

ELECTRONIC BANKING UPDATE

1. SECURITY UPDATE ON MERCANTILE BANK INTERNET BANKING

Mercantile Bank would like to highlight the importance of adhering to the security measures provided when utilising Internet Banking.

The importance of this update is due to the fact that recently a small number of Internet account holders at other Financial Institutions in South Africa have become victims of the latest international trend in Internet fraud called identity theft.

Fraudsters are targeting the personal computers of bank account holders by stealing their electronic access criteria and manage to gain unauthorised access to their computers and load software called key-stroke logging software which automatically copies everything they typed on their computers and sends this back to the fraudster without their knowledge.

The security of our Internet banking is a key priority to us and we have strived to provide a system that covers these aspects. Additional security measures that are available on our Internet client software product [BANK@bility](#) and our Internet web based product [BANK@bility.lite](#) are as follows:

- [BANK@bility](#) provides the ability to enter your password by using the keyboard or mouse option. We recommend strongly that the mouse option be utilised as the use of the keyboard introduces the risk of a security attack by outsiders. This option is available on the Log-on screen when accessing your

[BANK@bility](#) profile. Select the Mouse under Password entry on the "Open Profile" screen. The keyboard will then appear on your screen. The password can then be selected by using the mouse (ensure that the selection is in the correct case i.e. Upper "Caps" or Lower case.

- BANK@bility.lite requires a separate log-on code, which is randomly selected with each log-on.

Clients are requested to follow the following security measures to prevent key logging:

- Utilise the mouse log-on option when accessing BANK@bility
- Make sure that no one has unauthorised access to your Internet Banking access information and/or PC.
- Never disclose your password to anybody including Bank staff
- Security log-on codes to be kept in a safe place.
- Check and verify the date and time the profile was last accessed on the “Importance Notice” screen when entering BANK@bility.
- Ensure that you have the latest anti-virus applications loaded on your PC. Your local PC hardware and software supplier will provide you with details in this regard.
- Make sure that the software that is loaded onto your PC via a third party is licensed.
- Update your operating system and browser with the latest Microsoft patches to protect your PC from exploitation. These can be downloaded from the Microsoft website <http://www.microsoft.com>
- Do not open suspicious or unfamiliar e-mails.
- Ensure that you have control over the shared folders on your PC as a shared folder could make your PC vulnerable to unauthorized installation of suspicious software. A blue icon shaped in the form of a hand can identify a shared folder.

Should you require any additional information or assistance in this regard please contact our Electronic Banking Support Line on 0860 11 99 23.

2. PAYMENT REQUIREMENTS FOR ELECTRONIC FUNDS TRANSFERS TO BENEFICIARIES

Please ensure that the account number of the beneficiary is captured correctly to ensure that the correct account is paid.