Employee Theft: 10 Exposed Areas for Review
An Original Article by J. Patrick Murphy

Employee theft is nearly 50% of the losses for retailers. It's a $600 Billion crime across the nation for all businesses and growing. Employers are sometimes reluctant to discuss this topic or even acknowledge its existence but to adopt that approach will lead to financial disaster.

I develop loss prevention "programs". These are designed to deter, detect, or defend the loss of company assets. I put programs in quotations because in most cases, most (if not all) of the essential elements of asset protection are already in place. There may be some comfort in having everything compiled under one topic but the truth is that if policy and procedure were conducted as envisioned, the effect would be the same. With that said I am listing 10 areas that are generic to all businesses that can assist in closing some potential gaps that would allow employees to steal.

There is ample research that shows that happy work place is a theft free workplace. The person one sees at the office is the complex result of an entire lifetime of their environment and morals. It would be naive to think that everyone is 100% honest, 100% of the time and people are not likely to outwardly show any dishonest tendencies. The three factors of theft, need, opportunity and justification, hold true universally and we tend to judge others by our personal standards. What motivates and is justification for one person would pale in comparison for someone else. Opportunity is always the key factor. Removing that opportunity through monitoring and consistent handling is the best way to prevent theft.

When considering a solid approach to combating theft by employees here are 10 areas that you should consider:

1. **Pre-employment Screening**
2. **Employee parking.**
3. **Training and Awareness**
4. **Access Control**
5. **Postage and Shipping**
6. **Expense Monitoring**
7. **Payroll**
8. **Bookkeeping**
9. **Petty Cash**
10. **Lockers and Searches**

pat.murphy@lptoday.com
713.899.2402

1. **Preemployment screening**. Enough cannot be said about hiring quality employees. However, as you are reviewing their resume or application remember that nearly one third of all resumes and applications contain inaccurate information. This could be embellishing their experience, adjusting their dates of employment to appear to have been employed regularly, or leaving blank questions regarding criminal convictions.

- Read the information and then go back through and pick through each line in detail. Ask yourself (and then the applicant)
- Why there are gaps in employment? Were they unemployed or hospitalized or were they in jail during that time?
- Why do they only list the year of employment and not, at least, the month?
- Look at the SSN to determine if the issuing state is reasonable. These numbers can be checked on-line to determine where they were issued. If the application says they are life-long resident of California, why would they have a Florida issued Social Security number?
- Does the education seem reasonable? Did they graduate around the age of 18? Did they go straight into college? If not, there should be employment history for that time.
- Are all of the previous employers no longer in businesses? This is either a run of bad luck or an attempt to prevent reference checking.

Criminal Background checks are essential in today's workplace. Access to convictions is available through so many public and private entities that to not conduct one may be considered negligent if this was not determined and that same employee committed a criminal act. Hiring someone with the full knowledge that they do have convictions is an extremely high risk. Many companies ask only for felony convictions to be disclosed on their applications. This too, is a risky practice. Misdemeanor crimes such as carrying a concealed weapon, assault, stalking and some narcotic offenses are pertinent to your company. A company is entitled to know of all convictions as an adult. Lastly, suspended sentences and deferred adjudication ARE convictions. They are a form of probation that required a guilty plea. To make this clear to applicants, a statement should be included on the application that these types of sentences must also be disclosed. Keep in mind it will be rare for someone to openly disclose a conviction therefore an outside verification is needed.

A final recommended method is to consider"paper and pencil" honesty surveys. They are actually done either on paper or via computer but the concept and results are the same. These are simply questionnaires that probe the applicant's attitudes towards honesty and ethics. They ask questions such as "If you saw a co-worker steal something, you would..." and then there are multiple choice answers. They also ask drug and alcohol related questions such regarding having used drugs at work or coming to work under the influence. There is also usually a section where questions are asked if they have ever stolen from an employer and how much. Astounding as it may seem, many answer yes. In fact the results of the survey have a history of not recommending 30% of those taking them. While there is cost associated with this, the value is very high as the cost of training and turnover is greatly reduced.

2. **Employee parking.** Consider your employee parking area as a point of concern from both a security and safety perspective. We all like to get that parking space closest to the store at the mall but for most businesses, those parking spaces are reserved for clientele. There should be a designated

pat.murphy@lptoday.com
713.899.2402

parking area for all personnel and that area should be beyond the normal client/customer parking. The reason for this is easy: A thief has a reduced exposure if their car is parked closely.

Employee parking can be a thorny topic. Concerns for their vehicle seem to subside if they can at least occasionally, see their car. While there are no absolutes on this topic here are some suggestions:

- Never allow employees to park close to the entrance/exit. Have a designated parking area for them (regardless of the weather).
- Do not allow them to park next to loading docks or trash dumpsters.
- Don't allow "I forgot my badge" to be a free pass to park anywhere. Have a procedure in place to get them where they need to be and back that up with a counseling program to ensure it won't happen in the future.
- Encourage employees to leave the building together to reduce exposure to criminal acts while walking to their car.

3. **Training and Awareness.** The importance of training cannot be overstated but the varied methods and the materials make it difficult to define the best practices here. When someone if first hired the amount of paperwork required is enormous. Sometimes mixed in with the employment papers are company policies that require signature. To ensure that the new hire understands the importance of these sign off acknowledgements, time should be set aside that is dedicated to only those documents. At the very least, a new hire should acknowledge through signature that they have read and understand policy. On the practical side, it would be best that specific policies that are pertinent to the employee be presented upon hiring. Those policies and procedures that, if violated, result in immediate termination are also good candidates for the new hire package.

"Training" to whatever extent it is (classroom, OJT, video, Computer Based) is not truly effective unless there is some means to verify the person's level of understanding of the material. The argument cannot be made that because they were there and did not ask any questions about the material that they comprehended the subject matter.

For many companies, initial training/orientation is the sum total of all personnel policies and procedures. Changes are distributed through company mail, email, or conference calls. It is important that all employees have some means of being informed of significant policy changes. When it comes to prevention of employee theft, awareness is the best ongoing tool.

Awareness is simply reminding employees that the company monitors for this type of activity because it is a profit drain. There are many ways to approach awareness. The use of posters is probably most common and there are many companies that design generic versions. Meetings about inventory control, shrink, operating statements etc, are good platforms to openly discuss the results of internal theft. I saw a handwritten sign over a time clock in a grocery store that said "If you get caught stealing, you're going to jail." I do not recommend this approach and certainly think it sends the wrong message by saying "if you get caught". Now it almost seems like a challenge. The message should be about losses in general and some method of confidential communication should be in place so anyone can provide tips on suspicious behavior.

pat.murphy@lptoday.com
713.899.2402

4. **Access Control.** This is a simple objective that increases in complexity the larger the company. This subject concerns two specific areas: access by employees and access by non employees that is granted by employees.

External Access Control

- **Employee Access.** Start your review process from the outside in. In other words go to the furthest point that requires authorized access. Authorized access can be a key, a card, a pass code, or some other accept/deny point. The points could be gates, parking lots, exterior doors and alike. Everyone has some level of approved access. Access can be controlled by something as simple as a door lock or as complex as some type of biometrics. Regardless, maintaining proper control is really a function of keeping things current. Vehicles and people can easily gain entry through unmanned gates/doors by simply "drafting" (going through after someone else before the door closes). These are weak areas of security.

Entering a building with a key is good security because only that person can/should enter. However, how current is your key control. What happens when a key carrier leaves the company? What happens to the alarm code when someone leaves the company? The security of the security is extremely.

TIP: If your building has a burglar alarm that is monitored by a central station (i.e. ADT) generally there are mailed or on line reports available to check open and close times. Someone should be reviewing these reports to determine if there are any odd-hour entries by authorized personnel. If someone enters the building at 2:00AM on a Saturday, what was their purpose? Alarm companies will generally notify someone if a door is opened at unauthorized time. Check with your alarm company.

- **Non employee Access.** Employee theft does not necessarily need to be by the employee themselves. Collusion is a very high possibility. This is especially true with robberies in all business sectors. The "inside job" is more frequent than one might consider. CCTV as a second layer of security will, at least, provide possible identification of the parties involved. Collusion can be used for burglaries, corporate espionage, theft of trade secrets and vandalism (among others).

Internal Access Control.

- **Employee Access.** Once inside a building the security should be more restrictive. The most sensitive areas can be anything from a vault to employee record storage to the IT Department. Value cannot be determined by simply assigning a cash value to it, there are costs associated with theft that extend far beyond the actual property. There are potential costs of liability, customer good will, interruption of the business operation, etc. If an employee steals a laptop computer containing business records that are not backed up, the cost of the loss can be devastating. In short, anywhere an employee has access, theft can and will occur.

- Non employee Access. The person acting in collusion with an employee can only have access to areas that either have weak security measures (locked doors propped open) or are actively

pat.murphy@lptoday.com
713.899.2402

working with the employee. Getting into a business with the assistance of an employee is virtually risk free.

Tip: Even if you just use locks with keys, segregate the level of access everyone has to specific areas. Managers and supervisors with keys have to allow people to have occasional access somewhere. This is annoying to some. Their misguided remedy may be to disable the lock or give everyone a key by hanging it on a hook somewhere. This makes the security as rigid as tissue paper and defeats the purpose. If an area needs to be secure then limit access.

5. **Postage and Shipping.** Stamps! What is the harm of using one postage stamp to mail in my utility payment? The company has lots of stamps and certainly won't miss this one! And so goes the mentality. Do you know how much exposure you have when it comes to unauthorized use of postage and shipping?

   Parcel theft, the unauthorized use (and certainly nonpayment) of some method of shipping for personal gain. The scale of a company's mail function is certainly a factor but all companies face the same problem. Tight controls, frequent monitoring/auditing, and an absolutely defined company policy about misuse will help reduce theft. Keep in mind that this type of theft not only involves the mailing of Aunt Emma's Christmas package at the last minute but the theft and diversion of company product and property using the company's own mailing function.

Account numbers for common carriers, UPS, FedEx, DHL and others are pure gold. Little effort is required to ship a package if access to account numbers if uncontrolled. The security of these numbers is as important as safeguarding the combination to a safe. There are some areas where there is a great deal of vulnerability:

- **Mail rooms.** We'll take the obvious first because the exposure comes from two sources: employees of the mail room and employees outside the mailroom. In both cases however, the final checkpoint is in the mailroom itself.

- **Shipping Departments.** This is the same as above but usually involves larger packages and carriers such as UPS and FedEx. This area has potential for theft of company product, especially in retail and catalog environments, by shipping to themselves or accomplices. Additionally the driver for the carrier can also be in collusion and simply accept packages and then drop them somewhere along their route.

Tip: While cumbersome and time consuming, occasional audits should be conducted after the carrier has been loaded. All packages should be checked for proper labeling and screened for suspicious names and addresses.

6. **Expense Monitoring.** Expense accounts are often termed as "abused" when in reality it is theft. Expense accounts can be used in a number of ways for personal gain, most of which can be caught early on with proper oversight. A supervisor should always review submitted expenses or monthly credit card statements to ensure the propriety of money spent. A paper trail needs to exist for all expenditures and companies should refrain from adopting policies that do not require receipts for small dollar amounts.

pat.murphy@lptoday.com
713.899.2402

To combat possible fraud companies should do as much direct billing as possible and set strict limits with those vendors as to what will be paid for. A strict policy should be maintained regarding improper use of company funds and regular audits should be conducted for all employees. A distinction should also be made within the policy that the supervisor's approval signature is meant that all items have been properly reviewed and that they are legitimate. When there is accountability, there is less likelihood that a supervisor is passing down receipts to a lower level so that questions won't be raised on their own reports.

Abuse and fraud through the use of personal credit cards is also possible. One of the most frequent abuses I have seen is the use of a personal credit card that awards airline mileage to book travel reservations. The owner of the card will almost always be management and the reimbursement process will need to be prompt in order to pay the bill. Hundreds of thousands of miles can be amassed in a fairly short period of time.

7. **Payroll.** Using the company payroll to commit fraud is perhaps one of the oldest ploys around. "Ghosting" payroll means creating fictitious employees or continuing to submit payroll requests despite the employee no longer working. This also requires forgery of the endorsement of the check so the funds can be cashed or deposited in the forger's account. This type of fraud is usually committed by managers and can go undetected for long periods of time.

Even a small company can fall victim to this type of theft without occasional audits to reconcile the existence of employees. In high turnover industries a manager could simply postpone submitting termination paperwork to a payroll department for until the next person quit. This could be considered a form of identity theft but it is more a means to steal cash.

Tip: Field managers should be conducting these audits on a very regular basis.

8. **. The Bookkeeper**. The bookkeeper plays a critical role in a business because of their skills, their knowledge base, and their total familiarity with the company and their practices. These same areas can be used with a devastating effect if theft is involved. Even when a company becomes large enough to move into the stage that requires an Accounting Department, fraud can occur.

Consider the following areas:

- Banking. What process is in place to ensure that revenue and deposits are the same? What process is in place to ensure that the number and amount of checks and the amount of cash equal the receipts for the day? To steal cash, one would simply have to delay depositing funds. The subsequent days the cash that was taken would have to be replaced by checks from previous day's business.
- Vendor accounts. What prevents the bookkeeper from creating fictitious vendors and then creating payments they receive themselves? What prevents intentional overpayment of a vendor to receive a portion of the stolen funds? What monitoring is available to ensure that vendors do not develop personal relationships with critical employees? (Note: a review of policy regarding the receiving of gifts, trips, ball game tickets, rounds of golf, etc from vendors should be conducted).

pat.murphy@lptoday.com
713.899.2402

Horror Stories. A vendor for a very large company set out to woo the affection of the accounts payable clerk that who handled their account. Eventually becoming successful the AP clerk began charging various locations through journal entries for fictitious product. By sheer coincidence one of the locations' managers saw an unusual charge which eventually unraveled the case. Time to detect: 8 months. Loss: $1.2 million. Both were prosecuted

A busy realtor had an excellent bookkeeper. The bookkeeper was young, energetic and very territorial about her work. Even the realtor could not get into the password protected files. The realtor thought she was a gem of an employee because she even came in on her vacation to take the daily deposit to the bank. She was also efficient and had the realtor pre sign company checks to pay bills. The bank manager was alerted to some odd looking checks made out to the bookkeeper. Since the realtor had been a long time customer, the realtor was notified. The bookkeeper was creating checks to herself and depositing at the same bank. Time to detect: 12 months. Loss: $267,000. Side note: Realtor failed to conduct criminal background check which would have shown the bookkeeper's prior convictions for credit card fraud.

9. **Petty Cash.** Sometimes called a coffee fund or office supply money, petty cash is simply an amount of money that is used for various small purchases. There is no "Best Practice" as to how much the fund should be but regardless, it must be tightly controlled and must be used only for the intended purpose. Petty cash funds tend to become the "small loan department" for lunch or other needs when someone is short on cash. The money goes out and an IOU is substituted. This is not a recommended practice as company funds are being used for personal use.

Petty cash should be counted daily and documented somewhere for reference. This documentation should be audited and the cash personally counted (with a witness) by the person who is in charge of this fund. The cash plus any receipts for disbursed money should equal the total that should be present. Variances, over or short, should not be tolerated.

10. **Lockers and searches.** Lockers are considered by many employees to be "theirs" meaning there is an expectation of privacy of their contents and that searching a locker is an intrusion of their personal rights. This should not be the perception or the rule and is simple enough to remedy.

Company policy should clearly state that all employees and their vehicles are subject to search. Lockers present a challenge if employees are allowed to use their own locks. Check with your legal counsel as the "ownership" issue may change if the lock itself belongs to the occupant.

Searching lockers either randomly or for cause can be a human resource disaster if not handled with care, tact, and diplomacy. Ensure your method of search is approved by legal counsel. Is a "search" confined only to what is visible in the locker or does the search allow opening of backpacks, purses, and briefcases? Does the employee need to be present during any search? There is a reasonableness factor in this element. Check with your attorney to determine if a supervisor can be there instead. What is the action taken if someone refuses to allow the search of the locker? If your policy is clearly written, the resolution of that confrontation is spelled out.

pat.murphy@lptoday.com
713.899.2402

Consider this question: what expectation of privacy should an employee have while on company property? There are many arguments to this and policy should be chosen and written carefully.

Throughout this paper the overriding theme is audit. Policy and procedure without compliance review have little or no impact on a business. Policy and procedure without consistent application is an open invitation to liability.

pat.murphy@lptoday.com
713.899.2402