



Adam D.H. Grant is a principal with the Encino, Calif. law firm of Alpert, Barr & Grant, APLC. His practice areas include complex business litigation, construction law, real estate and general liability claims. He can be reached at agrant@alpertbarr.com.

If you are going to entrust the finances of your company to an employee, checking the employee's background is the starting point to ensure company finances are secure. A number of very cost-effective services can be utilized to perform public records checks. For example, you can quickly locate criminal records, civil litigation history and tax liens using Westlaw or Lexis/Nexis.

How to Prevent Employee Theft

Better to be proactive and safe than reactive and sorry

by Adam D.H. Grant

Be aware, that if you choose to investigate an employee's background on your own, some states require that employers disclose the information obtained from public records to the prospective employee within a reasonable time after obtaining the information. As the employer, if you fail to disclose the information, you may be subject to civil liability.

Use Proper Procedures

Do you have a clear and concise document preservation policy? When the policy is properly created and then communicated to all concerned, it gives directions and accountability. Documents to preserve can include vouchers, bills, receipts, books, ledgers, certificates and deeds. The policy provides the guidelines and necessary checks and balances needed to prevent theft.

The law recognizes that "documents" also include electronic data. Thus, your company should develop and implement a policy that protects such information. You

should consult an information technology (IT) consultant to address the issue of automatic purging of electronic data such as emails or backup tapes.

Consider changing passwords at irregular intervals to avoid the drastic results of inadvertent disclosure of such information. In California, a litigant is responsible for preserving both hard copy and electronic information if it reasonably could be used in actual or potential litigation. A well thought out and enforced IT backup procedure will minimize the risk

of loss and prepare the company for any possible litigation.

Identifying Red Flags

An astute employer can prevent losses by being aware of key employees' behavior. Some of the biggest red flags of possible employee embezzlement are 1) not taking vacations (for fear that someone will discover the illegal behavior); 2) overly protective about their workspace; 3) prefers to work unsupervised; 4) occasional disappearance of financial records; 5) unexplained debt; or 6) unexpected change in employee behavior.

By implementing internal controls that recognize such behaviors, you will identify the behaviors before they become a problem and require remediation. However, be sure to document thoroughly your investigative measures before you take any corrective employment action to reduce the possibility of later legal labor claims.

Encourage and Praise Employees

Creating and implementing a positive work culture at your business will dramatically reduce the likelihood of internal theft. A positive work environment instills in employees the intrinsic desire to help the company and minimize harmful actions. Educate your employees about workplace policies and internal controls and publicly praise them when they demonstrate proficiency and compliance. Create anonymous reporting procedures so employees can feel safe notifying management of anything that appears amiss. Be sure to investigate each report. Failure to investigate may undermine the effectiveness of the procedure.

No business is completely immune from employee theft. However, by following these guidelines and adapting them to the individual needs of your business, you can substantially reduce risk and minimize most losses.

