Bank of St. Helena Ltd.

www.sainthelenabank.com

CUSTOMER DATA SECURITY

GUIDANCE ON KEEPING YOUR DATA SECURE

The Bank of St. Helena Ltd. takes customer security very seriously. Whilst we employ a wide range of measures to help keep you protected, including multiple firewall solutions, data encryption, and fraud detection tools, you are ultimately responsible for the security of your data when engaging with our services.

With that in mind, we want to remind you of some useful tips and advice to help you keep your data secure:

Passwords and Passcodes

- Use strong passwords and passcodes. Passwords should be a mixture of upper and lower-case letters, numbers and special characters. You should avoid using information which is easy to guess, for example because it relates to a fact about you is commonly known.
- Do not use obvious numerical combinations for your passcodes (for example your date of birth or sequential numbering like "123456").
- Do not write down your passwords or passcodes. If you receive them in a letter or email, memorise them before carefully destroying that letter or deleting that email.
- Do not share your passwords or passcodes with anyone else and do not give anyone else access to your accounts.
- Use a different password or passcode for each account you use or service you access.
- Consider changing your passwords and passcodes on a regular basis.

General Security Measures

- Do not access private accounts on a public device or on a shared device.
- Beware of who is around you at all times when accessing your accounts and do not do so in a public space. Public Wi-Fi connections are less secure than mobile internet or private Wi-Fi connections.
- If you post on social media:
    - Take care not to post sensitive personal information; and
    - Make use of privacy settings, for example by limiting those who can view your information or postings.
- Log out of your accounts at the end of each session.
- Use secure web browsers to access any services in which are you are providing or accessing your data.
- Beware of suspicious emails, texts and other communications. Look out for warning signs such as:
    - Generic, non-personalised greetings;
    - Strange sender email addresses;
    - Poor spelling and grammar;
    - An urgent writing tone (for example stating that you need to act quickly in accordance with the sender's instructions); and
    - Offers or inducements which seem too good to be true.

- Do not click on links or attachments in suspicious emails or other communications and do not respond to these communications.
- Use robust anti-virus and anti-spyware software on your devices. Keep this software updated regularly.
- Use a spam filter on your email accounts.
- Follow all account security guidance issued by the providers of the services you use when engaging with us, for example email service providers.

Communicating with Us

- We will never ask you for your full password or security details.
- You must inform us promptly if any contact details you have provided to us have been compromised or are no longer up-to-date.
- You should comply with any data security updates or advice we may provide from time to time.

Contact Us

To report suspicious account activity, please contact us promptly at SAR@sainthelenabank.com

If you believe that your account (or an account which you use to engage with our services such as an email account) has been compromised, please contact us promptly at customerservices@sainthelenabank.com

If you have any questions on data security, please contact us at helpdesk@sainthelenabnk.com

Bank of St. Helena Ltd.
Last updated April 2019