Endurance | ENDURANCE INSURANCE

Discussion Paper

Professional Service Firms: Protecting Your Firm and Your Clients from Fraud

Discussion Paper
Professional Service Firms: Protecting Your Firm and Your Clients from Fraud

Introduction

Professional service firms have a duty to exercise reasonable care in protecting clients' funds and other assets that are under their care, custody and control whether the firm holds the funds for a short time, often in their trust accounts, or for longer periods. With client approval, firms may also assume responsibility for asset management and distribution of funds directly from their clients' accounts. Accounting firms can hold considerable funds in their wealth management divisions, and law firms may manage large accounts for their trust and estate clients, as well as for real estate and corporate transactions.

With alarming frequency, professional service firms are being targeted for theft of funds, often by third parties, and sometimes by or with the assistance of their own partners and staff. These frauds are in addition to the risk of data breach where professional firms' networks are penetrated by hackers seeking to profit from confidential or insider information for publicly traded companies, or extorting firms by locking out a firm from their own data until ransom is paid.

Criminals take advantage of firms' poor internal controls and are using increasingly sophisticated methods to defraud them. Firms should undertake periodic reviews of their internal operations to identify potential exposure to criminal activity and develop and implement steps to mitigate losses. Opportunities to protect themselves and their clients include tightening controls to avoid fraud in the first place as well as ensuring that any losses are minimized through risk transfer and other forms of recovery.

Examples of Losses Due to Fraud

a. A hacker sent instructions from a client's email account to their professional service firm to wire money from the client's checking and savings account, which the firm managed, to a third party. The "client" responded to and approved email confirmations from the firm. Only when the combined account was nearly exhausted did the firm contact the client by phone to discuss the transfers and discover that the client was unaware of the requests.

b. A law firm involved in a real estate closing received client funds in the firm's trust account and then received instructions to wire the funds to a designated bank. However, an illicit third party in the transaction changed the routing code, resulting in the funds going to an unapproved bank offshore where the criminal could access the money. The firm could be further exposed for loss of profit on the transaction if the closing did not go through at the original price.

c. A firm received instructions to transfer funds on behalf of a "client" to a third party. The firm did not pick up on red flags, such as the email address was not the same one the client had used previously, and payments were being sent to countries in which the client had not previously done business. When the firm finally checked with the client they realized that the request was fraudulent.

d. The chief financial officer (CFO) of a professional service firm was deceived by a third party who was posing as the firm's banker. The criminal had created a website that looked exactly like the website of the firm's bank. The CFO entered the firm's bank account number and password into the fake website and the firm's account was promptly depleted.

e. When the senior partner of a professional service firm was out of the office on business and unavailable, an email message purporting to be from him to the firm's CFO requested an immediate funds transfer to a third party. The email message came from a different address than the one usually used by the senior partner. The third party, who was perpetrating the fraud, was called at the phone number provided in the email instruction to verify the transaction. It was later learned that the server that sent the email request was located in Russia.

f. A "client" that retained a law firm to pay debts to companies the client did business with gave the firm what appeared to be a cashier's check that was to be used by the firm to immediately wire funds to various parties. The check bounced, but it was too late for the firm to stop the wire transfers from the firm's escrow account.

g. A new "client" deposited funds with a law firm, which the firm later determined had been secured illegally. In the interim, the funds were used to buy high value personal assets, opening the firm to potentially being sued for aiding and abetting such illegal transfers.

h. A partner of a firm opened an unauthorized bank account in the name of the firm with a bank the firm had not done business with previously. The partner, who was the sole signatory on the account, deposited checks made out to the firm and then instructed that the funds be transferred to his own personal account.

i. A partner of a firm set up a bank account for a vendor that was owned by the partner and not disclosed to the firm. When expenses of the vendor were paid by the client, the money went to the fraudulent partner.

j. A settlement of a law suit was to be resolved by payment of a check. However, at the last minute an email message purportedly from counsel of the party receiving the payment instructed the funds to be wired to an offshore account. The account turned out not to be legitimate.

k. A firm permitted a partner to act as corporate secretary for a client, including the authority to write checks on the client's behalf. The partner issued checks fraudulently for his personal benefit.

What Steps Can Be Taken To Avoid Losses

There are various steps that can be taken to help prevent losses due to fraudulent activity.

a. Create written guidelines and protocols that must be followed by authorized employees before any money transfers take place.

    - Firms should undertake a comprehensive background check, reference check and interviews of such employees in order to determine whether there are any red flags, such as living beyond their means, any side business, or any financial problems.

    - Procedures should designate the names of employees who are authorized to make and approve transfers and for what dollar amounts. Two approvals should be required for large transfers. There should be segregation of duties between those who make transfers and those authorized to approve them.

- Firms should maintain a list of payees pre-approved by their accounting department. The list should cover both clients and vendors and include the federal tax id number for companies and the social security number for individuals for confirmation of identity.
- Client funds that are designated to pay creditors should not to be distributed until the bank specifically confirms that the client's check is valid and has cleared.
- Incoming payments should be sent directly to a lockbox or the accounting department and not to individual employees.
- Firms should set up procedures with their banks to ensure that fund transfers do not take place unless the firm's guidelines have been complied with and strictly followed.
- Unscheduled audits should be conducted periodically of firms' financial records.

b. Agree in advance with the client how fund transfer instructions will be handled in order to avoid fraudulent requests and ensure that employees will know that the instructions received are from the actual client.

- A code word inserted in the authorization email message is one possibility, as well as accepting instructions only from a designated email account.
- Employees can be instructed that they must also check by phone to ensure the email messages requesting funds come from the designated email account of the client.
- Firms should also consider buying software that helps identify if email messages come from an unauthorized source.
- Employees can also be instructed to confirm with the client in writing other than email. For example, if any new payees are requested to receive payments, a signed authorization form must be provided by the client.
- Employees should ensure that the debtor has been properly contacted to confirm that the debt is owed before making payments. In addition, verify the contact information provided by a foreign client.

c. Implement employee training which, at a minimum, covers payment procedures, fraud awareness, ethics and money laundering risks. Firms should consider implementing a fraud reporting hotline.

d. Investigate new clients and conduct periodic reviews of existing clients.

- Has the client given references, including banks and other professional advisors, and have those references been checked?
- Has a senior member of the firm personally met with the client and have they reviewed original identification, including bank statements?
- Has a criminal background check of the client been performed and records of customer due diligence been maintained?
- Has a retainer been secured and cleared?

- Has the firm agreed to use only client accounts to hold client funds?
- Has the firm investigated large cash transactions requested by a new client as this is a money laundering red flag?
- Has the firm checked to ensure the potential client is not on the Office of Foreign Assets Control (OFAC) list?
- Has the firm identified the true beneficial owner of the transaction and the source of funds?

e. Pay particular attention to new clients that are based abroad. Authorized employees should be able to recognize countries which are high risks for money laundering. With respect to law firms with offices in the UK, the Solicitors Regulatory Authority requires that firms have measures in place to reduce exposure to money laundering, with enforcement powers within the regulator's office to ensure compliance. A lawyer with responsibility for compliance who failed to report money laundering activities could face jail time. Note that money laundered through law firms may not always involve legal transactions, and instead can involve passing money through the client account to make it look legitimate, but where no legal services have been provided.

f. Prohibit partners from holding positions in companies controlled by clients where they have responsibility over distribution or management of client funds.

g. Trust your instincts. If the transactions underlying the transfer don't make commercial sense, decline to provide services or refer the matter to another senior officer or partner for a second opinion.

h. Discuss recommendations to prevent or mitigate losses with your inside and outside auditors, banks, crime insurers and insurance brokers.

i. Buy crime insurance – see discussion below.

What Insurance Is Available Or Other Sources Of Recovery?

Crime Insurance

Crime insurance is a first party policy that indemnifies losses that the insured sustains for specified risks discovered during the policy period. There is no requirement for a claim to be asserted by a third party as there is no coverage for the defense or payment of claims by third parties. The policy typically covers the company or partnership for losses sustained due to fraud committed by its employees stealing firm assets. The definition of insured should include the partnership, partners and non-partner employees. The policy limits can be extended to cover theft of client assets and loss to clients caused by the firm's employees while on the premises of the client.

The policy limits can also be extended to cover what is known as social engineering (cyber crime) where a loss of client funds results from an employee of the firm making a payment or diverting funds based on fraudulent information. While limits of $100 million or more for crime coverage are available for most firms at relatively low cost and at low retentions, social engineering coverage for similar limits is normally available only if the insured can demonstrate that there are sufficient internal controls to mitigate loss.

Professional Liability Insurance

A professional liability policy typically covers a claim against the firm arising from conduct while delivering professional business services. The policy covers damages the firm is legally obligated to pay, including costs incurred in defending such claims. Normally for claims to be payable, the firm must show that a duty was owed to the claimant and that there was a breach of duty. It must also show that damages have been sustained and that there is causation between the breach and these damages. Some policies contain limited coverage grants and absent affirmative endorsements may not cover professional services delivered in the capacity of escrow agents or investment advisors. In addition to the above, a claim can be brought by a client for contributory negligence if the firm allowed their system to be hacked, and particularly if they knew of such attempts.

We have also often seen cases where a firm's partner has defrauded a client. In this case, the policy typically contains a fraud exclusion for the guilty partner, and the policy does not cover loss of firm assets. There may be coverage under both the crime policy and the professional liability policy for client losses. Typically the crime policy pays first and then, to the extent there is malpractice, the professional liability policy is excess. One advantage to the crime policy paying first is that this type of policy normally has a lower retention than the professional liability policy. Another is that there is no need to establish legal liability to a third party to secure coverage. Finally, as the professional liability policy normally has much higher premium than the crime policy, avoiding claims or reducing payments under the professional liability policy will mitigate future rate increases on policy renewals.

Recoveries from Third Parties: Transfer of Risk and Avoidance

Where funds have been improperly transferred from the firm's bank to a third party, it may be worth exploring whether the bank is willing to contribute to a loss payment, particularly if it can be established that the bank was negligent. One example would be if the bank wired funds not in accordance with the documented transfer procedures provided by the firm. If contacted promptly, the bank may also be able to recover funds or assist in contacting appropriate authorities to aid in such recovery.

Some professional service firms are now transferring the risk of funds management directly to the bank. The bank is often better equipped to handle these matters and can provide services directly to the client in a more cost effective manner. A number of firms are advising clients that they are no longer willing to act as escrow agents as the fees generated by the professional service firm for such services are often very small, particularly compared to the risks undertaken.

Bankers/Investment Advisors Errors and Omissions Insurance

Another alternative that firms should consider in order to potentially reduce exposure to the company or partnership is to transfer any investment advisory and money management services, including acting as a trustee, to a separate firm owned by the main firm. This separate firm would use their own engagement letter, and as they are not providing legal or accounting services, they may be able to limit their liability in such areas as statute of limitations, capping liability to a percentage of fees, eliminating punitive damages, avoiding jury trials, etc. However, in order to preserve the separation of legal liability, individuals cannot work for both entities to provide services to the same client. Insurance coverage is often available for lower retentions and lower rates than coverage under a standard professional liability policy.

Where the firm permits partners or other employees to act as a trustee for clients, they should require the trust to buy errors and omissions insurance so that funds are available if the client sues the firm's partner or employee arising from their trustee capacity. This is similar to situations where a firm permits a partner or employee to act as a corporate director, typically with the condition that separate directors and officers liability insurance is purchased.

Conclusion

With criminals becoming more brazen and sophisticated and millions of dollars of both firm and clients' assets potentially at stake, professional service firms need to be more proactive with respect to fraud. Steps should be taken to tighten controls in order to prevent loss and also to prepare for the worst case scenario by putting insurance and other risk transfer mechanisms in place.

It is worth noting that one risk that is not insurable is damage to a firm's reputation. Clients want to be confident that their advisors are ethical, have strong risk management procedures and can be trusted to manage significant funds. Failure to provide such assurance can result in loss of business to firms who have flawless reputations.

Firms with appropriate fraud prevention mechanisms in place will not only save time and effort, they are less likely to wrestle with the difficult question: "What could have been done to prevent this?"

CONTACTS

Stuart Pattison
Senior Vice President,
Professional Firms Leader, Endurance Pro
T +1.917.281.0744
E spattison@enhinsurance.com

John Muller
Vice President,
Professional Firms, Endurance Pro
T +1.917.421.4961
E jmuller@enhinsurance.com

Dennis O'Connell
Assistant Vice President, Endurance Pro
T +1.212.209.6524
E doconnell@enhinsurance.com

Brittany Lannan
Underwriter, Endurance Pro
T +1.212.471.5510
E blannan@enhinsurance.com

Matthew Foristel
Underwriter, Endurance Pro
T +1.917.281.0758
E mforistel@enhinsurance.com