Corporate and Investment Banking

Business Online Information Security

Standard Bank
Also trading as Stanbic Bank

Risk reduction: Ensuring your sensitive information is secure

Due to the nature of the transactions that you perform on Business Online, it is important to reduce your exposure to online fraud. In this brochure we take a look at the basic measures you can apply to avoid becoming a victim of crime, and suggest some specific preventative measures you can take.

The first line of defence for your business is to:

- Ensure that you conduct your banking activities in a safe and secure environment;
- Operate in a secure IT environment, for example, ensuring that anti-virus software is used and updated regularly.

What is the relevance of Financial Crime Control in your organization?

International benchmarks indicate that losses as a result of financial crime ranged between 3% to 5% of headline earnings **(Source: www.ACFE.co.za)**

Applied to the estimated 2011 gross world product, this figure translates to a potential projected global fraud loss of more than USD3.5 trillion.

That is enough one dollar bills to go around the equator of the earth approximately 13 620 times.

Approximately 87% of occupational fraudsters had never been charged or convicted of a fraud-related offense and 84% had never been punished or terminated by an employer for fraud-related conduct.

The Basics

Operator ID and password security

Your password is just like the key to your front door – don't gift wrap it for a criminal!

As a valued client, Standard Bank has precautions in place to help protect your information. However, similar to the security solution you have protecting your business; it simply will not work if you do not switch it on.

The same applies to the fight against online fraud.

One of our standard security features is controlled access through the use of operator IDs and passwords. You can help reduce your exposure to online threats by implementing sound password protection principles.

Below are a few simple guidelines to follow:

- Keep them guessing and choose a strong password – your passwords should be complex. Don't use details associated with you or your company.
- It's top secret – never share or write it down.
- Who's been watching? Change your password often just in case it has been compromised.
- Be unique – set different passwords for all accounts that you access through the Internet. This way, if one of your passwords is compromised, your other accounts are not also at risk.
- Think before you click – do not select the "save password" option if prompted.

Two Factor Authentication

Two factor authentication is a multi-level log on procedure which requires you to provide two passwords before being granted access to your Business Online banking profile.

- Only the password provided by the token at the time of logging on will be valid for a particular Business Online session.
- Ensure that you have your two factor token with you at all times to avoid unauthorised use of the token.
- As breaches of security are most likely to occur when you login, please exercise extreme care to keep your login credentials safe and secure.

Segregation of duties, limits and release levels

If only one person has access to and control over your business' bank accounts and payment procedures, the opportunity to commit fraud (and go undetected) is far greater than in a situation where several people are responsible for managing the business' bank accounts and payments.

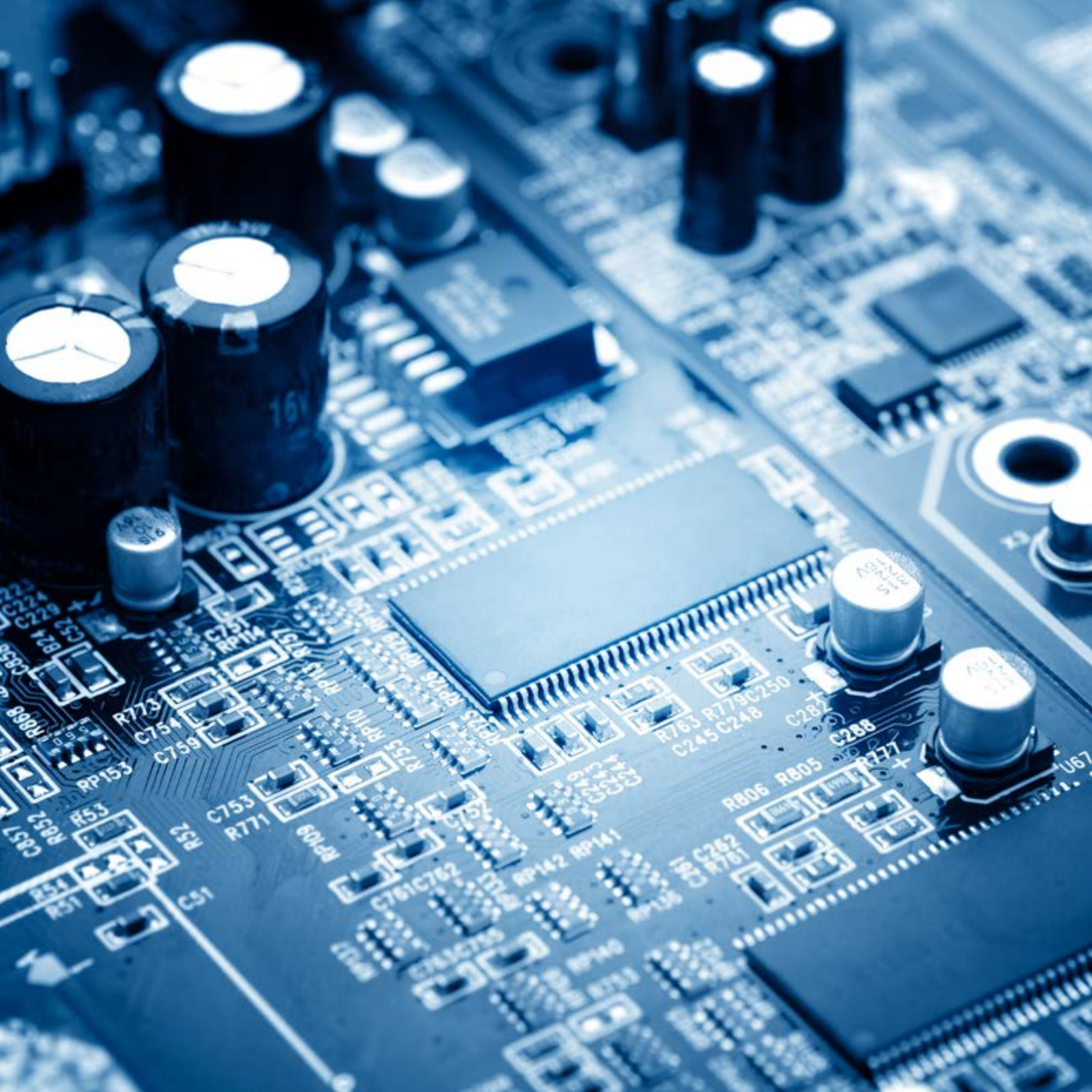
It follows that the more duties and roles are kept apart or segregated, the less opportunity there is for fraud to be perpetrated.

The segregation of duties is especially important for authorising access to the system and processing payments. We suggest that at least three roles be created in the department responsible for processing payments on behalf of your business, namely:

1. Designated person
2. User 1 – Capturer
3. User 2 – Releaser

The role of the designated person is to oversee and control the activities that take place on the business' Business Online profile. The designated person ensures that valid and authorised accounts, creditors and debtors are loaded; and that only authorised operators gain access to the Business Online profile.

It is of critical importance that this designated person advises the bank whenever there is a change in users and does not assign an existing ID to a new user.



The designated person should also ensure that appropriate limits and release levels are created and maintained to limit the amounts that can be processed, thereby reducing the size of the loss should fraud be perpetrated.

It is also suggested that one user captures the payments, and the other one verifies the validity of the transaction and releases the payments. This is where the roles of the two separate capturer and releaser roles are key.

The basic underlying principle of segregated duties is that no employee or group should be in a position both to perpetrate and conceal errors or fraud in their normal course of duties. The same would apply if their user credentials were compromised and used fraudulently.

Security Lock Out (Access Control)

Business Online's Security Lock Out (Access Control) feature allows you to completely deny access to your online banking profile at certain times of the day and on certain days of the week. The Security Lock Out feature is an optional add-on, available at no extra cost that allows pre-defined lock-out periods to be set according to your specific business requirements.

This feature also allows you to impose an immediate lock-out of a user profile or specific operator should the need arise.

The facility provides additional control over your Business Online banking platform, giving you increased peace of mind – especially outside of normal business hours.

Some facts about Security Lock out (Access Control):

- It is an optional feature, available on request
- If you subscribe to this feature it is imperative that you carefully consider your business's operational requirements when specifying the Business Online lock-out times for each day of the week
- The lock-out times are specified per user profile
- As soon as the profile is updated by the bank, the change is immediate
- All operators linked to the user profile will be denied access to Business Online during the lock-out time
- Subscribing for this feature does not affect any existing Business Online functionality or other security features
- Extensions to operating times can be arranged on an ad hoc basis, through the bank, should the need arise
- A warning message feature is available to alert operators when lock-out periods are about to commence
- If you do not subscribe, Business Online will continue to be available for 24 hours a day.

Account Verification Service (AVS)

Are you 100% certain that your payments are going into bona fide bank accounts? Our Account Verification Service (AVS) validates the details of your selected payees to ensure the funds you release are received by the correct parties.

AVS will verify the following information before allowing any transactions to take place:

- Account holder's name
- ID/company registration number
- Bank account number
- Bank branch code.

In addition, AVS will:

- Verify the target account status
- Confirm how long the account has been open
- Establish what type of account it is
- Determine whether the account accepts debits or credits.

Regular reports will be provided detailing information on all verified or unverified accounts.

Audit Reports

An interim report reflects an intention to pay, where the required releasing function is still pending.

Final audit reports submitted as confirmation of payment should not be accepted without confirming whether the credit is reflected on your account as an electronic payment and not as either a cash or cheque deposit.

Utilise the audit reports available on Business Online frequently, to highlight any irregular activity with regard to beneficiary profiles, and payment transactions. We recommend you review your audit reports at least once at the end of each day.

Common methods used to defraud

Key loggers

These are small programs or hardware devices that monitor each keystroke you enter on a specific computer's keyboard, including typos, backspacing and retyping.

This is a form of spyware used by cybercriminals to covertly watch and record everything you type on your PC in order to harvest your log-in names, passwords, and other sensitive financial or personal information, and send it on to the hackers.

Keyloggers have become very sophisticated. Once on a PC, they can track websites visited by the user and only log the keystrokes entered on the websites that are of particular interest to the cybercriminal, like online banking websites.

Keylogging security tips:

- Be cautious when you see new peripherals or cables attached to your keyboard. Implement and enforce physical security controls
- Ensure that your computer has the latest version of your anti-virus product installed
- Be alert to your computer hardware changes: Hardware key loggers can look similar to common computer equipment
- Be circumspect when installing programmes of any kind (software, music files, games, etc.) onto your computer. These programmes can conceal keystroke logging software.

Phishing

Phishing is an attempt, usually made via email, to steal your personal information and use it to defraud you.

Fraudsters will send you an email asking you to update your banking or personal information by clicking on a link to a bogus website.

Once the fraudster has your information, it allows them to load fraudulent accounts as beneficiaries and transfer your funds to the fraudulent beneficiary accounts.

Smishing (SMS Phishing)

This is the cellphone equivalent to phishing. Instead of being directed by email to a website, a text message is sent to your cellphone with a request to click on a link.

The link causes a Trojan to be installed on your cellphone.

Phishing security tips:

- Phishing sites, emails and SMS's often ask for information that Standard Bank would never ask you or will never request you to update, such as your personal or banking information
- Do not click on any links in emails to reach our Business Online Banking website. Always enter our website address, www.businessonline.standard.co.za in the address field to connect to our Business Online banking site
- Do not create shortcuts on your desktop to Business Online. Malicious software could redirect the shortcut to a phishing site
- Please forward any suspect phishing emails or any online fraud scams to phishing@standardbank.co.za
- Try and keep your electronic payment and daily withdrawal limits to a minimum.

Advance fee fraud (Nigerian 419 scam)

Advance fee fraud is often attempted through an unsolicited email, in which you are asked to pay fees in the hope of sharing in a much greater reward.

It is also known as Nigerian fraud or 419 scam (419 is the number of the law forbidding this practice in Nigeria).

Advance fee security tips:

- If it looks too good to be true, it probably is
- Do not open suspicious or unsolicited emails, also known as spam. Delete these emails immediately without opening them
- Never reply to a spam email, even if it is to unsubscribe. By replying you are verifying your email address to the scammers
- Never send your personal, credit card or online account details in an email
- If you still think the letter may be genuine, make sure you seek the advice of an independent professional (a lawyer, accountant or financial planner) before committing any money.

Change of banking details scam

In this case, you receive a letter on a company letterhead that appears to be authentic (or an email from a company that you believe is one of your trusted suppliers) informing you of a change of their bank account details.

The letter may be accompanied by a "cancelled cheque" showing the "new" bank account details.

As soon as you make a payment to the "new" account, the fraudster withdraws the funds immediately.

Change of banking details security tips:

- Always verify with the beneficiaries (Creditors) before updating or changing your beneficiaries (Creditors) banking details on your systems
- Make use of the Account Verification Service (AVS).

Deposit scam

Be wary if you receive any communication or advice that a deposit has been made into your account 'by mistake'.

The fraudster will fax you a bogus electronic transfer receipt as 'proof of payment' and ask for the overpaid amount to be refunded to them.

Deposit security tips:

- Before you release any goods, always confirm with your bank that the funds have been deposited and cleared
- Do not accept a faxed deposit slip/electronic receipt as proof of payment and never refund any amounts 'deposited in error' on the strength of a telephonic request
- Be skeptical of individuals or foreign government officials asking for your help in placing large sums of money in overseas bank accounts.

Cheque security tips:

- Never sign blank cheques
- Report the loss of your chequebook to the bank immediately
- Cross your cheques
- Try to avoid posting cheques as they could be intercepted
- Do not leave open spaces; draw a line to avoid any information being added
- Before releasing goods you have sold, verify that the deposit has cleared with the bank
- Check your bank statements often for any suspicious transactions.

Visit www.businessonline.standard.co.za
for more information on security.