NBCRFLI

National Bargaining Council for the Road Freight and Logistics Industry

Your Road Freight Partner.

HOW TO PREVENT EFT FRAUD

Fraud and corruption are extremely topical in South Africa, given the many companies that have been adversely affected. Often blame is placed on the banks, and yet more often than not, internal procedures, or lack thereof, enable corrupt employees to commit this crime with amazing ease.

In particular, electronic funds transfer (EFT) fraud has become rife and is one of the greatest ongoing risks faced in South Africa today. EFT fraud is basically the illegal transfer of funds from one bank account to another. Most often it occurs when a corrupt employee is responsible for loading payment details on the banking payment system and, instead of adding the correct information, they add alternative banking details, resulting in the money being paid into the incorrect account.

With electronic banking, the name of the account or person is not relevant, as the banking system focuses on the actual bank account number and branch details. This means that a corrupt employee could keep the correct supplier’s name, ensuring that no one picks up on a different name, but changes the bank account details and pays themselves instead.

So what can be done to prevent EFT fraud?

Audit changes to bank account details

Companies should mandate internal audits, in conjunction with their IT department, at least once a quarter in order to audit any changes made 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 then be verified with the service provider and bank in question. Banks are often reluctant to disclose account holder information; however, wherever bank account details have been altered, companies should insist on confirmation that the name of the account holder on their system matches the bank account number.

Clean up the vendor database

An additional control measure is a clean-up of the vendor database. All duplicated vendors should be removed from the system, as duplicates are often manipulated for fraudulent purposes. However, before removing duplicate vendors, stringent checks should be performed on them to ensure that there is no link to staff members and that no previous fraud has taken place.

Perform random reviews of the payment process

It is critically important for companies to perform frequent and random reviews of 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.

Ensure duplicate information is automatically detected

Make sure that your 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. To ensure complete peace of mind, a comprehensive EFT fraud risk review should be performed by EFT fraud experts.

Be aware of password abuse

Password abuse is alarmingly common among finance officials in finance teams.

Access to payment systems is typically restricted to staff in the finance department. EFT payment clerks are usually authorised to capture payments to suppliers who are registered as vendors on the company’s system. Another official, typically an accountant in the finance section, will then have the power to authorise the captured payments done by the clerk. Once the release takes place, the transaction is automatically uploaded into the banking institution system and the payment process is then initiated. A useful safety control to be considered here is to have a secondary authorisation required before any payment can be released.

According to the Council's forensic investigations, it has been found in the majority of cases under examination that staff in the finance team shared their passwords with fellow team members. This means that any one of the two or three employees empowered to process transactions is able to transact while the other colleague is out of office. This is a disturbing trend which renders the antifraud control null and void as there is no control over how many people are able to access funds.

Classify the sharing of passwords a dismissible offence

It is highly naive for finance officials to allow password sharing simply because the individuals in that section trust each other or do not want to incur the wrath of disgruntled service providers as a result of delayed payments. The sharing of passwords is a critical control breakdown and encourages fraudsters to commit EFT fraud.

Once an individual knows the user logon code and passwords of his or her colleague, they are able to log on to the system as a party other than themselves and transact. When they are logged on, they can surreptitiously amend supplier bank details and substitute these with their own account details or those of their colleagues. Once the amendments are made, they are able to process payments which appear legitimate and divert any number of Rands to destinations of their choice.

The unauthorised sharing of passwords should therefore be a dismissible offence. Employees should be educated on the seriousness of password abuse and should confirm, by way of signature, that they understand the risks involved. In addition, passwords that have been compromised should immediately be changed.

The authorisation by a head of department or chief financial officer should be a prerequisite for the amendment of any supplier bank account information on the system, and software service providers should be consulted to ensure that a built-in, early-warning system for bank account changes is implemented.