PAUL O'SULLIVAN & ASSOCIATES
FORENSIC AND LOSS CONTROL CONSULTANTS

Tel: 076 991 1666 P.O. Box 78200, Sandton, 2146, Republic of South Africa Fax: 086 234 5733

To whom it may concern **October 2015**

For the attention of all:

Directors, CFO's, Debtors & Creditors Managers, Risk Managers & Internal Auditors

Please ensure that anyone in your company, with an interest in reducing fraud, see this bulletin.

INTERNET FRAUD - AWARENESS BULLETIN

In the last few months, we have become aware of an increasing number of attempts (some successful) to obtain funds under false pretences. Along the way the criminals commit the offences of Forgery, Uttering a Forged Document and Fraud, as they target the debtors book of a company. The *modus operandi* looks like this:

- The perpetrators unlawfully access and/or acquire a company's list of debtors and the debtor contact details;
- They then forge a letter by creating a fake letterhead of the company addressed to its debtors falsely informing them that the Company's banking details have changed and all future payments are to be made to a new bank account;
- They also forge a letter using a fake letterhead of a chosen bank addressed '*to whom it may concern'* purportedly confirming the change in bank details, of the company;
- Next, they create a web-mail account (often in another country – but not necessarily so) using a name that passes off as the creditor company, thereby intending to mislead the recipient into thinking that the mail was actually from the debtor's own creditor;
- In some cases, they even manage to 'clone' an e-mail address, which makes the recipient believe the mail is truly coming from its supplier;
- The forged (fake) letters are then sent from the web-mail account, to certain debtors and the perpetrators then sit back and await payments into bank accounts to be used for receiving the diverted monies.
- Sometimes they even telephone the victim and demand payment of an overdue amount, repeating that the payment should be made to the new account.
- The unwitting 'victim' then pays over monies due to a creditor to a bank account that has nothing to do with the creditor.
- Quite often the damage can run into millions, or hundreds of thousands of Rand before the victims realise what is going on.

The company making the payments to the wrong bank account is the ultimate loser, as it has not discharged its debt and then has to pay again to the correct bank account.

WHAT CAN BE DONE TO MINIMISE THE RISK?

By following some very simple measures you can drastically reduce the chances of becoming a victim of this type of crime:

CREDITORS DEPARTMENTS

Only allow access to trusted persons into your creditors department.

Make sure all the employees and 'trusted persons' have been criminal record vetted.

Never allow creditor bank details to be changed without having followed proper procedures and safeguards. Make sure you have a proper procedure in place, that recognises this type of crime.

Assume, until you prove otherwise, that any e-mail, or written request, requesting you to change payee bank details is an attempt at fraud, and do not comply, until you have made 'proper' personal checks to verify the information.

Never telephone a number on the e-mail or letter, to verify the change. Speake **ONLY** to a senior manager, director or person you know at the creditor company and follow this up with an e-mail confirmation to an existing and known e-mail address.

Never, click 'reply' to the e-mail and send your query there. If it is a cloned address, you will be inadvertently notifying the perpetrator that you are suspicious, and may be walking into a trap.

Remember, if you pay your debt to the wrong bank account, you have not paid your creditor and you will still be liable for the full amount.

DEBTORS DEPARTMENTS

Only allow access to trusted persons into your creditors department.

Make sure all the employees and 'trusted persons' have been criminal record vetted.

Do NOT throw old debtors reports into the bin. They MUST be properly destroyed or shredded.

Regularly change passwords on the accounts computers.

Know your clients and maintain regular personal contact.

EVERYONE

Call the police and/or report any suspicious activity to the relevant manager **IMMEDIATELY.**

Paul O'Sullivan CFE

CERTIFIED FRAUD EXAMINER

FRAUD HOT-LINE 0800 118 118