

STANDARD TERMS AND CONDITIONS (Standard T & Cs)

Important Definitions:

- The words “you” or “your” means the person taking up the solution and includes any other person you allow to use (give instructions and transact on) the solution.
- The words “us”, “our”, “we” means FirstRand Bank Limited or the entity within the FirstRand group of companies who is the solution provider unless indicated otherwise or where it is clear from the context that another entity is referred to. The other entities in the FirstRand group of companies may also accept rights and benefits established by way of these Standard T & Cs, in which case these Standard T & Cs will also apply between you and such other entities.
- The word “solution” means any banking, lending, insurance, investment, telecommunications or other products, goods, services, benefits, policies and rewards you select with us. This excludes third-party providers products and services.
- The words “interface” or “channel” means any way you can use to interact with us or made available by us for interaction, for example through an app or a website without assistance, or through assistance from a representative, for example face-to-face with our employees, and any future methods made available through our platform.
- The “platform” is your key to trusted, innovative technology and solutions. You can use our platform to do many exciting things like browse, view, or take up offerings available in the country from where you are accessing the platform; connect and interact with us; shop at our virtual shopping mall; and connect with other consumers, suppliers, producers, retailers, wholesalers and other third-party providers of goods and services. Use of our platform is governed by our Platform Rules.

1. OUR AGREEMENT

- Each solution has its own solution agreement with applicable terms and conditions and other documents that may apply to that solution. In addition, these Standard T&Cs and our Platform Rules apply to each solution.
- Nothing in these Standard T & Cs is intended or must be understood to unlawfully restrict, limit, or avoid any right or obligation created for either you or us in terms of any other applicable laws. Applicable laws refer to the relevant laws and regulations that may apply to our platform, interfaces, channels or solutions.
- If there is a conflict (clash) between a clause in these Standard T&Cs and a clause in the Platform Rules the clause in these Standard T&Cs will apply.
- If there is a conflict (clash) between a clause in these Standard T&Cs and a clause in the solution agreement the clause of the solution agreement will apply.

2. RULES APPLICABLE TO INTERFACES AND CHANNELS

(This clause is applicable as soon as you register to use an interface or channel, get access to use an interface or channel or use an interface or channel whichever is the soonest.)

- You must be 18 years or older or a major to use our interfaces and channels. If you are younger than 18 years or a minor, you must have the consent of your parent or guardian to use our interfaces and channels.
- We will only process your instruction or transaction if we are permitted to do so in law and contract.
- If you transact or give instructions on our interfaces and channels, you agree that:
 - We do not have to process the instruction or transaction if you do not have sufficient funds in the relevant account.
 - There are instruction or transaction limits that apply for your protection. These limits may be set for your solution or account, for other persons allowed to transact on your solution or account or for the interface or channel. We do not have to carry out any instruction or transaction from you if you exceeded or will exceed the limit. If you need to exceed any limits, you need to arrange with us beforehand by way of our interfaces or channels. For security reasons, we reserve the right to adjust the limits at our discretion. Please refer to your solution agreement regarding credit limits for credit or lend solutions.

- You must give us correct and complete information when you give us instructions or when you transact. We are unable to, and do not, check or confirm all information related to the instruction or transaction.
- **We are not responsible if you do not complete an instruction or transaction or if you do not follow our instructions when you transact.**
- Some instructions or transactions cannot be reversed or stopped once you send them.
- Instructions or transactions on unassisted or assisted interfaces and channels take the same time to complete unless we state otherwise. Some instructions or transactions may take longer to be completed. Please obtain the turnaround times from our interfaces and channels, especially if you have an urgent instruction or transaction.
- You must not assume that we have received an instruction or transaction until we have confirmed receipt, or acted on the instruction or transaction, whichever happens first. If you are not sure if an instruction or transaction has been sent, received or processed you must contact us. Do not submit an instruction or transaction again as this can result in the same instruction or transaction being processed again and you will be responsible for the duplicated instruction or transaction.
- **You will be regarded as having accepted and authorised all instructions and transactions and changes to your interface, channel, solution or account settings made via the interfaces or channels.**
- **Software Risk:** From time to time, we may make third party software or applications available for download via our interfaces or channels. You download and use this software or applications at your own risk. We make no warranty about this software or applications. You will be bound to the license terms of the software licensor. You agree to indemnify us and hold us harmless if you breach the license conditions.
- If you interact, give instructions or transact with any third-party providers on our interfaces or channels, then you agree that:
 - **We will not be liable for any delays caused by third-party providers.**
 - **We are not responsible for links to third party websites, its content, for the third party's actions or omissions, or its products, goods or services.**
 - The interfaces or channels may allow you to view or access third party websites or content or purchase products, goods or services provided by third parties. Even though we may make third party websites, content or products, goods or services available to you, we do not endorse or recommend the third party or its products, goods or services. You alone are responsible for deciding whether the third party or its products, goods or services meet your requirements. Terms and conditions may apply to those third-party products, goods or services and form an agreement between you and the third party.
 - You alone are responsible for obtaining the terms and conditions that apply to you and the products, goods or services offered by the third party. The categories or types of third parties whose products, goods or services may be available from or associated with the interfaces or channels may vary from time to time. We have no control over such third parties or their products, goods or services. We are not a party to any disputes between you and the third party. You are responsible for ensuring that any transactions you make or instructions you give on these third-party sites are lawful.
 - **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, goods or services or your use of the products, goods or services. You take the risk of using or purchasing third party products, goods or services. You hereby agree to indemnify us and hold us harmless for any loss or damage you may suffer in this regard.**
- When you access our interfaces and channels, you agree to the following:
 - You play an important role in protecting yourself against fraud. For your safety you must follow the security tips we give you on the interfaces and channels, including the tips published at the Security Centre on our interfaces and channels.
 - You must logoff from the interface or channel after using it.
 - You should avoid using public communication facilities such as internet cafés, but if you do, you must take special care to protect your digital security.
 - You must have the necessary anti-virus or anti-malware software on your devices.
 - Each time you engage with us on or logon to non-face to face interfaces or channels (like our Apps or websites), you must enter the correct access information or take any other steps we may require for us to verify your identity and the electronic communications you send us. This is known as authentication. Access information

- includes access credentials, or Cell phone 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 do not meet the authentication requirements. We may require an additional layer of authentication for certain transactions. This may include transactions where a unique number known as a One Time PIN (OTP) is sent to your device or when an App Push Notification is sent to your App 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. Notify us immediately by calling the numbers available on our interfaces or channels to enable us to secure your profile. You may also call us via the App.
- You must, at your own cost, have the necessary equipment, hardware, software and access to third-party communication services (as applicable), including any upgrades you may require, to access our interfaces or channels. You are responsible for the equipment you use to access the interfaces or channels. We have no control over the equipment, software or service providers. **We are not responsible for any error or delay that may arise or if you are unable to access the interfaces or channels because of your equipment, software or services provider.**
 - We will act on and accept all instructions or transactions done after you entered your correct access credentials and met the verification requirements set by us. **We will assume that all such instructions or transactions were authorised by you, even if such instructions or transactions took place without your knowledge or consent or were not authorised by you.** This will not apply to instructions or transactions that occur after you requested that we cancel your access credentials.
 - 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 or channel). This means that these electronic communications will have the same legal effect as written and signed paper communications from you.
 - **IMPORTANT:** You must never give or show your access credentials to any person, including our employees or anyone claiming to work for or represent us in any way. You must never respond to requests to enter or “confirm” your 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. We will never ask you to give us your sensitive secret information, including access credentials by email, SMS, instant message or even over the telephone. **We will not refund you if you respond to these “phishing” messages and lose money as a result of doing so.** Fraudsters will also attempt to call you to get your access credentials (“Vishing”). You can also receive an SMS with a link (“Smishing”), and you should never interact with anyone who attempts to obtain information via “Vishing” or “Smishing”.
 - Certain financial aggregation apps (like apps that help you track your spending across different financial institutions) may ask you to enter your access credentials to use their service, but if you do so, you put yourself at risk and third parties will be able to access information about your accounts, instructions, transactions and other confidential information. **If you are defrauded because you used a third-party app or site, we will treat this as a voluntary compromise of your access 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.**
 - You are strictly prohibited from allowing any systems to log in on your behalf into our interfaces or channels. This includes payment gateways, data aggregation apps and screen scraping. For example, if you make a payment on a third-party application by using an instant EFT, the payment provider may require access to your banking profile with us and this could compromise your access credentials.
 - The same access credentials can be used to access different interfaces or channels. This means that if your access credentials are disclosed to someone else you can be defrauded across all the interfaces or channels. You must immediately contact us if you know or even suspect that your access credentials have been compromised to ensure that your profile is secured.
 - By allowing an authorised user to access your profile using the interface or channel, 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.

- You must notify us immediately when any user's access rights must be changed or cancelled by completing and signing the required forms. You can also do this on our interfaces and channels. Any cancellation of, or change to, a user's access rights will not affect any instruction submitted or transaction made by that user before the change has been made.
- You must ensure that your device which you use for instructions or transactions is always in your possession and protected with an additional access code, password or pattern lock. If your device to which your App or online banking is linked is no longer in your possession permanently (for e.g., due to theft, loss or if you sold it) or temporarily (your device is being repaired) you must contact us immediately and delink your App or online banking immediately.
- If you receive suspicious communications (including emails, SMSs) or if you suspect or know that your access credentials were lost, stolen or may be used without your permission, call us on the numbers available on our interfaces and channels and block your profile via the App or website. Standard network rates will apply.
- You must not keep your access credentials together with your access cards or other documents. Do not store your access credentials on the equipment you use to access our interfaces or channels. For example, never store your PIN or Cell phone Banking PIN on, with or near your mobile, computer, and devices. For security purposes, we recommend that you memorise your access credentials.
- You are not allowed to register for or access the interfaces or channels using someone else's access credentials or personal information.
- You must immediately ask us to cancel your access credentials if you suspect or know that your access credentials were lost, stolen, or may be used without your permission.
- **If there is a dispute about whether or when you told us to cancel your access credentials, it will be your responsibility to prove how and when you told us to cancel your access credentials. For this reason, you must request and keep any reference numbers we give you when you call us to cancel your access credentials or any other calls you make to us.**
- After we have cancelled your access credentials, we will reject all instructions and transactions done from the date on which your access credentials were cancelled.
- We reserve the right to block your access to the interfaces or channels at any time to maintain or restore security, if we reasonably believe that your access credentials were or may be obtained or are being used or may be used by an unauthorised person.
- 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 police service or law enforcement agency. We will investigate any loss that you suffered because of the alleged fraud. You must co-operate with us and the police service or law enforcement agency in any investigation.
- You must comply with the user guidelines we put on the interfaces or channels. If there is a conflict (clash) between these Standard T&Cs and the guidelines, these Standard T&Cs will apply instead of the guidelines.

3. FEES AND CHARGES YOU MUST PAY US

- In return for providing you with solutions, you will be liable to us for the fees, charges and interest as stated in the solution agreement, annual pricing letter, pricing guide or relevant interface and channels.
- We may, where permitted and without prior notice, charge all fees and costs which are due and payable against your demand deposit account or other account nominated by you for these purposes or, if you did not nominate an account or if the funds in those accounts are insufficient, against any account of yours held with us.
- We may charge you for enquiries we receive from you about a payment. We will inform you what the charge is before we start investigating your enquiry.
- We may, to the extent allowed by law, increase our fees and charges from time to time. We may waive, reduce or reverse fees or charges on a case-by-case basis. If possible, we will advise you of any changes to fees and charges by giving you notice of the changes within a reasonable time before the change takes effect, or as required by law or codes of conduct.

4. WHEN AND HOW WE WILL SEND YOU STATEMENTS

- We may provide you with the ability to view or download certain statements, if required by law, by making it available on our platform and it may be obtained by using one or more of the following interfaces or channels: Online, App, Automated Deposit Terminal (ADT), Automatic Teller Machine (ATM), Cell phone banking or at any of our branches. You may be charged for statements. **In exceptional circumstances we may email statements at your request and at your own risk.**
- Your statement will reflect all the transactions on your solution for the period shown on the statement. Transactions carried out, but not yet cleared, paid, deducted from your solution will not appear on your statement for that statement period. You may view pending transactions on the App or website.
- Certain information, including your account balance information that is made available to you on the interfaces or channels may be delayed and may not show your recent transactions. You can confirm your account balance information by contacting us.

5. YOU MUST CHECK YOUR STATEMENT CAREFULLY AND REPORT ANY MISTAKES

- You must check each entry on your statement carefully as soon as you get your statement.
- You must report any mistakes or transactions done without your permission to us within 30 calendar days from the date of the statement. Our contact details are available on our interfaces and channels. **If you do not do this, we will treat the entries and transactions shown on the statement as correct or done by you or with your permission.**
- **IMPORTANT: We will not be responsible for any loss or damage you suffer because you did not report errors or unauthorised transactions in time. If you receive inContact notifications, you must report any unauthorised transactions to us immediately, without any delay, to prevent further unauthorised transactions. If you do not do this, we can hold you responsible for those transactions.**

6. INCONTACT NOTIFICATIONS

- inContact is a messaging service which provides you with notifications of certain account activity via App Push Notification to your selected mobile number via a direct message to your linked App or via email to your selected email address or via SMS to your selected mobile number. It is important that you read your inContact notifications as soon as you receive them.
- In certain circumstances we will first try to send you a direct message via an App Push Notification, and if we cannot, we will send you an SMS or email.
- inContact is designed to help you track activity on your account and minimise potential unauthorised transactions.
- You may incur a fee for the inContact Notification Service. Kindly refer to our pricing guide located on our websites or Apps for the full fee structure.
- The types and values of transactions that we provide notifications for do change from time to time. You must take the necessary precautions by safeguarding your solutions, accounts, cards, device and access mechanisms, such as usernames, passwords, OTPs and PINs. You are responsible for ensuring that we have your correct mobile numbers and email addresses. Your inContact information may be updated through our interfaces or channels.
- You must keep your inContact details i.e., your selected cell phone number and or email address up to date at all times.
- **We will not be held responsible if your SMS or email is sent to the wrong number or address.**
- We cannot guarantee receipt or delivery of an SMS or e-mail as we and you use external third parties (like your telecommunications provider) for relaying of SMS or e-mail. Although we do send you inContact notifications, your statement will be the main and final record of all transactions on your account.

- If there is a dispute about when a notification was sent, the records on our system will be proof of the date and time of the sending of the notification unless you can prove otherwise.
- If you do not notify us of any unauthorised transaction, you agree that we can treat the transaction as correct and hold you legally responsible for the transaction as if you had done or approved it.
- In the event of fraud, you must report the suspicious or unauthorised transactions to us immediately. We will investigate any loss that you suffered because of any suspicious or unauthorised transactions and it may be necessary, as part of our investigation, for you to supply us with certain information, including a police services or law enforcement agency case number. You must co-operate with us and the authorities in any investigation and provide us with accurate information. We may refund you once it has been established that you suffered financial loss as a direct result of the fraud, but only if certain conditions are met, as determined by the specific solution agreement. This may include your negligent actions – like compromising your access credentials.
 - Note: This clause does not apply if the fraud or suspected fraud was committed by an authorised user or additional cardholder.
- inContact subscribers can access Cell phone Banking Lite by dialling *120*321# (note: airtime charges may apply) (applicable to South Africa only). You can use it to monitor your account by viewing transactions and balances on all accounts linked to your profile and to perform limited transactions.
- If you are registered for online banking or the App, your inContact number can be used to receive your OTP. Should your OTP and inContact numbers be different from each other you must maintain them individually. If your OTP number differs from your inContact number, your OTP number is not automatically updated when you change your inContact details.
- If you are a Cell phone Banking or inContact user and you notice anything suspicious you must also contact us immediately. Thereafter please also contact your service provider/network operator to report the suspicious activity e.g., SIM SWAP (a sudden loss of service can be an indication of a SIM SWAP).

7. HOW WE TREAT YOUR PERSONAL INFORMATION (Privacy Term)

- We may record all interactions with you to:
 - check that we carried out your instructions correctly and that we are meeting our regulatory obligations;
 - help detect or prevent fraud or other crimes; and
 - improve our services to you and other customers.
- Your personal information (which, for the purposes of this term, includes special personal information) will be held by entities within the FirstRand group of companies.
- To better understand the entities that form part of the FirstRand group of companies and how your personal information is treated, please refer to FirstRand's Group Customer Privacy Notice which forms part of this privacy term. The privacy notice can be found on our Apps and websites or contact us to request a copy.
- In this privacy term references to "we", "us" or "our" are references to the entities in the FirstRand group of companies, and all affiliates, associates, cessionaries, delegates, successors in title or third parties (authorised agents and contractors), when such parties are acting as responsible parties or operators in terms of applicable privacy laws, unless stated otherwise. References to privacy related terminology used in this term (such as personal information and responsible party) should also be read as to incorporate any similar terminology used in the jurisdiction in which your personal information is processed.
- By accepting these Standard T&Cs or by using any solution offered by us, you acknowledge that to:
 - conclude and fulfil contractual terms or obligations to you;

- comply with obligations imposed by law; or
- protect or pursue your, our, or a third party's legitimate interests, including offering solutions that best meet your needs,

your personal information may be processed through centralised functions and systems across entities in the FirstRand group of companies as well as cross-border and may be used for the purposes, in the manner, and with the appropriate controls as set out in our privacy notice.

- Where it is necessary to obtain consent for processing outside of this privacy term, we will explicitly seek your consent separately.
- We want to ensure that you fully understand how your personal information may be used. We described the purposes for which your personal information may be used in detail in our privacy notice. We also set out further information about accessing, correcting or objecting to the processing of your personal information in our privacy notice. We strongly advise that you read our privacy notice, given its incorporation into your agreement with us and in these Standard T&Cs.
- If you are a juristic person (for example, a company or a trust) it may also be necessary for the FirstRand group of companies to obtain personal information of parties who are related to your business or activity, such as members, directors, ultimate beneficial owners, shareholders or trustees (as applicable) and as set out in more detail in our privacy notice.
- For the purposes of these Standard T&Cs, the responsible party is the party with whom you are contracting a solution (using a solution), as well as other entities in the FirstRand group of companies, which are listed in our privacy notice as responsible parties. For the contact details of these responsible parties, see our privacy notice.

8. ADDRESSES FOR SENDING CORRESPONDENCE AND LEGAL NOTICES

- We may communicate with you using any communication method.
- We will send any communications to the contact details we have on record for you. We may also communicate with you using our platform interfaces and channels like our App or by means of a publication/advertisement in the media.
- Legal documents and notices that we serve or deliver, will be served at your physical address/employment address/mortgaged property address/registered address/ principal place of business/ last street address we have on record for you or your last known e-mail address or cell phone number as recorded on our system or the last known details we obtained. This is your chosen service address for legal documents and notices.
- You must send us any legal notices or summonses to the following address, which we choose as our domicilium: FirstRand Legal, 3rd Floor, 4 Merchant Place, Corner Fredman Drive and Rivonia Road, Sandton, 2196. [This address may differ for countries other than South Africa. Please refer to your solution agreement for an address in your country.]
- You must immediately tell us if any of your contact details change. You can do this on our platform by making use of our unassisted and assisted interfaces and channels like visiting any branch or by calling our call centre. If you change your street address, you must give us proof of your new address. It may take up to 15 days for the change to reflect on our systems.
- Where we may need to update your records, you agree that we may get your contact details from other companies in the FirstRand group of companies.
- Any correspondence we send to you will be considered to be delivered to you if:
 - delivered by hand during business hours (between 8h00 and 17h00) – on the date it was delivered.
 - posted by registered mail – at 10h00 on the fourth day after the post office issued the registration receipt.
 - posted by ordinary mail – at 10h00 on the fourth day after the document is posted.
 - sent by e-mail – on the date on which the document was e-mailed.

- sent by SMS or MMS – on the date on which the document was sent.
- sent by printable webpage – on the date the page is displayed.
- sent by instant message App Push Notification or messaging via platform – on the date of transmission.
- Any notices or correspondence we make available on our website, App, our ATM network, our bank branches or in the media will be considered to have been received by you on the date it was published.
- A notice actually received by you is considered delivered even if the delivery method or address is not aligned to this clause.

9. INDIRECT INTERFACE OR CHANNEL INSTRUCTIONS

- We make various interfaces and channels available to you and you have the right to choose which interface or channel you wish to use.
- We take reasonable steps to incorporate various verification and other security checks and measures into all our interfaces and channels. However, direct interfaces and channels (such as verified websites, cell phone banking and Apps) provide better protection to you than indirect and unsecured interfaces or channels (such as e-mail). We therefore encourage the use of direct interfaces or channels and discourage the use of indirect interfaces or channels. Indirect interfaces and channels are methods of interaction that do not require identification and verification for interaction, like emails.
- We make our indirect interfaces or channels available to you on the following basis only and you expressly acknowledge and agree that:
 - **Indirect interfaces or channels carry various increased risks. For example, indirect communications can easily cause errors or can be intercepted, changed without your knowledge or consent or sent by unauthorised individuals claiming to provide instructions on your behalf. There are also many factors associated with indirect interfaces or channels which are beyond our control. By using indirect interfaces or channels, you accept these risks.**
- Whilst we will take reasonable steps to verify the instructions we receive via indirect interfaces or channels:
 - **we cannot provide any assurances in this regard, nor can we guarantee that our checks will prevent fraud. You bear the risk of fraud.**
 - **you alone are responsible for ensuring that we receive your instructions and that they are correct.**
 - we will only be deemed to have received an instruction once we have confirmed receipt in writing or over telephone. For clarity (but by way of example only), if an instruction is received more than once, or not at all, or late, or in error, or if it contains inaccuracies, we cannot be held responsible.
- **You will have no claim against us for any loss or damage of any nature that you may suffer due to the use of indirect interfaces or channels, and you waive any such claim, except where such loss or damage was caused by our gross negligence.**
- **You hereby indemnify and hold us harmless against any claim of any nature which you or any third party may have, relating to the use of indirect interfaces or channels, except where such claim arises due to our gross negligence.**

10. SECURE CHAT AND CALL

- You can use Secure Chat on our Apps which allows users to chat with users or with us. Secure Chat may not be available on all Apps or in all countries.
- Secure Chat is available to the account holders of qualifying accounts who additionally may have the authority to mandate advisors to perform transactions on their behalf.

- You can only use Secure Chat if you meet the eligibility criteria and continue to comply with our solution agreements; applicable laws; regulations and industry rules.
- There is currently no fee for the use of the Secure Chat service; however, we reserve the right to charge a fee at a later stage.
- **We do not assume liability for loss; whether direct or indirect; or damage which you may suffer from using the service such as loss or damage resulting from typographical errors, duplicate instructions or delayed messages due to a loss of connectivity not occasioned by us.**
- Users of Secure Chat services must be 18 years of age or older or a major.
- Licence (relevant to the intellectual property held): With respect to your chats, you grant us a non-exclusive, perpetual (i.e., everlasting), world-wide, royalty free, irrevocable (i.e., irreversible), fully sub-licensable and non-exclusive license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute and display such posts throughout the world in any media.
- All chats will be between you and the other user only and we are not a party to the chats unless you are having a chat with our representatives.
 - While we may be capable of retrieving specific details of a chat, a retrieval can only be initiated based on a subpoena or to adhere to our Information Manual prepared in accordance with Section 51 of the South African Promotion of Access to Information Act 2 of 2000 or in terms of similar manuals or enabling legislation in the relevant country where we are established.
 - You must notify us immediately if you become aware of any unauthorised chat which are attributed to your profile. You can notify us using the contact details on our Apps or websites.
 - **Violation of these Standard T & Cs may lead to the immediate removal of all your chats, irrespective of your individual chats' compliance with these Standard T & Cs, without notice, warning or explanation to you and could also lead to you not being allowed to use the Secure Chat services.**
 - We will fully co-operate with any law enforcement authorities or court order requiring us to disclose the identity or other details of any person whose chats are in breach of these Standard T & Cs.

11. ELECTRONIC VOUCHERS AND REDEMPTION OF DISCOUNT BENEFITS

- Certain third parties offer electronic discounts on certain products or services via their computer system from time to time for redemption against products or services purchased. We offer qualifying users the opportunity to receive these discounts when paying with their qualifying accounts or cards. The qualifying cards may change from time to time and you are encouraged to ensure that you check our interfaces and channels periodically for updates.
- **We do 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 where the purchase was made. We do not have any control over the products or services that the discounts are offered for and cannot be held liable for the unavailability of these products or services in any way. Complaints regarding quality or quantity of the products purchased must be directed to the third-party concerned. Whilst we make every endeavour to ensure the accuracy of the discount offered, changes may be implemented from time to time. We do not accept any responsibility for any loss which may arise from accessing or reliance on the information from a third-party and to the extent permitted by 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 discounts or benefits.**

12. AUTHORISED USERS

- We will allow another person to act on your behalf and to use, transact and access your solutions if you followed our prescribed process to give that person such authority. This includes the submission of know-your-client information about the authorised user, submission of relevant resolutions, authorisations or appointments of agents related to the authorised user, acceptance of terms and conditions applicable by the authorised user and our verification and confirmation of the information and final acceptance of the authorised user. We refer to these persons as authorised users.
- **Anything done by your authorised user will be regarded as your actions or transactions and you will be liable for consequences of those actions or transactions.**
- **You will be responsible for all debts authorised users incur including fees and charges, any overdrawn amounts plus interest on those amounts. You will be responsible for anything they do or fail to do.**
- There is risk involved in appointing someone else as your authorised user. You must consider if restrictions or limits must apply.
- You must provide correct and up to date information about the authorised users. You are responsible for deciding and checking what rights must be given to authorised users.
- You must immediately notify us of any changes to your authorised user on the relevant interface. The changes will be effective when we update our records which may take up to 30 calendar days. There might be legal requirements that must be met before a newly appointed authorised user can transact, e.g., know your customer requirements and resolutions.
- You can cancel an authorised user's rights at any time. You will be liable for all actions of an authorised user until our process to remove the authorised user has been finalised, including any future dated payments.
- The rights you gave to any authorised user will also come to an end where the law requires it, such as on your death or if you become legally incompetent or by court order.

13. EVENTS BEYOND OUR CONTROL

- At certain times, we may be prevented from providing solutions to you or fulfilling our obligations to you because of things or events that are outside of our control. This includes, but is not limited to:
 - involuntary interruptions outside of our control such as electricity failures or blackouts or the unavailability of any telecommunications system or networks;
 - government actions; or
 - wars, fires, floods, strikes, civil unrest, epidemics.
- **In such cases we will not be responsible for any failure to perform any of our obligations to you or any person (including users of our platform), and our obligations will be suspended, for as long as such interruptions continue. We may if we choose to, where possible, give you prior notice of interruptions and changes, but we have no duty to do so.**
- **Without limiting the clauses before, we will not be legally responsible to you or any person for any loss, costs, expenses, damages, or any claims, lawsuits, demands, of any kind whatsoever, whether brought by an individual or any entity, because of any service interruptions that were beyond our reasonable control.**

14. PREVENTION OF HARM AND EXCLUSION OF LIABILITY

- **Although we take reasonable care to prevent harm or loss to you, we 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 platform, interfaces, channels or solutions.**

- **TAKE NOTE: We are not liable for the following:**
 - any loss or damage, which you or any other party may suffer due to unauthorised interception or surveillance;
 - any loss or damage if you did not take reasonable steps to safeguard your account, the PIN or passwords, cards, devices or other access mechanisms or follow the steps recommended by us from time to time; and
 - late or delayed transactions not caused by our gross negligence.

15. PREVENTION OF CRIMINAL ACTIVITIES AND TERMINATION OF CUSTOMER RELATIONSHIP

- In this clause, references to “we”, “us” or “our” are references to the entities in the FirstRand Group of companies (which includes but is not limited to FirstRand Bank Limited (Registration Number 1929/001225/06) (and acting through any of its divisions), and all affiliates, associates, cessionaries, delegates and successors in title.
- The entities within the FirstRand Group of companies (as defined in the FirstRand Group Customer Privacy Notice and which can be found on the FirstRand website or you can contact us to request a copy) try to stop or prevent criminal activities including tax crimes, money laundering, terrorist financing, weapons proliferation financing and international sanctions circumvention and are obligated in terms of its regulatory requirements to start measures to prevent these.
- You must use our solutions, interfaces and channels in compliance with all applicable laws and our requirements including but not limited to preventing bribery and corruption, human trafficking, money laundering, terrorist financing, weapons proliferation financing, tax crimes and avoidance, counterterrorism and local (from any country) and international sanctions.
- In keeping with our legal and regulatory obligations and in line with our contractual rights, the FirstRand group of companies may:
 - choose the customers we wish to do business with;
 - identify risks that customers may expose the group to; and
 - within our discretion, may decide whether the banking relationship should continue.
- These decisions will always be carefully considered, and we will not make decisions based on grounds which are not allowed such as race, nationality, gender, or religion.
- Various laws, including but not limited to the Financial Intelligence Centre Act, 2001 as amended (FICA) requires that we know and understand our customers.
- We also need to manage our risk exposure, including reputational risk, in a responsible manner. To manage risk as needed, we identify and monitor any risk that our business relationships may pose to us on an ongoing basis.
- As a result of this, the FirstRand group of companies can do any of the following things if we consider it necessary to do so, or domestic laws or international laws, rules, regulations, restrictions or policies require us to do so:
 - We may check and confirm the identity of any customer and entity as well as that of any related persons to or acting on behalf of or involved with such customers or entities and of any recipients of funds regardless of where they bank. This includes, but is not limited to, mandated persons, directors, trustees, signatories, ultimate beneficial owners, members, shareholders and related entities or persons. We will do this at the start of the business relationship and as often as we or the law considers necessary thereafter. We may also request, check and confirm information related to source of funds and any other information which we may reasonably need.

- We are obligated to monitor any transactions and instructions on your solutions at the beginning and/or on a continuing basis.
- We can request further information to verify the transaction, source of funds, instruction or beneficiary before acting on any instruction or transaction in accordance with various laws. This may result in a delay in us carrying out the instruction or transaction.
- We may refuse to carry out any instruction or transaction.
- We may refuse to do business with any person or entity where we consider their behaviour or associations to be outside of our risk appetite or where they are involved in ethically sensitive activities, as determined by us.
- We will not willingly and knowingly do business with any person or entity:
 - that appears on any sanction list, as set out by legislation or used by us in the management of our risk, including any person or entity who facilitates or is involved in activities with sanctioned persons,
 - deals with high-risk countries,
 - who is in any way linked to any person or entity that appears on such sanction list,
 - is linked to any restricted countries or the government agencies of such restricted countries as determined from time to time.
- In the case of fraud, suspected fraud, or where the law requires us, we can freeze your solution or terminate the banking relationship or service, or we can decline receipt of funds or refuse to carry out any instruction or transaction without notice to you. Fraud or suspected fraud includes (but is not limited to) instances where you receive funds through misrepresentation; you allow your solution to be used by a third party for fraudulent purposes such as a mule account or you provide false or not enough information to us. Please refer to the Security Centre tab on our Apps and websites for more information on the different types of fraud.
- We can terminate or temporarily restrict our relationship with you or your applicable solution (subject to the solution agreement) if we are made to do so by law or if we have reason to believe that a continued relationship will expose us to reputational, business or any other risk which may be outside of our risk appetite. Risk appetite means the level or type of risk we are prepared to accept, from time to time.
- Where we choose to terminate the relationship, and to the extent permitted by law, we will provide you with reasonable notice of termination.
- You may also terminate the relationship with us, or your applicable solution (subject to the solution agreement).
- We will, to the extent possible, provide reasonable assistance to you to close, terminate or transfer to another bank a solution upon us receiving a request from you for us to do so. We will not impose any unreasonable barriers to you in these circumstances.

- We can monitor any transactions and instructions on your solutions at inception and/or on a continuing basis.
- We can place a hold on any account, facility or solution.
- You agree to assist us to comply with the law and our internal risk requirements by providing us with all the information and documents we need. If you fail to do so or provide false or inadequate information or if the information you provide is outdated, we can refuse to enter into a relationship with you, refuse to carry out an instruction (including an instruction to transfer available funds and close a solution), suspend access to your participation in and the use of any rewards and/or customer benefits associated with any solution, restrict access to your solution, our channels and interfaces by placing a hold on your solution and can also terminate our relationship with you.
- **TAKE NOTE:** While we do our best to provide service to you, there might be certain situations beyond our control in providing these services. If we need to take actions to comply with the law, or if a foreign bank is unable to carry out an instruction due to their policies or governmental regulations, we unfortunately cannot take responsibility for any resulting loss or inconvenience to you.
- **IMPORTANT:** Our Guide and all necessary documents containing the circumstances that may lead to our refusal to provide a solution or render a financial service, or the withdrawal, termination or closure of a solution or withdrawal or termination of a financial service, is available on our Apps and websites. Alternatively, you can contact us to request a copy. Please refer to the Legal tab on our Apps and websites to access these documents.

16. ADMINISTRATION, DEBT REVIEW, INSOLVENCY, SEQUESTRATION AND BUSINESS RESCUE

- You must tell us immediately if you apply for, are placed under, an administration order, debt review, sequestrated, liquidated, placed under business rescue, judicial management, curatorship, receivership or any similar limitation is applied to you (whether provisional or final), or any government agency exercises any resolution powers or option in respect of you or you become legally incompetent, is deregistered or is in the process of deregistration, or failed to maintain your corporate identity, dissolves or if you cease to conduct business in the ordinary course.
- If you are sequestrated, liquidated, wound-up, deregistered, failed to maintain your corporate identity, dissolved, or any similar limitation is applied to you (whether provisional or final) the full amount you owe us will be payable and access to any money in your solutions will be restricted.
- If you pass away, the full amount you owe us will be payable and third-party access to any money in your solutions will be restricted.

17. CERTIFICATES OF BALANCE AND RECORDS

- If we need to take legal action against you, one of our authorised employees whose authority need not be proved will produce a certificate, which shows the amount you owe us. If you do not agree with this certificate, you will have to prove that it is wrong.
- If there is a dispute about any matter or record, our records certified as correct by any authorised employee whose authority need not be proved, will serve on the face of it as proof. This means it will be treated as correct unless you can prove it is wrong.

18. SET-OFF

- Where the law gives us the right, we may:
 - Place your money (credits) on hold until we have a discussion with you about any amount you owe us.

- Set-off any outstanding amounts that are due and payable by you to us against money (credits) in other solution accounts you have with us.
- We will notify you if we apply set-off.

19. JURISDICTION AND COSTS

- We can take legal action against you in a Magistrates' Court or lower court that has jurisdiction. We may also take legal action against you in the High Court, Supreme Court or any other competent court with jurisdiction in our sole discretion.
- You agree that we may charge legal and collection fees, stamp duty, costs and charges and taxes to your solution and that it will form part of the outstanding balance.
- You will be liable for our legal fees, costs and charges we demand subject to any requirements of the law. Such costs may include, but are not limited to, tracing costs, collection commission, legal costs to issue and serve summons, obtain judgment, issue warrants or writs, effect attachment and arrange a sale in execution, disbursements and sheriff's/bailiff's fees.
- These fees, costs and charges remain due, owing and payable by you until settled in full.

20. CHANGES TO THESE STANDARD TERMS AND CONDITIONS

- No changes to these Standard T & Cs and no waiver (giving up) of any of our rights will be binding on us unless it is recorded in writing and signed or issued or accepted by our authorised representatives.
- We may change or update these Standard T & Cs at any time. Changes may be required for reasons including (1) new regulations or regulator guidance has been introduced or existing regulations or regulator guidance has changed; (2) we updated or changed our interfaces, channels or solutions; (3) we introduced new ways in which to combat fraud; or (4) changes in technology or our processes or industry standards.
- Where the changes are in our view important, we will notify you of the changes via the interface, channel or by sending a notice to you, for example a letter, e-mail, SMS or App Push Notification. A change will be regarded as important if such change may have a significant impact on you including your rights, a change that could lead to a penalty to you or a change to the relationship between us. Your continued use of our interfaces, channels and solutions will be regarded as an acceptance of the change.
- If you do not want to accept any of the changes, you may cancel your whole relationship with us by cancelling and settling each solution agreement in accordance with the terms specified in the solution agreement. Termination of a solution agreement shall only take effect once all obligations in terms of the applicable solution agreement are complete.
- Changes will only apply to rights and obligations from the date of the change going forward.

21. VALUE-ADDS

- To qualify for any value-added solutions, your FirstRand group of companies' relationship must be in good standing. Good standing means that none of your solutions should be overdrawn, or be in arrears, or be in default, or be subject to any legal process with the FirstRand group of companies.
- Legal process means any legal proceedings in any court of law involving you and the FirstRand group of companies including but not limited to business rescue, judicial management, curatorship, receivership, collections, liquidation, administration, wounding-up and sequestration proceedings.
- For the purposes of this clause, legal process will exclude debt review, but this will still have an effect on the qualifying criteria of all value-added solutions.

22. BREACH OF CONTRACT

- In the event of either party committing a breach of any of these Standard T&Cs, the non-breaching party may give notice, provided that such breach is capable of being remedied, to the party in breach to remedy such breach within a period of 7 calendar days after receipt of the written notice.
- If the breaching party fails to remedy the breach within the notice period, the non-breaching party may, in its sole discretion and without prejudice to any of its other rights in law, either claim specific performance, or cancel these Standard T&Cs on immediate written notice.
- In addition, the non-breaching party shall be entitled to claim and recover damages from the breaching party.
- We may cancel these Standard T&Cs at any time on immediate written notice to you if:
 - you commit a breach of these Standard T&Cs which cannot be remedied;
 - you are, other than for the purposes of reconstruction or amalgamation, placed under voluntary or compulsory liquidation, winding-up, business rescue, judicial management, placed under curatorship, receivership, deregistered or the equivalent of any of these in any jurisdiction;
 - a judgment against you for which no appeal lies or for which the period for lodging an appeal (excluding any period to seek condonation) has expired and remains unsatisfied for a period of at least 30 calendar days;
 - you make or offer to make a general assignment or any arrangement or composition with or for the benefit of your creditors generally (or any class of its creditors) for releasing you wholly or partially from your debts;
 - you are or become a sanctioned entity;
 - you contravene any sanctions or are placed on any sanctions list by any sanction's authority; or
 - participate in, facilitate, are or become the beneficiary of any sanctioned transaction.

23. ASSIGNMENT, CESSION AND DELEGATION

- You may not cede, assign, transfer or make over any rights or delegate any obligations in terms of these Standard T&Cs.
- You consent to any cession of our rights and to any delegation of our obligations including security held under these Standard T & Cs.
- You agree to splitting of claims which may arise as a result of a cession and/or delegation by us as contemplated in these Standard T&Cs.
- Without notice to you, we (or any person to whom our rights and obligations are ceded, delegated and assigned) will be allowed to cede, delegate and assign any or all of our rights and obligations under these Standard T&Cs, either absolutely or as collateral security to any third party.
- If any agreement and document must be entered into by or on your behalf about the cession or delegation, you agree to action either your signature or acceptance upon our request.
- Upon cession, delegation and assignment and on notice to you, you must make payment directly to the cessionary, without any set-off, deduction or withholding.
- You agree that we may share these Standard T&Cs and information about you with any person to whom we cede, delegate and assign our rights and obligations under these Standard T&Cs.
- If these Standard T&Cs are ceded and delegated (assigned) to another, the payment instruction may also be ceded and delegated (assigned) to that person.
- Personal information and information related to a user of the platform may be transferred to another entity in the FirstRand group of companies – this may include your personal information, information, and data. That entity will adhere to all privacy laws, all privacy undertakings the FirstRand group of companies has given and all processing and marketing

consent preferences you have provided the FirstRand group of companies (including opt-ins and opt-outs). We will provide you with notification of this transfer of personal information and information.

24. FACTUAL REPRESENTATIONS

- By entering into these Standard T & Cs, you admit that no reliance is placed, on any warranties, representations, disclosures or expressions of opinion which were not included in these Standard T&Cs.
- **We shall not be held responsible for any errors or discrepancies in respect of any information provided in respect of any consumer goods prior to the conclusion of these Standard T&Cs.**

25. ERRORS AND OMISSIONS

- We reserve the right in our discretion to alter, modify, upgrade, update, suspend or withdraw any advertisements, any advice or information provided by our interfaces or other vendors of our solutions.
- **We will not be held responsible for any errors or discrepancies in the information provided. We strive to keep our information up to date and it is to our, and our vendor's, best knowledge that the information contained herein is correct, however we will not be held responsible if an error is found.**

26. MISCELLANEOUS MATTERS

- While we may give you extra time to comply with your obligations or decide not to exercise some of our rights, you must not assume that this means that these Standard T&Cs changed or that it no longer applies to you. We can still insist on the strict application of any or all our rights at a later stage.
- Every clause of these Standard T&Cs is severable from the others. If one or more of the clauses is invalid, it will not mean the rest of these Standard T&Cs are invalid. The rest of these Standard T&Cs will still apply.
- If you live or are registered outside the common monetary area (South Africa, Namibia, eSwatini, and Lesotho) additional rules may apply to you.
- For purposes of interpreting these Standard T&Cs, any reference to us includes our successors and assigns, and any of our officers, agents, staff and authorised representatives acting on our authority.
- Our relationship and these Standard T&Cs are governed by the law of the country where the entity in the FirstRand group of companies, who is providing you with the relevant solution, is incorporated.
- Any reference to 'days' shall be construed as a reference to calendar days. The term 'business day' shall mean a weekday from Monday to Friday excluding any official public holiday.
- Any number of days prescribed shall be determined by excluding the first and including the last day or, where the last day falls on a Saturday, Sunday or public holiday, the next business day.
- We may in our sole discretion require the signature of any agreement, any amendments or any other documents by way of an 'electronic signature' (as defined in the relevant legislation) provided to you or another method of electronic signature notified to you by us.
- The rule of interpretation that a contract will be interpreted against the party responsible for the drafting or preparation of a contract will not apply to these Standard T&Cs.
- A reference to any statutory enactment or any specific section thereof shall be construed as a reference to that enactment as amended or substituted from time to time and to the relevant replacement section in any amended or substituted enactment.

27. FINANCIAL ADVISORY AND INTERMEDIARY SERVICES ACT 37 OF 2002 "FAIS" – REGULATORY DISCLOSURES - THE FOLLOWING IS APPLICABLE TO SOUTH AFRICA ONLY.

Full name, registration number and FSP Number	<ol style="list-style-type: none"> 1. First National Bank a division of FirstRand Bank Limited Registration No. 1929/001225/06 (FNB). FSP No. 3071. 2. FNB Financial Advisory, a business unit of First National Bank, a division of FirstRand Bank Limited. Registration No. 1929/001225/06. FSP No. 3075. 3. FNB Premium, a segment of First National Bank, a division of FirstRand Bank Limited. Registration No. 1929/001225/06. FSP No. 624. 4. FNB Commercial which is part of FNB a division of FirstRand Bank Limited. Registration No. 1929/001225/06. FSP No. 20081. 5. FNB Fiduciary (Pty) Ltd. Registration No. 1986/003488/07. FSP No. 574. 6. FNB Stockbroking and Portfolio Management (Pty) Ltd. Registration No. 1996/011732/07. FSP No. 182. 7. WesBank, a division of FirstRand Bank Limited. Registration No. 1929/001225/06. FSP No. 19233. 8. Direct Axis SA (Pty) Ltd. Registration No. 1995/006077/07. FSP No. 7249. 9. Direct Axis SA (Pty) Ltd. Registration No. 1995/006077/07 FSP No. 5. 10. The Engine Room Direct Solutions (Pty) Ltd. Registration No. 2009/005040/07. FSP No. 45528. 11. Motorite Administrators (Pty) Ltd. Registration No. 1997/000637/07. FSP No. 9140. 12. Small Area Repair Technology Underwriting Managers (Pty) Ltd. Registration No. 1999/016066/07. FSP No. 9861. 13. FNB Investor Services (Pty) Ltd. Registration No. 2011/139123/07. FSP No. 44341. 14. First Risk and Advisory Services (Pty) Ltd t/a FNB Brokers Registration No. 2022/755819/0.7 FSP No. 52961. 15. Rand Merchant Bank, a division of FirstRand Bank Limited Registration No. 1929/001225/06 (RMB). FSP No. 664. 16. Pointbreak Wealth Management (Pty) Ltd. Registration No. 2000/429. FSP No. 18470 17. Pointbreak Investment Management (Pty) Ltd. Registration No. 2007/016805/07. FSP No. 34381.
Physical and Postal Address	4 Merchant Place, Fredman Drive, Sandton, 2196
Contact details for general enquiries	Tel – 0860 11 22 44/ +27 11 369 1088 (International) website- www.fnb.co.za
Compliance Department	fscacompliance@firstrand.co.za FAIScompliance@fnb.co.za
Complaints	Tel – 087 575 9408 Email – care@fnb.co.za

- Certain impacted entities within FirstRand Limited are approved as FAIS Category I, II and III licensees. These impacted entities within FirstRand Limited are accordingly authorised by the Financial Sector Conduct Authority to provide FAIS financial services for the financial products approved in these license categories. A list of the approved financial products sub-categories may be obtained on www.fsca.co.za.
- We declare that the impacted entities in the FirstRand group of companies:
 - holds the prescribed professional indemnity insurance.
 - earns commission or remuneration, according to the Long-Term and Short-Term Insurance Acts.

- performs binder and outsourcing functions for FirstRand Life Assurance Limited and other insurers and receive binder and outsourcing fees for doing this.
- takes responsibility for the actions of its authorised representatives as far as they are providing financial services (some of whom may be providing FAIS financial services under supervision).

Entities in the FirstRand group of companies may be Financial Services Providers (FSPs) in terms of section 3A(2)(a) of the FAIS General Code of Conduct and are required to have a conflict-of-interest policy and complaints management policy. A copy of the FirstRand Conflict of Interest Management Policy Statement and FirstRand Complaints Management Framework, that also covers these FSPs, can be found on the FirstRand Limited website at <https://www.firstrand.co.za/investors/esg-resource-hub/policies-and-practices/>.

Certain financial institutions within the FirstRand group of companies are licensed Financial Services Providers (FSPs). These FSPs provide solutions which are financial products and services regulated under the FAIS Act but also provide non-financial products and services which are not afforded the protection of the FAIS Act. These non-financial products and services may be regulated by other legislation. Please engage us if you are not sure what law applies to your solution with us.

FAIS Ombud

- The contact details of the FAIS Ombud are published on our website at www.fnb.co.za and the rules. You can also contact us on 0860 11 22 44 to get this information.
- You can request assistance from the FAIS Ombud if you believe that your complaint has not been resolved satisfactorily by us within 6 weeks of lodging your complaint. You need to refer the dispute to the FAIS Ombud within 6 months of the issue remaining unresolved with the entity in the FirstRand group of companies.

28. COMPLAINTS – THE FOLLOWING IS ONLY APPLICABLE TO SOUTH AFRICA

The following additional ombuds and regulators may be useful to you. Their contact details are available on their websites and on our websites, Apps and branches.

Consumer Goods and Services Ombud https://www.cgso.org.za/cgso/contact-us/	The National Credit Regulator https://www.ncr.org.za/index.php/contact-us/ncr-contancts
National Financial Ombud Scheme South Africa NPC https://nfosa.co.za/contact-us/	
The Information Regulator (South Africa) https://info regulator.org.za/contact-us/	
The National Consumer Commission https://www.thencc.gov.za/contacts	The Johannesburg Stock Exchange https://www.jse.co.za/contact-us
The Independent Communications Authority South Africa consumer@icasa.org.za	Advertising Regulatory Board https://www.arb.org.za/contacts.html

29. CURRENCY AND PAYMENT RISK

- All exchange rate, currency fluctuation, volatility risk and losses arising from any cause will be for your account.
- Any foreign or cross border transaction or purchase, or transaction involving or referencing foreign currency (regardless of the interface or channel or method of payment) could result in VERY SIGNIFICANT UNFORESEEN additional costs, charges or losses and risks (over which we have no control), which you or we might not be aware of, or which might not be disclosed by a third party or anyone to you before you approve or make payment. Before making payment, you should determine whether the proposed transaction involves or references any foreign currency, has a cross border component, whether the third party that will get paid is a foreign national and what additional costs and charges will be incurred and what the risks are. You hereby agree that you understand these risks and you agree to pay to us on demand

all such additional costs, charges and make good any losses, regardless of whether you had knowledge of such additional costs, charges or losses.

- You understand and confirm that transactions may be delayed, blocked and/or cancelled for reasons that are outside of our control and you indemnify us against and holds it harmless from all demands, claims, actions, losses, costs and damages of whatever nature that may be brought against us as a result thereof. This includes reasons such as the local or international laws or policies that apply to the transactions.
- We will make every effort to process orders placed via the various interfaces or channels available without any delay. However, you understand that delays can sometimes occur due to applicable local or international laws or policies that apply to transactions; technical problems and/or matters out of our control and hereby holds it harmless from all demands, claims, actions, losses, costs and damages of whatever nature that may be brought against us as a result thereof. If a payment interface or channel is no longer available or cannot be used for any reason and a different interface or channel needs to be used, we will not be liable for any losses, failures or delays caused thereby.
- We uses reasonable care and skill in providing the solutions to facilitate the dealing in foreign currency; however, we do not warrant that access to these solutions shall be continuous and/or error free.

30. PREVENTION OF TAX CRIMES

- The FirstRand group of companies endeavours to stop or prevent any criminal activities in relation to tax crimes such as tax evasion, tax fraud, illegitimate tax avoidance and the circumvention of tax reporting. We are also required to manage our tax risk exposure, including reputational risk, in a responsible manner. To manage tax risk appropriately, we identify and monitor any tax risk that our business relationships may pose to us on an ongoing basis.
- In accordance with the law and any International Agreement administered under the law, any of the companies within the FirstRand group of companies may be required by legislation or by agreement with tax authorities to obtain tax information and report certain information about you, related persons or parties or your relationship with us, including information about your transactions and solutions:
 - to the South African Revenue Services (SARS) (for South Africa) or other tax authority who will then report directly to the tax authorities in other countries (where we reasonably think or are required to presume or where you have specifically indicated that you are subject to tax or might have a reporting obligation);
 - to any other relevant tax authority.
- If we are required to report information about you, related persons or parties or your relationship with us (or both), we may also need you to give us further information, documents or certifications about your identity, tax residence, citizenship, nationality and residency status. The obtaining of such information may be limited to certain transactions or solutions in accordance with the relevant tax laws.
- If we are required to report information about your transactions, solutions or that of related persons or parties, you agree to provide additional information and documents that we need. Failure to provide this information may result in restrictions on the account activation/opening or may be required to limit/freeze any transactions on account(s) and in addition, the information may be reported to SARS (for South Africa) or other tax or revenue authorities who may in turn levy penalties. Furthermore, where tax information is not provided in respect of certain transactions, withholding taxes at the maximum withholding rate may be applied.
- In the case of tax evasion, tax fraud, suspected tax evasion/fraud, illegitimate tax avoidance and the circumvention of tax reporting, or where required by the law, we can freeze or close your solutions, or we can refuse to carry out any instruction or transaction without notice to you. Tax evasion/fraud or suspected tax evasion/fraud includes (but is not limited to) instances where you receive tax refunds through misrepresentation; you allow your solution to be used by a third party for fraudulent tax purposes such as a mule account or you provide false information to us. You agree to assist us to comply with tax laws by providing us with all the information and documents we require. If you fail to do so or provide false or inadequate information, we can refuse to enter into a relationship with you, refuse to carry out an instruction (including an instruction to transfer available funds and close a solution), suspend access to your participation in and the use of any rewards and/or customer benefits associated with any solution, restrict access to your solution by placing a hold on your solution and can also terminate our relationship with you.

PLEASE NOTE that we will not be liable to you for any loss you may suffer because of our compliance with legislation or agreements with tax authorities.

31. DEPOSIT INSURANCE

Qualifying products held with FirstRand Bank Limited may fall within qualifying deposits covered by the Corporation for Deposit Insurance (CODI) up to the limit of cover and if held by a qualifying depositor, as specified in the Deposit Insurance Regulations made in terms of the Financial Sector Regulation Act 9 of 2017. You may access more information on deposit insurance and CODI on the webpage of the South African Reserve Bank. Further information about qualifying deposits and qualifying depositors can be found on our websites.