

SBM Bank Internet Banking and Mobile Banking Terms & Conditions

TERMS OF USE

These terms and conditions explain the rights and obligations pertaining to the Internet Banking and Mobile Banking Service (defined below) and information that the Customer may use or request from the Bank or that the Bank may provide to the Customer through the Internet Banking and Mobile Banking Service. The Bank reserves the right to add, amend, revise, change or cancel any of these terms and conditions and also reserves the right to modify any features of any products or services offered by the Bank. The Customer unconditionally accepts these terms and conditions applicable to such Account (defined below) and the services relating thereto and shall always be bound by and abide with them and their amendments from time to time. The Customer understands and acknowledges that this Internet Banking and Mobile Banking Service is an extension of the Online Banking Services (defined below) provided by the Bank and the Customer accessing such Internet Banking and Mobile Banking Service shall also be bound by the terms and conditions that govern the Online Banking Services. These terms and conditions are in addition to and not in substitution / derogation of the general business terms and conditions; the wealth management terms and conditions; and such other terms as may be prescribed by the Bank from time to time in relation to the Services.

• DEFINITIONS

“Account” shall mean the bank account maintained by the Customer with the Bank for which the Internet Banking and Mobile Banking Service is being offered.

“Applicable Laws” shall mean and include any statute, law, regulation or a stipulation by the RBI or any other regulatory authority whether in effect as on date or as amended from time to time.

“Application” shall mean the mobile application which will be downloaded on the mobile phone of the Customer to access and use the Internet Banking and Mobile Banking Service.

“Bank” shall mean SBM BANK (INDIA) LIMITED.

“Customer” shall mean the existing holder of an Account with the Bank or the holder of the Bank's debit / credit cards who has made an application to the Bank to use the Internet Banking and Mobile Banking Service and / or downloaded the Mobile Banking App and thereby agreed to these terms and conditions.

“Customer Identification Data” shall mean the Customer account number / card number, mobile phone number, user ID and other information that are to be used by the Customer to authenticate themselves prior to accessing the Internet Banking and Mobile Banking Service which may be the same as the information used by the Customer for accessing the Online Banking Services.

“Internet Banking and Mobile Banking Service” means any and all of the Services offered by the Bank to the Customer on phone and / or any electronic gadgets owned by the Customer.

“Mobile Phone Number” shall mean the number registered by the Customer in relation to the use of Services offered by the Bank.

- **“Data Fiduciary”** means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data

- “Data Principal” means the individual to whom the personal data relates and where such individual is—
 - a child, includes the parents or lawful guardian of such a child;
 - a person with disability, includes her lawful guardian, acting on her behalf;
- “Data Processor” means any person who processes personal data on behalf of a Data Fiduciary
- “Personal data” means any data about an individual who is identifiable by or in relation to such data.
- “Personal data breach” means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.
- “Personal Identifiable Information” means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.
- “Sensitive personal data or information” of a person means such personal information which consists of information relating to:
 - Password.
 - Financial information such as Bank account or credit card or debit card or other payment instrument details.
 - Physical, physiological and mental health condition.
 - Sexual orientation.
 - Medical records and history.
 - Biometric information

“RBI” shall mean the Reserve Bank of India.

“Service” shall mean current / savings account and / or other related service / operations including inter alia wealth management services and / or such additional features as may be added / removed from time to time.

“SMS” shall mean Short Messaging Service, being a service offered by Telephone Service Providers and / or any other similar method of electronic communication that may now or at any time in the future be offered by Telephone Service Provider(s).

“SMS Banking” means a service that allows Customers to access their account information via Mobile phone using SMS messaging.

“Telephone Service Provider” shall mean the provider of the mobile phone connectivity services and Mobile Phone Number used by the Customer on their mobile phones.

“Website” shall mean the domain of the Bank located at url <https://www.sbmbank.co.in> owned and controlled by the Bank.

• ACCEPTANCE OF TERMS AND CONDITIONS

- On the terms and conditions hereinafter provided, the Bank offers the Internet Banking and Mobile Banking Service to the Customer. These terms and conditions made by the Bank and accepted by the Customer shall form the contract between the Customer. These terms and conditions shall be in addition to and not in derogation of other terms and conditions relating to any Account or Service of the Customer and / or the respective product provided by the Bank unless otherwise specifically stated.

- To access the Internet Banking and Mobile Banking Service, the Customer is required to download the Application on their mobile phone and / or any electronic gadgets owned by the Customer provided such mobile phone and / or any electronic gadgets is compatible with the Application.

- In order to transact under the Internet Banking and Mobile Banking Service, there are transaction data verification / re-authentication requirements for the Customer. The Customer may use the Online Banking Services credentials or the Customer Identification Data to effect such verification / re-authentication. The Customer will use the same Customer Identification Data for both the Online Banking Services and Internet Banking and Mobile Banking Service. The Customer must strictly adhere to privacy procedures to ensure safe keeping of the log in credentials.

- **USAGE OF FACILITY**

- By accepting the terms and conditions on the mobile phone while registering for the Internet Banking and Mobile Banking Service, the Customer:

- a) agrees to use the Internet Banking and Mobile Banking Service for financial and nonfinancial transactions offered by the Bank from time to time,

- b) irrevocably authorizes the Bank to debit the Accounts which have been enabled for Internet Banking and Mobile Banking Service for all transactions / services undertaken by using Customer Identification Data,

- c) authorizes the Bank to map the account number, User ID and Mobile Phone Number for the smooth operation of Internet Banking and Mobile Banking Service offered by Bank and to preserve the mapping record in its own server or server of any other third party and to use such data at its discretion for providing / enhancing further banking / technology products that it may offer,

- d) agrees to the usage of the Customer Identification Data as an authentication factor for the Internet Banking and Mobile Banking Service,

- e) confirms to the acceptance of the terms and condition of the Internet Banking and Mobile Banking Service offered by the Bank,

- f) agrees that the Internet Banking and Mobile Banking Service will enable him / her to transact using Customer Identification Data within the limit prescribed by the Bank and will be deemed as bonafide transaction,

- g) agrees that the transactions originated using the mobile phones are non-retractable as these are instantaneous / real time,

- h) understands and explicitly agrees that the Bank has the absolute and unfettered right to revise the prescribed ceilings from time to time which will be binding, and

- i) agrees that while the Information Technology Act, 2000 ("IT Act") prescribes that a subscriber may authenticate an electronic record by affixing his digital signature which has

been given legal recognition under the IT Act, the Bank is authenticating the Customer by using Mobile Phone Number, Customer Identification Data or any other method decided at the discretion of the Bank which may not be recognized under the IT Act for authentication of electronic records and this is acceptable and binding to the Customer and hence the Customer is solely responsible for maintenance of the secrecy and confidentiality of the Customer Identification Data without any liability to the Bank.

In agreement with all Data Protection Legislation means the legislation and regulations relating to the protection of Personal Data and processing, storage, usage, collection and/or application of Personal Data or privacy of an individual including (without limitation):

- The Digital Personal and Data Protection Act, 2023 (DPDPA), the Aadhar Act, 2016, the Information Technology Act, 2000/2008A (as amended from time to time), including the Digital Personal and Data Protection Rules, 2025 and Master Circular on Customer Service in Banks issued by Reserve Bank of India and any other applicable rules framed there under
- **“Personal Data”** shall have the same meaning as ascribed to the term 2(t) under the DPDA, 2023 and under the Digital Personal and Data Protection Rules, 2025 or any other applicable rules (as amended from time to time).

- The guidelines issued by the RBI on “Know Your Customer (KYC)”, “Anti Money Laundering (AML)” and “Combating the Financing of Terrorism (CFT)” from time to time would be applicable to the Internet Banking and Mobile Banking Service.

- The Bank shall file “Suspicious Transaction Report (STR)” to the “Financial Intelligence Unit – India (FIU-IND)” for Internet Banking and Mobile Banking transactions as in the case of normal banking transactions

- **ACCURACY OF INFORMATION**

- It is the responsibility of the Customer to provide correct information to the Bank through the use of the Internet Banking and Mobile Banking Service or any other method. The Bank will endeavor to correct the error wherever possible on a best effort basis, if the Customer reports such error in information promptly.

- The Customer accepts that, in case of any discrepancy in this information, the Bank shall not be responsible for any errors which may occur in spite of the steps taken by the Bank to ensure the accuracy of the information and shall not have any claim against the Bank in an event of any loss / damage suffered as a consequence of an information provided by the Bank found to be not correct.

- **FEE STRUCTURE**

The Bank reserves the right to charge the Customer a fee for the use of the services provided under the Internet Banking and Mobile Banking Service and change the fee structure at its discretion. Fees may be collected from the Customer in such manner and at such intervals as the Bank may specify as per the above guidelines. The charges payable by the Customer are exclusive of the amount payable to the Telephone Service Provider and would be debited from the account of the Customer instantly.

- **RESPONSIBILITIES AND OBLIGATIONS OF THE CUSTOMER**

- The Customer shall act in good faith, exercise reasonable care and diligence in keeping the Customer Identification Data and all other personal and confidential information in secrecy. At no time and under no circumstances shall the Customer disclose the Customer Identification Data and related details to any other person or permit the information to come into the possession or control of any other person.

- The Customer confirms that all persons whose personal or other data is transmitted, processed or otherwise handled, have consented to such transmission, processing or other handling under these terms and conditions in accordance with the extant laws, or the Customer shall obtain their consent prior to any such transmission, processing or other handling.

- The Customer will be responsible for all transactions, including fraudulent / erroneous transactions made through its mobile phone, SIM card and Customer Identification Data regardless of whether such transactions are in fact entered into or authorized by him / her. The Customer will be responsible for the loss / damage, if any suffered. Customer must immediately notify the bank of SIM change or mobile number change. He should also notify the Bank in case of change of email id

- It will be the responsibility of the Customer to notify the Bank immediately if he / she suspects the misuse of the Customer Identification Data. He / she will also immediately initiate the necessary steps to change his Customer Identification Data.

- The Customer shall be liable and responsible for all legal compliance and adherence of all commercial terms and conditions in respect of the mobile connection / SIM card / mobile phone through which the Internet Banking and Mobile Banking Service is availed and the Bank does not accept / acknowledge any responsibility in this regard.

- The Customer shall keep himself / herself updated with regard to any information / modification relating to the services offered under the Internet Banking and Mobile Banking Service which would be published on the Website and sent to the Customer for acceptance in case of a change.

- **NON-TRANSFERABILITY**

The grant of the Internet Banking and Mobile Banking Service to a Customer is not transferable under any circumstance and shall be used only by the Customer. However, the Bank shall have the right to transfer, assign or sell all its rights under these terms and conditions, which shall continue to be in force and effect for the benefit of the successors and assigns of the Bank.

- **CONFIDENTIALITY AND DISCLOSURE**

- To the extent permitted by the Applicable Laws, the Bank shall be entitled to transfer any information relating to the Customer and / or any other information given by the Customer for utilisation of the Internet Banking and Mobile Banking Service to and between its branches, subsidiaries, representative offices, affiliates, representatives, auditors and agents of the Bank, intermediaries and third parties selected by the Bank, wherever situated, for confidential use on a need to know basis and in connection with the Internet Banking and Mobile Banking Service. The Bank shall take necessary explicit consent from the Customer prior to various services offered.

- The Customer agrees and provides his / her express consent that the Bank may disclose any information whatsoever regarding him / her and / or his / her Account(s) to:

- a) any person or organization providing any service to its Customers, whether within or outside India for the purpose of providing the Services including but not limited to investigating discrepancies, errors or claims;

- b) under operation of the Applicable Laws;

- c) banks, financial institutions or credit reference agents for the purpose of assessing the Customer's creditworthiness or otherwise; and

- d) any person (whether or not related to the Bank) for purposes of that person or entity marketing any product or service to the customer, whether by electronic means or otherwise.

To the extent not prohibited by applicable law, the Bank shall be entitled to transfer any information relating to the Customer and / or any other information given by the Customer for utilization of the Internet Banking and Mobile Banking Service or Service to and between its branches, subsidiaries, representative offices, affiliates, representatives, auditors and third parties selected by the Bank, wherever situated, for confidential use in and in connection with the Internet Banking and Mobile Banking Service or Service. Further, the Bank shall be entitled at any time to disclose to any other bank / association / financial institution or any other body. This clause will survive the termination / usage of the Internet Banking and Mobile Banking Service or Service. For giving basic services for Internet and Mobile Banking, request of law enforcement agency, and intra banking services no prior consent will be taken.

- **NO WARRANTY**

Without prejudice to anything contained in these terms and conditions, the Bank, third party service provider, and their respective third party suppliers, licensors, and partners makes no express or implied warranty or make any representations regarding the use, merchantability or the results of the use of the with respect to the Internet Banking and Mobile Banking Service provided hereunder including, without limitation, any warranties of non-infringement of third party rights, title, marketability, of correctness, accuracy, adequacy, reliability, suitability, satisfactory quality and fitness for a particular purpose or otherwise.

The Customer expressly agrees that use of the Internet Banking and Mobile Banking Service is at its risk. The Internet Banking and Mobile Banking Service and any data, information, third party software, reference sites, services, or software made available in conjunction with or through the Internet Banking and Mobile Banking Service are provided on an "as is" basis.

The Customer agrees, undertakes and understands that the Bank would not be held liable and or responsible for any claims made by third parties arising from issues related to any failure, delay or interruption of the products and/or services as provided by the Bank's Internet and Mobile Banking services.

The Customer shall be solely responsible for ensuring that any device used to access the Bank's services (including without limitation a computer, smartphone, or tablet) is maintained in a secure and updated condition.

The Bank shall not be liable for any loss, damage, or unauthorized transaction arising from circumstances beyond its reasonable control, including but not limited to phishing, spoofing, fraudulent applications, social engineering, SIM swap, malware or virus attacks, credential

compromise, device tampering, unauthorized access through rooted/jailbroken devices, screen overlay or remote-access tools, or any other fraudulent or malicious activity perpetrated by third parties. Further, the Bank shall not be liable for any loss where the Customer has, under the influence of any person, phone call, message, advertisement, social media post, or any other inducement, voluntarily initiated or authorized a transaction, even if such transaction is later discovered to be fraudulent or part of a scam. The Customer agrees to exercise due caution and verify the authenticity of any request or offer before initiating transactions.”

The Customer acknowledges and agrees that access to the Bank's internet banking and/or mobile banking services through public or unsecured networks, including but not limited to open Wi-Fi hotspots, internet cafés, or any network not controlled or secured by the Customer, shall be undertaken entirely at the Customer's own risk.

The Bank does not claim any liability for loss, damage, interception, unauthorized access, or fraudulent activity arising from the Customer's use of public, unsecured, or untrusted networks. The Customer further agrees that the Bank shall bear no responsibility for any data interception, malware infection, unauthorized access, or transactions effected through the use of such networks. The Customer shall maintain updated antivirus software, operating system patches, bank app version and avoid using rooted/jailbroken devices. The Bank shall not be responsible for losses resulting from malware infections or device compromise due to the Customer's failure to maintain device security.

The Customer needs to get his PCs/laptops scanned on a regular basis and be updated with the latest antivirus software available. The Bank shall not be responsible in case of any data loss or theft due to the virus transmitted in the system through the usage of Internet Banking.

• LIMITATION OF LIABILITY

The Customer shall remain solely liable and responsible for all transactions initiated through the use of their internet banking or mobile banking credentials.

Without prejudice to any other provisions of these terms and conditions, the Bank shall not be liable to the Customer for any loss or damage (whether actual or contingent) whatsoever or howsoever caused arising directly or indirectly in connection with the Internet Banking and Mobile Banking Service and / or these terms and conditions. Notwithstanding the generality of the above, the Bank expressly excludes liability for consequential loss or damage or loss of profit, business, revenue, goodwill or anticipated savings which may arise in respect of the Internet Banking and Mobile Banking Service.

The Customer acknowledges and agrees that the Bank's liability, if any, shall be strictly limited to the remedies prescribed under applicable law and regulation, and the Bank shall not be liable for any losses arising from the Customer's own acts, omissions, or security lapses.

Notwithstanding anything contained herein, the Bank's liability under this terms and conditions, whether arising in contract, tort, negligence or otherwise shall in no circumstances exceed the transaction amount under dispute. Under no circumstances shall the Bank be liable for indirect, incidental or consequential damages.

• INDEMNITY

The Customer agrees to indemnify, hold harmless and defend Bank and its affiliates against any loss and damages that may be caused from or relating to

- a) Breach of Terms of Service (Terms & Conditions) mentioned herein.
- b) Improper use of the Internet Banking services and Mobile Banking Services by the Customer/customer.
- c) The use of products/ Internet and Mobile Banking services in any manner which violates the Terms of Service (Terms & Conditions) or otherwise violates any law, rule, conditions or regulation.

In consideration of the Bank providing the Internet Banking and Mobile Banking Service, the Customer agrees to indemnify and keep the Bank safe and harmless from and against all actions, claims, demands, proceedings, loss, damages, costs, charges and expenses whatsoever which the Bank may at any time suffer or be put to as a consequence of or arising out of acting in good faith or omitting or refusing to act on any instructions given by use of the Internet Banking and Mobile Banking Service. The Customer shall indemnify the Bank for unauthorized access by any third party to any information / instructions / triggers given by the Customer or breach of confidentiality.

- **DISCLAIMER**

- The Bank or its employee / contractual staff will not be liable for:

- a) any unauthorized use of the Customer's Identification Data or
- b) mobile phone number / instrument or unauthorized access to e-mails received at his notified email address for any fraudulent, duplicate or erroneous instructions given by use of the same; or
- c) acting in good faith on any instructions received by the Bank; or
- d) error, default, delay or inability of the Bank to act on all or any of the instructions; or
- e) loss of any information / instructions / alerts in Transmission; or
- f) unauthorized access by any other person to any information / instructions given by the Customer; or
- g) any failure in relation to administration or operations of the Bank

- The Bank reserves the right to limit the amount and frequency of payments that a Customer may make by using the Internet Banking and Mobile Banking Service, with prior intimation to the Customer. The Bank further reserves the right to alter / amend / modify the limits as imposed with prior intimation to the Customer.

- The Bank shall not be liable for any loss or damage that the Customer may incur due to negligence, act or omission of any third party.

- The Customer shall be solely responsible for the selection of the device / Telephone Service Provider(s) and for all issues / disputes between the Customer and the Telephone Service Provider(s) and / or the manufacturer of the device.

- **ADDITION AND WITHDRAWAL OR TERMINATION OF INTERNET BANKING AND MOBILE BANKING SERVICE**

- The Internet Banking and Mobile Banking Service is made available to the Customer, at the sole discretion of the Bank and may be discontinued by the Bank at any time, without notice.

- The Bank reserves the right to introduce additional services with or without giving any notice to the Customer. The Bank reserves the right to send SMS to the registered mobile phones regarding its products, services or any related matter, without the express consent of the Customer.

- **GOVERNING LAW AND JURISDICTION**

Any dispute or differences arising out of or in connection with the Internet Banking and Mobile Banking Service shall be subject to the exclusive jurisdiction of the Courts and tribunals of Mumbai and shall be governed by the laws of India.

- **GRIEVANCE REDRESSAL**

The Customer is advised to familiarize with the Grievance Redressal procedure available on our website for details on how to address a grievance that the Customer may have concerning Bank's Services .

For any queries or clarification customer can call on the Toll Free number 18002099335/18001033817 or drop an email to customercare@sbmbank.co.in

Please find the below link for grievance redressal on the SBM Website

<https://www.sbmbank.co.in/notice-board/grievance-redressal-mechanism>

STOP Payment

"Since the transactions initiated through Mobile Banking/Internet Banking are processed instantaneously, any STOP PAYMENT requests pertaining to these transactions shall not be accepted or processed"

FaceID Authentication Login Service - Terms and Conditions

Terms Of Use

- These terms and conditions apply to and regulate the use of FaceID Authentication Login Service (defined below) through the mobile banking application by a customer on his / her Authorized Mobile Device.
- For the purposes of these terms and conditions FaceID means a facial recognition system to access the Mobile Device.
- For the purposes of these terms and conditions FaceID Authentication Login Service means the feature to access the Application of the Bank through the FaceID instead of a numeric username and password.
- For the purposes of these terms and conditions Authorised Mobile Device / Mobile Device shall mean the mobile device which may from time to time be enabled with equivalent face detection functionality which has an interface that is capable of and permits face recognition as an authentication system.
- The Bank offers the FaceID Authentication Login Service to the Customer on these terms and conditions. The Customer understands that usage of the Application will imply the deemed acceptance of these terms and conditions. These terms and

conditions made by the Bank and accepted by the Customer shall form the contract between the Customer and the Bank.

- The Customer understands that the FaceID Authentication Login Service allows the Customer to use his / her face (as registered on the Authorized mobile device) in lieu of the mobile or online banking username and password to login; as a prerequisite to the Customer accessing and using the Mobile Banking Service.
- The Customer understands and acknowledges that the FaceID Authentication Login Service is a feature that is only permitted to be used on an authorized Mobile Device which supports face authentication in addition to other modes available to access a Mobile Device.
- The Customer understands and acknowledges that the FaceID Authentication Login Service is an extension of the Mobile Banking Service provided by the Bank and the Customer while using such FaceID Authentication Login Service shall also be bound by the terms and conditions that govern the Mobile Banking Service.
- Bank has taken proper security control and due diligence in protecting customers PII data stored in our system.
- These terms and conditions are in addition to and not in substitution / derogation of the general business conditions; the wealth management terms and conditions; and such other terms as may be prescribed by the Bank from time to time in relation to the Services.

Acceptance Of Terms And Conditions

- The Customer unconditionally agrees and acknowledges that for him / her to be able to use the FaceID Authentication Login Service, the Customer must:
 - possess an Authorized Mobile Device which supports the feature of FaceID authentication as a passcode to unlock the Mobile Device;
 - enable and use the FaceID as a passcode to unlock his / her Mobile Device instead of a numeric passcode;
 - be an existing and valid user of the Bank's Mobile Banking Service; install the Application on his / her Authorized Mobile Device; and
 - enable the FaceID Authentication Login Service feature to login into the Application on the Authorized Mobile Device.
- The Customer undertakes to ensure that only the Customer's face is recognized by the Authorized Mobile Device to access the device and the Customer unconditionally acknowledges that upon enabling of or the successful registration of the FaceID Authentication Login Service, any face that is registered and stored on the Authorized Mobile Device shall be used to access the Application, including access to the Customer's account details and statements.
- Upon enabling FaceID Authentication Login Service on this Application, any registered and identifiable face on this Mobile Device will have access to this Application.
- The Customer undertakes to take all measures to ensure the protection of the passcode/ security code. The Customer undertakes to prevent unintentional

registration of multiple faces (if so permitted) on the Mobile Device to avoid giving unauthorized access of the Customer's bank account through the Application.

- To access the FaceID Authentication Login Service, the Customer is required to log into the Application and enable the feature of a FaceID Authentication Login Service authentication Customer will thereafter provide the Application with his / her login credentials and proceed to login into the Application
- Upon enabling the face authentication on the Authorized Mobile Device the face used as a passcode to unlock the Authorized Mobile Device will be encrypted and stored on the Application and shall be retrieved for future logins. The Customer may disable this function at any time, by deregistering or disabling this feature on the Application.
- The Customer understands and acknowledges that each face that is registered as a passcode to unlock the Mobile Device will be synced with the Application and upon enabling the FaceID login feature such FaceID shall be recognized as an authorized access to the Application. As a consequence of this recognition, the Customer understands that the Application shall be automatically logged in whenever app is opened by any of registered face on the device.

Authorised Transactions

- The Customer understands and acknowledges that it shall comply with Applicable Laws and the RBI guidelines while using the FaceID Authentication Login Service.
- In order to prevent any fraudulent or unauthorized transactions, the Bank provides a two-factor authentication process prior to the Customer undertaking any financial transactions through the Application. The Customer understands that once the Mobile Device is unlocked, it amounts to an automatic login into the Application using any of the registered face on the device and access to the Customer's bank account on the Mobile Device
- The Customer has the option of accessing the Application through using his/her registered username and password instead of the FaceID Authentication Login Service.
- The Customer unconditionally agrees that in the event the Application recognizes a face on the Authorized Mobile Device, the Customer is deemed to have accessed the Mobile Banking Services and / or instructed the Bank to provide access through the Application.
- The Customer understands and acknowledges that the face authentication by the Application is done by interfacing with the face authentication module on the Authorized Mobile Device.
- The Customer has the option to deactivate the FaceID Authentication Login Service at any time.
- The determination and attribution of liability of the Customer and / or the Bank in relation to any unauthorized transaction will be determined in accordance with the RBI Circular on 'Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transactions' dated July 06, 2017 (Circular)
- The Customer undertakes to inform the Bank of any unauthorized transaction through the Application at the earliest after the occurrence of such transaction or from the Customer receiving information about the same

- In the event, that the Customer informs the Bank about any breach or compromise of security in relation to the face or other passcode / security code, the Customer may be required to change the registered face on the Mobile Device, deactivate or disable the FaceID Authentication Login Service and / or cease the use of the Application forthwith

Representations And General Undertakings

- The Customer unconditionally agrees and provides consent to the Bank for accessing and using any and all information limited and in relation to the FaceID Authentication Login Service
- The Customer undertakes and agrees to protect his / her Authorized Mobile Device at all times and shall be responsible for any access / usage on and through the Application (whether undertaken and/or authorized by the Customer or otherwise)
- The Customer understands and agrees that the face authentication is a feature that is inbuilt in the authorized Mobile Device and is provided by the relevant provider and is not created or developed by the Bank. The Customer acknowledges that the Bank does not, in any way, warrant or represent in relation to the security or the extent of security of such FaceID feature on the Mobile Device or the functionality as per the design of the concerned manufacturer, and the role of the Bank is limited to providing an Application that interfaces with this feature and recognizes the face(s) used to unlock the Mobile Device, to replace the requirement of entering a username and password with a face authentication
- The Bank does not guarantee or warrant the undisturbed functioning, availability or access of the FaceID Authentication Login Service and this shall be solely subject to the Mobile Device, the software, the network and / or any other stipulations under the SBM Bank Internet Banking and Mobile Banking Terms & Conditions
- The Bank undertakes that subject to Applicable Laws, the Bank shall not be held responsible for any damage, harm or loss incurred or suffered by the Customer in the event of an attempted or an unauthorized use of the FaceID Authentication Login Service or the Application or any instructions or request made by the Customer (whether undertaken and / or authorized by the Customer or otherwise) or the consequence of any unauthorized transactions, otherwise to the extent provided for in the Circular.

Touch ID / Fingerprint Login Service - Terms and Conditions

- **TERMS OF USE**

- These terms and conditions apply to and regulate the use of Fingerprint Login Service through Mobile Banking Application by a Customer on his / her Authorized Mobile Device.

For the purposes of these terms and conditions Fingerprint Login Service means the feature to access the Application of the Bank through a fingerprint authentication instead of an numeric username and password.

For the purposes of these terms and conditions Authorised Mobile Device / Mobile Device shall mean any device which supports the Touch ID / Fingerprint authentication feature.

— The Customer unconditionally accepts that upon enabling the fingerprint authentication on the Application he / she shall be bound by these terms and conditions .

— The Bank offers the Fingerprint Login Service to the Customer on these terms and conditions. The Customer understands that usage of the Application will imply the deemed acceptance of these terms and conditions. These terms and conditions made by the Bank and accepted by the Customer shall form the contract between the Customer and the Bank.

— The Customer understands that the Fingerprint Login Service allows the Customer to use his / her fingerprint (as registered on the Authorized mobile device) in lieu of the mobile or online banking username and password to login; as a prerequisite to the Customer accessing and using the Mobile Banking Service.

— The Customer understands and acknowledges that the Fingerprint Login Service is a feature that is only permitted to be used on an Authorized Mobile Device which supports fingerprint authentication in addition to other modes available to access a Mobile Device.

— The Customer understands and acknowledges that the Fingerprint Login Service is an extension of the Mobile Banking Service provided by the Bank and the Customer while using such Fingerprint Login Service shall also be bound by the terms and conditions that govern the Mobile Banking Service.

Bank has taken proper security control and due diligence in protecting customers PII data stored in our system.

— These terms and conditions are in addition to and not in substitution / derogation of the general business conditions; the wealth management terms and conditions; and such other terms as may be prescribed by the Bank from time to time in relation to the Services.

- **ACCEPTANCE OF TERMS AND CONDITIONS**

- The Customer unconditionally agrees and acknowledges that for him / her to be able to use the Fingerprint Login Service, the Customer must:
 - Possess an Authorized Mobile Device which supports the feature of fingerprint authentication as a passcode to unlock the Mobile Device;
 - enable and use the fingerprint / Touch ID as a passcode to unlock his / her Mobile Device instead of an numeric passcode;
 - be an existing and valid user of the Bank's Mobile Banking Service;
 - install the Application on his / her Authorized Mobile Device; and
 - enable the Touch ID / fingerprint feature to login on the Application on the Authorized Mobile Device
- The Customer undertakes to ensure that only the Customer's fingerprints are recognized by the Authorized Mobile Device to access the device and the Customer unconditionally acknowledges that upon enabling or the successful registration of the Fingerprint Login Service, any fingerprint that is stored on the Authorized Mobile Device shall be used to access the Application, including access to the Customer's account details and statements
- Upon enabling Fingerprint Login on this Application, any registered and identifiable fingerprint(s) on this Mobile Device will have access to this Application.

- The Customer undertakes to take all measures to ensure the protection of the passcode / security code. The Customer undertakes to prevent unintentional registration of multiple fingerprints on the Mobile Device to avoid giving unauthorized access of the Customer's bank account through the Application.
 - To access the Fingerprint Login Service, the Customer is required to log into the Application and enable the feature of a Fingerprint ID / fingerprint authentication. The Customer will thereafter provide the Application with his / her login credentials and proceed to login on the Application.
 - Upon enabling the fingerprint authentication on the Authorized Mobile Device the fingerprint used as a passcode to unlock the Authorized Mobile Device will be encrypted and stored on the Application and shall be retrieved for future logins. The Customer may disable this function at any time, by deregistering or disabling this feature on the Application.
 - The Customer understands and acknowledges that each fingerprint that is registered as a passcode to unlock the Mobile Device will be synced with the Application and upon enabling the fingerprint login feature shall be recognized as an authorized fingerprint. As a consequence of this recognition, the Customer understands that the Application shall be automatically logged in, every time the Mobile Device is unlocked by a registered fingerprint.

- **AUTHORISED TRANSACTIONS**

- The Customer understands and acknowledges that it shall comply with Applicable Laws and the RBI guidelines while using the Fingerprint Login Service.
- The Customer has the option of accessing the Application through using his/her registered username and password instead of the Fingerprint Login Service.
- The Customer unconditionally agrees that in the event the Application recognizes a fingerprint on the Authorized Mobile Device, the Customer is deemed to have accessed the Mobile Banking Services and / or instructed the Bank to provide access through the Application.
- The Customer understands and acknowledges that the fingerprint authentication by the Application is done by interfacing with the fingerprint authentication module on the Authorized Mobile Device.
- The Customer has the option to deactivate the Fingerprint Login Service at any time.

- **UNAUTHORISED TRANSACTIONS**

- The determination and attribution of liability of the Customer and / or the Bank in relation to any unauthorized transaction will be determined in accordance with the RBI Circular on 'Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transactions' dated July 06, 2017 (Circular).
- The Customer undertakes to inform the Bank of any unauthorized transaction through the Application at the earliest after the occurrence of such transaction or from the Customer receiving information about the same.

- In the event, that the Customer informs the Bank about any breach or compromise of security in relation to the fingerprints or other passcode / security code, the Customer may be required to change the registered fingerprints on the Mobile Device, deactivate or disable the Fingerprint Login Service and / or cease the use of the Application forthwith.

- **REPRESENTATIONS AND GENERAL UNDERTAKINGS**

- The Customer unconditionally agrees and provides consent to the Bank for accessing and using any and all information limited and in relation to the Fingerprint Login Service.
- The Customer undertakes and agrees to protect his / her Authorized Mobile Device at all times and shall be responsible for any access / usage on and through the Application (whether undertaken and / or authorized by the Customer or otherwise).
- The Customer understands and agrees that the fingerprint authentication is a feature that is inbuilt in the authorized Mobile Device and is provided by the relevant provider and is not created or developed by the Bank. The Customer acknowledges that the Bank does not, in any way, warrant or represent in relation to the security or the extent of security of such fingerprint authentication / Fingerprint ID feature on the Mobile Device or the functionality as per the design of the concerned manufacturer, and the role of the Bank is limited to providing an Application that interfaces with this feature and recognizes the fingerprint(s) used to unlock the Mobile Device, to replace the requirement of entering a username and password with a fingerprint authentication.
- The Bank does not guarantee or warrant the undisturbed functioning, availability or access of the Fingerprint Login Service and this shall be solely subject to the Mobile Device, the software, the network and / or any other stipulations under the SBM Bank Internet Banking and Mobile Banking Terms & conditions
- The Bank undertakes that subject to Applicable Laws, the Bank shall not be held responsible for any damage, harm or loss incurred or suffered by the Customer in the event of an attempted or an unauthorized use of the Fingerprint Login Service or the Application or any instructions or request made by the Customer (whether undertaken and / or authorized by the Customer or otherwise) or the consequence of any unauthorized transactions, otherwise to the extent provided for in the Circular.

- **Amendments**

The Bank has the absolute discretion to amend or supplement any of the Terms of Service (Terms & Conditions) at any time, without prior notice. However the Bank will endeavor to notify the changes by posting it on the website or through advertisement or any other means as the Bank may deem fit which will be binding on the Customer. The existence and availability of the new functionalities/facilities/features will be notified to the Customer as and when they are made available. By using these new services, the Customer agrees to be bound by the Terms of Service (Terms & Conditions) applicable there for.

