LAW SOCIETY
OF SOUTH AFRICA

CYBERCRIME: BUSINESS eMAIL COMPROMISES

Business eMail compromises (BECs) are a form of cybercrime where electronic communications are accessed, monitored and at appropriate times intercepted and replaced with eMails that are so similar to eMails that may be expected by the recipient that they deceive the recipient into accepting the trustworthiness and integrity of the eMail and acting thereon. Typically, the interception occurs when a payment is to be made and the bank account into which the payment is to be made reflected in the fraudulent communication is a bank account under the control of the criminals.

While attorneys have been victims of this fraud, this advisory is aimed at attorneys ensuring that their clients are aware of the risk of a potential fraud with a view to their not falling victims to the fraud. While there will be further information security relating to BECs that will be provided to attorneys by the LSSA in the future, this advisory is aimed primarily at attorneys' fulfilling their duty of care to clients by making them aware of the potential risk.

It is suggested that in all instances where clients may be required to make payment to an attorney that on initially engaging with the client and wherever appropriate in subsequent communications (whether by letter or eMail) the first paragraph in the communication, emphasised in bold, contains the following wording (or similar wording) alerting the client to BECs:

> ***"Criminal syndicates may attempt to induce you to make payments due to [firm's name] into bank accounts which do not belong to the firm and are controlled by criminals. These frauds are typically perpetrated using eMails or letters that appear materially identical to letters or eMails that may be sent to you by [firm's name]. Please take proper care in checking that these eMails do emanate from [firm's name].***
>
> ***Before making any payment to [firm's name] please ensure that you verify that the account into which payment will be made is a legitimate bank account of [firm's name].***
>
> ***If you are not certain of the correctness of the bank account you may contact [firm's name] and request to speak to the person attending to your matter. They will assist you in confirming the correct bank details.***
>
> ***[Firm's name] will not advise of any change in bank details by way of an eMail or other electronic communication. If you should receive any communication of this nature please report it to the person attending to your matter."***

In light of the increase in the prevalence of this type of fraud it is strongly suggested that this or similar wording in instances where banking transactions of high value may be performed (for instance

conveyancing matters) that this wording appears on all communications to clients and is prominently displayed at the beginning of the communication.

It is also suggested that a similar notice appears in a prominent place on attorneys' websites or other mechanisms that it uses[1] to communicate with clients.

[1] LSSA Cybersecurity helpdesk advisory 1