

Electronic Banking Terms & Conditions

Effective 11 August 2013

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").
- Please read carefully and then keep this document in a safe place.
- 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). Copies of the specific terms and conditions for your account(s) may be obtained from our website, from any of our Branches or by ringing our Contact Centre.
- In the event that there is any inconsistency between these Terms and Conditions and any other terms and conditions applying to your account(s) or any service, 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.
- We are happy to explain anything that is not clear to you.

1. Electronic Banking Security

- 1.1 You should take care when selecting your Password(s), PIN(s), and Security Questions. Please refer to the PIN(s) and Passwords section of our General Terms and Conditions for further information.
- 1.2 The requirements under the PIN(s) and Passwords section of our General Terms and Conditions also applies to Security Questions as if they were a PIN or Password.
- 1.3 If you forget your Password, PIN or any of your Security Questions, call our Contact Centre on freephone 0800 727 2265 and we will ask you to identify yourself before arranging to reset the relevant security settings.
- 1.4 You have a responsibility to exercise reasonable care to prevent unauthorised access to the computer or Mobile Device that you use to access our Electronic Banking Services. This includes:
 - a. Not leaving your device unattended and logged into our Electronic Banking Services;
 - b. Locking your device or taking other steps to stop unauthorised use of our Electronic Banking Services; and
 - c. Notifying us as soon as practicable if your device is lost or stolen.
- 1.5 Regularly examine your transaction history to identify any instances where Electronic Banking Services have been used without your authority. Notify us immediately where you identify any unauthorised transactions.
- 1.6 You must take reasonable care when accessing our Electronic Banking Services to ensure that your Password, PIN and answers to Security Questions are not seen by or disclosed to anyone else.
- 1.7 You must change your Password, 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, PIN or Security Questions" section.
- 1.8 SBS does not support or condone the use of third party account aggregators which interface with any of our Electronic Banking Services and require you to input your customer information including any combination of your Customer Number, Password, PIN or Security Questions. The use of these services by you breaches these Terms and Conditions and is entirely at your own risk and liability. The Bank reserves the right to terminate your access to Electronic Banking Services without notice when use of third party account aggregators on your accounts breaches these Terms and Conditions, our General Terms and Conditions and conditions or any of our other terms and conditions
- 1.9 You should not open attachments or run software from untrusted or unknown sources on any of the devices that you use to access our Electronic Banking Services.

2. Notification of Loss, Theft or Unauthorised use of your Password, PIN or Security Questions

- 2.1 You must notify the Bank immediately when:
 - a. you know or suspect that someone else knows your Password, PIN or any of your Security Questions;
 - b. you discover or suspect an unauthorised use of your Password, PIN or Security Questions has occurred; or

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

- 2.2 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 checking transactions against your statements.
- 2.3 During Business Hours, call us immediately and we can reset your login details and/or reset your Security Question status.
- 2.4 Outside of Business Hours, cancel your Internet Banking access online through the "Contact Us" section within Internet Banking. Suspension is permanent until the Bank is contacted by you and normal identification procedures are satisfied. This functionality is not available to customers who access Internet Banking through i-bank. Within New Zealand you should call our Contact Centre on freephone 0800 727 2265. Outside New Zealand telephone +64 3 211 0700.

3. Payments

- 3.1 With the exception of future-dated payments, electronic payments authorised after 8.30pm or on weekends 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.
- 3.2 When you set up a payment, you authorise us to debit your Nominated Account held with the Bank, with the amounts you request to be paid to a specific account.
- 3.3 Payments from a Nominated Account to another Nominated Account will be debited and credited immediately (unless specified that the payment to be made will occur on a future date).
- 3.4 A payment is irreversible once the instruction to make the payment has been completed using our Electronic Banking Services (unless specified that the payment to be made will occur on a future date).
- 3.5 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. When a future date is chosen, the payment will be automatically debited from your Nominated Account on the date requested in accordance with your instructions.
- 3.6 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.
- 3.7 We will endeavour to make the payments you request, although we accept no responsibility or liability for any refusal or omission 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.
- 3.8 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).
- 3.9 In the event of a future-dated payment not able to be made on 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 3 Business Days. Following that period arrangements for that payment will become your sole responsibility.
- 3.10 We may in our absolute discretion conclusively determine the order of priority of payments 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. Payments in excess of your daily limit may not be actioned by us.

- 3.11 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.
- 3.12 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.
- 3.13 For payments to Registered Payees the Bank relies on the account numbers and required reference details provided from time to time by the Registered Payee. The Bank cannot guarantee either at the time payment instruction is received or when the payment is made that these Registered Payee details remain current and are correct.
- 3.14 You may elect to skip one or more recurring future-dated payments made from your Nominated Accounts. In order to be actioned, an instruction from you to skip a recurring future-dated payment must be received before the date the payment is scheduled to be made.

4. Reversing Transactions

- 4.1 You cannot cancel a payment instruction once it is given 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.
- 4.2 Notwithstanding that transactions are irreversible once authorised, if a request for reversal of a payment is made in writing within 24 hours of a payment error being made, we will attempt to recover the payment. There is no guarantee that we will be able to recover the payment.
- 4.3 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.
- 4.4 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).

5. Transactions

- 5.1 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.
- 5.2 The Bank may set minimum and maximum limits for transactions carried out via any of the Electronic Banking Services.
- 5.3 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).
- 5.4 You agree that aggregation of any available balance or credit limit on Nominated Accounts is not possible when determining the available balance or credit limit for the selected Nominated Account.
- 5.5 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.

6. Changes to these Terms and Conditions

- 6.1 The Bank has the right to vary these Terms and Conditions and any other terms and conditions applying to your Nominated Accounts and to vary, change or withdraw any of the Bank's services or service brochures at any time.
- 6.2 You will be given at least 14 days notice of any variation either by post to your last known address, telephone call, notice in your Branch, notice on our website or via an electronic banking channel used by you.
- 6.3 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.
- 6.4 From time to time we may advertise financial products or services on the medium through which you access the Electronic Banking Services. You consent to receiving such advertising material when using the Electronic Banking Services.

7. Privacy

In addition to our 'Privacy Statement' in our General Terms and Conditions you authorise us to give information about you and any of your Nominated 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.

8. Restrictions and Termination of Access to the Electronic Banking Services

- 8.1 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. there are insufficient funds to cover payments or payment instructions given;
 - d. 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);
 - e. we are complying with a court order;
 - f. we are notified by any party of a dispute over either the ownership of funds or the operation of any account; or
 - g. we are protecting one or all of the parties to a Nominated Account, the Bank, or a third party who has reasonably claimed an interest in the Nominated Account.
- 8.2 You may cancel your access to any of the Electronic Banking Services at any time by giving us written notice or contacting us during Business Hours. You will remain responsible for any instructions made on your Nominated accounts via the Electronic Banking Services up until the time of cancellation.

9. Liability

- 9.1 Once you have notified the Bank that either your Password, PIN or Security Questions 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 General Terms and Conditions or you have acted fraudulently or negligently.
- 9.2 You will only be liable to pay 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, PIN or Security Questions;
 - c. disclosed your Password, PIN or Security Question 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, PIN or Security Questions down; or
 - e. failed to take reasonable care to prevent unauthorised access to the computer or Mobile Device that you use to access our Electronic Banking Services.
- 9.3 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 via Electronic Banking Services during that time.
- 9.4 If you have, in the Bank's sole opinion, contributed to the cause of the unauthorised transactions, you may be responsible for some or all of the actual losses occurred before notification of the disclosure of your Password, PIN or Security Questions 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;
 - c. fraudulent or negligent conduct by an employee 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.
- 9.5 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 computer or Mobile 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 computer, Mobile 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.
- 9.6 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.
- 9.7 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 your either your PIN or Password and your Security Questions.

- 9.8 Subject to the exceptions set out in the preceding bullet points in this section, 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:
- your use of any of the Electronic Banking Services;
 - any unauthorised use of your Password, PIN or Security Questions
 - any system or telecommunications link failure; or
 - 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.
- 9.9 Although the Electronic Banking Services will normally be available 24 hours a day, maintenance of the systems will be required from time to time with the result that the services may not always be available.

10. Accessing your Accounts

- 10.1 In order to access Electronic Banking Services you must be a member of the Bank and hold an account with us or be a Signatory or Authorised user of an account with us.
- 10.2 You may only use the Electronic Banking Services to perform transactions on those accounts you have nominated. If the terms and conditions of a Nominated Account such as, but not limited to, a fixed term deposit or loan account provide a transactional restriction on that account then that restriction will apply when using the Electronic Banking Services.
- 10.3 If you are a Signatory to a Nominated Account that can be operated on the instructions of any one Signatory to the account, you may access the account through Electronic Banking Services.
- 10.4 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, PIN or Security Questions and that we are not obliged to make any further enquiries.
- 10.5 If any Nominated 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.
- 10.6 The Bank may restrict which of your accounts you can nominate for access via Electronic Banking Services and may also restrict the Electronic Banking Services available to those accounts.

11. Fees/Charges

- 11.1 You agree to pay all fees and charges relating to any Electronic Banking Services in addition to any applicable account 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 viewed on our websites at www.sbsbank.co.nz
- 11.2 The Bank may deduct such fees and other charges from your account(s) in accordance with the "Fees, Costs and Deductions"

12. Internet Banking Your Password

- 12.1 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.
- 12.2 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.
- 12.3 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.
- 12.4 To restore your Internet Banking access and reset your Password you will need to contact the Bank directly.
- 12.5 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.
- 12.6 You should ensure that your computer contains up-to-date anti-virus and security software before using Internet Banking.
- 12.7 We recommend that you shut down all the windows of the browser you have used to gain access to the Internet Banking Service when you finish using 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.
- 12.8 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.

13. Business Customers

- 13.1 Where you use Internet Banking for business purposes, then without prejudice to any other provisions of these Terms and Conditions, you must ensure that your Passwords are kept secure and are only used by those authorised in writing to do so for the purpose of your business. Whilst you may share your Passwords with persons authorised in writing to use them for the purpose of your business, you do so at your sole risk, and you are solely responsible for any use or misuse of the Passwords by such persons. You must change your Passwords immediately if you revoke any persons authorised to sign on your accounts which are accessible by Internet Banking.
- 13.2 You should reconcile your business or financial records with your bank statements at least monthly so that your instructions via Internet Banking can be monitored.
- 13.3 To the extent allowed by law, the provisions of the Consumer Guarantees Act 1993 will not apply to Business Customers using Internet Banking.

14. Liability for Business Customers

- 14.1 The ability to utilise Internet Banking by your business exposes your business 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 Internet Banking exposes your business to these risks and that, except in the case of fraudulent or negligent conduct by an employee or agent of the Bank, the Bank:
- is not liable for any loss which your business suffers as a result of any use (including unauthorised use) of Internet Banking; and
 - may rely on all instructions received from, and is not required to verify the identity of, any person using an Customer Number and Password issued to your business.

15. Security Questions

- 15.1 Security Questions are an additional security feature of Internet Banking. You must select at least three questions and answers in order to use Internet Banking.
- 15.2 Security Questions are not available for customers who access Internet Banking through i-bank.
- 15.3 Certain actions that you may request within Internet Banking will require that you respond to an automated challenge based on your chosen Security Questions before that action can be initiated.
- 15.4 Where you haven't set your Security Questions you will have access to three grace log-ins. During this period you will have access to limited Internet Banking functionality. On your fourth login you will be prompted to set up your Security Questions, if you do not do so at this time your Internet Banking access will be unavailable until you log-in and set your Security Questions.
- 15.5 You must select your questions from a pre-set list plus you may choose to create one personalised question.
- 15.6 The answers you set for your questions are personalised answers provided by you.
- 15.7 When you are prompted to answer a challenge against one of your questions, your response must match against the answer you originally gave for that particular question in order to proceed with the nominated action. If your response is incorrect, a new challenge will be presented. If you answer 3 challenges incorrectly in one session the nominated action will not proceed and your access to Internet Banking functionality which requires authentication by way of Security Question challenge will be suspended.
- 15.8 To restore your Internet Banking access and reset your Security Questions you will need to contact the Bank directly.
- 15.9 We will not ask you in person, by telephone or in writing (including by email) any of your Security Questions.

16. Alert notifications

- 16.1 SMS Alerts are only sent to customers who have opted in to receive such alerts, however if you are registered for Internet Banking then you will automatically be opted in for Security Alerts when you confirm your New Zealand mobile phone number.
- 16.2 SMS Alerts are not available for customers who access Internet Banking through i-bank.
- 16.3 SMS Alerts are only available for specific transactional and savings accounts which the Bank makes available for the service.
- 16.4 SMS Alerts can only be received by New Zealand mobile phone numbers within New Zealand.
- 16.5 You can opt in to receive SMS Alerts in a Branch, by phone or online.
- 16.6 You can opt out of receiving SMS Alerts in a Branch or by phone.
- 16.7 The Bank will not charge a fee for sending Security Alerts. Fees may be charged for Convenience Alerts, please refer to our 'Account Charges' document for further information.

- 16.8 Standard mobile carrier fees may also apply for the sending and/or receiving of SMS Alerts.
- 16.9 Opting into Security Alerts will not change any of the terms in the 'Liability' section of this document.
- 16.10 The Bank does not guarantee that SMS Alerts will be received by you.
- 16.11 The Bank does not guarantee that the SMS Alerts service will be available at all times.
- 16.12 Information sent by SMS Alert will be correct as at the time it is sent by the Bank.
- 16.13 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 device.
- 16.14 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.
- 16.15 Changes to your mobile phone number you advise to us will change where your SMS Alerts are sent to.
- 16.16 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.

17. Definitions

- **"Authorised users"** (of Customers using i-bank) means users authorised by the account holder(s) including Partner(s), Trust Administrator and Trust Supervisor.
- **"Bankruptcy or bankrupt"** 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.
- **"Bank", "we", "us" or "our"** means Southland Building Society trading as SBS Bank and HBS Bank – a registered bank with a mutual building society structure.
- **"Branch"** means one of the Bank's branches in New Zealand and "Branches" has a corresponding meaning.
- **"Business Customer(s)"** means any person(s) operating a business account(s) with a view to making a profit, or organisation.
- **"Business Day"** means Monday to Friday excluding New Zealand public holidays.
- **"Business Hours"** means the hours of operation of the Bank's freephone number 0800 727 2265 is 8.30am – 5.30pm local standard time.
- **"Convenience Alerts"** are SMS Alerts that are not Security Alerts, which you set up within Internet Banking. Convenience Alerts can notify you of activity occurring on your Nominated Account(s). These alerts can be customised to your requirements.
- **"Customer Number"** means the identification number issued to you by the Bank. This enables us to identify you when you access any of the Electronic Banking Services.
- **"Electronic Banking Service(s)"** means the electronic banking services provided by the Bank to provide access to Nominated Accounts for customers including Internet Banking.
- **"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.
- **"i-bank"** means i-bank products and services accessed via our i-bank login page.
- **"Internet Banking"** means the internet banking service provided by the Bank to provide access to Nominated Accounts for customers using a unique Customer Number, Password and Security Questions.
- **"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 tablets.
- **"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.
- **"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 it gives you access to Internet Banking.
- **"PIN"** means a confidential 4 digit personal identification number to prevent unauthorised access to and use of your accounts, used with your Customer Number it gives you access to telephone banking.
- **"Recurring payment"** means a payment that is set up by the customer, or on behalf of the customer by the Bank, which is made at regular intervals (e.g. weekly, monthly etc) for a set amount. Also known as an automatic payment.
- **"Registered 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.
- **"Security Alerts"** are SMS Alerts which alert you to actions made on your Nominated Account(s) through Internet Banking. Security Alerts are designed to notify you of:
 - Initiation of payments (current or future) greater than \$500.
 - Creation or alteration of your payees.
 - Creation or alteration of your recurring payments.
 - Changes made to your personal details or security settings.
 - Suspension of access to Internet Banking Services.
 - Maximum Internet Banking login attempts have been exceeded.
- **"Security Questions"** means the questions and answers you select used to help authenticate particular instructions provided by you within Internet Banking.
- **"Signatory"** means any person who is listed on the Account Operating Authority for your account(s) as being able to complete transactions.
- **"SMS Alerts"** means an automated notification service which sends text messages from the Bank to a mobile phone number provided by you.
- **"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 Internet Banking.