THE 2017 HISCOX Embezzlement Study™

A report on white collar crime in America

HISCOX
encourage courage®

Introduction

We often spend more time with our work 'families' than we do with our actual families. We trust our family members implicitly, but the employer-employee relationship can be much more transactional; it can be described as a circle of trust. The employee trusts the employer to treat them fairly and compensate them for their work. The employer trusts the employee will do what needs to be done to advance the business. When that trust is breached because an employee steals, it can have far-reaching implications for the organization. Beyond the financial loss, it can negatively impact the morale of other employees and the company culture. It can even damage the company's reputation in the marketplace.

Surprisingly, employee theft happens more often – and for longer periods of time – than you might think. For the past three years, Hiscox has looked at employee theft cases that were active in the US federal court system. Over the course of our research, some trends have started to emerge:

- Small businesses face disproportionately high costs for white collar crime compared to large firms.
- More embezzlement is committed by women than men, albeit by a small margin.
- More perpetrators have positions in finance and accounting than any other function, but embezzlement happens in every department, at any level.
- The financial services industry continues to have the highest number of cases of employee theft, but no industry is immune.

In previous reports, we have focused on those employee theft cases occurring in companies with fewer than 500 employees. For the first time this year, we are also examining theft cases at companies with more than 500 employees to see if there are similarities or differences in the perpetrators and the types of thefts taking place. We also looked at the length of time the schemes lasted before the perpetrator was caught and were quite surprised at what we found.

This year's report supports the conclusion that every business is vulnerable. There are specific steps you can take to protect your business, including thoroughly vetting employees before you hire them, establishing internal controls, and monitoring business activities. Recognizing the warning signs of embezzlement is also critical. Armed with this information, you'll be better equipped to lower the risk of employee theft in your organization.

Doug Karpp
SVP, National Product Head — Crime and Fidelity

Hiscox | Encourage Courage

Embezzlement by the numbers

$1.13 million
Average (mean) loss

$319,350
Median loss

55%
of cases occurred at companies with fewer than 100 employees.

37%
of cases were committed by someone in the finance or accounting function.

30%
of cases occurred in the financial services or government sectors.

48
years old

48 is the median age of perpetrators.

37%
of cases involved losses of more than $500,000.

23%
involved losses of over $1 million.

51%
are women

Women commit more embezzlements but men are close behind.

28.7%

Over a quarter (28.7%) of schemes lasted for more than five years.

Contents

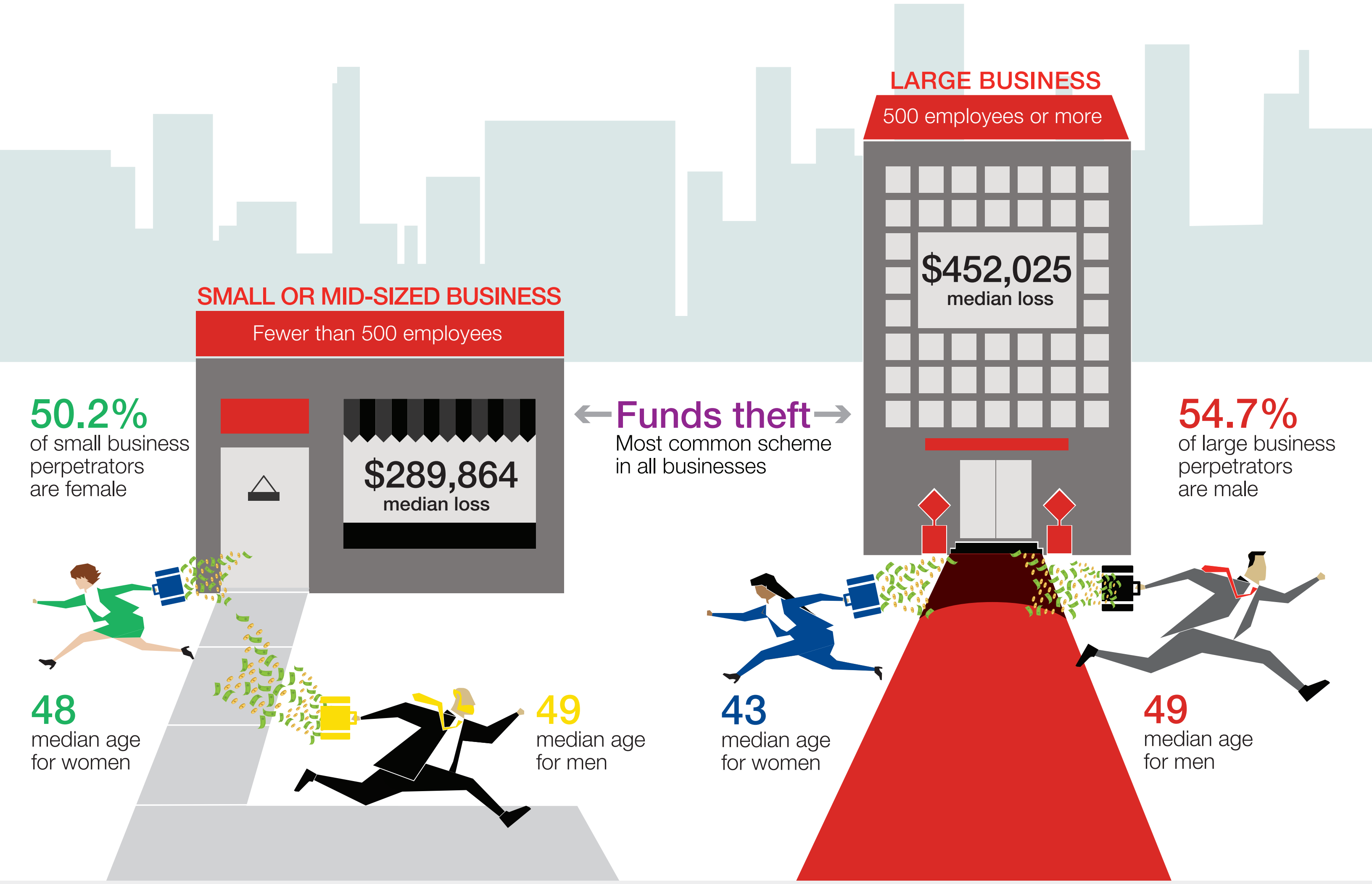
About us

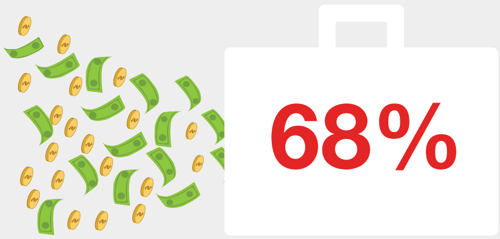
Hiscox is a specialty insurance company with offices in major cities across the US and part of the $3 billion Hiscox Group, with over 100 years of history and staff in 13 countries. Hiscox Insurance Company Inc. is rated A (Excellent) by A.M. Best and licensed to do business in all 50 states and Washington, D.C.

Hiscox strives to be a long term partner for clients, giving them the courage to build their business. Hiscox specializes in helping our clients manage and mitigate employee theft and other executive risks through a balanced blend of underwriting acumen, innovative thinking and service in both underwriting and claims.

Every company is at risk

Companies of any size are at risk for embezzlement. While small and mid-sized companies continue to be disproportionally victimized by employee theft, larger companies suffer a higher median loss.



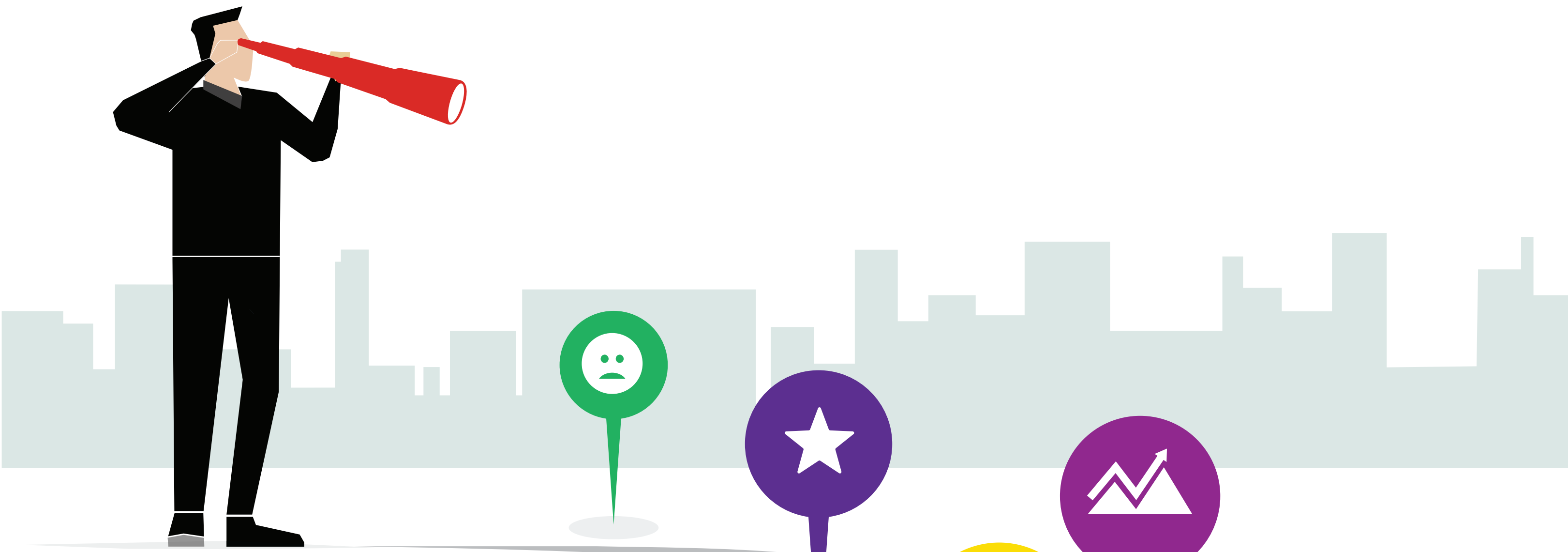


Embezzlement by number of employees

68 percent of cases occurred at companies with fewer than 500 employees.

Warning signs of embezzlers

When an embezzler is discovered, particularly after a long-running scheme, those in charge often ask, “Why didn’t I see this sooner?” To catch a thief, you need to know the warning signs. Here are some common characteristics.



Intelligent and curious

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

Extravagant

Embezzlers will often flaunt their wealth, so watch for employees who are clearly living a lifestyle that is out of proportion to their salary.

Egotistical risk-taker

Rule breaker in and out of work life – from speeding tickets to overusing ‘sick time.’

Diligent and ambitious

An embezzler may come in early and leave late, and never take vacations. This can appear to be dedication to the company, but in fact it is an effort to keep from being found out.

Disgruntled

An employee who feels they are being treated unfairly may be tempted to steal to ‘even the score.’ They may be unable to relax, or may experience severe changes in behavior.

Anatomy of a long-running scheme

Many of the largest cases of employee theft involve schemes that repeatedly divert small sums of money over time, making them difficult to detect. These schemes can continue for years, even decades, and the losses are often staggering when they are totaled up.

The longest-running scheme we found went on for an astonishing **41 years**.

$2.2 million
Five years or more

$5.4 million
Ten years or more

The average loss for cases that continued for five years or more was $2.2 million, and for schemes of ten years or more it was $5.4 million.

29%
of employee theft schemes persisted for more than five years.

37%
of schemes in financial services lasted longer than five years.

Bad actors working alone
Most long-running schemes involve individual employees working alone.

Funds Theft

Check Fraud

Most common schemes
The most common methods used in long-running schemes were check fraud and funds theft.

A scheme dating back to the Carter administration?

It's hard to fathom a scheme lasting the better part of four decades, but with two sets of books, an Iowa credit union employee orchestrated a theft from the time of her hiring in 1978 until 2015. The bookkeeper withdrew funds and funneled customers' deposits into accounts held by her and her children. As a result of the $2.5 million embezzlement, the credit union became insolvent and was forced into liquidation.

> **"We need to dispel the myth that embezzlement is all about elaborate schemes constructed by financial wizards. Oftentimes the most damaging cases result from simple skimming of relatively small amounts over time; just enough to fly below the radar. There may be no long-term diabolical plot at all. The employee errs, thinking 'I'll never do it again.' And it gets easier and easier to do the next time, and the next."**

M. Jeffrey Beatrice
Partner at Bradley

Former Managing Director and General Counsel for Anti-Money Laundering at Citigroup and longtime Assistant United States Attorney in the District of Columbia

A whopping $54 million loss

In a case involving the largest dollar loss in this year's research, a private equity fund manager was implicated in an elaborate $54 million embezzlement scheme. The indictment alleges that over a decade, the employee submitted false invoices, substantially overstated the prices of international business deals, and set up fraudulent bank accounts in the employer's name and the companies in which his employer invested.

> **"During my time with the FBI, I saw a number of devastating cases of employee theft. Oftentimes, the perpetrators of the long-running schemes were trusted individuals who were perceived by the business owners to be part of the inner circle."**

Jerome C. Pontrelli
12-Year Veteran
Federal Bureau of Investigation

Executive privilege, executive theft

One of the more egregious forms of embezzlement occurs when executives, arbiters of leadership and professional integrity, breach corporate trust. In a case ongoing in Minnesota federal court, six executives were indicted for conspiring to steal more than $20 million from their employer. Their decade-long scheme included controlling a complicated web of sham companies and dummy entities, awarding themselves restricted stock and embezzling funds.

> **"In prosecuting embezzlement schemes, I was always struck by a strange psychology. The more times an employee gets away with stealing a small amount, the more emboldened he or she becomes. Of course, the opposite is true: the persistent fraudster leads him or herself inexorably to being revealed as the culprit."**

M. Jeffrey Beatrice
Partner at Bradley

Former Managing Director and General Counsel for Anti-Money Laundering at Citigroup and longtime Assistant United States Attorney in the District of Columbia

At-risk businesses

No industry is immune from employee theft, but it is more prevalent in some industries than others. **Here's a breakdown of the most-targeted sectors.**

FINANCIAL SERVICES

- Most cases for the third year in a row.
- This sector had the highest single loss at $54 million, as well as the highest total loss at over $120 million.

MUNICIPALITIES/ GOVERNMENT

- The median loss of $68,705 was among the smallest of any industry.
- Most of the embezzlers were employees, and most theft happened at small organizations.

MANUFACTURING

- Tied for the second largest single loss at $20,000,000.
- Managers made up the highest proportion of embezzlers (57.5%) compared to employees (35%).

REAL ESTATE/ CONSTRUCTION

- Managers were much more likely to steal than employees.
- Check fraud and direct funds theft occur equally in cases, but check fraud was responsible for 3.5x higher dollar losses.

LABOR UNIONS

- 92% of fraud occurs at organizations with fewer than 100 employees.
- Nearly two-thirds of theft was committed by managers.

HEALTHCARE

- Targeted equally by managers and employees, although managers stole considerably higher sums of money.

RETAIL

- 76% of cases happened at companies with fewer than 100 employees.
- Employees were responsible for more cases at nearly 65%.

IT/TELECOM

- Represented just 3.3% of cases but 9% of dollar losses, with the highest median loss at $2.4 million.
- Managers were much more likely to be perpetrators than employees.

Even nonprofits are vulnerable

Twenty-two percent of total cases involved nonprofit entities with a median loss of approximately $118,000. Over 80% of the nonprofit cases occurred in organizations with less than 500 employees. Of the nonprofit perpetrators, nearly one-third were over 55 years old and 60% were men. Check fraud and funds theft were the primary schemes for the nonprofit cases.

Industry Class	% of Cases	Median $ Loss
Financial Services	17.8%	273,843
Municipality/Government	12.4%	68,705
Manufacturing	10.2%	558,172
Real Estate/Construction	9.6%	352,805
Labor Union	6.1%	36,647
Other Services	6.1%	165,000
Healthcare	5.1%	437,016
Retail	4.3%	485,800
IT/Telecom	3.3%	2,400,000

Common themes, common schemes

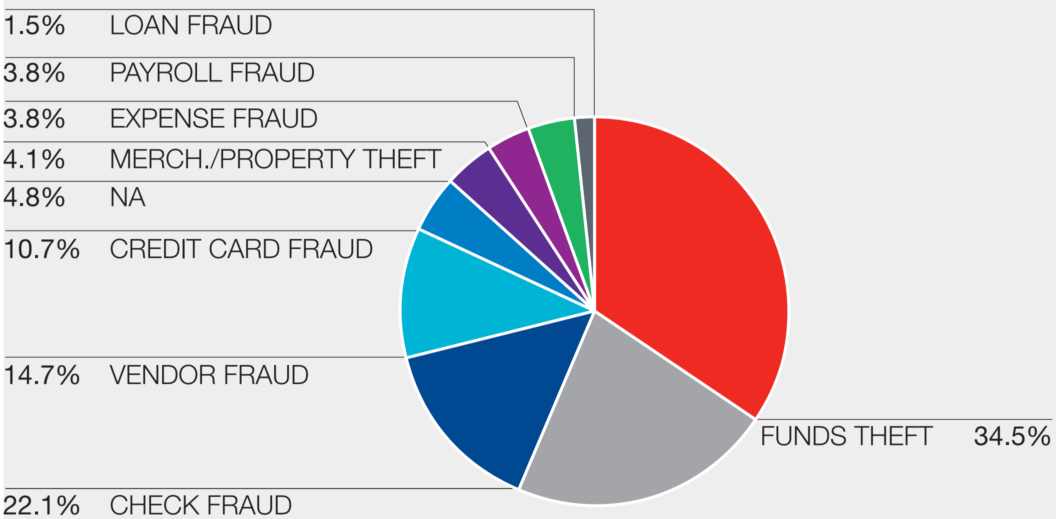
There is more than one way to embezzle money, and many perpetrators will use more than one method. Whether it's the simplest approach or the most complex, understanding how these schemes work helps in prevention.

Schemes	What is it?	How it's done
Funds Theft accounts for 34.5% of cases, and 56% of cases perpetrated by women.	Perpetrators take cash or bank deposits and transfer the funds to an account they control.	The accountant for a property management company directed company funds to a personal account which she used to pay her personal expenses, embezzling over $1 million over a five-year period.
Check Fraud is used in 22.1% of cases. Managers committed more than half of check fraud cases, and nearly 70% occurred at small companies.	Checks are altered or forged to be made payable to the perpetrator.	The office manager for a Washington, D.C. lobbying firm issued company checks to herself, making false entries in the firm's books to cover her theft.
Vendor Invoicing and False Billing is responsible for 14.7% of cases but accounts for 42% of dollar losses.	Invoices from vendors are fabricated or inflated, or fictitious vendor companies are invented.	An instructor at a marine training institute issued false invoices for navigation training certifications and pocketed the payments, netting over $300,000 over a six-year period.
Credit Card Fraud accounts for 10.7% of cases. 60% of these schemes were perpetrated by managers, and more than half occurred at small companies.	Company credit cards are used for personal purchases, or unauthorized credit cards are issued.	The financial secretary of a labor union had a union credit card that he used for personal expenses, including a family vacation to Bermuda.
Merchandise/ Property Theft is responsible for 4.1% of cases.	The perpetrator steals property or merchandise belonging to the company. This may be the most underreported category of employee theft.	An art handler stole $600,000 worth of artwork from a New York dealer, which he then attempted to sell at a flea market.
Expense Fraud makes up 3.8% of cases.	Expenses that are reimbursed by the company are fabricated or inflated.	The vice president in charge of the credit card program at a defense contractor used his credit card for personal purchases, then replaced the charges with fabricated business expenses.
Payroll Fraud accounts for 3.8% of cases. Nearly two-thirds of perpetrators were women and three-fourths of cases were at small companies.	The perpetrator pays fictitious or terminated employees and diverts the funds to personal accounts.	For nearly ten years, the payroll clerk at a jewelry company processed direct deposits into a personal account in the names of several former and fictitious employees.
Loan Fraud is used in 1.5% of cases.	An embezzler takes out a loan in the name of the business but diverts the proceeds to an account in their control.	A loan officer forged customers' signatures and falsified loan documents in order to embezzle funds that she used for personal expenses.

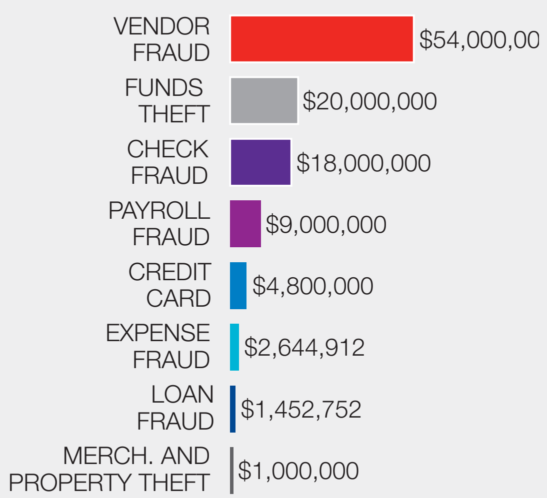
How the data breaks down

Funds theft was used in the most cases, but vendor fraud produced the largest losses. Nearly every case employed one or more of these methods.

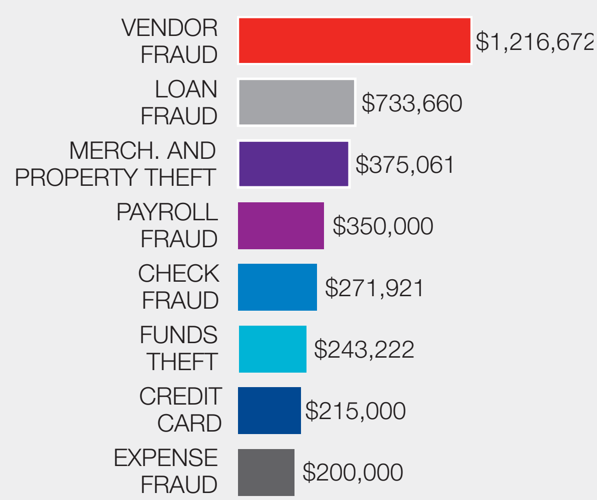
Federal cases by primary scheme type



Maximum Loss by Scheme Type



Median Loss by Scheme Type



Meet your chief embezzlement officer

Steve Stickyfingers is the President and Chief Executive Officer of a venture capital firm. Here's how he became a thief.

1 Founded firm
Steve started the VC firm seven years ago, and soon brought in several other investors to take advantage of all of the great investment opportunities that were available.

2 Worked hard
The other investors received profits based on the percentage of their investment in the company. Steve felt that he was doing most of the work, so he began to resent how little the others were contributing relative to their share of the profits.

3 Big payout
The company had invested in a startup that was about to be acquired by a large company. The payout for the VC firm would be significant, and it would be divided based on each investor's stake in the company.

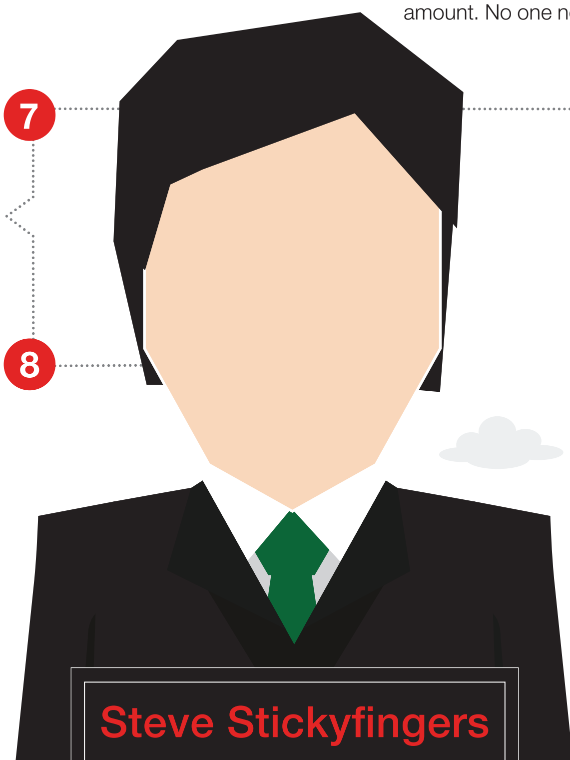
4 Resentment
Steve felt this was unfair, so he set up a separate account in the name of the company with himself as the sole signer. He diverted 20% of the company's payment upon the sale of the startup into this new account, understating the revenue to the other investors by the same amount. No one noticed.

5 Funds siphoned
For the next four years, Steve used this and other tactics to siphon funds from the company to his own account. He then wrote checks from the account to fund a lavish lifestyle that included several homes, a boat, expensive cars and lengthy vacations.

6 Unraveled during vacation
It was during one of these vacations that Steve's scheme was discovered. One of the portfolio companies decided to buy back the equity the VC had acquired, and a large payment came into the company unexpectedly. One of the other investors gave it to the bookkeeper, and she offhandedly mentioned that she would deposit 20% in the account opened by Steve and the rest in the corporate account, as she had been trained to do. This triggered suspicion, and after a quick examination of the company's records, Steve's scheme began to unravel.

7 $4.5 million shock
The other investors were shocked at the brazenness of his actions, which ultimately defrauded them of $4.5 million over the course of four years.

8 Above Suspicion
They were also shocked at how simple it was. A C-suite title, combined with the fact that he was the founder of the company, put Steve above suspicion.



As with similar embezzlement crimes, Steve needed the following things to get away with this kind of theft:

Means
There were large sums of money coming into and going out of the company with some regularity. As CEO, Steve had control over the money and over the staff who handled it and was able to ensure his separate account went undetected.

Motive
Steve was feeling under-appreciated by his partners, which prompted the first theft. Once he succeeded, he was motivated by greed to continue embezzling.

Opportunity
Steve took advantage of the fact that the other investors in the company maintained a hands-off attitude toward the company.

If you suspect an employee is on the take

Create a team
Put together a small team of trusted individuals to investigate. Share information on a need to know basis only.

Keep notes
About everything.

Review records
Begin a discreet review of records that may quickly confirm or refute your suspicions. Look for evidence among financial, payroll and personnel records

Contain damage
If the suspected employee works in finance and may be stealing from company bank accounts, restrict their access.

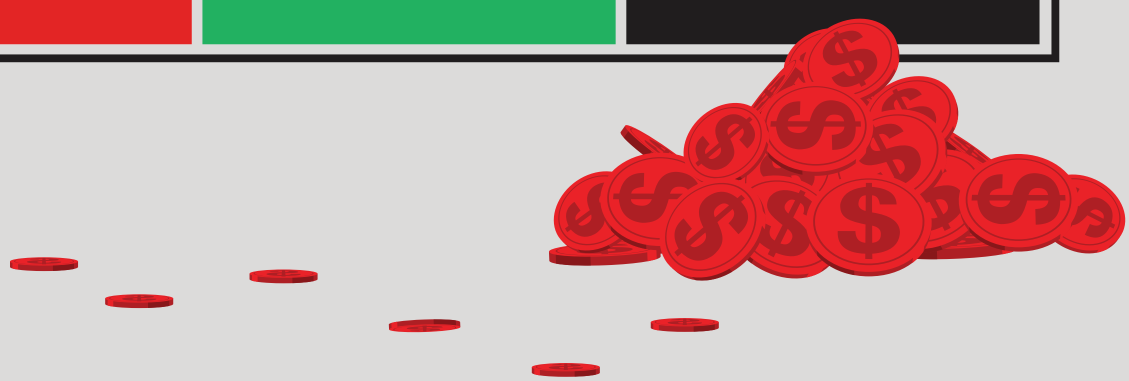
Find witnesses
Craft a list of potential witnesses. Remember, don't share information about the investigation outside the investigative team.

Fix internal controls
Figure out what went wrong. Fix the internal control failures that allowed for the theft.

Bring in help
Consider hiring outside counsel or consultants. They can help with complex investigations and offer more objectivity and credibility.

Report crime
If a loss is discovered, contact your insurance company to report it. Talk to a lawyer, and report the crime to law enforcement.

Praise honesty
If another employee raised the red flag, make sure to praise internal reporting efforts and let employees know the company values and rewards speaking up.



How to catch an embezzler

The losses from embezzlement extend beyond the balance sheet. The distraction it creates can reduce productivity and negatively impact corporate reputation and culture.

PREVENT

embezzlement before it happens.

- Institute a system of checks and balances, including a review of all bank statements and cancelled checks by someone other than the bookkeeper. Ensure that more than one person sees every transaction.
- Have corporate bank statements delivered to an owner or trusted executive, preferably at their home address.
- Perform complete background checks for all employees, putting those with accounting responsibility under particular scrutiny.

DETECT

fraud early to keep small losses from becoming larger.

- Watch out for employee lifestyles that don't match their salaries, especially if sudden changes seem to take place.
- Beware of the employee who comes in early, leaves late, and never takes a vacation. Don't ignore red flags because an employee has been with the company for a long time.
- Managers and even executives aren't immune to greed.

MITIGATE

the impact on your bottom line.

- If you find that someone has embezzled from you, press charges. Keeping it quiet sends the wrong message to other employees and makes it more likely the perpetrator will do the same thing at another company.
- Insure your business. In most cases, only a small fraction of embezzled funds are recovered, and demands for restitution are often unfulfilled. The right insurance coverage can make your business whole again.

What not to do

When you think an employee may be stealing, resist the urge to rush to judgment. Here are some things to avoid doing.

1. Don't jump to conclusions. Falsely accusing an employee of a crime can cause permanent damage to the individual and leave the company exposed to liability.
2. Don't conduct group interviews where potential witnesses are questioned together.
3. Don't interview an employee by yourself. Have an HR person in the room with you. Take good notes during the meeting and write a summary right after the interview.
4. Don't rush to confront the suspicious employee. You have one chance to question someone for the first time. Be prepared and armed with evidence. An incriminating email or financial record can improve your chances of getting the truth.
5. Never interfere with law enforcement. Cooperate, cooperate, cooperate. If you are worried about any exposure, hire a lawyer to maintain privileged communications.

> Employee embezzlement schemes are often the product of an absence of proper internal controls or a breakdown of those controls. Regular audits and control testing can help to mitigate exposure. And never underestimate the importance of adequate due diligence in the hiring process.
>
> **Steven J. Durham**
> Former Chief of the Fraud and Public Corruption Section
> United States Attorney's Office, Washington D.C.

Methodology

All information assembled in this report was derived from publicly available data on US federal court activity related to employee fraud. We focused on the federal system both for its uniform public reporting as well as the fact that federal actions generally involve larger and more complex schemes that illustrate the need for enhanced internal controls. Sources included public announcements from the Department of Justice, company websites and common news aggregators. These cases, almost 400 in total, either became publicly known or were active in the federal system during calendar year 2016, including where an arrest, charge, indictment, sentencing or other significant event occurred that revealed employee theft. The data set includes some 80 cases that appeared in prior studies and were reported again in 2016. While federal jurisdictions may have had additional cases related to employee fraud under investigation or in early stages of case development during 2016, we reported solely on those matters that have progressed to the point where they generated some manner of public announcement.

Organizations included in our results are public and private corporations, limited liability companies, municipal and government agencies, nonprofit organizations, and Native American tribal businesses. Companies of all sizes (employees <100, <500, and >500) were included in this report.

For the purposes of calculating various percentages for this report, we have occasionally excluded those cases for which the relevant information was not available or elected to exclude results where the findings were deemed insignificant due to the limited number (<10) of cases.

Where available, in calculating total loss to the organization we included any legal, accounting or other costs incurred by the organization to uncover the fraud. To establish regional percentages, we assigned cases to the location of the U.S. district court in which the case was filed. We organized our information in accordance with the U.S. Census Bureau's latest regional divisions. Puerto Rico was not included. In several instances, perpetrators utilized more than one scheme to defraud employers.

In cases of multiple schemes, we listed as primary the scheme that resulted in the greatest loss to the organization or the scheme most often utilized by the perpetrator. Where that information was not available, we assigned primary scheme to that which was listed first by the U.S. Attorney's office prosecuting the case. With regard to larger organizations, we assigned company size based on the number of employees of the whole organization rather than a specific branch/location. We did not include cases involving kickback schemes if it was not clear that employee theft occurred. Scheme type year-over-year comparisons were excluded from our calculations as the classifications and filters (e.g. company size) changed from last year to this year.

Hiscox
520 Madison Avenue
32nd floor
New York
NY 10022

T 646 442 8322
www.hiscoxbroker.com

Doug Karpp
SVP, National Product Head — Crime and Fidelity
doug.karpp@hiscox.com
+1 213 412 1223

HISCOX
encourage courage®