Daily Journal – October 23, 2023

Part 2 – Internal and external threats

The most common ways your Client Trust Accounts may be compromised from both internal and external sources, and how to help protect yourself and your clients from these risks.

By Jennifer Stalvey, Principal Program Analyst, Division of Regulation at the State Bar of California

Jennifer Stalvey

Principal Program Analyst, Division of Regulation, State Bar of California

This is Part 2 of a three-part series about Client Trust Accounts: "Protecting yourself and your clients." In this article, we will discuss threats to your client trust accounts – both internal and external to your practice. The first article of this series addresses the basics, and the third will look at money laundering and other illegal activity.

You may feel confident you are managing your CTAs in accordance with your professional obligations, including proper recordkeeping, performing monthly three-way reconciliations, notifying your clients within 14 days of funds received on their behalf, and other requirements under rule 1.15 of the California Rules of Professional Conduct. However, are your trust accounts still at risk of compromise? Absolutely. Here are the most common ways your CTAs may be compromised from both internal and external sources, and how to help protect yourself and your clients from these risks.

This article provides insight into commonly known threats to help you consider your firm's current practices and offer suggestions and practical tools to help minimize harm to yourself and your clients.

Internal threats

Internal threats are those that originate from within your practice. This includes employees, advisors, vendors, and staff.

Inadequate training and internal controls

Internal threats may arise from poor training, inadequate or nonexistent procedures and safeguards, and ineffective communications from management and those generally tasked with

firm operations. For example, a new accounting clerk may be professionally trained to manage the firm's operating account but not the specific rules that apply to CTAs and, therefore, may believe it is acceptable to pay firm expenses from the firm's Interest on Lawyers' Trust Accounts (IOLTAs). Inadequate or nonexistent training or procedures greatly increase the likelihood of improperly maintaining trust account records, which may lead to the firm's mismanagement of client funds in violation of rule 1.15 and place the attorney at risk of a State Bar investigation and potential discipline.

Internal fraud

Another internal – and more serious threat – may originate from intentional acts of staff. No one wants to believe their most faithful, trusted, long-term employee would take advantage of their access to information and your trust accounts, but trusted employees can be the most common perpetrators and facilitators of internal fraud.

Internal fraud is more likely to be successful when three elements exist: motivation, opportunity, and rationalization. Trusted employees generally have the greatest opportunity to commit fraud, as they may know passwords or are added signatories to trust accounts. Employees motivated by jealousy or financial hardship may rationalize their behavior by believing they are worth more than they are paid, that they will return the stolen funds in the future, or that no one will find out or be harmed by them taking some of the clients' money. Although curbing an employee's motivation and rationalization is challenging, there are tangible and effective ways you can minimize their opportunity.

Aside from a direct withdrawal from bank accounts, employees can also misappropriate funds by:

1. Cashing clients' checks.
2. Setting up counterfeit clients or third parties and directing payments to their own accounts.
3. Providing information to others that allows third-party access to your accounts.

Preventative controls for internal threats

1. Implement office procedures related to the handling of funds and bank accounts, including CTAs, and regularly train and supervise staff to ensure the procedures are followed.
2. Notify clients of funds received as soon as possible, but absent good cause no later than 14 days as required by rule 1.15(d)(1).
3. Task someone other than the person(s) added as signatories to your CTAs to perform the monthly CTA reconciliations. The person who can move money in and out of CTAs should not be the same person who is confirming the accuracy of the accounting, if possible.

4. Do not use shareable electronic signatures, rubber stamp signatures, or pre-sign blank checks. It is strongly encouraged that you or another person licensed to practice law are the only ones who can execute checks issued from the CTAs.
5. If you are considering having a non-attorney as a signatory on a client trust account, be mindful that you are asking that person to take on significant fiduciary responsibilities, and that you as the attorney are always responsible for the safekeeping of your clients' funds. Implement full criminal background checks and other protective measures for any personnel involved with client trust accounting.
6. Account for all cash deposits by requiring that both you and the client sign a receipt.
7. Require two signatures on checks over a certain amount.
8. Proactively send client ledger or account balance information to your clients monthly. Not only will your clients appreciate your proactive communications about their running balance, but clients will provide feedback about any expenses or unusual items in the trust account activity related to their funds.
9. PDFs of monthly bank statements or other financial bookkeeping forms can be easily altered. Independently download the monthly bank statement through online bank access of your CTA monthly statements to make sure ending balances match the monthly reconciliation form.
10. Make sure you or another employee are trained to perform the bookkeeping function for your trust accounts to cover an employee tasked with the day-to-day bookkeeping during vacations or other time off. It is a common pattern for someone who is embezzling funds to not take time off from work to prevent someone from discovering their scheme.

External threats

The unique role of the attorney and their practice makes them susceptible to fraud, theft, and deceptive schemes – including money laundering – from external parties.

Check scams

An external party intending to defraud may retain you or your firm on a false legal matter to issue a counterfeit check or other instrument through your trust account, in order to receive real money. These scams can be sophisticated, providing real-looking settlement agreements, IDs, and other counterfeit documents that convince you they need your services to process a settlement agreement, debt collection, real estate transaction, divorce settlement, or other legal matter.

Examples of Check Scams:

- A new "client" contacts you, a litigator, to assist in the collection of funds from a settlement agreement. The "debtor" appears legitimate and is willing to settle the debt

quickly. You deposit the settlement funds into your IOLTA. The "client" then tells you they have an emergency and need their portion of the settlement funds immediately. You wire funds to the "client," then discover that the settlement funds were a scam. Your IOLTA is now overdrawn, and one or more of your other clients' funds has been misappropriated. The bank notifies the State Bar.

- A new "client" contacts you, a real estate attorney, to help purchase a property they saw online. They send a check as a deposit for the property, which you deposit into your IOLTA. They then tell you they are no longer interested and want to cancel the deal. You wire funds to them, minus your processing fee, and learn from your bank three days later that the "client's" original check was fraudulent. Your client trust account is not overdrawn; however, one or more of your other clients' funds has been misappropriated.

Preventative controls for check scams:

1. Confirm the identity of any new client. Obtain personal identifiable information and cross-check the information online
    a. If the client is a business, identify the business online and with the Secretary of State.
    b. Verify address information on Google Maps.
    c. Reverse search the provided phone number.
2. Do not accept "the client does not want to be known" as a response to your inquiries about the identity of the client. As the client's attorney, it is important to know who you are assisting, and the true nature of their request for services to ensure you are not participating in illicit activity. See rules 1.2.1, 8.4. See also ABA Model Rule 1.16(a).
3. If your client is seeking to recover funds from a business, find contact information for the business online and independently confirm the debt or settlement payment directly.
4. Ensure your trust account does not allow for "provisional credit" to be issued by the bank. Provisional credit is an optional feature that allows the bank to disburse funds before a deposited check or other instrument has cleared the bank. Suppose funds are returned to a "client" by provisional credit before clearing the bank. If the bank informs the attorney that the check was counterfeit, the attorney is responsible for replenishing the trust account funds.
5. Speak with your bank to understand the length of time required for deposited funds to clear the bank in which your CTA is held. The length of time can differ based on the type of deposit. Hold the funds in your account for as long as your financial institution advises you it takes for funds to clear before you disburse any funds.
6. Make sure every employee or signatory of your trust account understands the time frames, and always politely decline the "client's" urgent requests to receive the funds sooner.

Forged trust account checks

Suppose an external party intending to defraud you obtains your trust account bank information. They prepare fake checks and forge your signature to cash the checks. While you will likely be able to recover the funds, the consequence of this external threat is overdrawing your IOLTA and misappropriating one or more of your clients' funds, at least temporarily. You may also have to close the IOLTA altogether and open a new one, which will take your valuable time. The State Bar will also be notified of the overdrafts to your account.

Preventative controls for forged trust account checks

1. Discuss the matter with your bank and enroll in a bank's positive pay program so only law firm approved checks are honored.
2. Review your trust accounts regularly to look for unapproved or unidentified transactions.

Unauthorized changes to wire instructions

Real estate is the most common area of law targeted by unauthorized changes to wire instructions, but other practice areas may be affected. Suppose an external party gains access to the email account of a party to a real estate transaction and learns the details of the transaction. They then email you – the attorney for the transaction – with wire instructions for the seller's funds. You wire the money to the "seller's" account. The bank will likely deny liability because it followed your instructions as the attorney.

Preventative controls for unauthorized changes to wire instructions

1. Set up wire instructions with your clients ahead of time and agree to change the instructions only by calling the law firm or client at an agreed-upon telephone number, regardless of any phone number in an email requesting a change in wire instructions.
2. Double-check the email address sent on behalf of the seller. The scammer may create a similar-looking address by adding an extra letter or number or changing character.
3. Independently verify any instructions by calling to verify written instructions.

What to do if you fall victim to a scam

Although prevention measures will decrease your vulnerability to internal and external threats, even the most sophisticated firms and companies may fall victim to scams. What do you do if this happens to you or your firm?

The nature of the scam will determine the measures you will want to take to address the matter and prevent further harm. Below are some potential steps you may take:

1. Contact your bank. If embezzlement or fraud caused unauthorized activity in your trust account (or any other type of bank account), you should contact your bank immediately.

The bank will likely suggest closing the trust account and opening a new one – especially if the perpetrator has your bank account information.

2. Contact law enforcement. You should report the unlawful act to law enforcement. Preparing a timeline and gathering pertinent information and documents will assist their investigation.
3. Contact your client. If your client's funds have been stolen or their confidential information has been breached, you are required to inform your client. See rule 1.4. Also see Ethics Opinion 2020-203, which addresses data breaches and states, "lawyers have an obligation to conduct a reasonable inquiry to determine the extent and consequences of the breach and to notify any client whose interests have a reasonable possibility of being negatively impacted by the breach."
4. Communicate with the State Bar. If the scam resulted in fraudulent activity in your trust account, your trust account may have been overdrawn. Your bank is required to notify the State Bar of all overdraft activity, regardless of the reason for the overdraft. Timely communications with the State Bar will help investigators resolve the matter more quickly. If you had to close your trust account and open a new one, rule 2.2 requires that you report any such changes to your trust account within 30 days, which you can do in the Client Trust Account Protection Program (CTAPP) section of your My State Bar Profile, or your firm administrator can do through Agency Billing.

Up next

In the third and final article of this three-part series, we will focus on the most serious and potentially career-ending types of external risk: money laundering and other criminal activity.