Electronic Banking Terms & Conditions

Effective 10 July 2019

Important

- *Southland Building Society operates under the brand "SBS Bank". The name of the registered bank is Southland Building Society (referred to as "the Bank").*
- *These Terms and Conditions (which can be amended or replaced from time to time) apply in addition to the Bank's General Terms and Conditions, and any specific terms and conditions, applying to your account(s) with the Bank. Copies of the specific terms and conditions for your account(s) with the Bank may be obtained from our website (sbsbank.co.nz), during Business Hours from any of our Branches or by calling our Contact Centre on 0800 727 2265, or outside New Zealand on +64 3 211 0700.*
- *In the event that there is any inconsistency between these Terms and Conditions and any other terms and conditions applying to your account(s) with, or any service provided by, the Bank, these Terms and Conditions will prevail to the extent of that inconsistency.*
- *By using any of the Bank's Electronic Banking Services you agree to comply with these Terms and Conditions.*
- *Some of the functionality of the Electronic Banking Services is only available for Nominated Accounts and is not applicable to Credit Card Accounts (particularly payment services).*
- *Please read these Terms and Conditions carefully. We are happy to explain anything to you that is not clear.*

1. Electronic Banking Security

1.1 You should take care when selecting your Password(s) and Mobile Banking App PIN(s)and you must comply with the Passwords and Pins section of our General Terms and Conditions.

1.2 Do not use the same Password(s) or Mobile Banking App PIN(s) that you use elsewhere.

1.3 In cases where you have forgotten your Password or Mobile Banking App PIN, you can arrange in your security settings for your access to the Electronic Banking Services to be reset if you have registered for Second Factor Authentication. To do this you need to:

a. Select either 'Reset Password' (for Internet Banking), or 'Forgot PIN' (for the Mobile Banking App) from the login screen and follow the prompts.

b. Enter the SMS Code sent to your registered mobile number before setting your new Password or Mobile Banking App PIN and logging in.

If you are not set up for Second Factor Authentication, do not receive an authentication code or are unable to successfully complete the password reset process, you will need to visit any of our Branches or call our Contact Centre on freephone 0800 727 2265, or outside New Zealand on +64 3 211 0700, during Business Hours to reset the relevant security settings.

1.4 You have a responsibility to exercise reasonable care to prevent unauthorised access to the Device that you use to access our Electronic Banking Services. For example, this includes:

a. Not leaving your Device unattended and logged into our Electronic Banking Services;

b. Not recording your Password or Mobile Banking App PIN including using the password storage options provided within internet browsers;

c. Locking your Device or taking other steps to stop unauthorised use of our Electronic Banking Services; and

d. Notifying us as soon as practicable if your Device is lost or stolen.

1.5 You should regularly examine your transaction history to identify any instances where Electronic Banking Services have been used without your authority. You must notify us immediately if you identify any unauthorised transactions.

1.6 Your Password, Mobile Banking App PIN or SMS Code identifies you and allows you access to the Electronic Banking Services. The Bank is not required to take any further steps to verify that the person using your Password, Mobile Banking App PIN or SMS Code is you, and they will be allowed access to the Electronic Banking Services regardless of whether or not you have given your permission.

1.7 You must take reasonable care when accessing our Electronic Banking Services to ensure that your Password and Mobile Banking App PIN are not seen by or disclosed to anyone else.

1.8 You must change your Password, Mobile Banking App PIN and any other security information promptly if anyone else does or may know it. You must also notify the Bank in accordance with "Notification of Loss, Theft or Unauthorised use of your Password or PIN" section.

1.9 You should not open attachments or run software from untrusted or unknown sources on any Device that you use to access our Electronic Banking Services.

2. Notification of Loss, Theft or Unauthorised use of your Password or Mobile Banking App PIN

2.1 You must notify the Bank immediately when:

a. you know or suspect that someone else knows your Password or Mobile Banking App PIN;

b. you discover or suspect an unauthorised use of your Password or Mobile Banking App PIN has occurred; or

c. your transaction history contains any instances of unauthorised use or errors.

2.2 Please contact the Bank immediately if your Mobile Device or your mobile phone containing your registered mobile number is lost or stolen. We can then arrange for the Mobile Device or the registered mobile number to be either temporarily deactivated until you relocate it or deregistered to prevent any unauthorised use of our Electronic Banking Services.

2.3 We recommend that you record all receipt numbers, payment or transfer reference numbers that are issued to you by any of the Electronic Banking Services to assist in following up with us if you identify any issues when checking transactions against your statements.

2.4 During Business Hours, call us immediately and we can help you reset your login details including your Password and Mobile Banking App PIN.

2.5 You can cancel your Electronic Banking Services access during Business Hours at any of our Bank Branches or by calling our Contact Centre on 0800 727 2265, or outside New Zealand on +64 3 211 0700.

3. Payments

3.1 When you set up a payment using Electronic Banking Services, you authorise us to act in accordance with, and acknowledge that we will rely on, those instructions. You cannot set up any payment from any Credit Card Account.

3.2 Subject to compliance with these Terms and Conditions, payments can be requested to be made on the same day or on a future date when you enter the payment details.

3.3 If you have requested us to make a same day payment to an External Account, we will automatically debit the payment from your Nominated Account. We will endeavour to send any same day payments to External Accounts every 30 minutes between 9am and 9.30pm on Business Days.

3.4 Future-dated payments will be automatically debited from your Nominated Account on the date requested in accordance with your instructions.

3.5 With the exception of future-dated payments, electronic payments authorised after 9.30pm, on weekends or public holidays to External Accounts will be debited from your account on the day of authorisation but may not be sent to the receiving bank until the next Business Day.

3.6 Payments between any two of your Nominated Accounts will be debited and credited immediately (unless specified that the payment to be made will occur on a future date). This includes Nominated Accounts for different entities which you manage but does not include any payment to a Credit Card Account, which will be processed as an External Payment.

3.7 A payment is irreversible once the instruction to make the payment has

been completed using our Electronic Banking Services (unless the payment to be made will occur on a future date).

3.8 It is your responsibility to ensure that there are enough funds in your Nominated Account(s) to meet any payments that you authorise. Instructions for payments will not be actioned if there are insufficient funds available in your Nominated Account.

3.9 We will endeavour to make the payments you request, although we accept no responsibility or liability for any delay, omission or refusal to make any or all of the payments, or for late payment. In particular, we accept no responsibility or liability for the accuracy of the information you supply to us when setting up, changing, or deleting payment instructions.

3.10 All payment instructions received from you will be subject to any other arrangements you may have with us in relation to your Nominated Account(s).

3.11 In the event of a future-dated payment not able to be made on the due date for any reasons referred to in these Terms and Conditions, we will attempt to complete that payment request twice daily for the following three Business Days. Following that period arrangements for that payment will become your sole responsibility.

3.12 We may in our absolute discretion conclusively determine the order of priority of payments and transfers requested pursuant to any payment instruction or cheque drawn on a Nominated Account. A limit of $50,000 per customer per day applies to the total of all payments initiated using the Electronic Banking Services. Payments in excess of your daily limit may not be actioned by us.

3.13 Any payment instruction given by you is irrevocable, notwithstanding your death, Bankruptcy or other revocation of this authority, until actual notice of such event or revocation is received by us, subject to these Terms and Conditions.

3.14 We are authorised to advise your payees of your full name, address and account number if requested by them in respect of a payment authorised by you.

3.15 For payments to Approved Payees the Bank relies on the account numbers and required reference details provided from time to time by the Approved Payee. The Bank cannot guarantee either at the time payment instruction is received or when the payment is made that these Approved Payee details remain current and are correct.

3.16 The timing of receipt of any payment sent by us during Business Days will depend on the frequency that the recipient's bank processes its payments. This may occur less frequently than the rate at which we send payments (either during the day or overnight).

4. Multi-payments

4.1 Within Internet Banking, you can set up and manage Multi-payments and create templates for Multi-payments (the latter being a preset combination of payments to a number of accounts which can then be copied to set up new Multi-payments).

4.2 The terms outlined in clause 3 above apply to Multi-payments subject to any modification outlined in this clause 4.

4.3 Multi-payments cannot be set up to reoccur and can only consist of payments from one Nominated Account. You can set up separate Multi-payment and templates for different Nominated Accounts.

4.4 You can import either Multi-payments or templates in Comma Separated Value (CSV) file format.

4.5 You can maintain (both edit and delete) future dated Multi-payments in Internet Banking up to the date the Multi-payment is to be actioned.

4.6 We will attempt to action individual payments in the Multi-payment in the order which you have entered them.

4.7 If we are unable to action any individual payment within the Multi-payment for any reason (in most cases due to insufficient funds), then that payment will not be actioned and you will need to set up a replacement payment (either alone or as part of another Multi-payment). We will attempt to action any remaining payments within the Multi-payment.

4.8 The retry rule under clause 3.9 above does not apply to Multi-payments and we will not retry to action any failed individual payment within a Multi-payment (either on the same or subsequent days).

4.9 We will display the status of Multi-payment batches within Internet Banking from when you begin creating a Multi-payment batch through to when it is actioned.

5. Signing Rule Application

5.1 Any instructions made within the Electronic Banking Services in respect of Nominated Accounts must comply with the Signing Rule. If a Signing Rule requires two or more people to authorise instructions, for instructions initiated in Internet Banking we will require the authorisation to be provided by the Authorised Signatories within Internet Banking for the applicable account(s) in accordance with the Signing Rule.

5.2 To authorise instructions initiated on an account using the Electronic Banking Services, Signatories must also have registered for and have access to Internet Banking.

5.3 Any instructions initiated using the Electronic Banking Services must be authorised prior to 8:30pm on the date the instruction is to be actioned. If the instruction is not authorised by this time it will be automatically cancelled.

5.4 Only the customer who initiates an instruction for authorisation may edit/delete an instruction before it has been authorised in accordance with the Signing Rule.

5.5 Any Signatory for an account with Internet Banking access may edit or delete an authorised future dated instruction. Authorised instructions will only be edited or deleted following reauthorisation of those changes. If the request to edit or delete the instruction is not authorised prior to 8:30pm on the date the instruction is to be actioned, then it will still be actioned as originally authorised.

5.6 Instructions authorised for the same day cannot be edited or deleted once they have been authorised.

5.7 If the source account for an instruction is edited to an account which has a different Signing Rule, only the Signing Rule of the new source account will be required to authorise the edited instruction.

5.8 Once an edited instruction is authorised the original instruction will no longer be actioned and will be replaced by the edited instruction.

5.9 Signatories who may authorise an instruction may also decline an instruction.

5.10 If an instruction is declined by a Signatory, then that instruction cannot proceed even if there are sufficient additional Signatories who may have been able to otherwise authorise the instruction in accordance with the Signing Rule.

5.11 The Signatory who declines an instruction is prompted to provide a reason for declining the instruction which is provided to the initiator as a secure message within Internet Banking.

5.12 You can view any instructions awaiting approval in Internet Banking for accounts that you have access to.

5.13 If instructions are authorised by another account Signatory in accordance with the applicable Signing Rule, Second Factor Authentication will not be triggered. However, Second Factor Authentication may be triggered where a Signing Rule only requires one Signatory.

6. Reversing Transactions

6.1 If you have provided a payment instruction in the Electronic Banking Services, you cannot cancel that payment instruction except where the instruction relates to a future-dated payment and you instruct us to stop the payment prior to the stipulated date for payment in line with the Signing Rule for the applicable account.

6.2 Notwithstanding that transactions are irreversible once authorised, if a request for reversal of a payment is made, we will attempt to recover the payment. There is no guarantee that we will be able to recover the payment and a fee will apply for requesting the reversal.

6.3 If funds are paid to an incorrect account in error, those funds will not be recoverable unless the owner of the account to which the funds were transferred consents to the recovery.

6.4 You agree to meet the Bank's fees and costs in respect of any attempted reversal of a payment or transfer, whether or not the attempt is successful. You agree to the Bank debiting any such fees and costs from your Nominated Account(s). Fees are set out within the Bank's Account Charges document (which can be found at sbsbank.co.nz/resource/fees).

7. Transactions

7.1 You will not be able to draw via any of the Electronic Banking Services on any cheques and/or deposits deposited to your Nominated Accounts until they become cleared funds.

7.2 The Bank may set minimum and maximum limits for transactions carried out via any of the Electronic Banking Services.

7.3 Any action taken by the Bank to:

a. close, or suspend access to your accounts in accordance with our General Terms and Conditions; or

b. terminate or suspend access to your Credit Card Account following request by SBS Money Limited,

may impact your access to your Nominated Accounts and/or Credit Card Accounts through our Electronic Banking Services.

7.4 In the absence of any daily or other periodic transaction limit arrangements between you and the Bank, you can only withdraw funds or make payments up to the available balance of your selected Nominated Account (including the unused portion of any credit limit

relating to that account).

7.5 You agree that when determining the available balance or credit limit on any Nominated Account we will not include the available balance or credit limit from any of your other accounts with the Bank.

7.6 You acknowledge that third parties such as merchants or other financial institutions may impose additional restrictions on the amount of funds you may withdraw, deposit or transfer.

8. Changes to these Terms and Conditions

8.1 The Bank has the right to vary these Terms and Conditions and any other terms and conditions applying to your Nominated Accounts and Credit Card Accounts and to vary, change or withdraw any of the Bank's services at any time.

8.2 Subject to the exception under clause 8.3 below, you will be given at least 14 days' notice of any variation either by post to your last known address, email, telephone call, notice on our website and/or via an electronic banking channel used by you.

8.3 We are not obliged to give you advance notice if an immediate change to these Terms and Conditions is deemed necessary for the security of the Electronic Banking Services or individual accounts.

9. Privacy

9.1 In addition to our 'Privacy Statement' in our General Terms and Conditions (for Nominated Accounts), you authorise us to give information about you and any of your Nominated Accounts and Credit Card Accounts to others in order to execute your instructions to us via Electronic Banking Services or where we reasonably think it necessary for the provision of that service. However, you may instruct us not to share your information by giving us written instructions to that effect. By doing so you acknowledge that this may compromise the Bank's ability to both act on your instructions and effectively provide Electronic Banking Services to you in accordance with these Terms and Conditions.

10. Restrictions and Termination of Access to Electronic Banking Services

10.1 Access to Electronic Banking Services may be suspended or cancelled:

a. in the case of Nominated Accounts, in accordance with our General Terms and Conditions (including the sections titled "Suspending Accounts and Transactions" and "Closing of Accounts and the Withdrawal of Products and Services"); and

b. in the case of Credit Card Accounts, on receiving a request or instruction from SBS Money Limited.

10.2 In addition, we may suspend or withdraw your access to any of the Electronic Banking Services at any time without prior notice if:

a. you have breached these Terms and Conditions or have acted fraudulently;

b. we learn of your death, Bankruptcy or lack of legal capacity or that you have committed an act of Bankruptcy or that a Bankruptcy application has been made against you;

c. we consider that we have other reasonable grounds to do so (in which case all reasonable efforts will be made to advise you of the circumstances of withdrawal or suspension);

d. we are complying with a court order;

e. we are notified by any party of a dispute over either the ownership of funds or the operation of any account; or

f. we are protecting one or all of the parties to a Nominated Account or Credit Card Account, the Bank, or a third party who has reasonably claimed an interest in the Nominated Account or Credit Card Account.

10.3 You may cancel your access to any of the Electronic Banking Services at any time during Business Hours by visiting any of our Branches or by calling our Contact Centre on 0800 727 2265, or outside New Zealand on +64 3 211 0700. You will remain responsible for any instructions made on your Nominated Accounts or Credit Card Accounts via the Electronic Banking Services up until the time of cancellation.

11. Liability

11.1 Once you have notified the Bank that either your Password or Mobile Banking App PIN have been disclosed to someone else, or you suspect that this may have occurred, either in New Zealand or overseas, you will not be liable for any unauthorised transactions carried out after that time unless you have breached these Terms and Conditions or the General Terms and Conditions, or you have acted fraudulently or negligently.

11.2 You will only be liable for up to $50.00 for any unauthorised transaction that has taken place before you notified the Bank unless you have:

a. unreasonably delayed notifying the Bank;

b. selected an unsuitable Password or Mobile Banking App PIN;

c. disclosed your Password or Mobile Banking App PIN to anyone else, either deliberately or inadvertently, such as if you failed to take reasonable steps to prevent disclosure of any of these when keying them in;

d. written your Password or Mobile Banking App PIN down; or

e. failed to take reasonable care to prevent unauthorised access to the Device that you use to access our Electronic Banking Services.

11.3 If any of the above apply you will be liable for all transactions completed prior to you notifying the Bank up to the maximum amount that you yourself could have transferred from your Nominated Accounts or Credit Card Accounts via Electronic Banking Services during that time.

11.4 If you have, in the Bank's sole opinion, contributed to the cause of any unauthorised transactions, you may be responsible for some or all of the actual losses incurred before notification of the disclosure of your Password or Mobile Banking App PIN to the Bank except for:

a. any amount that exceeds any applicable transaction limit;

b. any portion that exceeds the balance of your Nominated Account or Credit Card Account;

c. fraudulent or negligent conduct by a team member of the Bank or agent or other party involved in the Electronic Banking Services; and

d. any other unauthorised transactions where it is clear that you could not have contributed to the loss.

11.5 The Bank will not be liable for any unauthorised use of the Electronic Banking Services in circumstances where you have failed to take reasonable steps to ensure that protective systems such as virus scanning, firewall, anti-spyware, and anti¬spam software on your Device are up to date or where you have failed to take reasonable care to safeguard any Device that is used by you to access the Electronic Banking Services. You agree to allow the Bank access to your Devices and any relevant related equipment to enable the Bank to determine whether you have taken all reasonable steps to protect the security of your Devices.

11.6 If you incur a direct loss that is due to a security breach of the Electronic Banking Services and caused as a result of our failure to take reasonable care and that loss is not caused or contributed to by you, then we will reimburse you for that loss.

11.7 We will reimburse you for any losses caused by transactions not authorised by you and completed before you had access to the Electronic Banking Services or during any period where you did not have access to Electronic Banking Services including, if applicable, before you have selected either your Mobile Banking App PIN or Password.

11.8 Subject to the exceptions set out in the preceding sub-clauses in this clause, to the extent permitted by law the Bank will not be liable to you or any other person and accepts no responsibility for any claim, loss, damage, cost or expense whether direct or indirect, consequential or economic which arises in connection with any one of the following:

a. your use of any of the Electronic Banking Services;

b. any unauthorised use of your Password or Mobile Banking App PIN

c. any system or telecommunications link failure; or

d. any default, error or defect in design or engineering of the Electronic Banking Services or any delay, fault, malfunction, unavailability or loss of access to the Electronic Banking Services.

12. Accessing your Accounts

12.1 In order to access Electronic Banking Services, you must hold an account with us, hold a Credit Card Account or be a Signatory or Authorised User of an account with us.

12.2 When accessing Electronic Banking Services, you will be able to select and switch between the different account relationships you have with the Bank (i.e. company, trust, partnership, individual and joint holdings) using the 'account management' option without having to manage separate logins for each account relationship.

12.3 You can set one account relationship as the default account relationship which you view when you log in. You must then switch between account relationships to be able to transact and view details for each particular account relationship.

12.4 You may only use the Electronic Banking Services to perform transactions on your Nominated Accounts and/or Credit Card Accounts. Any transactional restrictions that apply to a particular Nominated Account (such as a fixed term deposit account or a loan account) or Credit Card Account will apply when using the Electronic Banking Services.

12.5 If you are a Signatory to a Nominated Account, you may access the account through Electronic Banking Services subject to any Signing Rules for the account.

12.6 You acknowledge and agree that we are authorised to act on instructions given by you through Electronic Banking Services by using any combination of your Password or Mobile Banking App PIN and that we are not obliged to make any further enquiries.

12.7 If any Nominated Account or Credit Card Account is in the name of more than one person, the liability of all account holders under these Terms and Conditions will be joint and several for any transactions carried out on that account in accordance with these Terms and Conditions.

12.8 The Bank may restrict which of your accounts (including Credit Card Accounts) you can nominate for access via Electronic Banking Services and may also restrict the Electronic Banking Services available to those accounts.

13. Fees/Charges

13.1 You agree to pay all fees and charges relating to any Electronic Banking Services in addition to any applicable account, credit and transaction fees. Fees and charges are subject to change. Our current fees and charges are available on request and free of charge from any Branch of the Bank or can be viewed at sbsbank.co.nz/resource/fees.

13.2 The Bank may deduct such fees and other charges from your account(s) in accordance with the "Fees, Costs and Deductions" section of our General Terms and Conditions.

14. Internet Banking

14.1 When you first log into Internet Banking, you will be asked to select your own Password. Passwords must be 8 to 32 characters in length, may consist of a combination of permitted characters on your keyboard and must contain (in any order you choose) at least two numeric digits and at least two characters that are not numeric digits, including one upper case and one lower case letter.

14.2 You must change your Password the first time you use Internet Banking and at frequent intervals thereafter, for example, monthly. It is your responsibility to change your Password regularly.

14.3 When accessing Internet Banking you will have three attempts to successfully enter your Password. Upon the third unsuccessful attempt your Internet Banking access will be suspended.

14.4 To restore your Internet Banking access follow the steps set out in clause 1.3.

14.5 To use Internet Banking you will need to have access to the internet on a Device running a current version of a supported internet browser. Details of supported internet browsers are available at sbsbank.co.nz or by contacting the Bank in person at any of our Branches during Business Hours or by calling our Contact Centre on 0800 727 2265, or outside New Zealand on +64 3 211 0700.

14.6 Check your last log-in details, which will appear every time you log into Internet Banking and notify us immediately if the last log-in details are incorrect.

14.7 You should ensure that your computer contains up-to-date anti¬virus and security software before using Internet Banking.

14.8 When you finish using Internet Banking, we recommend that you shut down all the windows of the browser you have used to gain access to Internet Banking and then restart the browser in order to ensure that the "Back" function (or similar function in your browser) cannot be used to trace your activities.

14.9 If you require assistance with clearing your browser's cache, we suggest you review your browser help facility or contact a PC support or maintenance service for instructions on how to complete this process.

15. Mobile Banking App

15.1 To use the Mobile Banking App you must:

a. have a Mobile Device running a Compatible Mobile Operating System;

b. accept these Terms and Conditions;

c. register for Second Factor Authentication (if not already registered);

d. setup a 5-digit personal identification number (the Mobile Banking App PIN) to access the Mobile Banking App on your Mobile Device.

15.2 You may register to use the Mobile Banking App on more than one Mobile Device. You will need to register each Mobile Device separately and each will have a separate Mobile Banking App PIN.

15.3 Resetting the Mobile Banking App PIN for one Mobile Device will not change any Mobile Banking App PIN you have assigned to any other Mobile Device you have registered for the Mobile Banking App.

15.4 Each Mobile Device can have the Mobile Banking App registered for only one customer at a time.

15.5 Not all Electronic Banking Services are available on the Mobile Banking App. More comprehensive Electronic Banking Services are available through accessing Internet Banking. Specifically, Multi-payments and instructions where a Signing Rule requires two or more people to authorise those instructions cannot be initiated or authorised within the Mobile Banking App.

15.6 You must not allow other persons to use the Mobile Banking App on Mobile Devices you have registered for Electronic Banking Services (and have not since deregistered).

15.7 For security reasons, you are recommended to deregister Mobile Devices which you no longer use for the Mobile Banking App. To deregister a Mobile Device from using the Mobile Banking App you will have to contact the Bank directly.

15.8 The accounts you nominate for Balance Peek will be the same across all Mobile Devices you have registered for the Mobile Banking App.

16. Non-Personal Customers

16.1 Where you use Electronic Banking Services for non-personal purposes, then without prejudice to any other provisions of these Terms and Conditions, you must ensure that your Password(s) and Mobile Banking App PIN(s) are kept secure as you are solely responsible for any use or misuse of the Password(s) and Mobile Banking App PIN(s) by any persons authorised to sign on your accounts which are accessible through the Electronic Banking Services.

16.2 You should reconcile your financial records with your bank statements at least monthly so that your instructions via the Electronic Banking Services can be monitored.

16.3 To the extent allowed by law, the provisions of the Consumer Guarantees Act 1993 will not apply to Non-Personal Customers using the Electronic Banking Services.

17. Liability for Non-Personal Customers

17.1 The ability to utilise Electronic Banking Services for non-personal purposes exposes your organisation to a higher risk of fraud, either by Authorised Users or by any unauthorised person to whom an account number and Password has been disclosed. You acknowledge that Electronic Banking Services exposes your organisation to these risks and that, except in the case of fraudulent or negligent conduct by an employee or agent of the Bank, the Bank:

a. is not liable for any loss which your organisation suffers as a result of any use (including unauthorised use) of the Electronic Banking Services; and

b. may rely on all instructions received from, and is not required to verify the identity of, any person using a Customer Number and Password issued to your organisation.

18. Second Factor Authentication

18.1 To utilise the full functionality of Internet Banking and gain access to the Mobile Banking App, you must register for Second Factor Authentication. Some features will not be available if you choose not to register.

18.2 To register for Second Factor Authentication, you will need to provide an active mobile phone number for your Mobile Device which can receive SMS messages. This can be done by contacting the Bank during Business Hours either in person at any of our Branches or by calling our Contact Centre on 0800 727 2265, or outside New Zealand on +64 3 211 0700.

18.3 Once registered for Second Factor Authentication you are not able to switch it off, nor change the criteria which triggers the process.

18.4 Second Factor Authentication is triggered when certain account activity requires separate validation of an instruction being provided to the Bank.

18.5 To authenticate an instruction given to the Bank which triggers Second Factor Authentication:

- Your registered mobile phone number will be sent an SMS Code.
- You must enter the SMS Code provided within the applicable Electronic Banking Service.

18.6 If you are unable to successfully complete the Second Factor Authentication process you will need to contact the Bank during Business Hours for assistance either in person at any of our Branches or by calling our Contact Centre on 0800 727 2265, or outside New Zealand on +64 3 211 0700.

18.7 The Bank does not guarantee that SMS Codes will be received by you.

18.8 The Bank does not guarantee that the Second Factor Authentication

service will be available at all times.

18.9 You accept that SMS Codes are not encrypted and contain confidential information. The Bank takes no responsibility for any SMS Codes that are read/ accessed by an unauthorised third party on your mobile phone.

18.10 The Bank takes no responsibility for ensuring that the mobile phone number you provide is correct and shall not be liable for any failure of Second Factor Authentication, and associated instructions which have triggered it, resulting from a mobile phone number which you have provided which is neither current nor correct at the time the Second Factor Authentication is triggered.

18.11 You are responsible for any fees charged by your mobile service provider.

18.12 You must notify us of any changes to your registered mobile phone number and we will change where your SMS Codes are sent to.

18.13 To the extent permitted by law, the Bank will not be responsible for any direct or indirect costs, losses, damages, or other liability resulting from any failure or delay in receiving SMS Codes.

19. SMS Alert notifications

19.1 When you register for Internet Banking and confirm your mobile number:

a. you may opt to receive Account Alerts; and

b. you will automatically be opted in for Internet Banking Alerts.

19.2 SMS Alerts are only available for Credit Card Accounts and specific transactional and savings accounts which the Bank makes available for the service.

19.3 You can opt in or out of receiving SMS Alerts (excluding Internet Banking Alerts) within Internet Banking or alternatively during Business Hours either in person at any of our Branches or by calling our Contact Centre on 0800 727 2265, or outside New Zealand on +64 3 211 0700.

19.4 The Bank will not charge a fee for sending Internet Banking Alerts. Fees may be charged for Account Alerts (please refer to our 'Account Charges' document for further information).

19.5 Standard mobile carrier fees may also apply for the sending and/or receiving of SMS Alerts.

19.6 The Bank does not guarantee that SMS Alerts will be received by you.

19.7 The Bank does not guarantee that the SMS Alerts service will be available at all times.

19.8 Information sent by SMS Alert will be correct as at the time it is sent by the Bank.

19.9 You accept that SMS Alerts are not encrypted and may contain confidential information. The Bank takes no responsibility for any SMS Alerts that are read/ accessed by an unauthorised third party on your mobile phone.

19.10 The Bank takes no responsibility for ensuring that the mobile phone number you provide is correct and shall not be liable for the disclosure of your personal or confidential information to a mobile phone number which you have provided which is neither current nor correct at the time the information is sent.

19.11 Changes to your mobile phone number you advise to us will change where your SMS Alerts are sent to.

19.12 To the extent permitted by law, the Bank will not be responsible for any direct or indirect costs, losses, damages, or other liability resulting from any failure or delay in receiving SMS Alerts or inaccurate information received in alerts.

20. Continuity of Service

20.1 We will endeavor to provide access to the Electronic Banking Services on a continuous basis, subject to any necessary downtime that may be required for system maintenance, repairs and updating, or loss of access resulting from matters beyond our control.

20.2 We reserve the right to suspend, terminate or otherwise alter access to some or all of the Electronic Banking Services at any time and without notice. Particularly in cases of:

a. periodic maintenance and updates; or

b. where a threat has been identified to the security of any, or all, of the Electronic Banking Services.

20.3 We will not be held liable for any loss which you or your organisation suffers as a result of any loss of continuity for any of the Electronic Banking Services. If the Electronic Banking Services are unavailable, it is your responsibility to use other means to effect transactions and do your banking.

20.4 Some of the Electronic Banking Services also rely on the provision of third party services to you including internet access, mobile network data and cellular coverage. By using the Electronic Banking Services, you agree that the Bank will also not be liable for any failure in the Electronic Banking Services caused by failures of third parties either in part or in full.

21. Definitions

- **"Account Alerts"** means SMS Alerts that you set up within Internet Banking to notify you of activity occurring on your Nominated Account(s) and/or Credit Card Account(s). These alerts can be customised to your requirements.
- **"Account Operating Authority"** means the current account operating authority form completed and signed by the customer for an account with the Bank.
- **"Approved Payee"** means any organisation or individual who has provided their payment details to enable payments to be made to them by the Bank's customers using the Electronic Banking Services.
- **"Authorised User"** means a user authorised by the account holder(s) including Partner(s), Trust Administrator and Trust Supervisor.
- **"Balance Peek"** means the Mobile Banking App feature that allows you to view the available balance of selected Nominated Accounts and Credit Card Accounts without logging into the Mobile Banking App using your Mobile Banking App PIN.
- **"Bank", "we", "us"** or **"our"** means Southland Building Society trading as SBS Bank, a registered bank with a mutual building society structure.
- **"Bankruptcy"** includes the loss of capacity, insolvency, receivership, liquidation, removal from the register, statutory management or any similar occurrence, and petition for Bankruptcy includes any step taken for or towards these.
- **"Branch"** means one of the Bank's branches in New Zealand and "Branches" has a corresponding meaning.
- **"Business Day"** means Monday to Friday excluding New Zealand public holidays.
- **"Business Hours"** means the hours of operation of either or the Bank's Branches or the Bank's Contact Centre which can be found at sbsbank.co.nz.
- **"Compatible Mobile Operating System**" means the minimum version or newer of a Mobile Device's operating system specified on an official download screen for the Mobile Banking App.
- **"Credit Card Account"** means the account(s) you hold with SBS Money Limited that can be accessed using your SBS Visa Credit Card(s) and that has/have been nominated by you to be accessed via our Electronic Banking Services.
- **"Customer Number"** means the identification number, alternatively referred to as a "member number", issued to you by the Bank. This enables us to identify you when you access any of the Electronic Banking Services.
- **"Device"** means any electronic device used to access any of the Bank's Electronic Banking Services (this includes desktop, laptop, tablet and other handheld computers along with mobile phones).
- **"Electronic Banking Service(s)"** means the electronic banking services provided by the Bank to provide access to Nominated Accounts and Credit Card Accounts for customers including Internet Banking and the Mobile Banking App.
- **"External Account"** means an account not held with the Bank or any of its operating brands.
- **"General Terms and Conditions"** means the Bank's General Terms and Conditions as amended from time to time (located at sbsbank.co.nz/terms-conditions).
- **"Internet Banking"** means the internet banking service provided by the Bank to provide access to Nominated Accounts and Credit Card Accounts for customers using a unique Customer Number and Password.
- **"Internet Banking Alerts"** means SMS Alerts which alert you to actions made on your Nominated Account(s) or Credit Card Account(s) through Internet Banking. These are designed to notify you of:
  - Changes made to your Password or Mobile Banking App PIN;
  - Maximum Internet Banking login attempts have been exceeded; or
  - Changes to your mobile phone number initiated within the Electronic Banking Services.
- **"Mobile Banking App"** means the Bank's software application designed to run on Mobile Devices and provide a selection of key Electronic Banking Services.
- **"Mobile Banking App PIN"** means a confidential 5-digit personal identification number to prevent unauthorised access to and use of the Mobile Banking App on your Mobile Device.
- **"Mobile Device"** means any portable device using a wireless internet connection to access any of the Bank's Electronic Banking Services including but not limited to smartphones and tablet computers.
- **"Multi-payments"** means payment instructions provided in Internet Banking consisting of multiple payments together.
- **"Nominated Account"** means the bank account(s) you hold with the Bank that has/have been nominated by you to be accessed via our Electronic Banking Services (but does not include a Credit Card Account).
- **"Non-Personal Customer(s)"** means the account is either owned by (in part or in full) or operated by an organisation (including any company, trust, partnership, incorporated or unincorporated group, or entity), or

person(s) operating in a professional or business capacity.

- **"Partner"** means a nominated employed person within a professional business, who holds various levels of involvement in the operational decisions of a business entity.
- **"Password"** means a confidential password used to prevent unauthorised access to and use of your accounts, used with your Customer Number to give you access to Internet Banking.
- **"Second Factor Authentication"** means the SMS Code verification process used by the Bank to ensure security of the Electronic Banking Services.
- **"Signatory"** means any person who is listed on the Account Operating Authority for your account(s) as being able to complete transactions.
- **"Signing Rule"** means the rule set out within the Account Operating Authority for either an individual or group of accounts, which specifies how many Signatories are required to authorise and transactions or instructions in relation to the applicable account(s).
- **"SMS Alerts"** means an automated notification service which sends text messages from the Bank to a mobile phone number provided by you, including Account Alerts and Internet Banking Alerts.
- **"SMS Code"** is a short code sent by the Bank by text message to the customer's registered mobile number.
- **"Terms and Conditions"** means these terms and conditions.
- **"Trust Administrator"** means a nominated employee of the entity practicing in trust management, who holds levels of operational authority for processing trust accounting activities.
- **"Trust Supervisor"** means a nominated partner of the professional entity, who holds the Trust Account Supervisor position, and is therefore responsible for all account administration of accounting for that entity.
- **"you" or "your"** means the account holder, including (as may be applicable) any holder of a joint account, any company, firm, partnership, trust, estate, society (whether incorporated or unincorporated), lodge, club or user of Electronic Banking Services.