

Management

Critical measures to protect against rocketing EFT fraud risk

STEVEN POWELL

Fraud is often described as a cancer which permeates every sphere of business life; no industry or profession is immune to its pervasive effects. Proactive anti-fraud measures to identify control weaknesses and vulnerable areas have been a business imperative for many companies over the past few years.

The economic downturn has, however, created a rampant increase in the amount of fraud committed in South Africa, yet very few companies have taken additional steps to counteract it. In fact, the inverse is happening. As companies cut costs and reduce head count, limited segregation of duties and greater transactional powers in the hands of fewer people, coupled to poor control environments, have made many organisations soft targets for both corrupt employees, as well as sophisticated fraud syndicates, which are able to commit fraud with amazing alacrity and ease. The result of fraud committed by either of these threats can culminate in unsustainable losses amounting to millions of rand within disturbingly short periods.

EFT fraud is the latest threat to businesses in SA

There is a particular sub-species of the fraud cancer which is creating havoc in businesses across the country, sometimes with catastrophic consequences. It is, accordingly, critically important to have an understanding of this new threat which is known as electronic funds transfer (EFT) fraud.

EFT fraud is the illicit electronic diversion of funds to parties to whom the funds are not due

It usually involves manipulation of the accounting software programmes used to pay suppliers or service providers.

In the past year EFT fraud has become one of the greatest risks faced by organisations in South Africa. Both the public and private sectors are at risk.

When electronic funds transfers are made, banking systems in South Africa rely only on the account numbers to remit funds to its intended destination. The name of the entity being paid is not critical to concluding the transaction. This creates opportunities for corrupt staff to create the illusion that they are paying legitimate suppliers, whereas, in truth and, in fact, they are transferring funds to themselves or friends and family. Larger corporate entities, accustomed to making thousands of payments to suppliers can easily lose millions in this manner without even noticing the misappropriation.

EFT fraud is not a bank problem – most of the time it is an account holder problem

Management often labour under the misapprehension that EFT fraud is committed at retail bank level, by corrupt employees of the bank. However, in most cases of EFT fraud, almost invariably the banking payment system simply captures the transactions loaded onto it by finance staff entrusted with making payments to suppliers. If the payment that is loaded and released is legitimate, your vendor will be paid. Where, however, an illegitimate payment has been loaded onto the payment system, the funds will be diverted to whatever account was loaded in the vendor payment profile prior to authorisation.

This does not mean, however, the possibility of bank employee fraud should be automatically excluded.

EFT fraud has assumed near-epidemic proportions over the past year

EFT fraud has assumed near-epidemic proportions over the past year, with cases negatively impacting both small and large organisations with equal impunity. In most identified cases, the EFT fraud has been committed over many months and even years, before the fraudster became greedy or careless which resulted in the fraud being detected.

In many instances the amounts stolen are purposefully designed to stay beneath certain thresholds to make detection difficult. In a recent investigation performed for a large liquor company in the Western Cape, a financial accountant stole R4,2m over several years. Most of the 698 illicit EFT transactions conducted by the fraudster were for amounts below R4 000. She became greedy when she generated a false credit on the accounting system to facilitate an EFT payment of R1,3m to a local law firm, which the investigation revealed was the transaction and transfer fee related to the purchase of her home.

There are a number of basic steps which should be initiated, as a matter of urgency, to ensure that EFT fraud risk is mitigated.

Password abuse is prevalent amongst staff members in finance teams

Access to the vendor payment system is typically restricted to a handful of staff in the finance department. EFT payment clerks are usually authorised with delegated powers to capture payments to suppliers who are registered as vendors on the organisation's financial system. Another official, typically an accountant in the finance section, will have the power to authorise payments captured onto the system by the clerk.

Management



Powell

A useful control often built into the payment process is a secondary authorisation requirement before payments can be released. Often that final control resides with a director or financial manager. Once the release takes place, the transaction is automatically uploaded into the banking institutions system and the payment process is then initiated.

In performing forensic investigations into EFT fraud we have noted that, in the majority of cases under examination, staff in the finance

team had shared their passwords with fellow team members enabling any one of the two or three officials empowered to process transactions to transact while the colleague is out of office. This is a disturbing trend which ren-

ders the anti-fraud control, via individual passwords and segregation of duty, null and void.

It is shockingly naïve for finance officials to circumvent this critical control simply because the individuals in that section trust each other and do not want to incur the wrath of disgruntled service providers as a result of delayed payments.

The sharing of passwords should be classified as a dismissible offence

As indicated, the sharing of passwords is a critical control breakdown which allows fraudsters to commit EFT fraud. Once an individual knows the user log-on code and passwords of his or her colleague, he or she can log onto the system as another party and transact; that person can surreptitiously amend supplier bank details and substitute these with their own account details or that of their colleagues, or they can create new vendors with banking details for themselves, a friend or family member. Once the amendments are made by processing payments which, on the face of it appear legitimate, they can divert hundreds of thousands of rand to their destinations of choice.

The sharing of passwords, which allows access to the electronic payment

Management

system, should accordingly be regarded as a dismissible offence. Organisations should ensure that passwords have a regular, system-generated change. Staff must also protect their passwords when they work on their computer as fraudsters are often easily able to identify the passwords by watching their colleagues or going through desks or diaries where passwords have been recorded.

Staff must be educated about the risk created by password abuse and should confirm by way of signature that they understand the risk and that they have not shared their passwords or been negligent regarding this. In addition, compromised passwords should be changed immediately.

Changes to supplier banking information should require senior management intervention

Senior management authorisation should be made a prerequisite for the amendment of any supplier bank account information on the system, and software service providers must be consulted to ensure that a built-in early warning system for bank account changes is implemented.

Many companies believe that, when they register a new vendor, a cancelled cheque coupled to an invoice which reflects the banking and company registration information will prevent fraud. While these steps have some merit as a control, management must appreciate that, when the dishonest staff member wants to divert payments to him or herself, they register a fictitious company and open a bank account for it, in which case they are able to adhere to both requirements. Payments can then flow to this entity which in reality is just an empty shell; a letterhead and a bank account, with no business premises and no business operation.

Audit changes to bank account details at least once a quarter

As a result of the pervasive threat posed by EFT fraud, organisations should mandate internal audit teams, in conjunction with the information technology department, to audit any changes to the banking system. IT software service providers should be consulted to ensure that there is a clear

audit trail identifying users who have implemented those changes. The amendments must be verified with the service provider and bank in question. Banks are often reluctant to disclose account holder information, however, and the company should be able to insist on confirmation that the name of the account holder on their system matches the bank account number which has been adjusted.

The vendor database must be cleaned

An additional control measure that should be adopted by the organisation is a cleanup of the vendor database. All duplicated vendors should be removed from the system as these are often manipulated for fraudulent purposes. However, before removing duplicate vendors, stringent checks should be performed on them to ensure there is no link to staff members.

Perform random reviews of the EFT payment process

It is critically important for the organisation to perform frequent and random reviews on EFT payments. Often additional payments are slipped into the payment process without any paperwork or, questionable false invoices or previously paid invoices, are used to create the appearance of legitimacy.

Systems should automatically detect duplicate invoice numbers and amounts

To prevent EFT abuse it is vital to ensure that the accounting system has built-in controls to block a duplicated payment of a previously paid invoice or a payment of identical amounts. If the control is not inherently built into the system, consult your software service provider.

These controls should mitigate the risk of EFT fraud. To ensure complete peace of mind, a comprehensive EFT fraud risk review should be performed by EFT fraud experts. ♦

Powell is Director of Forensics at Edward Nathan Sonnenbergs