Preventing Employee Theft & Fraud

One of the most serious threats to the success of a small business is employee theft. Whether it’s downloading and sharing company confidential information (an increasingly common problem today), manipulating expense reports, or stealing company property—employee theft and fraud is a serious issue for business owners. Misplaced trust, lax hiring and supervision, and a failure to implement basic financial controls can lead to an environment that is ripe for internal theft and fraud. In fact, studies show that occupational fraud currently results in the loss of six percent of an organization’s annual revenue.

Here are some tips for preventing and managing employee theft and occupational fraud:

1. Use Pre-Employment Background Checks Wisely

One of the first steps to preventing fraudulent employee behavior is to make the right hiring decision. Basic pre-employment background checks are a good business practice for any employer, especially for those employees who will be handling cash, high-value merchandise, or have access to sensitive customer or financial data.

Under the Fair Credit Reporting Act (FCRA), businesses must obtain an employee’s written consent before seeking an employee’s credit report. If you decide not to hire or promote someone based on information in the credit report, you must provide a copy of the report and let the applicant know of his or her right to challenge the report under the FCRA.

Note: To what extent a private employer may consider an applicant’s criminal history in making hiring decisions varies from state to state. Check with TPM or your local EEOC office for the laws in your area before initializing background checks.

2. Check Candidate References

Surprisingly, very few employers reach out to check candidate references. Typically, hiring managers assume that a reference will never be anything but glowing. However, it’s a good practice to check references, particularly references from former employers or supervisors of the applicant. If your candidate has a history of fraudulent behavior, it’s best to learn about it before you hand them a job offer.

3. Proactively Communicate Conduct Guidelines

Every business needs a policy regarding an employee code of ethics and conduct. While a policy alone won’t prevent criminal or fraudulent behavior, the standards it outlines will set a clear benchmark for employee behavior regarding ethical and lawful conduct.

Trying to establish a positive work environment will also encourage employees to follow established policies and procedures and act in the best interests of the organization. Fair employment practices, written job descriptions, clear organizational structure, comprehensive policies and procedures, open lines of communication between management and employees, and positive employee recognition will all help reduce the likelihood of internal fraud and theft.

Once developed, the code of conduct should be documented and agreed to by all new employees (and existing employees if you haven’t put a code in place yet). TPM can provide you with many templates for basic codes of conduct, but as a rule of thumb you should include policies that cover the protection of company data, the avoidance of conflict of interests, and of course, obeying the law.

CONTINUED ON NEXT PAGE
4. Implement Internal Controls
Internal controls are measures that ensure the effectiveness and efficiencies of operations, compliance with laws and regulations, safeguarding of assets, and accurate financial reporting. These policies and procedures should address the following points.

▲ Separation of duties: No employee should be responsible for both recording and processing a transaction.
▲ Access controls: Access to physical and financial assets and information, as well as accounting systems, should be restricted to authorized employees.
▲ Authorization controls: Develop and implement policies to determine how financial transactions are initiated, authorized, recorded, and reviewed.

5. Create an Anonymous Reporting System
Every organization should provide a reporting system for employees, vendors, and customers to anonymously report any violations of policies and procedures.

Promote and encourage the use of the reporting system whenever possible, and take the reports seriously. The fact that they are anonymous does not mean they are any more or less credible; they should be investigated just as thoroughly as any reported misconduct.

6. Don’t be Afraid to Audit
Conducting regular audits can help you detect theft and fraud. Audits can also be a significant deterrent to fraud or criminal activity because many perpetrators of workplace fraud seize opportunity where weak internal controls exist.

As a rule of thumb, identify high risk areas for your business and audit for violations on a six to 12 month basis - these could include business expense reports, tool and machinery count, cash and sales reconciliation, vacation and sick day reports, violations of email/social media or web-use policies, and so on.

7. Recognize the Signs
Studies show that perpetrators of workplace crime or fraud do so because they are either under pressure, feel under-appreciated, or perceive that management’s behavior is unethical or unfair. These employees rationalize their behavior based on the fact that they feel they are owed something or deserve it.

With this in mind, some of the potential red flags to look out for include:

▲ Not taking vacations - many violations are discovered while the perpetrator is on vacation;
▲ Being overly-protective or exclusive about their workspace;
▲ Prefers to be unsupervised by working after hours or taking work home;
▲ Financial records sometimes disappearing;
▲ Unexplained debt;
▲ Unexpected change in behavior.

8. Set the Right Management Tone
One of the best techniques for preventing and combating employee theft or fraud is to create and communicate a business climate that shows the company takes stealing very seriously. Here are some simple steps you can take:

▲ Reconcile statements on regular basis for fraudulent activity;
▲ Hold regular one-on-one review meetings with employees;
▲ Offer to assist employees who are experiencing stress or difficult times;
▲ Encourage open-door policies giving employees the opportunity to speak freely and share their concerns about potential violations;
▲ Create strong internal controls;
▲ Require employees to take vacations;
▲ Treat unusual transactions with suspicion;
▲ Trust your instincts.