Best Practices for Employers and Counsel

How to Respond When Clients Suspect Financial Fraud

When fraud hits the workplace, knowing how to respond the right way can help curb losses and increase the chances of recovery.

STEP 1: ASSEMBLE A TEAM

This is no time for a do-it-yourself approach. Bring in professionals who are experts in forensic techniques and whose skills will complement each other in an investigation, including:

Financial Investigator. Financial investigators, such as certified fraud examiners, have experience collecting, analyzing, and presenting evidence. They can maximize the efficiency and effectiveness of the investigation.

TIP: Don't hire your regular outside accountants. They may not be independent of the situation being investigated.

Computer Forensics Specialist. A specialist can ensure that digital evidence is properly collected and handled and will deploy forensically sound methods to recover information.

TIP: Avoid the temptation to use your internal IT staff. Most IT teams aren't trained to recover and preserve evidence.

Legal Counsel. Lawyers well-versed in white-collar criminal law and employment law can develop and execute on an investigative plan and help avoid mistakes that may lead to additional liability.

TIP: Hiring a specialized team may not be cheap, but it can be far less costly than the expense of a botched investigation.

STEP 2: SECURE THE EVIDENCE

Move as rapidly as possible to safeguard any data that can assist investigators and serve as evidence in a prosecution or civil suit.

Computers and Other Electronic Media. Secure electronic devices such computers, thumb drives, discs, cell phones, and related software and storage programs. **Caution:** Do not examine devices on your own, and don't turn them off. Doing so can be viewed as altering evidence.

> **TIP:** Have relevant hard drives mirror imaged by a computer forensic specialist. Creating a copy allows examination without disturbing the data on the original and preserves the chain of custody.

The Employee's Workspace. Secure the employee's desk, office, and any other physical workspaces used by the employee. Again, avoid the temptation to examine workspaces on your own, as this can alter their original state and render them useless as evidence.

STEP 3: DEAL WITH THE ALLEGED PERPETRATOR

Act with restraint when dealing with an employee suspected of fraud to improve investigative results and reduce legal risks.

Don't Fire the Employee—Yet. Why should keep a fraudster on the payroll—even temporarily? Gathering information from employees is far easier while they are on the payroll. As long as they are employees, they have a duty to cooperate and can be interviewed by the fraud investigator, which can be crucial in obtaining evidence and even confessions.

> **TIP:** A fraud investigator often has more leeway than law enforcement in seeking information. They can ask an employee to submit to an interview without seeking warrants or issuing Miranda warnings, significantly simplifying evidence collection.

STEP 4: RESTRICT ACCESS

Once an employee has been notified that they are the subject of an investigation, immediate steps should be taken to limit their access to the workplace and its systems.

On the Premises. The employee should not be allowed to touch or remove anything from the office, except personal items. The employee should also be accompanied while in the office and escorted from the premises.

Information Systems. Passwords should be deactivated, and any access to company information systems (computer networks, software accounts, or email, for example) should end as soon as possible.

TIP: Don't delay in denying a suspected employee access to information systems. Disgruntled employees can wreak havoc with a company's computer networks in a matter of seconds, steal sensitive trade secrets, and attempt to cover-up evidence.

Internal Communications. In addition to the employee, information about the investigation should be restricted as well. Only those who are on a need-to-know basis—preferably senior company leaders—should be informed about the progress or details of a fraud investigation.

TIP: Restricting the flow of information to the smallest-possible group will help prevent news from spreading quickly through the company ranks and may allow investigators to catch fraudsters before they have time to destroy evidence.

STEP 5: CONTACT THE INSURER

Failing to contact an insurer about a financial fraud can lead to severe financial consequences for the enterprise.

Notification Requirements. Most insurance policies carry a 30- or 60-day notification provision from the first day a potential loss has been discovered. Failure to notify the insurer can result in a loss of coverage. Once the insurance carrier is notified, a proof of loss must be filed within a specified time frame.

TIP: Do not be afraid to ask an insurer for extensions of time to ensure proper documentation of a claim.

Forensic Strategic Solutions is a national financial investigation firm with a long track record of assisting counsel and corporations facing occupational fraud issues. If you have any questions, please contact us for a consultation.