REMOTE BANKING AGREEMENT

This agreement applies to you if you use any of the following self service banking channels: Online Banking, Cellphone Banking, FNB.mobi, FNB Banking App for smartphones and tablets and Telephone Banking. In this agreement we refer to these as self service banking channels ("the service channel"). This document was last updated on 05 October 2016.

ACCEPTANCE AND REGISTRATION

This important document sets out the rights and duties between you and First National Bank Botswana Limited, with registration number 24/1988 ("the bank"). Please read this document carefully. If you do not understand any part of this document you must contact the bank for further clarification.

This agreement forms a legally binding agreement between First National Bank of Botswana Limited ("FNB" or "the bank") and the bank's customer and if applicable, any natural persons the customer has chosen to access or transact on its accounts, using the service channels ("users"). For convenience, in this agreement "you" or "your" refers to both "the customer and user(s), or the customer or a user, as the context requires" and (where appropriate) also refers to any separate legal entity, such as a company. In this agreement "we, us, or our" only refers to the bank. This agreement governs your and our rights and obligations when you use any of the service channels. Read this agreement carefully. Do not use the service if you don't agree to any part of this agreement. Contact us if you don't understand any part of this agreement.

Before you can use the service channels you must register for the service channel. Refer to http://www.fnbbotswana.co.bw, or +267 364 2670 for assistance on how to register for the different service channels. To use the service channels you must be at least 18 years old or have your parent/legal guardian's consent or be emancipated."Emancipation" means that the court has given you the right to act without the supervision of a parent or guardian. By registering to use the service channel you confirm that you are at least 18 years old or have your parent/legal guardian's consent or have been emancipated, as the case may be.

You will become bound to the most recent version of this agreement when you do any of the following:

- If you register to use any of the service channels.
- If you obtain access rights; access mechanisms and/or access codes to use any of the service channels.
- If you use any of the service channels.

The bank may change this agreement or add new terms and conditions for the use of the service channels or value added services at any time. The bank will notify you about changes. If you do not agree to the changes, you have the right to terminate this agreement before the expiry of 7 (seven) days after the changes take effect. If you do not notify the bank of your intention to terminate the agreement within this period, you will be deemed to have accepted the amended agreement/new terms and conditions.

Because of this we recommend that you read the terms and conditions before each use, as these terms and conditions may change from time to time.

OTHER TERMS AND CONDITIONS ALSO APPLY TO YOU

This agreement applies along with other terms and conditions of the bank that govern your accounts, our services and our relationship with you.
Prepaid products like airtime and electricity. (see network operator or service provider terms and conditions that apply)

Prepaid products are subject to the terms and conditions of the applicable Network Operator or service provider. We have no control over these terms and conditions. You must read the terms and conditions of the third party service provider before you purchase as we are unable to give you a refund on prepaid products. For your convenience we have placed links to the relevant third party service providers websites.

- Mascom – (www.mascom.bw)
- Orange – (www.orange.co.bw)
- B mobile – (www.bmobile.com.bn)
- Electricity BPC – (www.bpc.bw)

Certain products and services that you use or access via the service channels are subject to their own terms and conditions, such as the bank accounts or services you access, your ATM card, credit and debit card. This agreement (governing the use of the service channels) must be read together with, and forms part of, each product agreement. In there is a difference between this agreement and such other terms, the provisions of such other terms will prevail to the extent of the conflict.

If you use FNB eWallet the following terms & conditions apply to you: http://www.fnbbotswana.co.bw/electronic-services/ewallet.html

You must also comply with the guidelines published on the service channel from time to time. If there is a conflict between this agreement and such guidelines, this agreement will override the guidelines.

From time to time we may include hyperlinks to terms and conditions ("Terms") on the service channels which are available elsewhere. Where it is not possible to use a hyperlink we may refer to the Terms on the service channel. You must follow our instructions or follow the hyperlink and read the Terms, as they form part of the agreement between you and us. If the service channel you are using does not enable you to access the Terms via a hyperlink or if we merely refer to the Terms you must visit our website, our branches or contact us or follow our instructions, to obtain a copy of the Terms. If you do not agree with the changes you must no longer use the services.

FEES

Refer to our pricing guide on our website for more information on any monthly access fees or transaction fees that apply. A copy can be obtained on the website www.fnbbotswana.co.bw, or from any of our FNB branches. Fees (if applicable) will be debited from your nominated bank account. If you don't pay our fees we may refuse you access to the service channel.

ACCESS CODES

For security, identification and verification purposes, when using the bank's service channels, you will make use of a variety of access codes to identify yourself, such as your access number. 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 communication you send us using the service channels each time you logon to the service channels. This known as verification. All electronic communications that are sent to us after you have met our verification requirements during logon will be treated as valid and authentic. This means that these electronic communications will have the same legal effect as written and signed paper communications from you. For your protection we reserve the right to refuse any instruction that you send us if we suspect that your account may have been compromised. This includes when you don't meet the verification requirements or enter an incorrect access code. For your protection and security you must enter the correct access information to identify yourself whenever you use or logon to the service channels.

Access information, includes any physical devices we give you to allow you to logon to the relevant service channel like your Telephone Banking card or your e-Reg Card, which you use with your PIN (personal identification number) or access number, or Cellphone Banking PIN. We are entitled to act on and accept all transactions done after your access codes have been entered or applied.

We will assume after verification that all such transactions or instructions 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 codes.

AUTHORISED USERS ACT ON YOUR BEHALF AS YOUR AGENT

We may require of an additional layer of security (verification) for certain transactions. Such as where a unique number (OTP or one time PIN) is sent to your device before the transaction can be completed. 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 you should check your account immediately or notify the Bank to minimise your loss**.

Take note: For your convenience, the same login or access details can be used to access different electronic channels. This means that if your access details or lost or stolen or disclosed to someone else "compromised" your details on one channel you can be defrauded across all the electronic channels which can expose you to greater losses. **You must immediately contact the Bank if you know or even suspect that your access details have been compromised to ensure that your loss is minimised.**

We are entitled to act on and accept all transactions done after your access codes have been entered or applied

Since we deal with you non-face-to-face we will act on and accept all instructions or transactions ("transactions") done after your correct access codes 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 codes.

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). For your convenience, we may allow you to access other FNB products, services or sites through or on the self-service channels without requiring you to log on to these sites. Note: This means that anyone who is able to log on to the self-service channel, including your authorised users, will also automatically have access to these products, services or sites and be able to use them. Their actions when using these products, services or channels will also be attributed to you i.e. we will assume that you authorised them to take such actions or use such sites. If you are signed up for FNB Connect all your online banking users will also be able to transact on FNB Connect, this includes cancelling services you have subscribed to or adding services such as auto top ups.

STEPS YOU MUST TAKE TO PROTECT YOUR ACCESS INFORMATION (ACCESS CODES, 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 codes, 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 codes 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. This will not apply to transactions that occur after you have requested that we disable any access code. If you receive suspicious communications (including emails, SMSs) call the bank's Fraud Team on +267 364 2670 or send an

email to: 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.

Do not keep your access codes together with other Banking documents or any devices you use to gain access to the bank's service channels. (E.g. your Cellphone or tablet device). The customer has the right to demand the return of any physical devices we provided to its users. The customer, however, is not entitled at any time to use, have any knowledge about or access to any other user's access codes. When the customer repossesses such physical access device it must notify the bank in writing or via the helpline, and the card or device must be destroyed or returned to the bank.
Service channel users ("users") must follow the tips for creating/safeguarding their access codes, as published in the bank's Security Centre from time to time. Users may not register for the service or access the service channel using someone else's access codes, information or device.. User's must tell us immediately if you know or suspect that their access code(s) have been lost, stolen or may be misused. If there is a dispute about this, the duty is on the customer or user to prove the bank was notified and when it was notified. After the bank has disabled a user's access codes the bank can reject instructions received after such access codes were disabled. The bank may also (if possible) suspend or reverse instructions received (but not yet processed) before the access codes were disabled. The bank may refuse to process instructions/communications or can disable your access, if you don't meet the verification criteria required by the bank from time to time.

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 channels from time to time. You must also read the tips published at the bank's Security Centre and the online banking Communications Page. You must (where applicable) log off from the service channel 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. You must use our recommended hardware and software. This includes security software that is recommended by us. Please refer to the bank's Security Centre and Online Banking Communications Page for more information. Failure to use the recommended hardware and software may result in the service channel not being available or not operating properly or may also expose you to a greater security risk.

Cellphone Banking Customers:
If you are a cellphone banking customer and you notice anything suspicious you must also contact your service provider/network operator to report the suspicious activity e.g. SIM Swaps:

- Mascom – (www.mascom.bw)
- Orange – (www.orange.co.bw)
- B mobile – (www.bemobile.co.bw)
- Electricity BPC – (www.bpc.bw)

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). If you use our FNB App you must notify us immediately if your cellphone is lost or stolen and ask us to delink your cellphone from your online banking profile. In instances whereby you suspect or know that your access code(s) have been lost, stolen or may be used without your permission, immediately call the bank's Fraud Team on . 00267 370 6000
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 channels 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 **Botswana Police Services** office. We will investigate any loss that you suffered because of the alleged fraud. You must co-operate with us and the **Botswana Police Service** 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.

Cancelling the Access Code(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.

We may monitor your use of the service channels and record our conversations with you

For security purposes, to maintain the proper functioning and safety of our systems and the service channels, or to investigate or detect any unauthorised use of the service channel or our systems, or when the law requires us to do so, we may monitor and record communications or traffic on the service channel. Telephone-Banking customers: For your protection as well as ours, all conversations between you and us during Telephone Banking 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. All calls to the service channels customer services desks may be recorded.

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 channels may be delayed and may not show your recent transactions. You can confirm your account balance information by contacting us. Forex rates shown on the FNB App are indicative values only.

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 channels, 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.

Transaction limits apply to transactions done on the service channels

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.

Please contact our call centre to find out what the transactional limits are on our service channels. Each service channel has its own limits.

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.

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

Certain transactions cannot be reversed or stopped once you send them to us, for example, when you buy pre-paid products.

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 channels. 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.

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.

Nothing on the service is an offer or professional advice to you

Unless we actually make an offer to you, all material on the service channels is only an invitation to you to do business with us. Nothing on the service channel is given as advice or an offer which is meant to get you to buy or sell anything, or enter into any investment or transaction.

Availability of the service channels.

The service channels may not be available from time to time. You must use our other banking channels during this time

You can access the service channels seven days a week, 24 hours a day. However, at certain times, some or all of the service channels or services on them may not be available due to routine maintenance or emergency repairs or because of circumstances outside our control, such as electricity outages/blackouts, or the unavailability of any telecommunication system or networks. In this case you must use our other available banking channels and take reasonable steps to minimise or prevent loss or risk to you. If we need to change the scope of our services, we will try to give you prior notice of such interruptions and changes, but we cannot guarantee that such notice will be given to you. We may stop providing the service channels or any services provided on the service channels at any time. We will however, notify you of this within a reasonable time of these changes being made. You agree that a notice published on the website or a notice sent to you via an email, an SMS or via post will be sufficient notice to you. You will be regarded as having accepted all transactions and changes to your account settings made via the service channels unless you notify the bank of your objection within 5 (five) hours of receiving a notification from us, by any means, including inContact and inContact-Pro.

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 channels 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. Without changing your responsibility to obtain terms and conditions and rules the following terms and conditions apply to the following services:

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.

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.

IMPORTANT: The bank's liability will be limited for loss caused by use of the service channels

The bank will to the best of its ability ensure that the service channels are provided to you in a secure and reliable manner. The bank shall take reasonable care to prevent harm and loss to you. Although the bank takes reasonable care to prevent harm or loss to you, the bank will not be liable for any kind of loss or damage you may suffer, including direct, indirect, special, incidental or consequential damages, because of your use of, or inability to use, the services. This will not apply where the loss/damage arose because of the bank's negligence or intent. In addition to the above the bank is not liable for the following (except where such loss or damage is caused by the bank's negligence or intent):

- **any loss or damage, which you or any other party may suffer due to unauthorised interception and/or monitoring ;**
- **any loss or damage if you didn't take reasonable steps to safeguard the account, the access codes and/or follow the steps recommended by the bank from time to time;**
- **late or delayed transactions;**
- **loss or damage arising from the unauthorised use of the service channel including where a user exceeds their authority;**
- **the bank is not responsible for any errors or delays in communication systems outside of its control.**

We own the intellectual property rights in the service channel and its content

The contents of the service channels, including all registered and unregistered trade marks, copyright and patents are owned by us and are our intellectual property rights. You may not copy, reproduce, display, reverse engineer or use any intellectual property in any manner whatsoever without our prior written consent. Nothing on the service channels must be seen as granting any licence or right of use of any intellectual property. You may not establish any connection, including via a hyperlink, frame, meta tag or similar reference, whether electronically or otherwise to any part of the service channel or the bank's website without our prior written consent.

How we will communicate with you

You agree that we can send you information about the service channels or this agreement by any means, including but not limited to publishing a notice on the service channel itself or using electronic means, including SMS or email.

We can change this agreement at any time

We have the right to change this agreement or add new terms and conditions for the use of the service channels or value added services at any time. Whenever we change this agreement we will electronically update this agreement. We will notify you of these changes. The use of the service channels will be taken as an acceptance of the agreement. If you do not agree to the changes, you have the right to end this agreement before the end of 7 (seven) days after the changes take effect. If you do not notify us of your intention to end the agreement within this 7 (seven) day period, we can assume that you have accepted the amended agreement or new terms and conditions. A certificate made by the relevant bank's employee, whose authority to do so doesn't need to be proven, will be the proof of the version of the agreement that applies to you.

Ending this agreement

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

We can also end this agreement and your right to use the service channels 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.
- If you breach this agreement.
- If you no longer have access to the equipment or services necessary to use the service channels. 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 for a period of 6 (six) months or more. If we end the agreement because of this the accountholder will have to register again.

You may end this agreement by notifying us in writing or by phoning our call centre. If you or we end this agreement you will still be responsible to us for all transactions, instructions and fees.

NOTE: It is your responsibility to cancel any scheduled top ups and any recurring services or payments you set up on the service channel. The service channel 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.

INCONTACT TERMS AND CONDITIONS

The inContact Service is a messaging system which provides you with notifications of certain account activity via SMS and/or email to your selected mobile number and/or e-mail address. You need to be registered for inContact in order to use any of the service channels.

These terms and conditions apply to inContact and inContact PRO (an enhanced form of inContact). They form a binding agreement between you and FNB. You must read these terms and conditions carefully. Contact us if you don't understand any part of these terms and conditions. These terms and conditions must be read with the FNB General Terms and Conditions located at http://www.fnbbotswana.co.bw. By using inContact and/or inContact PRO you agree to be bound to these terms and conditions.

The types and values of transactions that we provide notifications for do change from time to time. Because of this you must still take the necessary precautions to safeguard your accounts, cards and banking channel access mechanisms, such as passwords and PINs. You are responsible for ensuring that the Bank has your correct mobile numbers and/or email addresses. We will not be held responsible if your SMS and/or email is sent to the wrong number or address. Your inContact information can be updated electronically using the Online Banking channel, by contacting the customer contact centres or by visiting a Branch.

We cannot guarantee receipt or delivery of an SMS and/or e-mail as the Bank uses external third parties for relaying of SMS and/or e-mail. Although we do send you inContact notifications your statement will be the main and final record of all transaction on your account. You must therefore check all entries on your statement immediately upon receipt of your statement. You must report any unauthorised transaction or errors within 30 (thirty) days from the date of the statement. Should you fail to do so all entries will be assumed to be correct and authorised. FNB will not be held responsible for any losses suffered as a result of your failure to notify us timeously of suspicious or unauthorised transactions.

Notification Services

inContact is designed to assist you to track activity on your account and minimise potential unauthorised transactions. It is important that you read you inContact notifications as soon as you receive them. You must notify FNB about any suspicious or unauthorised transactions on your account within 24 (twenty four) hours. If you fail to do this, you agree that FNB can treat the transaction as correct and hold you legally responsible for the transaction as if you had done or approved it. In the event of a dispute regarding when a message was sent our system records will serve as proof of the date and time of the sending of the message unless you can prove otherwise.

inContact subscribers can access Cellphone Banking Lite by dialling *130*392# This allows you to monitor your accounts as it enables you to view transactions and balances on all accounts linked to your profile. Further you can perform limited value transactions. Should you wish to not avail of this service the functionality can be disabled by using Online Banking or visiting an FNB branch.

NOTICE TO CELLPHONE BANKING CUSTOMERS

You agree that the bank can obtain your cellphone number from your network operator. For your protection, the bank may (but is not obliged to) use your cellphone number for authentication purposes.

ACCOUNT INFORMATION

Certain account balance information that is provided on the service channels may be delayed and may therefore not reflect recent transactions. You can confirm your account balance information by contacting us or by dialling the relevant the dial string or by using FNB dot Mobi or the App.

NO OFFER

Unless clearly stated, all material on the service channel merely constitutes an invitation to do business with us. It does not constitute advice or an offer or solicitation to buy or sell, to dispose of, or enter into any investment or transaction.

INSTRUCTIONS RECEIVED WILL NOT BE PROCESSED IF FUNDS ARE NOT AVAILABLE

Any instructions we receive, including an instruction to pay a third party or transfer funds between your accounts will be subject to the availability of sufficient funds. If there are not have sufficient funds in the relevant account we will not carry out the instruction.

INSTRUCTIONS WILL NOT BE PROCESSED IF THEY EXCEED THE TRANSACTION LIMITS SET BY YOU OR THE BANK

All instructions we receive, including an instruction to pay a third party or transfer funds between your accounts, are subject to the transaction limits set by you or the bank. If you have exceeded your transaction limits we will not carry out the instruction. If you have any queries contact +267 364 2670 for assistance.

USERS ACT ON YOUR BEHALF

When you register to use any of the service channels you can appoint other person(s) (“user/s”) to perform transactions and/or give the bank instructions, or view account information on your behalf, via the service channels. By allowing a user to access the account via the service channel, you give that person the authority to act as your authorised agent. Any act or omission by the user will be attributed to you and will be regarded as your act or omission.

CHANGES TO A USER’S ACCESS RIGHTS

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). Any cancellation of, or change to a user’s access rights will not affect any instruction submitted by the user before we have confirmed that the change has been made.

BANK IS NOT RESPONSIBLE FOR INCORRECT INFORMATION OR INCOMPLETE INSTRUCTIONS

You are responsible for giving us correct and complete information and instructions when you transact.
We do not check or confirm any information, including the identity or bank account details of the recipients of any funds. It is your responsibility to check that the information you give us is correct. We will not be liable for any loss or damage if you provide the wrong or incomplete information. We will not be liable if you fail to complete an instruction or if you do not follow our instructions.

WE DO NOT VERIFY OR CONFIRM INSTRUCTIONS

We can, but are not required to, request confirmation or verification of any transactions/instructions that you have submitted.

TRANSACTIONS CANNOT BE CANCELLED

Certain transactions cannot be reversed or stopped once confirmed by you/finally submitted to us, including, the purchase of pre-paid products.

TURNAROUND TIMES

Unless otherwise stated by us (on the service channel or otherwise), all transactions will be subject to the same turnaround times that apply to the same transaction, account and customer, when concluded at any bank's branch. You are advised that payments to other financial service institutions may take up to 3 (three) business days to reflect. Please also refer to the guidelines published on the service channel from time to time.

WHEN WE WILL BE DEEMED TO HAVE RECEIVED INSTRUCTIONS AND COMMUNICATIONS FROM YOU

You may not assume that we have received an instruction until we have specifically confirmed receipt of that instruction, or given effect to that instruction, whichever happens first. Messages of an "automated nature" or messages that were sent using auto response software or programs must not be regarded as a response or confirmation. If you don't know whether a transaction has been sent/received or processed you must contact us. You must not resubmit an instruction as this can result in the same transaction being processed again. If this happens you will be responsible for such duplicated transactions.

WE MAY RECORD OUR COMMUNICATIONS WITH YOU, INCLUDING OUR TELEPHONE CONVERSATIONS AND WE MAY MONITOR USE OF THE SERVICE CHANNEL

For purposes of security, to maintain the integrity and security of our systems and the service channel, or to investigate and/or detect any unauthorised use of the service channel and our systems, for customer care or when the law requires us to do so, we may monitor and record communications/traffic on the service channel. You hereby agree that we can monitor and record your communications/transactions with us or your use of the service channel.

FRAUD

We strongly recommend that you ensure that your device which you use for transacting is always in your possession and protected with an additional access code, password or pattern lock. We further advise that should your device to which your Banking App is linked is no longer or 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 should delink your Banking App immediately.

If you receive suspicious communications (including emails, SMSs) call the Bank's Fraud Team on (00267) 3959881
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

Note: This section only applies where the fraud was committed by persons other than an authorised user or users who have been authorised to act on the account holder's behalf. We will investigate any loss that a customer suffers which is alleged to have occurred as a result of fraud.
You must inform us immediately on becoming aware that a suspicious transaction has taken place and must open a case at the nearest Police Station.
You will be required to co-operate with us and the Police in any investigation.
We will reimburse you once it has been established that you suffered financial loss as a direct result of the fraud provided:
you have complied with the safety tips specified by bank and this agreement;
And you had registered the account in question for inContact and were actively using the service at the time the fraud occurred.

HOW WE CAN COMMUNICATE WITH YOU

You agree that we can send you information about the service channels or this agreement by any means, including by publishing a notice on the service channel itself or using electronic means, including SMS or email.

YOU ARE RESPONSIBLE FOR MAKING SURE YOU HAVE THE NECESSARY HARDWARE, SOFTWARE OR ACCESS TO SERVICES TO USE THE SERVICE CHANNELS

You are alone responsible for making sure that you have the necessary hardware, software and access to third-party communication services to make use of the service channels. You alone are responsible for paying the costs of obtaining the necessary hardware, software or third party communication services. For example if you want to use cellphone banking you need to obtain the recommended cellphone and software, and are responsible for paying the relevant cellphone network service provider charges that you incur when using the service channel.

We have no control over the equipment, software or service providers. It is your responsibility to ensure that you have the necessary antivirus or anti-malware software on your device. 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 channels because of your equipment, software or services provided to you by third parties.

NO WARRANTIES

No warranties, whether express or implied, are given in respect of the service channels or the value added services, including in respect of their performance, quality; security; suitability; content; information; availability; accuracy; safety or reliability.

CUSTOMER AND USERS USE SERVICE CHANNELS AND VALUE ADDED SERVICES AT THEIR OWN RISK. BANK IS NOT LIABLE

You will use the service channel and the value added services ("the services") at your own risk. You hereby indemnify the bank against any claims by third parties or loss the bank suffers which arises from your use of the services or your breach of this agreement. For purposes of this clause "bank" includes its affiliates, shareholders, agents, consultants or employees, in whose favour this constitutes a stipulation for the benefit of another.
Although the bank has taken reasonable care to prevent harm or loss to you, the bank will not be legally responsible for any kind of loss or damage you may suffer, including direct, indirect, special, incidental or consequential damages, because of your use of, or inability to use, the services. This applies regardless of when or how such loss/damage arose (contract, delict or otherwise) and regardless of whether the loss/damage was foreseen or reasonably foreseeable by the bank. This will not apply where the loss/damage arose because of the bank's gross negligence or wilful intent. In addition to the above the bank is not liable for the following:

- Any loss or damage, which you or any other party, may suffer due to unauthorised interception and/or monitoring.
- Unauthorised transactions that were submitted after your access codes were entered.

  any loss or damage if you didn't take reasonable steps to safeguard the account, the access codes and/or follow the steps recommended by the bank from time to time.
- Late or delayed transactions.
- Loss or damage arising from the unauthorised use of the service channel including where a user exceeds their authority.
- Any loss or damage that you, the recipient of the notice or beneficiary of the payment, may suffer because of the notification service. You hereby indemnify the bank against any loss, expense, claim or damage (direct, indirect and consequential) that you or a third party may suffer, including users, recipients or beneficiaries because of the use of the services or because of any delay or failure by the bank to send the notice.

The bank is not responsible for any errors or delays in communication systems outside of its control.

YOUR PRIVACY

We respect your privacy. Our privacy policy is incorporated into this agreement and forms part of it.
Please read our Privacy Policy published on the website. Our privacy policy explains how, why and when we collect, use, share and store your personal information. Our privacy policy forms part of this agreement with you.

YOUR SECURITY

NOTE: Information that is transmitted over an unsecured link or communication system is susceptible to unlawful monitoring, distortion or access. For your safety you must follow the security tips/recommendations given to you via the service channels from time to time and published at our Online Security Centre on our website. You must never disclose your access codes to any person, including any staff member of the bank or any person claiming to work for or representing the bank in any way. You must (where applicable) log off from the service channel (e.g. Online banking) when you have finished transacting. You must use recommended hardware and software. Failure to do so may result in the service channel not being available or not operating properly. Failure to do so may also expose you to security risk.

AVAILABILITY OF SERVICE CHANNELS AND VALUE ADDED SERVICES

The service channels and value added services may not be available from time to time due to routine maintenance or emergency repairs or because of the unavailability of electricity, any telecommunication system or networks. In this case you must use the bank's other available service channels and take reasonable steps to minimize/prevent your loss or risk. Refer to the alerts or notifications published on the service channels from time to time.

THE BANK MAY CHANGE, SUSPEND OR CANCEL THE SERVICE CHANNELS OR VALUE ADDED SERVICES

We may stop providing the service channels or value added services any time. We will however, notify you of this within a reasonable time of these changes being made. You agree that a notice published on the website or a notice sent to you via an email, an SMS or via post will be sufficient notice to you. You will be regarded as having accepted all transactions and changes to your account settings made via the service channels unless you notify the bank of your objection within 5 (five) hours of receiving a notification from us, by any means, including inContact and inContact-Pro. You must ensure that the bank has the correct contact details, including cellphone numbers, e-mail addresses and postal addresses for purposes of sending you notifications, including those to be sent for purposes of inContact/inContact-Pro.
We cannot guarantee the accuracy or arrival of any communication, as we may depend on external service providers for delivery.

THE BANK IS NOT RESPONSIBLE FOR LINKS TO THIRD PARTY CONTENT, PRODUCTS OR SERVICES

For your convenience only, the service channels may allow you to view 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 are alone responsible for deciding whether the third party or its products or services meets 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. .

We have no control over such third parties or their products or services. We will not become a party to any disputes between you and the third party. You alone are responsible for ensuring that the transaction is lawful. We will not be liable for any loss or damage you suffer, whether directly or indirectly, as a result 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 indemnify us fully against any loss or damage you may suffer, or cause, in this regard.

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 will be bound to the license terms of the software licensor. You hereby indemnify us if you breach the license conditions.

We make no warranty about the software, whether express or implied. You download and use the software at your own risk.

THE BANK OWNS THE INTELLECTUAL PROPERTY IN THE SERVICE CHANNELS AND ITS CONTENT

The contents of the service channels, including all registered and unregistered trade marks, constitutes our intellectual property rights. You may not copy, reproduce, display or use any intellectual property in any manner whatsoever without our prior written consent. Nothing on the service channels must be seen as granting any licence or right of use of any intellectual property. You may not establish any connection, including via a hyperlink, frame, meta tag or similar reference, whether electronically or otherwise to any part of the service channel or the website without our prior written consent.

HOW AND WHEN WE OR YOU CAN TERMINATE THIS AGREEMENT

We can at any time terminate this agreement and/or the user's right to use the service channels, after giving you reasonable notice. This will not affect instructions given to us via the service channels before termination.
We reserve the right to terminate this agreement and your access rights immediately if any or a combination of the following happens:

- Fraud or suspected fraudulent activity.
- We believe that your behaviour was inappropriate or constitutes misconduct.
- You have breached this agreement.

- You no longer have access to the access device or facilities, e.g. Cellphone Network Service Provider terminates the user's registered cellphone number from its network.
- Your account is closed.
- We are compelled to do so by law.
- You have not used the service channel for a period of 6 (six) months. If termination occurs due to dormancy the customer will have to reapply for registration.

You may terminate the agreement by notifying us in writing or by contacting the relevant bank's helplines.
In the event of termination you will remain liable to the bank for all transactions, instructions and fees.
It is your responsibility to cancel scheduled top ups and any recurring services or payments you have set up using the remote banking channel.

GENERAL

Any communication from us to you will be deemed to have been sent at the time shown on the communication or on the bank's transmission logs. In any proceedings or dispute, the bank's records certified as correct by the bank's employee in charge of the service channel, will be sufficient proof of any instructions a user has provided/transaction a user has performed on the service channels, the content or services on any service channel or value added service, unless you can prove the contrary.

No changes to this agreement and no waiver of any of the bank's rights are binding unless reduced to writing and issued or signed by the bank's duly authorised representative/s. You may not amend this agreement. A certificate issued by a duly authorised bank's employee, whose authority need not be proved, will serve as proof as to which version of these terms as applied to you.

Where dates and times need to be calculated the international standard time (GMT) plus 2 (two) hours will be used.
The indulgence, extension of time, waiver or relaxation of any of the provisions or terms of this agreement, or failure or delay on the bank's part to exercise any of its rights will not operate as an estoppel against it nor shall it constitute a waiver by use of such right. We will not thereby be prejudiced or stopped from exercising any of our rights against you which may have arisen in the past or which might arise in the future.
Any provision in this agreement which is or may become illegal, invalid or unenforceable shall be ineffective to the extent of such prohibition or unenforceability and shall be treated as if it were not written and severed from this agreement, without invalidating the remaining provisions of this agreement.

This agreement will be governed by the laws of the Republic of **Botswana** without giving effect to conflict of laws provisions.
You must not keep your access codes together with your access cards or other banking documents. Do not store your access codes on the equipment you use to access the bank service channels. 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 or on your smart phone. For security purposes, we recommend that you memorise your access codes. 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.