your access code(s) were cancelled. If possible, we will also temporarily stop or reverse instructions that we received but which we have not yet processed before your access code(s) were cancelled, however we cannot guarantee that this will be done.

We reserve the right to block your access to the service interfaces at any time to maintain or restore security, if we reasonably believe that your access code(s) have been or may be obtained or are being used or may be used by an unauthorised person(s).

What you must do if you suspect or know about fraud on your account?

Note*: This section does not apply if the fraud or suspected fraud was committed by authorised users (persons who have been authorised by the account holder to transact on the account holder's behalf).*
You must tell us immediately when you become aware that a suspicious transaction has taken place and you must open a case at the nearest Zambia Police Services (ZP) office. We will investigate any loss that you suffered because of the alleged fraud. You must co-operate with us and the ZP in any investigation. We will pay you back once it has been established that you suffered financial loss as a direct result of the fraud if the following conditions are met:

- You have followed the safety tips we recommended and have complied with your duties under this agreement, in particular, those mentioned to you above as '**Steps you must take to protect your access information (access code(s), cards and equipment)' and 'steps you must take to protect yourself'**
- Your account was registered for the InContact/InContact-Pro notification service and you were actively using the service when the fraud occurred.

(h) Cancelling the Access Credentials(s) of Authorised Users - You must tell us in writing if an authorised user's access rights must be changed or cancelled

When an authorised user is no longer allowed to transact on your account you / we have the right to demand that they return any physical devices we gave them to enable them to transact, including their Telephone Banking card or e-Reg Card. When you as the account holder takes back the authorised user's physical access device you must notify us in writing or via the helpline that the authorised user's access rights must be cancelled, and the card or device must be destroyed or returned to us. The account holder is not allowed to use any authorised user's access code(s). For your security, the access code(s) must be cancelled. We will issue new authorised users with new access information.

You must notify us immediately when any user's access rights must be changed or cancelled by completing and signing the required mandates/Bank form(s). This can also be done by yourself on the website within your online Banking platform. Any cancellation of, or change to a user's access rights will not affect any instruction submitted by that user before the change has been made.

(i) You must comply with any user guidelines we publish on the service interfaces

For your protection and to ensure that the service channel works correctly, you must comply with the user guidelines we put on the service interfaces from time to time. If there is a conflict (difference) between this agreement and the guidelines, this agreement will apply instead of the guidelines.

5. PRIVACY

(a) **We respect your privacy. Read our privacy notice for more information**

This relationship is governed by our First National Bank Zambia Limited Privacy Notice. Our privacy notice explains how, why and when we collect, use, share and store your personal information. Our privacy notice forms part of this agreement with you. Please note: If you use certain services, such as the Firstprepaid services, FNB may need to share and collect certain personal information about you, including your identity number with third parties.

(b) **We may monitor your use of the service interfaces and record our conversations with you**

We may monitor and record communications or traffic on the service interface. This may be for security purposes; to maintain the proper functioning and safety of our systems and the service interfaces; or to investigate or detect any unauthorised use of the service interfaces or our systems; or when the law requires us to do so. For your protection as well as ours, all conversations between you and us are recorded. These recordings will be the proof of your instructions to us, unless you can prove otherwise. By using the service channel you consent to such monitoring and recording.

(c) We may make use of cookies for various purposes including to gather information about your general use of our interfaces and for statistical purposes but we will not use cookies to collect personally identifying information from you. Please read our First National Bank Zambia Limited Cookie Notice which is available on our website.

(d) **Cellphone numbers required to enable Cellphone Banking service.**

If you are a cellphone Banking customer the Bank may get your cellphone number from your cellphone network operator. This is done to assist the Bank to authenticate you and to obtain history regarding sim swop history from your provider. For your protection, the Bank can (but does not have to) use your cellphone number to identify you. Additionally, only Cellphone numbers are processed and no additional information such as device data or personally identying data can be obtained from the network operator.

6. GENERAL

(a) How we make terms & conditions and other information available to you

From time to time we may include links to terms and conditions on the service interfaces. Where it is not possible to use a link, we may refer to the terms on the service interfaces. You must follow our instructions or the link and read the Terms, as they form part of the agreement between you and us. If the service interfaces you are using does not enable you to access the Terms via a link for any reason, you must visit our website, our branches or contact us (contact details are available on the website) or follow our instructions to get a copy of the Terms. Any Terms & Conditions we refer to are important. You must read them carefully because they contain important contractual information. Due to space constraints on some interfaces we sometimes only refer to terms & conditions as “T&Cs”.

(b) Fees you must pay to use the Service Interfaces

The fee you must pay includes a services fee for use of the service channel and a transaction fee for the transactions you do on the service interface/s. For more information about the service channel fees please refer to our pricing guide. A copy can be obtained on the website or from any branch of the Bank. The fees will be collected (debited) from your relevant account fees and are not paid or billed separately.

(c) Certain information, including your account balance information, may be delayed

Certain information, including your account balance information that is made available to you on the service interfaces may be delayed and may not show your recent transactions. You can confirm your account balance information by contacting us.

(d) We cannot act on or process your instructions unless you have enough money in your account

Any instructions we receive from you on the service interfaces, including an instruction to pay a third party or transfer money between your accounts will only be carried out if you have enough money in your account or credit in your overdraft facility.

(e) Transaction limits apply to transactions done on the service interfaces

These limits apply whether these were set for your account, for the authorised user or for the service channel itself. Transaction limits are there for your protection. Because of this we will not be able to carry out any instruction from you if you have exceeded your transaction limit or if a transaction will result in you exceeding your transaction limits. If you need to exceed any limits you need to arrange with us for this beforehand. You can do this by phoning our call centre or visiting your nearest branch. For security reasons we reserve the right to adjust your transactional limits at our discretion. Please contact our call centre to find out what the transactional limits are on our service interfaces.

(f) You are responsible for giving us correct and complete information and instructions when you transact

You are responsible for giving us correct and complete information and instructions when you transact. Unfortunately we are unable to and do not check or confirm any information. **We do not verify the identity or Bank account details of the person / entity you are paying and do not compare the account number against the details of the person / entity you are paying, therefore it is your responsibility to make sure that the information you give us is correct. We will not be responsible to the person or entity you are paying for any loss or damage you suffer because you gave the incorrect or incomplete information. We are not responsible if you do not complete an instruction or if you do not follow our instructions when transacting.**

(g) Certain transactions cannot be reversed or stopped once you send them to us

FNB will not reverse any payment instruction after it has been processed. FNB may (if possible) try to reverse an instruction if the person so paid has an account with FNB and they give FNB written consent to do so. If the beneficiary has an account with another bank or financial institution (bank), FNB's role is only to pass on your instruction to the other bank or financial institution. FNB will not be responsible for anything FNB does on your instruction. FNB will not accept an instruction to stop the payment of a validly drawn instrument after it is paid. Some instructions cannot be reversed or cancelled once you submit them. This includes pre-paid purchases.

(h) How long does it take to process transactions?

Unless we say otherwise (whether on the service channel or anywhere else), all transactions will be completed in the same amount of time that they generally take to be completed when you perform them at the branch or ATM. Some transactions take longer. It can take up to 2 (two) business days for money to reach persons you are paying by EFT (electronic funds transfer) via the service interfaces. Please read the guidelines and notices published on the service channel from time to time or contact us to check on the turnaround times especially if your payment is urgent.

(i) How do I know if the Bank has received my instruction?

You must not assume that we have received an instruction until we have specifically confirmed that we received that instruction, or acted on that instruction, whichever happens first. **If you are not sure if a transaction has been sent or received or processed you must contact us. You must not submit an instruction again as this can result in the same transaction being processed again. Should this happen you will be responsible for such duplicated transactions**. Messages sent by us of an "automated nature" or messages that were sent using auto response software or programs must not be regarded as a response or confirmation.
You will be regarded as having accepted all transactions and changes to your account settings made via the service interfaces unless you notify the Bank of your objection as soon as you become reasonably aware.

(j) The timing of communication

Any communication from us to you will be regarded as having been sent at the time shown on the communication or on our transmission logs. In any proceedings or dispute, our records certified as correct by the Bank's employee in charge of the service channel, will be sufficient proof of any instructions you have provided or transaction you have performed on the service interfaces, the content or services on any service channel or value added service, unless you can prove otherwise. Where dates and times need to be calculated the international standard time (GMT) plus 2 (two) hours will be used.

(k) The Bank is not responsible for third party software

From time to time we may make third party software/applications ("software") available for download via the service channel. You download and use the software at your own risk. We make no warranty about the software, whether express or implied. You will be bound to the license terms of the software licensor. You hereby indemnify us and hold us harmless if you breach the license conditions.

7. ENDING THIS AGREEMENT

(a) Notice
We can end this agreement at any time or end your right to use the service interfaces, after giving you reasonable notice. This will not affect instructions given to us using the service interfaces before the agreement ended.

You may end this agreement by notifying us in writing If you or we end this agreement you will still be responsible to us for all transactions, instructions and fees levied prior the notification can be given effect to.

(b) Specific conduct

We can also end this agreement and your right to use the service interfaces immediately if any one or more of the following happens:

- If you commit fraud or we suspect you have done so;
- If we believe that your behaviour was inappropriate or constitutes misconduct, such as utilising your profile to the detriment of other users and clients;
- If you breach this agreement;
- If you no longer have access to the equipment or services necessary to use the service interfaces. e.g Cellphone Network Service Provider removes your registered cellphone number from its network or ends your contract;
- If your account is closed.
- If the law requires us to do this.
- If you don't use the service channel App for a period of 12months or more. If we end the agreement because of this the accountholder will have to register again.

NOTE: It is your responsibility to cancel any scheduled payments and/or top ups and any recurring services or payments you set up on the service interface. The service interface is just a means of setting up scheduled top ups and recurring services, ending the agreement does not mean these scheduled top ups or recurring services will also be cancelled.