



*The 2015 Hiscox Embezzlement Watchlist:*

---

A Snapshot of Employee Theft in the US

# CONTENTS

---

Introduction ..... 1

The At-Risk Organization..... 2

Common Themes, Common Schemes ..... 3

Industries in Focus ..... 4

The Employee, The Perpetrator ..... 7

Managing Exposure, Mitigating Risk ..... 9

Methodology..... 11

## ABOUT US

Hiscox USA is a specialty insurance company with offices in major cities across the US and a part of the \$3 billion Hiscox Group, with over 100 years of history and staff in 14 countries worldwide. Hiscox Insurance Company Inc. is rated A (Excellent) by A.M. Best and licensed to do business in all 50 states and DC.

We strive to be a long-term partner for clients and give 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.

# INTRODUCTION

---

Employee theft corrodes trust, damages culture and can have a devastating financial impact on organizations. The typical organization loses 5% of revenue each year to fraud, a potential projected global fraud loss of \$3.7 trillion annually according to the ACFE 2014 *Report to the Nations* study of global fraud.

Understanding the dynamics of employee theft enables organizations to more effectively detect, deter and mitigate risks related to employee theft. The Hiscox Embezzlement Watchlist examines employee theft cases that were active in US federal courts in calendar year 2014. We focused specifically on entities with fewer than 500 employees to provide a better understanding of the range of employee theft risks these organizations face.

More than **40%**

of thefts were committed by an employee in the finance/accounting function



Four of every five victim organizations had fewer than 100 employees; just over half had fewer than 25 employees

**21%**

of employee thefts involved an organization in the financial services category, which includes banks, credit unions and insurance companies

AVERAGE LOSS  
**\$842,403**

MEDIAN LOSS  
**\$280,000**

While we see women orchestrating the majority (61%) of actions across the data set, their schemes resulted in a median loss of **\$243,447** nearly 30% less than their male counterparts

**32%**

of cases involved projected losses in excess of \$500,000; over 19% in losses of \$1 million or more

More than **1/3** (35%) of cases involved multiple schemes

**50**  
The median age of the perpetrator

# THE AT-RISK ORGANIZATION

The majority of employee thefts are occurring in organizations with 500 employees or less. The sizes and types of thefts vary by industry, but smaller organizations across the spectrum exhibited high incidences of embezzlement overall.

## The unfortunate reality of employee theft is every organization is at risk.

When we looked at the totality of federal actions involving employee theft over the calendar year, nearly 72% involved organizations with fewer than 500 employees. Within that data set, we found that four of every five victim organizations had fewer than 100 employees; more than half had fewer than 25 employees.

Is there a connection between the size of an organization and the size of the loss? Our research suggests that there may be. While some of the largest losses occurred in organizations with fewer than 50 employees, in the aggregate, we note the following:

Our findings support the assumption that financial services organizations were squarely at risk. Indeed, over 21% of employee thefts, the largest industry concentration in the data set, involved an organization in the financial services category, including banks, credit unions and insurance companies.

Other organizations with a high concentration of employee thefts were non-profits (11%), labor unions (9%) and municipalities (10%). Surprisingly, those organizations with a mission to serve others had the highest incidence of employee theft.

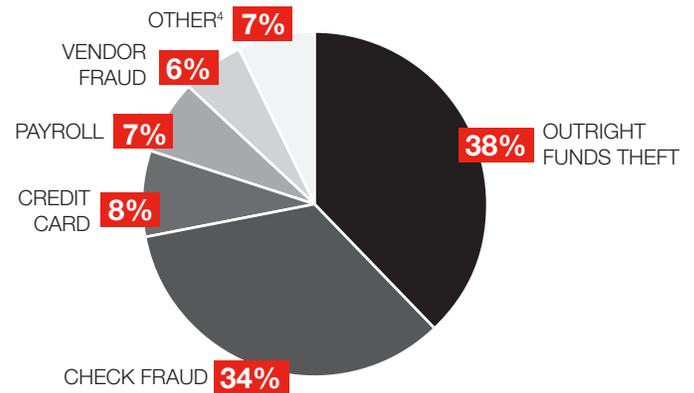
Organizations in the financial services, real estate/ construction and non-profit sectors had the greatest number of cases in our data set, while retail entities and the healthcare industry had the largest median losses.



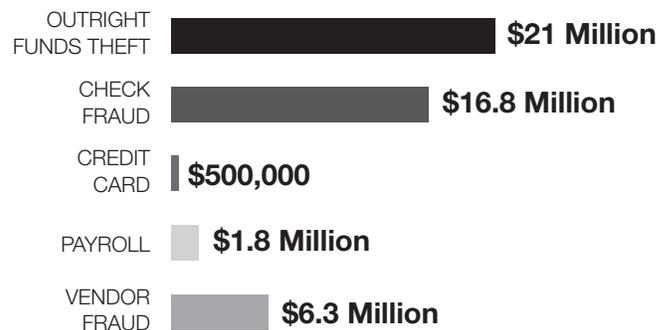
# COMMON THEMES, COMMON SCHEMES

- ▶ **Outright Funds Theft**, which includes the direct theft of cash or misuse of bank deposits or transfers, resulted in nearly three-fourths of total losses. Women accounted for 60% of the perpetrators.
- ▶ **Check Fraud** occurs when a perpetrator alters, forges, or makes payable to himself checks or money orders as part of a scheme to divert funds. Individuals in management positions were responsible for over 60% of these cases. 81% of cases occurred in companies with fewer than 50 employees.
- ▶ **Credit Card Fraud** involves the fraudulent use, authorization, or creation of an employer's credit or debit cards. 60% of the frauds were initiated by a person in a management role. 80% of credit card fraud cases occurred in companies with fewer than 50 employees.
- ▶ **Payroll Fraud** occurs when an employee uses the payroll system to issue checks to himself, others or otherwise divert payroll funds. More than three-quarters of the perpetrators in payroll frauds were female. Almost two-thirds of the actions involved organizations with fewer than 50 employees and almost 90% of the cases involved companies with fewer than 150 employees. Nearly 30% of payroll theft was committed in the municipal sector.
- ▶ **Vendor Fraud** involves a perpetrator diverting employer funds through the creation and submission of false invoices issued by fictitious companies. A full two-thirds of these cases were committed by males, with an average age of 51 years.

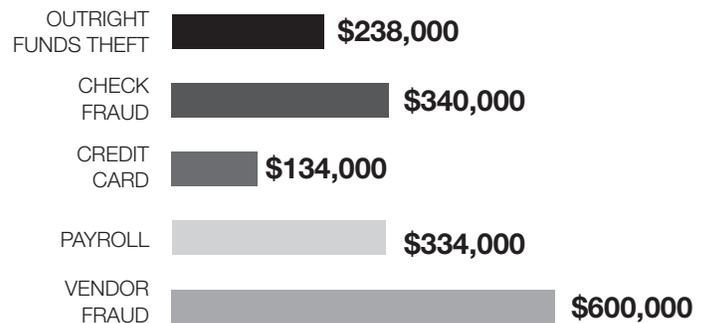
## FEDERAL CASES BY PRIMARY SCHEME TYPE<sup>3</sup>



## LARGEST LOSS BY SCHEME TYPE



## MEDIAN LOSS BY SCHEME TYPE



<sup>3</sup> Based on our analysis of cases for U.S. firms with less than 500 employees.

<sup>4</sup> We do not analyze case types where there were fewer than 10 cases in a given category.

SECTOR	MEDIAN LOSS	PERCENT OF SAMPLE
 Retail	\$606,012	5%
 Healthcare	\$446,000	7%
 Real Estate/ Construction	\$300,000	13%
 Municipalities	\$293,717	10%
 Financial Services	\$271,000	21%
 Professional Services	\$234,641	5%
 Non-Profit	\$202,775	11%
 Other <sup>1</sup>	\$174,473	6%
 Labor Unions	\$41,599	9%

Typical business and property insurance policies often don't cover employee theft.

# INDUSTRIES IN FOCUS<sup>2</sup>

## RETAIL

- ▶ While employee theft in the retail segment was relatively uncommon in our sample (5% of the cases), the median loss in these cases was significantly higher than others at \$606,012
- ▶ Smaller organizations—those with fewer than 50 employees—accounted for nearly 70% of these matters
- ▶ The largest theft was a \$17 million check fraud and credit card scheme perpetrated for eight years by a male executive in a family-owned and operated bakery

## HEALTHCARE

- ▶ While actions in the Healthcare segment represented just 7% of the total surveyed, this sector reported a high median loss of \$446,000
- ▶ The biggest loss, of \$3.7 million, involved a check fraud and credit card scheme perpetrated by a female office manager at a DC-based orthopedic medicine practice
- ▶ Women represented 82% of the perpetrators with a median age of 51
- ▶ 59% of the cases were perpetrated by employees in the finance/accounting department

<sup>1</sup> Of the fifteen companies in the other category, most relate to Native American businesses.

<sup>2</sup> Industries with 10 or more cases are included.



## REAL ESTATE/ CONSTRUCTION

- ▶ Fraud in this sector accounted for 13% of actions, with a median loss of \$300,000
- ▶ 43% of actions were perpetrated by individuals in management positions
- ▶ While 63% of the fraudsters were women and resulted in a median loss of \$257,000, fraud committed by males resulted in a median loss of \$448,000
- ▶ Check fraud and outright funds theft occurred most frequently, but the largest loss (\$3.9M) involved expense and payroll fraud



## MUNICIPALITIES

- ▶ Municipalities accounted for 10% of the fraud actions surveyed, with a median loss of \$293,717
- ▶ Check fraud accounted for half of the schemes in the municipal sector, with an alarmingly high median loss of approximately \$422,000
- ▶ 63% of the fraudsters held management positions



## FINANCIAL SERVICES

- ▶ 21% of the employee theft cases surveyed occurred in the financial services industry, with a median loss of \$271,000
- ▶ Females were responsible for nearly four out of five actions, yet thefts by males had 27% higher median loss of \$336,000
- ▶ Bank tellers committed over 30% of fraud, with outright funds theft used over 76% of the time



## PROFESSIONAL SERVICES

- ▶ While this sector accounted for just a handful of cases (less than 5% of the sample), the median loss was \$235,000
- ▶ More than half of the actions surveyed involved law firms
- ▶ 90% of the perpetrators were female with a median age of 45



## NON-PROFIT

- ▶ Non-profit organizations accounted for 11% of cases
- ▶ Almost two-thirds of the cases involved either check fraud (33%) or outright funds theft (30%)
- ▶ Over half (56%) of the crimes were committed by individuals in management positions, with a median loss of \$183,354
- ▶ Two-thirds of the cases involved organizations with fewer than 50 employees, with a median loss of \$530,000



## LABOR UNIONS

- ▶ Labor Unions accounted for 9% of the sample, with a median loss of \$42,000
- ▶ Males committed 73% of the frauds
- ▶ While 68% of the cases involved individuals in management positions, the biggest theft resulted from a payroll fraud orchestrated by an executive secretary, with a loss of \$206,000
- ▶ More than half of the cases involved individuals in the finance/accounting department

According to Hayes International's 26<sup>th</sup> Annual Retail Industry Survey, one in every 39.5 employees was apprehended for employee theft in 2013, up 6.5% over the prior year.

## LARGEST SCHEME BY REGION

### MIDWEST:

A grain elevator manager colluded with a farmer to steal more than **\$6.7 million** from his employer



### NORTHEAST:

The COO of a natural gas drilling company conspired to embezzle more than **\$9 million** in forged checks and phony invoices



**\$3.3 million**



### WEST:

A security company fell victim to a **\$3.3 million** scheme perpetrated by its controller

**\$6.7 million**

**\$9 million**

**\$21 million**



### SOUTH:

A bank director charged with investing a local bank's capital, stole, misappropriated and embezzled more than **\$21 million**

## IN PLAIN SIGHT

A 62 year old teller at a small local bank in Illinois stole some \$2 million over a 17 year period. She had access to the vault and personally participated in audits of how much cash was on hand. She disguised the embezzlement by representing that a currency bag contained cash when the bag was just stuffed with other empty bags.

# THE EMPLOYEE, THE PERPETRATOR

---

Employees who embezzle breach the trust their organizations place in them. Most instances of employee theft involve employees with long tenures. Organizations can better protect themselves by understanding the characteristics of a typical embezzler.

- ▶ Women represented more than 60% of employee perpetrators
- ▶ The median age of wrongdoers was 50
- ▶ More than 40% of the actions surveyed were perpetrated by a professional in a finance or accounting role
- ▶ Just over half of all employee theft schemes (53%) were perpetrated by employees in senior roles within the organization, with those stakeholders engaging in schemes with a median loss of \$313,939<sup>5</sup>
- ▶ Non-management employees perpetrated 43% of embezzlements with a median loss of \$234,641

## COMMON MYTHS

---

*“My employees are seasoned professionals.”*

*“We do background checks.”*

*“Employees would never steal from a non-profit.”*

*“They’ve been with me for years.”*

*“Nobody signs checks but me.”*

*“Thieves are disgruntled; my people are happy here.”*

*“The office manager is on top of everything.”*

*“We’re a close-knit organization, like family.”*

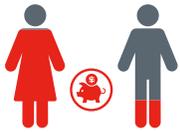
<sup>5</sup> In examining the positions of employee fraudsters, we excluded principals from the calculations. Business owners account for 4% of all actions surveyed.

## EYES ON THE GATEKEEPER

While companies often staff audit teams with employees from the accounting and finance function, our research shows that fraudsters in these positions accounted for more than 40% of the schemes surveyed. And in some cases, the fraud starts where the buck stops: the CFO. In one such action in New Jersey, the accused CFO was suspected of diverting more than \$6 million from the company to pay a host of personal expenses such as real estate taxes, motor vehicle costs and credit card bills. For a full seven years, the CFO designated his own business as a company vendor, cutting checks for services that were never performed, which he deposited into his personal bank accounts. He was asked for copies of the invoices, prosecutors said, but he informed colleagues he kept the invoices in his office.

## PROFILES OF SCHEMERS

### Financial Services

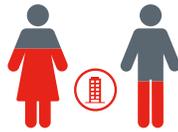


78% 22%  
FEMALE MALE

MEDIAN AGE: 45

MOST COMMON POSITION:  
Teller

### Real Estate/Construction



63% 37%  
FEMALE MALE

MEDIAN AGE: 46.5

MOST COMMON POSITION:  
Bookkeeper

### Non-Profit



63% 37%  
FEMALE MALE

MEDIAN AGE: 51

MOST COMMON POSITION:  
Bookkeeper or Executive Director

### Healthcare



82% 18%  
FEMALE MALE

MEDIAN AGE: 49

MOST COMMON POSITION:  
Business Manager/  
Office Manager

### Municipalities



67% 33%  
FEMALE MALE

MEDIAN AGE: 58

MOST COMMON POSITION:  
Business Manager/  
Office Manager

### Labor Unions



27% 73%  
FEMALE MALE

MEDIAN AGE: 48

MOST COMMON POSITION:  
Treasurer

### Professional Services



91% 9%  
FEMALE MALE

MEDIAN AGE: 44

MOST COMMON POSITION:  
Bookkeeper

### Retail

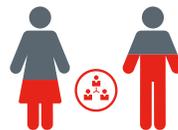


46% 54%  
FEMALE MALE

MEDIAN AGE: 49

MOST COMMON POSITION:  
Office Manager

### Other



40% 60%  
FEMALE MALE

MEDIAN AGE: 51

MOST COMMON POSITION:  
General Manager/  
Office Manager

## Know what you don't know:

Background checks will only turn up criminal convictions. Not settlements. Not slaps on the wrist. And not suspicions.

# MANAGING EXPOSURE, MITIGATING RISK

---

With 58% of cases surveyed by the ACFE showing absolutely no recovery of losses, maintaining adequate coverage to insure against crime-related losses is mission critical to every organization.

While no entity can completely insulate itself from employee misconduct, there are critical steps every organization should take to minimize the likelihood and impact of losses related to employee theft. Even the most basic controls may have prevented many of the criminal actions in our study by creating a 'perception of detection,' which is the most powerful deterrent to employee wrongdoing. Risk mitigation tactics are particularly important for small to medium-sized businesses, which can be devastated by an employee theft incident.

▶ **ESTABLISH BEST PRACTICES IN THE ACCOUNTING DEPARTMENT.**

We encourage businesses to mandate dual signatures or dual review on disbursements (checks and wires). It is also important to create separation in key business processes. For instance, separate the money from record-keeping so that no single employee can control a process from beginning to end and don't let the accounts payable person reconcile bank accounts.

▶ **BRING FRAUD DETERRENCE INTO THE LIGHT.**

Provide a short training session for all employees to illustrate the damaging impact of fraud and abuse and provide practical advice on how to spot fraud.

▶ **SET 'TONE AT THE TOP'.**

Have everyone from management, audit and the leadership team talk about fraud prevention. Be sure employees are aware of internal controls and ask employees if they know of any weaknesses in the controls and how to improve them. Hotlines are an excellent way to promote reporting of misconduct and reflect a culture of integrity. According to the ACFE, more than 40% of all cases were detected by a tip, nearly half of which came from employees.

▶ **CONDUCT COMPREHENSIVE AUDITS THAT SPECIFICALLY LOOK FOR FRAUD.**

Surprise audits are particularly effective because fraudsters will not have time to alter, destroy or misplace records and other evidence.

## A FAMILY AFFAIR?

Twelve years. Nearly 2,500 acts of theft. Close to \$1 million stolen. The perpetrator, a 63 year old woman who served as Treasurer of two real estate-related entities in Missouri. In astonishing brazenness, the perpetrator paid thousands of dollars from company accounts to her son and teenage daughter for unauthorized work; she gave her daughter a company credit card and paid her elderly mother for services never performed. When the partners discovered the scheme, they allowed her to stay on with a promise to clean up her act. But she continued to steal, even after her employment was terminated. As if the embezzlement wasn't enough, she sabotaged the company's books, stealing years of records and using her son to clear computers and password-lock important documents. The company principals filed a civil suit to recoup losses but couldn't afford to maintain the litigation.

▶ **THOROUGHLY SCREEN PROSPECTIVE EMPLOYEES.**

Background checks are a good place to start, but keep in mind that they do not reveal arrests without convictions, let alone plea deals and settlements. The comprehensive screening should also include credit checks (where allowable), reference checks and interviews. Don't be afraid to ask about an employment gap. We've heard many stories where a fraudster had submitted a resume with an employment gap and was never asked about it...only to find out that they had been serving prison time for embezzlement from their prior employer.

▶ **MIND YOUR VENDORS.**

Do not retain vendors that are owned by friends or family of existing employees. Conduct background checks on all vendors and always separate the vendor approval process and authorization of payments to vendors.

▶ **RESPOND TO SUSPECTED THEFT SWIFTLY.**

Where fraud is suspected, leadership should immediately retain legal counsel to conduct an internal investigation. This is critical to protect organizational interests on many fronts including discouraging copycat actions and potential employment claims down the road. Appropriately determining the nature and extent of the loss and who is responsible will facilitate civil actions to recover stolen funds and enhance the entity's ability to recover restitution if a referral to law enforcement is made. Law firms with experience in white collar crime will also have recommendations for forensic accountants and can hire those firms to work hand-in-hand with legal counsel under the protection of the attorney-client privilege.

▶ **MAINTAIN APPROPRIATE INSURANCE COVERAGE.**

With 58% of cases surveyed by the ACFE showing absolutely no recovery of losses, maintaining adequate coverage to insure against crime-related losses is mission critical to every organization. This means understanding the limits and exclusions of existing and prospective policies. Typical business owner's and property insurance policies often exclude coverage for employee thefts. The best protection against employee theft is a strong crime policy, which typically includes:

- ▶ a broad definition of employee including coverage for employees known to have prior incidents of theft or dishonesty
- ▶ no conviction requirement for coverage to apply
- ▶ coverage for theft from the organization and any of its clients
- ▶ coverage for theft perpetrated by employees of vendors

Good crime policies also include coverage for losses caused by outsiders through cyber deception, social engineering, vendor theft, funds transfer fraud, computer fraud, telephone toll fraud and other instances of misconduct. Crime policies can even be written to cover expenses such as hiring an investigator to respond to a possible loss.

Three Tips for Small Business Owners: (1) send bank statements directly to your home for a review to ensure they can't be falsified prior to reconciling accounts (2) periodically review payroll reports to look for anomalies (3) sign all of the checks yourself or keep the signature stamp under lock and key.

# 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, Federal Bureau of Investigations, the Internal Revenue Service, company websites and common news aggregators. These cases, nearly 350 in total, either became publicly known or were active in the federal system during calendar 2014, including where an arrest, charge, indictment, sentencing or other significant event occurred that revealed employee theft. While federal jurisdictions may have had additional cases related to employee fraud under investigation or in early stages of case development during 2014, 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.

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.

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.



**DOUG KARPP**

*SVP, National Underwriting Leader –  
Crime & Fidelity*

doug.karpp@hiscox.com

+1 213 412 1223

**[www.hiscoxbroker.com](http://www.hiscoxbroker.com)**

HISCOX  
520 MADISON AVE., 32ND FLOOR  
NEW YORK, NY 10022

© 2015 Hiscox Inc. All rights reserved.