Business Bits - ‘Tis the season… for embezzlement!

As the New Year begins, many people are facing financial strains. Holiday overspending, unpaid taxes and the impacts of inflation drive distress. Even worse, January is the busiest month for divorce attorneys, creating further financial strain.

Unfortunately, financial strain often leads to desperate behaviors and today we’ll talk about an especially toxic desperate behavior - stealing from your employer, also known as embezzlement.

Today on Business Bits we’ll take a look at the crime of embezzlement.

We’ll review why this topic is important, how widespread the problem is, who embezzles, what drives this crime, what it looks like while it's happening.

Next, we will discuss how to protect yourself and we’ll explore a relevant concept from the field of accounting called internal controls, also known as checks & balances

This topic is important for both business owners and for employees.

- Employees need to be aware of evidence of embezzlement because most cases are cracked by tips from employees.
- Understanding how embezzlement works will also help honest employees spot problems in internal controls that could result in they, themselves being at risk of being wrongly accused of theft.

How widespread is embezzlement?

A recent study found that more than 80 percent of embezzlement thefts occurred at companies with fewer than 150 employees, and **nearly 50 percent of embezzlement thefts occurred at companies with fewer than 25 employees.**

- It’s estimated 75% of businesses will be impacted by some form of this crime.
- It’s known that employee theft is the root cause of almost one third of business failures annually.
- We hear a lot about equity and inclusion these days and embezzlement is an exemplary model of inclusion
    - Women are slightly more likely to embezzle (51%) than their male counterparts.
    - Embezzlers are typically in their mid- to late-40s.
- Embezzlement can occur in any department, with 37% of reported incidents occurring in finance or accounting.
- Embezzlers are most likely to be individuals who mostly work alone.
- **Embezzlers love January**, when everyone is cleaning out old files, reorganizing workspaces and getting ready for the new year. Security is especially lax and easy access can be gained to confidential materials.

The very worst embezzlement statistics

The first worst statistic is that 100% of embezzlement is preventable. Employee theft is enabled by what my parochial school teachers would call sloth, or laziness. I’m sorry if this sounds like victim shaming but it kind of is.

Victims of embezzlement frequently say that internal controls were too cumbersome, or that they didn’t want to look like a bully to their beloved employees (who are robbing the employer blind), or that they want a family atmosphere (when family owned businesses have the highest incidence of internal theft!).

The second worst embezzlement statistic is that very few instances of employee theft are reported to authorities. Victimized business owners don’t want to look foolish, and don’t want to worry lenders, vendors or customers. Owners don’t want other employees to know about the crime and are fearful of negative publicity. Many hope it’s a one time thing and want the problem to just go away.

Because of embarrassment, shame and even a terribly misplaced sense of charity, **a vast majority of embezzlement crimes are never reported.** This very poor choice makes it possible for the embezzler to slink away and do it again to someone else. This is the origin story of every embezzler - they grow accustomed to that extra income and look for ways to grow that resource. Every embezzler is a serial embezzler, virtually none are “first time offenders,” it’s a lifestyle. They all start out taking a little, and soon graduate to taking as much as they can.

Sadly, it’s a lifestyle that will keep on hurting businesses until the offender is reported and a criminal record is established. A criminal record makes it possible for future employers to avoid these miscreants and all the trouble embezzlers will bring to your door.

Specific drivers of embezzlement

Employers and employees should be on the lookout for workers who exhibit symptoms of +

- Narcissism - I deserve this
- General personal financial problems
- Spousal pressures, e.g.,
    - Refusal of one spouse to work
    - Medical costs
    - Keeping up with the Joneses
- Triumvirate of addiction - in either the employee, spouse or close family member

- Drug addiction - with access to additional funds, any drug addiction will grow at a vastly accelerated pace, increasing the need for even more money. The addicted embezzler will have increased absenteeism and other workplace performance problems that should call attention to the issue.
- Gambling addiction - when an embezzler starts spending employer money at a gambling establishment, the gambler receives additional gambling benefits like junkets and trinkets, delivering an additional reward for the original theft. The gambling embezzler will often have unexplained trips or possessions that can tip off the observant.
- Shopping addiction - one of the easiest embezzlers to catch for those who take the time to notice. Possessions clearly beyond the means of the employee’s pay grade can be the downfall of this type of thief.

The four determinants of embezzlement (like ‘means, motive and opportunity’ in a murder mystery):

1. Pressure – they need more money because of those increased medical expenses, personal financial losses, credit card or gambling debts
2. Opportunity – often through having access to company funds from **end-to-end without any checks and balances**
3. Capability – they have the skills and knowledge about how and where to hide money
4. Rationalization – they tell themselves they are doing it for their family, or they are underpaid, or that others are also stealing

What all of this means to our listeners is that, because of all of these factors, there is a greater than 50% chance that embezzlement is happening right now, in your company or at your employer’s business.

What do embezzlers look like?

Intelligence and curiosity
Embezzlers are often eager to know how everything in the office works. Once they learn the processes, they manipulate them for their own gain.

Egotistical risk-taking.
Embezzlers often break rules, from traffic laws to company policies to social norms, both at work and in their personal lives.

Disgruntlement.
Employees who feel they are being treated unfairly may be tempted to get even by stealing.

Business Bits - ‘Tis the season… for embezzlement!

Unusual Working Hours

An employee misusing company funds may prefer to work during hours when no other people are in the office, such as early mornings, late nights or weekends. Working off-peak hours may enable the employee to engage in illegal behavior without the immediate threat of being caught.

Refusal to Take Vacations/Time Off

An employee misappropriating funds on a regular basis may insist on working on vacation days to ensure that they can keep their behavior hidden. This prevents someone else from taking over their duties and discovering the fraud.

Insistence on Independence

A high level of independence can ensure that an employee embezzling funds is not caught. The employee may insist on learning about processes outside the scope of their role to avoid relying on others. The employee may also be reluctant to delegate their own responsibilities.

Possessive Attitude

Embezzlers frequently act possessive toward their work area, devices or tasks and will overreact if someone touches their computer or accesses their files.

Accessing Restricted Areas or Information

Embezzlers seek to gain unauthorized access to commit fraud. Take note of failed login or access attempts on programs, files, safes and office areas.

What are internal controls, or checks & balances?

Internal financial controls help ensure money and business records are properly managed. Most are simple and inexpensive or free, implementing internal controls makes some business owners uncomfortable.

Owners who avoid uncomfortable conversations now will likely be facing much more uncomfortable conversations later. Business owners sometimes turn to ‘the faceless other’ to reduce the discomfort of implementing internal controls.

“Our bank required us to put these practices in place…”

“Our insurance carrier mandated these processes to support claims of loss…”

Our tax accountant wants us to start using these procedures this year…”

Business Bits - ‘Tis the season… for embezzlement!

Top ten internal controls

1. Conduct background checks before hiring. Period.

2. Review monthly business bank statements in detail and have bank statements sent directly to your personal email or home address, so you are the first to see them.

3. Have all credit and debit card statements reviewed for accuracy and appropriateness by a team member other than the cardholder. Require employees to document all business expenses with detailed receipts.

4. If you have inventory, control methods are critical. Create checks and balances for order placement and inventory receiving. Conduct surprise physical inventories of products or materials.

5. Require a second employee to authorize any cash transactions. Record all transactions, and balance cash frequently.

6. Require vendors to submit detailed invoices. and review all outgoing payments. Compare payments to invoices. Watch for duplicate invoices, new vendors, or multiple invoices from the same vendor in a short time. Embezzling employees often use these tactics to pay themselves.

7. Avoid using signature stamps on checks. Require all outgoing checks and payments to be signed or authorized by the business owner.

8. Review payroll before paychecks go out. Watch for any variations in the amounts. Use direct deposit to reduce your risk of payroll fraud.

9. Break up and delegate financial duties. If one person has control of bookkeeping, payments, and payroll, it's easy for them to steal from your business. Employees, it's also easy for you to be unjustly charged with theft - internal controls protect you, too.

10. Cross train employees involved with your business finances. Require these employees to rotate roles and change who handles specific duties. Misconduct is often discovered this way.

Final Thoughts on Embezzlement

It’s important to be an engaged business owner. Pay attention, ask questions and review detailed reports. Deploy technology to control access and approval levels, and provide early warning of anything unusual. Most of all, implement checks and balances in your processes to

make sure no single employee has complete control. Steps like these help protect the livelihoods of everyone in the business.

If you do suspect embezzlement, contact your insurance company and local law enforcement for guidance on investigating, documenting and reporting the crime.

Learn more in these examples taken from 25 Examples of Embezzlement and Workplace Theft, Published: Sep 26, 2019 Last Updated: May 19, 2022, by Anita Campbell, in *Small Business Trends*, an award-winning online publication for small business owners.

Specific examples of embezzlement and tips for prevention

Forging Checks

The employee writes company checks or makes electronic payments to himself. The employee then cooks the books to hide the theft.

This classic embezzlement example is made easier when a company uses a signature stamp of an executive’s signature. A signature stamp is literally like handing employees a blank check because they can “sign” checks without your knowledge.

Prevention: Separate responsibilities: one worker to process checks and another to reconcile transactions and approve documentation. If you don’t have enough staff for separate functions, then reconcile bank statements yourself. Require purchase orders or invoices for every payment. And stop using a signature stamp — or keep it under lock and key.

Cashing Customer Checks

The employee endorses and cashes customer checks payable to the company, then keeps the funds.

Today, as more payments become electronic the essential crime is the same. The employee may set up a bank account with a fictitious name similar to the employer’s to divert electronic payments into. Small banks and credit unions can be lax in allowing accounts to be established by the employee using fake “doing business as” names.

Prevention: Separate the functions so that one person is responsible for processing payments and another for reconciling accounting entries. Implement controls to track customer payments at every step to avoid this kind of embezzlement.

Faking Vendor Payments

Next on our list of embezzlement examples is when an employee steals company funds, but tries to hide them as payments to vendors. Faithless employees may create fake vendor invoices and change accounting system entries to hide their tracks.

Prevention: Regularly review detailed expense reports (not just summary reports) broken down by vendor, amount and purpose. If you stay familiar with your numbers, it’s easier to spot when a payment or accounting entry looks suspicious. If your company is big enough, separate the functions employees perform.

Overbilling Customers

The employee overbills customers, keeps the extra money and covers it up with false accounting entries.

Sometimes this a large-scale fraud where each customer or transaction is overbilled by a small “fee” for years, this is the classic “salami slice scam.” Other times it involves double billing the same amount twice or tacking on charges for items the customer did not buy.

Prevention: Conduct a periodic audit of customer billings. Pay close attention to customer complaints about billing errors and require thorough explanations from staff of how they occurred. Complaints may be a warning sign of a bigger problem.

Theft of Customer Data - 60% of departing employees take customer data when they leave

An employee who takes phone orders may later use the customer’s credit card data to charge personal purchases online. Or a gas station manager may use a skimmer device to skim card data from terminals at the pumps.

A more nerdy version is when an employee downloads personal information, email addresses and credit card data from company IT systems. Then he or she sells it on the dark web.

Prevention: Limit access to customer data to only those who need it. Deploy technology that redacts credit card numbers or only prints out the last digits, to limit trash harvesting or unintentional sharing. Change permissions when someone with IT access leaves the company. If you use card terminals, install anti-skimming technology — some municipalities now require it.

Padding An Expense Account

Padding examples range from the occasional attempt to justify an expensive lunch using a “creative” description, all the way to elaborate embezzlement schemes.

Prevention: Have a written policy detailing what is — and is not — reimbursable. Go over the policy in staff meetings. If employees do a lot of business travel, control approvals and review receipts all in one place.

Double Dipping

Next on our list of embezzlement examples is when there’s a single legitimate business expense, but the employee gets two reimbursements. She first pays for an expense with the company credit card. Later she submits a cash reimbursement request for the same expense.

Prevention: Insist on seeing underlying receipts for all expenses (don’t just review the credit card statement). Use expense management software if your employees incur a lot of reimbursable expenses.

Using a Company Credit Card For Personal Use

The employee pays for personal expenses using a company credit card. The good news is, often these thefts are sporadic and the amounts are small.

However, what if the same employee also manages the accounting system and realizes no one but her pays attention? Using a company credit card for personal use can turn into massive embezzlement examples when combined with falsified accounting records.

Prevention: Always have two people involved in the process: one to approve expenses and one to handle accounting. Require documentation of the expense purpose.

Voiding Transactions At The Cash Register

An associate at the cash register voids transactions and pockets the cash. This is a common way of skimming money from a retail small business.

Prevention: Check and balance - one person counts the drawer, another balances to the register report tape.

Siphoning Off Cash Deposits

Before dropping off the cash deposit bag at the bank in the evening, the employee pockets some of the cash.

Prevention: Personally count the day’s cash, complete the deposit slip and enter the amount into the accounting records yourself before handing off the bag. Or separate the functions so two people are involved. Other strategies may help, such as security cameras in the area where cash is counted along with using locked deposit bags. See more tips for cash processing.

Raiding the Petty Cash Box or Safe

This theft can be as simple as the employee taking $200 out of the safe or petty cash box.

Prevention: Lock up large sums and keep the key yourself, to minimize access and temptation by employees. Or use security cameras.

Pocketing Cash From Fundraisers

Skimming fundraiser money is all too common in non-profits. But this type of fraud also occurs in businesses that take on a charitable cause. If one person has complete control over the money, from start to finish, the temptation to steal can prove too great.

Prevention: Always have at least two people involved in the workflow of collecting, recording, depositing and remitting donations. Don’t give temptation a chance.

Stealing Office Supplies

It’s shocking how many employees seem to feel it is okay to take large amounts of office supplies home. Theft of supplies usually involves consumable items like postage stamps, Post-it notes or coffee supplies.

Prevention: Put most of your supplies under lock and key and replenish an open supply area sparingly, to keep shrinkage small. A security camera may help. Discuss the use of supplies in a company meeting to set the tone and convey company values.

Stealing Equipment or Raw Materials

In construction and manufacturing businesses, an employee may hide company property in a dumpster or storage area and retrieve it after hours. Equipment theft also occurs in offices. Think laptops or small document scanners that can be slipped into a backpack or handbag.

Prevention: Lock up or bolt down valuable items if feasible. Label important equipment with a number and let employees know you plan regular audits to ensure items are still on site. Use security cameras and electronic access systems.

Stealing Products

Employees “shoplift” far more than customers

The employee steals company products. Examples include jewelry or perfume from a high end retail shop. Typical victims are small retailers that lack shrinkage controls. It is stunning how many owners simply stuff inventory into a storeroom with no tracking system.
Another variation is when a waiter does not charge friends for food or drinks in a restaurant.

Prevention: Use security cameras. Implement an inventory management system and regularly check inventory levels. There’s even POS technology that tracks voided transactions and discounts, and alerts the owner or manager.

Burglarizing Company Premises

Think classic inside job — with or without accomplices. The employee leaves a door unlocked or uses a key to get in after hours. Your company gets ripped off.

Prevention: Install security cameras. Implement an electronic security system to secure after-hours access, and record who is coming and going.

Stealing Returned Merchandise

This theft can occur in a retail or ecommerce setting, or in any business that swaps out old equipment. The employee simply takes returned items home or resells them on Craigslist or eBay.

A lack of controls makes this theft easier. In some small businesses, returns may be stacked haphazardly in a corner. Is it any wonder they disappear?

Prevention: Implement control systems for managing returns and other property.

Setting Up Fake Employees

The embezzling employee sets up fake employees, pockets the pay, and cooks the books to hide the transaction. This happens in businesses with absentee owners or over-trusting owners who do not pay attention.

Prevention: Implement systems to reconcile headcount with staffing expenses. Regularly review a detailed headcount report breaking down expenses by employee. Remember, detailed reports are your friend. Embezzlement is much harder to spot if all you ever look at are summary reports or a high-level P&L.

Falsifying Overtime

This may include schemes where co-workers clock in and out for each other. Or it may involve a payroll clerk creating false entries for supposed overtime that he pays himself.

Prevention: Use electronic timesheet systems. Watch overtime pay closely for unusual increases. Compare detailed reports to identify exactly which employees are getting overtime and when — you may spot suspicious patterns.

Business Bits - ‘Tis the season… for embezzlement!

Failing To Remit Payroll Tax Money

The employee embezzles money earmarked for the employer’s payroll tax remittances or other tax money. Eventually the taxing authority will come down hard on the business owner for not sending in the tax money, and may file a lien against the business or seize property. So not only do you face losses from embezzlement, but you have the IRS on your tail — a double whammy! This embezzlement example is perpetrated by dishonest bookkeepers, financial staff, payroll clerks and even small outside payroll services.

Prevention: Outsource to a large reputable payroll service such as Paychex or ADP. It goes a long way to prevent an embezzlement nightmare. Or require a regular audit by an outside accounting firm.

Collecting Kickbacks From Vendors

In this scheme, the employee gets vendor kickbacks and you are unaware. Kickbacks can be cash. They also can take the form of additional products and services used in an employee’s side business or home. A warning sign is an unusually close relationship between a vendor and an employee.

Prevention: Get involved in choosing vendors yourself. This minimizes collusion between vendors and faithless employees.

Selling Trade Secrets; Corporate Espionage

The employee sells sensitive information to a competitor. Or the employee takes confidential documents and trade secrets with him when switching jobs.

You see this in high tech startups. For example, a former Google executive was indicted on criminal charges for stealing 14,000 files for self-driving car technology and taking them to a startup later acquired by Uber.

Prevention: Have strong employee agreements. Shared cloud storage systems help you manage and track who has access to what.

Business Identity Theft

An employee secures a line of credit or loan in your company name, using the money for personal purchases. The embezzler then uses company funds to make the payments. Typical embezzlers are finance staff or bookkeepers with access to accounting records and legitimate accounts used to cover their tracks.

A similar theft is when a partner or family member in a family business takes out unauthorized loans in the company name.

Prevention: Implement internal controls for checks and balances. Require detailed reports to see where money is going. Sudden cash flow issues or a negative change in your company credit score may be warning signs of embezzlement. Pay particular attention to services like PayPal and others that allow pre-approved loans or advances against your account.

Starting A Business Using Company Resources

In this situation, employees start their own businesses on company time. In the worst situations employees use company resources such as software code in their new software product, or steal raw materials.

Make no mistake about it: this is theft. Yet, some delusional souls brag on social media about what they are doing!

Still, the employer may get the last laugh. Why? Because generally speaking, an employer owns all work products created on company time.

Prevention: Set expectations properly with employees — and make your policy clear, whatever is. Some employers encourage side businesses but others have a no moonlighting policy. Even if you allow side businesses, make it clear that activities should not be conducted during work hours, and company resources may not be used.