JacksonLewis

What Employers Need to Know Today — Dealing with Criminal Misconduct by Employees

Unfortunately, no organization is immune from criminal conduct by employees, including management-level officers. Theft, embezzlement, and fraud are the most common offenses. Theft may include cash, merchandise, property or data and proprietary information.

Given that employee theft or fraud may pose a significant threat to a company's assets and reputation, it is crucial to have a strict policy that clearly states the consequences employees will face if found to have engaged in such prohibited conduct. Employees need to understand that the prohibited action will be dealt with swiftly and severely, leading to potential termination or criminal charges.

A written policy should be in place to protect employees who report misconduct and encourage them to speak up. Employees need to be assured that they will remain anonymous and that the company will protect them from retaliation.

Ensure your policy covers diverse types of theft or misconduct. The policy should be written in straightforward language everyone understands. It should be provided to and understood by employees when they first join the company.

The decisions to be made upon learning of suspected criminal conduct are:

- Whether to investigate;
- How to investigate and who should do so;
- What other preliminary steps should be taken, if any;
- Whether law enforcement should be notified;
- What actions should be taken based on investigative findings; and
- Whether additional follow-up measures are warranted.

A. Whether to investigate

Not every incident is complex or serious enough to require a formal investigation. In some circumstances, the criminal conduct is self-evident and decisions can be made without an investigation. However, it is usually best to investigate allegations of even relatively minor offenses to avoid hasty or inaccurate conclusions that could result in subsequent legal action. If the company is leaving open the option of a referral to law enforcement, having investigated and documented the results will be essential.

B. How to investigate and who should do so

Investigations should be conducted by someone who can impartially gather and assess the evidence and has no stake in the outcome. Attention to detail and good people skills are essential traits of a good investigator. Experience handling internal investigations is also important in selecting an investigator or investigative team.

Many investigations can be effectively conducted using internal resources and expertise, often a member of the HR team or legal staff. In more serious or complex situations, using outside counsel may make more sense, particularly if the outside counsel has experience in law enforcement, auditing or compliance.

If the theft was related to digital data, one of the investigators should be from an internal or external data security team. If the theft was financial and potentially significant, bringing in a forensic accounting expert is recommended.

C. What other preliminary steps should be taken, if any

Before starting an investigation, steps should be taken to protect any accusers or sources of information from retaliation or harassment.

Another important consideration is whether the suspected employee has access to company data, assets or resources that need to be secured to avoid further loss or harm while the investigation proceeds.

Some employers may place the suspected employee on paid or unpaid administrative leave while conducting the investigation. Others may choose to avoid disclosing the existence of an investigation until it is completed. Both strategies have merit, and the choice of strategies depends on the circumstances.

If your organization has insurance, your agent should be notified before an investigation begins. The investigation’s outcome may involve the termination of the dishonest employee(s) and recovery of stolen assets, which may result in potential lawsuits against the company. Obviously, employment practices liability insurance or commercial crime insurance coverage would be beneficial if the dishonest employee decided to sue for wrongful termination or harassment during the investigative process. Commercial crime insurance would assist in efforts to recover stolen assets or reimburse documented losses.

D. Whether law enforcement should be notified

This is a key decision for companies or organizations in this unfortunate situation. The decision often turns on (i) the significance of the crime, (ii) the amount of the loss, (iii) the potential disruption law enforcement involvement may cause to ongoing operations and (iv) the risk of adverse and unwanted publicity.

If the employer is inclined to refer the matter to law enforcement for possible prosecution, then conducting a thorough investigation and documenting the results is crucial. Those of us that do this work for employers or who were once on the receiving end of such referrals understand that there is a far greater likelihood that a prosecution will result if you present the case to law enforcement on a silver platter.

Companies need to understand that a referral for prosecution often results in the loss of an element of control and may disrupt its operations with evidence gathering, employee interviews and subpoenas for records and information. Although law enforcement is sensitive to the risk of unwanted media attention and will usually agree not to mention the company's name in charging documents (instead using designations such as "Company A"), the risk of media attention needs to be considered by the victim-employer. Some companies decide they cannot be viewed as having allowed an employee to engage in criminal misconduct.

E. What actions should be taken based on investigative findings

If the investigation indicates the employee is guilty of criminal conduct, the company must take prompt and appropriate disciplinary action. This action usually involves termination and may also involve a referral for criminal prosecution.

If the investigation fails to support the accusation or suspicion of unlawful conduct, transparency is called for, which begins with an adequate apology to the employee.

If no conclusion can be reached following an investigation or there is insufficient proof, a judgment needs to be made on whether the employment relationship should continue. If the employment relationship continues, closer scrutiny of the employee(s) in question would certainly be warranted going forward.

If a company can document the criminal conduct but does not wish to involve law enforcement, it may use the threat of a future criminal referral to extract restitution or a legally binding obligation of repayment from the terminated dishonest employee.

F. Whether additional follow-up measures are warranted

Employers can often turn an unpleasant situation into a long-term advantage. For example, the results of an internal investigation may reveal ways to mitigate the future risk of loss. Changing internal operations that enabled the theft, such as lax accounting, open petty cash boxes, unmonitored access to company credit cards or sloppy or incomplete recordkeeping, is recommended.

Proactive employers wishing to get serious about deterring misconduct also may want to conduct regular external audits to examine internal policies, procedures, and recordkeeping.

Rather than waiting for a problem to arise, employers should regularly revisit their internal policies and procedures to ensure they are current, known by employees, observed, and enforced at all levels of the organization.

Investigating employee theft can become a drawn-out, tiring process for employers and employees. Good planning can make the investigation go as smoothly as possible without excessive disruption to the business. The ideal scenario is to avoid the need for an investigation entirely. This is why measures to prevent such criminal conduct by employees are strongly advised.

Create a positive work environment in which employees feel appreciated. Even though a good salary does not guarantee employees will not steal from the company, employers should ensure they pay and treat their employees fairly. This is often the first step in deterring criminal conduct.

When hiring someone new, it is important to conduct thorough background checks for any history of fraudulent or dishonest behavior. It is also recommended to have all new employees read and sign any anti-theft policies.

Finally, companies and organizations should purchase adequate insurance to help protect the business. Employment practices liability insurance and commercial crime insurance are welcome security when handling a situation involving suspected theft or fraud by an employee.