EFT FRAUD PREVENTION TOOLKIT

FOR ATTORNEYS

MADE AVAILABLE BY THE LAW SOCIETY OF SOUTH AFRICA

Drafted on behalf of the attorneys' profession by Edward Nathan Sonnenbergs

EFT fraud risk check list

an overview of the fraud threat to the legal fraternity, including the particular threat posed by electronic funds transfer fraud

Fraud is often described as a cancer in our society which permeates every sphere of business life; no industry or profession is immune to its pervasive effects and the legal fraternity is certainly no exception in this regard.

law firms are particularly susceptible to fraud

In fact, it is argued that law firms are, in many respects, even more susceptible to fraud and theft than other business entities as attorneys are often deficient in respect of accounting and financial skills, which, in turn, tends to induce them to delegate control over procurement and accounts payable functions to secretarial and accounting personnel. Additionally, most organisations in the corporate sector are acutely aware of the risk posed by fraud and theft to their business and consequently have strong anti-fraud measures and controls in place, with well demarcated segregation of duties and independent reconciliations and regular oversight and review. Whereas attorneys, in general, with some notable exceptions, have limited appreciation of basic accounting concepts and consequently place strong reliance on trusted individuals, with poor or non-existent segregation of duty and a complete absence of independent review over accounts and reconciliations. This makes it easy for dishonest personnel in law firms to not only misappropriate funds with alacrity and ease, but to also cover their tracks and thereby avoid detection.

Quantification of the extent of fraud and theft in the legal profession is difficult for a number of reasons. There are numerous cases where trust accounts have been plundered by corrupt staff as well as by dishonest practitioners some of which have never been detected, nor, often in the few cases that are discovered, reported to the authorities. The non-reporting of fraud and theft at law firms is often ascribed to the negative stigma and reputational harm attached to any law firm admitting that its internal systems and controls have been breached. Firms are, understandably, reluctant to disclose the fact that its own funds, as well as those of clients, are potentially at risk.

It is, however, very important to point out that the failure to report certain criminal offences can amount to a criminal offence on the part of partners, executives or managers at firms which have experienced fraud or theft. In terms of Section 34 of the Prevention and Combating of Corrupt Activities Act (Act 12 of 2004), any person in a position of authority, who knows, ought reasonably to have known, or suspected, that an act of fraud, theft, extortion, forgery & uttering as well as acts of corruption, involving an amount

exceeding R100, 000.00, must report such knowledge or suspicion to the SA Police Services. Despite the criminalisation of the non-reporting, what often happens when fraud is detected in practise is that accounting or secretarial personnel implicated in irregularity are often simply dismissed or asked to leave, with no referral of the matter to the authorities for prosecution. This can have terrible consequences for the profession as those dishonest employees often simply move to other firms where, within a very short period of time, they find themselves tempted to avail themselves of fraud opportunities once more, particularly if the new environment does not have robust anti-fraud measures in place. Perpetrators of fraud or theft, who have enjoyed the proceeds of crime without appropriate sanction, or those who have simply evaded the criminal justice process, will find it immensely difficult to overcome the temptation to steal when the opportunity next presents itself.

It is accordingly critically important for law firms to properly check criminal histories of employment candidates (with the consent of the applicant), prior to appointment to positions of trust and further, to do proper reference checks to ensure they are not inheriting dishonest staff that have left their previous employer under suspicious circumstances; in which case their record may be clear despite them having been implicated in acts of dishonesty. It is equally important for firms to have comfort that accounting and/or secretarial staff members are not experiencing extreme financial pressure while they enjoy access to firm or client funds. Regular proactive credit vetting, which is permissible to address the fraud risk in terms of the regulations to the National Credit Act of 2005, has become a business imperative.

A compilation of possible red flags to look out for and best practices to prevent EFT fraud are listed below. The checklist is critical to small and medium sized legal firms where there is limited scope for proper segregation of duties and many accounting responsibilities are vetted in the hands of a small number of individuals, with limited overview. Firms who deal with estates are further susceptible to fraud and dishonesty as often these practises are run as separate entities with their own trust accounts and, again, limited overview. It is critically important to ensure some form of independent and random overview, coupled with spot checks, occurs. Given the nature of estates, fraud can occur with relative ease and more vigilant attention needs to be paid to the accounts in these matters.

the psychological process behind fraud

Before fraud takes place there is usually a convergence of a number of factors. These factors are described as pressure and opportunity, followed by a process of rationalisation. Consider the following checklist when evaluating staff:

phase one: **pressure to commit fraud**

fraud risk indicators or red flags	yes (give details)	no
Does the firm screen all new employees for criminal history or bad credit record?		
▪ Ensure that employment application forms ask questions relating to criminal record and bad debt.		
▪ The form should warn applicants that the firm will verify information and the submission of false information may lead to dismissal.		
Do staff members enjoy lifestyles that are not commensurate with their income?		
▪ expensive cars,		
▪ luxurious houses or holiday homes,		
▪ private schooling for children,		
▪ frequent or extravagant holidays.		
Are staff members financially stressed? ▪ Has the firm noted creditor's demand letters being delivered?		
▪ Are there regular telephone calls or messages to particular staff members from debt collectors?		
▪ Is there a high volume of emolument attachment orders on payroll? (Garnishee orders)		

fraud risk indicators or red flags	yes (give details)	no
Are there employees whose personal circumstances may place them under pressure?		
▪ Are there employees who have recently divorced?		
▪ Are there employees who are involved in extra-marital affairs?		
Are there staff members with dependency problems?		
▪ Gambling,		
▪ Alcohol, or		
▪ Drug problems.		

phase two: **opportunity to commit fraud**

fraud risk indicators or red flags	yes (give details)	no
internal controls		
Do many people have transactional authority?		
Are these authorities consistent with job descriptions and/or requirements?		
Is there appropriate segregation of duties as well as independent oversight regarding payments and reconciliations?		
Are accounting staff properly trained to service the internal accounting needs of the firm e.g. Do they attend law society training on basic book-keeping for attorneys?		
Are payments streamlined?		
Can the staff member processing EFT payments access supplier banking details? Are they able to amend banking details without partner /management authorisation?		
Is the person who creates the invoices the same person who attends to the credit notes?		

fraud risk indicators or red flags	yes (give details)	no
Do all staff members declare their interests? (external business links and/or directorships)		
Are the activities all staff reviewed regardless of seniority?		

phase three: **rationalisations for committing fraud**

fraud risk indicators or red flags	yes (give details)	no
Are there staff members who are disgruntled with the firm?		
▪ staff members who verbalise that they are worth more than the firm is paying them,		
▪ staff overlooked for promotion,		
▪ staff who have not had an annual salary increase,		
▪ staff under performance management.		
Are regular performance assessments held where these issues are addressed?		

fraud syndicates have discovered that law firms, and their clients, are soft targets for fraud

Many law firms have found themselves targeted by fraud syndicates who intercept their invoices in the post and then forward an adapted invoice with amended banking details to unsuspecting clients, who then make payment to an account which has been created for fraudulent purposes.† The fraudulent invoice is usually sent per facsimile to the client and followed up with phone calls demanding immediate payment.† Because the syndicate has intercepted the original invoice, the details of the amount owed and the work performed is completely accurate, which makes the fraudulent invoice appear legitimate, thereby inducing staff to accept its authenticity and simply to effect payment to the account designated on the invoice. By the time the law firmís own credit controllers query the non payment of the fees owed by the client at which point the fraud is discovered, the funds in the fraudulent bank account have been depleted and the syndicate has moved on.

Consider the following checklist when evaluating your internal controls:

the external EFT syndicate threat	check	comments
Are clients notified that the firm has not amended its banking details?		
Are clients supplied with key contacts with whom to liaise to verify account details and check payment requests?		
Are clients notified that genuine firm invoices are only distributed in a certain format; clients will not ordinarily be sent facsimiles or photocopies?		
Are authorised signatories attached to relevant documents?		
For large transactions, are two authorised signatories required from directors/partners in different departments?		
Are spot checks conducted on business payments?		
Are random spot checks done where original invoices are viewed in order to ensure expenses are allocated correctly?		
Are electronic signatures verified with sample signatory lists (electronic signature scanners)		
Are clientís banking details confirmed with cancelled cheques or a stamped letter from the bank?		
Are matters closely controlled by practitioners?		
Are there alerts in place indicating when a matter is linked to an entity in which a staff member has an interest?		
Are general powers of attorney not permitted; only powers of attorney for specific transactions?		

EFT fraud is the latest threat to law firms in SA

There is a particular type of fraud causing havoc in businesses across the country, and negatively impacting many law firms. This new threat is known as electronic funds transfer (EFT) fraud. EFT fraud is essentially the illicit electronic diversion of funds from the firm's bank account to third parties to whom the funds are not due, usually involving manipulation of the accounting software programmes that are 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 with both the public and private sectors being 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 enables corrupt staff to create the illusion that they are paying legitimate suppliers, whereas, they are, in fact, transferring funds to themselves or friends and family. In larger firms the risk is that small amounts can easily be concealed amongst the myriad of daily transactions. In smaller firms the risk is that the accounting and procurement functions often resides in a single or handful of employees which makes the manipulation easier. Fictitious vendors can be created for services that are to be expected and as long as the amount requisitioned for payment is consistent with the expected charge, partners or directors will ordinarily authorise the payment.

consider the following checklist when evaluating your internal controls:

	check	comments
Are payment requisitions supported by vouchers and invoices?		
Is there a confirmation procedure in place for goods or services that have been rendered?		
Does someone other than the party requesting payment, independently confirm proof of delivery or rendition of services?		
Is the sharing of passwords in the firm a dismissible offence? (particularly applicable to passwords to the firms accounting system)		
Is there a regular system generated password change?		

	check	comments
Do staff safe-guard their passwords? (Not written down in diaries or readily accessible to third parties).		
Are staff members educated on the risk of password abuse?		
Do staff members agree in writing that they will not compromise their passwords?		
Are compromised passwords immediately changed?		

changes to supplier banking information should require senior partner authorisation

	check	comments
Is senior management/partner authorisation a prerequisite for the amendment of any supplier bank account information on the system?		
Are software service providers consulted to ensure that a built-in early warning system for bank account changes is implemented?		
Is there sufficient confirmation information when registering a new vendor? (Note: cancelled cheque coupled to an invoice which reflects the banking and company registration information is not sufficient to prevent fraud)		

audit changes to bank account details at least once a quarter

	check	comments
Do internal audit/finance management, in conjunction with the information technology department, audit changes to the banking system periodically?		

	check	comments
Is there a clear audit trail identifying users who have implemented changes to bank account details?		
▪ If not, consult your IT service provider to create the requisite trail.		
Are amendments to banking details verified with the service provider and bank in question?		
▪ The firm 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

	check	comments
Are vendors screened before they are registered as suppliers to the firm?		
▪ The firm should perform checks on suppliers to ensure that they are genuine and are not linked to staff members and further that they have competence in their professed area of expertise.		
Are there duplicate vendors on your supplier database?		
▪ Duplicate vendors must be removed from the system as the duplicates are often manipulated for fraudulent purposes.		
▪ Stringent checks on duplicate data bases before removing them to ensure that there is no link to staff members		

	check	comments
Does your system automatically detect duplicate invoice numbers and amounts?		
▪ Consult IT service provider to automate this check, or		
▪ Perform manual checks.		
Are frequent and random reviews on EFT payments conducted?		
▪ Be aware that often additional payments are slipped into the payment process without any paperwork. Questionable false invoices as well as previously paid invoices are used to make the fraudulent invoice look legitimate.		
Has an independent review of the firm's anti-fraud controls ever been performed		
▪ If not, consult fraud experts for advice on additional proactive measures.		