**Are you losing money through EFTs?**

**By Simthandile Kholelwa Myemane**

Attorneys must be aware of the risks, vulneabilities and control considerations around Eletronic Funds Transfers. A practitioner that does not anticipate fraud happening through EFT payments may find himself or herself out of business. Payments through EFTs are identified as highrisk areas within attorneys' practices as a result of limited and/or cumbersome controls.

An EFT is the electronic exchange or transfer of money from one account to another, either within a single financial institution or across multiple institutions through computer-based systems. In an attorney's firm, EFT payments include transfers from trust account to business account and vice versa.

Historically, payments were effected through issuance of cheques. However, with technological advancements, the use of EFT payments has and continues to grow tremendously, and is beginning to overtake cheque payments. The legal fraternity is also following suite and engages in many EFT payments. Although there are advantages associated with EFT payments, there are also risks that go with them. This article seeks to address these risks in order to assist and guide practising attorneys of potential pitfalls.

Here are some of the advantages of paying through EFTs:

• The payee receives money faster (between one and three days) compared to issuance of a cheque, which takes between five to seven days to clear. and risks they are exposed to. Once this is defined, they can then put plans in place and follow those plans with actions. As with any other payment system, attorneys should look out for the following risks and take the necessary precautionary measures:

• It is less expensive to pay by EFT than paying by cheque.

• There are minimal administration duties such as applications for new cheque books, as well as less stationery as there are no cheque books to hold.

• There are no risks of replica cheque books being fraudulently produced and payments effected through the practitioner's account.

• EFT payments effected in a controlled environment are safer than cheque issuance, as there is no risk of a cheque being lost in the mail.

• There is no risk of staff members writing out unauthorised payments and forging signatures.

• The payment system outrightly refuses to effect payment if funds in the account are insufficient.

• The banking system generates and maintains proof of payment that assists in resolving disputes that may arise.

However, risks are always prevalent where there is flow of money. Risk can be seen as the probability that a hazard will turn into a disaster. Taken separately vulnerability and hazards are not dangerous, but if they come together, they become a risk or a probability that a disaster will happen. It is possible to prevent and mitigate disasters from occurring. This refers to actions that a practitioner can take to make sure that a disaster does not happen or, if it does happen, that it does not cause as much harm as it could. Practitioners should recognise that in order for them to put the necessary prevention and mitigation measures in place, they first need to know which hazards and risks they are exposed to. Once this is defined, they can then put plans in place and follow those plans with actions.

As with any other payment system, attorneys should look out for the following risks and take the necessary precautionary measures:

| **Risk elements** | **Precautionary measure** |
|---|---|
| Invalid payments may be made and/or payments made to incorrect accounts. | • Develop finance policies that contain prescripts on EFT payments.<br><br>• Have properly defined payment requisition, authorisation and release processes.<br><br>• Ensure sufficient segregation of duties. The person requesting payment should be different from that/those releasing the payment. An example of such a process could be as follows (this will depend on the size of the practice) –<br>– one person may request payment through completion of a requisition; the next person may authorise the requisition;<br>– the next one may request payment;<br>– the next may approve/authorise payment; and<br>– the last person/persons may release payment. Where it is not practical to have all these check points due to the size of the practice, the practitioner bears more burden to ensure that fraud does not occur. It should also be borne in mind that the controls put in place should not be so cumbersome that they affect the smooth running of the practice.<br><br>• The person responsible for releasing payments should satisfy himself or herself of the correctness of the payee's banking details provided. Care should be taken by practitioners to ensure that they thoroughly check the account number to be paid as the payment system recognises an account number and not an account name. This means that the same account number can be paid with different account names. |
| Invalid payments may be made and/or payments made to incorrect accounts. | • In cases where the payee provided the banking details through an e-mail, the person releasing the payment should ensure that they have sight of the original e-mail from the payee and not a forwarded or reply message as the details could have been altered.<br><br>• In cases where payment is triggered by an invoice from a service provider, the banking details provided in the payment requisition must be verified against those provided in the invoice.<br><br>• The source documents that trigger the payment should always be verified or reviewed before a payment is released.<br><br>• In medium-sized to large practices, payments should be released by at least two people at two different levels.<br><br>• Everyone involved in the payment chain should satisfy themselves of the correctness of the payment details and not |

| | |
|---|---|
| | rely on the next or previous person to check, as the payment may end up not being checked by anyone and processed. |
| EFT payment system may not be adequately secured. | • Have designated computer terminals for EFT payments.<br><br>• Restrict access to the EFT system to authorised personnel only through the use of individualised passwords. Access codes should never be shared by two or more personnel.<br><br>• Where one-time-pin security is possible, this should be implemented so that the trust account partner is aware of all potential changes to payment information and the actual payments effected.<br><br>• Immediately revoke access rights for persons that terminate their services either through resignation, retirement, ill-health, etcetera. |
| Insufficient audit trail for payments. | • The various rules issued by the law societies and the draft uniform rules advocate for maintenance of accounting records for a period of five years. Source and all other supporting documents should also be maintained for the same period as the accounting records that they support. Invoices and any other payments records, namely, payment requisitions and proof of payments should always be maintained as source and/or supporting documents. |

There is no single solution to a challenge and practitioners are urged to consider their environments carefully before applying any precautionary measures.

Practitioners who put controls in place are more likely to thrive in business than those who allow risks or disasters to manifest themselves.

Be in charge of your practice and ensure that you can account for each and every cent that leaves your account.