



# THE 2016 HISCOX

## Embezzlement Study

A report on white collar crime in America

# Introduction

The impact of employee theft can rock an organization to its core. It threatens the trust employers place in their teams, damages morale, and can cause financial devastation. In 2015, the first Hiscox watchlist shed light on at-risk organizations and the profile of a perpetrator. This year we dig deeper into why seemingly good people go bad, and further highlight the greater risk of embezzlement for mid-sized and smaller organizations. Managing an employee's control of and access to transactions is key to preventing and detecting embezzlements.

The 2016 Embezzlement Study incorporates employee theft cases that were active in the US federal court system in 2015, specifically those cases occurring in companies with fewer than 500 employees, which represents 69% of all Federal cases reviewed.

**Hiscox**

Encourage Courage

## Embezzlers by the numbers



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

More than **40%**

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



One out of every three employee thefts involve organizations in financial services or non-profit industries.

**AVERAGE LOSS**  
consistent with 2015 report

**\$807,443**

**MEDIAN LOSS**  
increased by 5%

**\$294,354**

**36%**

of cases involved projected losses in excess of \$500,000

**49**

The median age of the perpetrator

**Women** commit more embezzlements (56.3%), but **men** are close behind (increasing 5% over prior year)

**20%**

of losses involved \$1million or more.

# Contents

---

The criminal next door .....	4
Why good people go bad .....	5
Every company is vulnerable .....	11
Common themes, common schemes .....	13
How companies protect themselves .....	16
Cyber deception .....	17
Methodology .....	18

---

## 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.

# The criminal next door

Embezzlers vary in age, profession, and motivation, but the commonalities are that they're often the most trusted and least expected.

## Meet Helen Helps-Herself



1

### Unexpected Culprit

**Fifty-one** year old Helen Helps-Herself has been the **bookkeeper** for a construction company for **twelve years**.



2

### Desperate Times

Helen's **husband got sick** and couldn't work. The lack of income and family medical expenses make Helen desperate. She **'borrowed'** some money from her employer until they got back on their feet by writing a \$5,000 check to herself, juggling the books to cover it up.



3

### Under the Radar

**No one noticed** the missing money, so Helen wrote another check to herself, recording it as payment to a vendor in the books. Again, no one noticed. The pattern continued for **four years**.



4

### Living in Excess

Eventually the medical bills were paid off, but Helen continued to write the checks. She bought **new furniture** and put a **new deck** on their house.



5

### Caught Red Handed

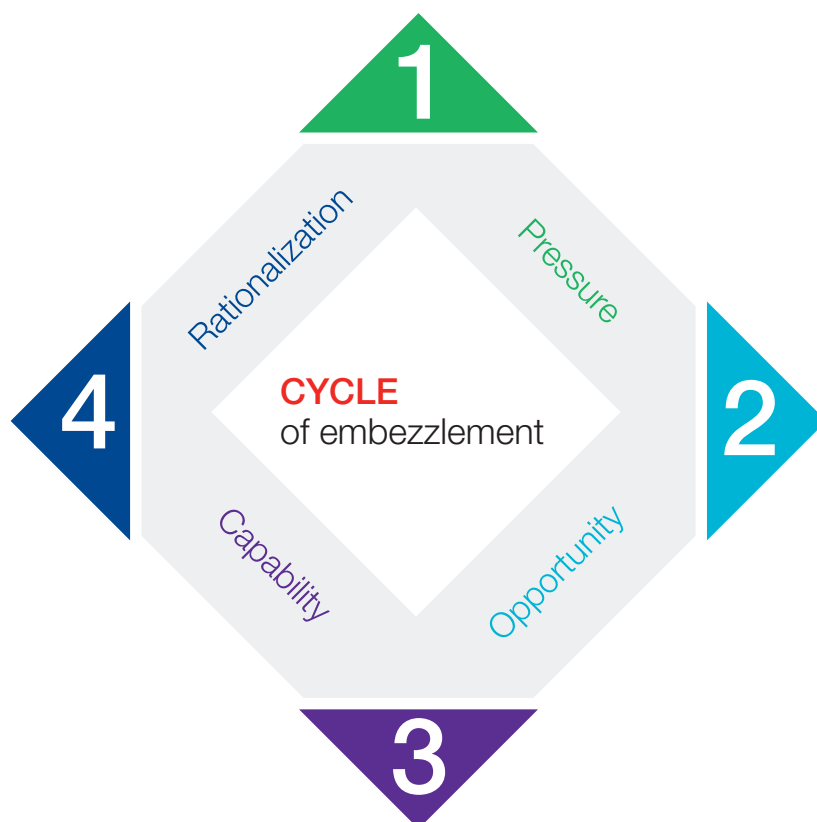
A vendor whose account she had marked as paid contacted the company CEO looking for their unpaid funds. Careful examination of the company's books showed that Helen had helped herself to just over **\$300,000**.

Helen's scheme succeeded because she was a long-time **trusted employee** with **sole control** of the company's bookkeeping.

# Why good people go bad

Why do people steal from the hand that feeds them? The motivations of embezzlers are often different from those of other criminals. Perpetrators are often regular people who are smart, well-liked, and those you'd least expect to steal. How does a trusted employee turn into a criminal?

- 📍 Motivation to start stealing money. For example, the employee may be under severe financial pressure at home and feel that they have no other option.<sup>1</sup>
- 📍 Access to money through title or tenure. Authority over controls allow older, more trusted employees to fix the books without detection.<sup>1</sup>
- 📍 Skills and knowledge to commit the fraud.<sup>1</sup>
- 📍 Theft often begins as a "loan" that the employee has every intention of paying back. The employee feels the loan is justified because they must provide for their family, consider themselves underpaid, or may even think others are stealing too! When they don't get caught, the cycle continues.



<sup>1</sup> Wolfe, David T. 'The Fraud Diamond: Considering the Four Elements of Fraud'. The CPA Journal. December 2004.

## Money matters

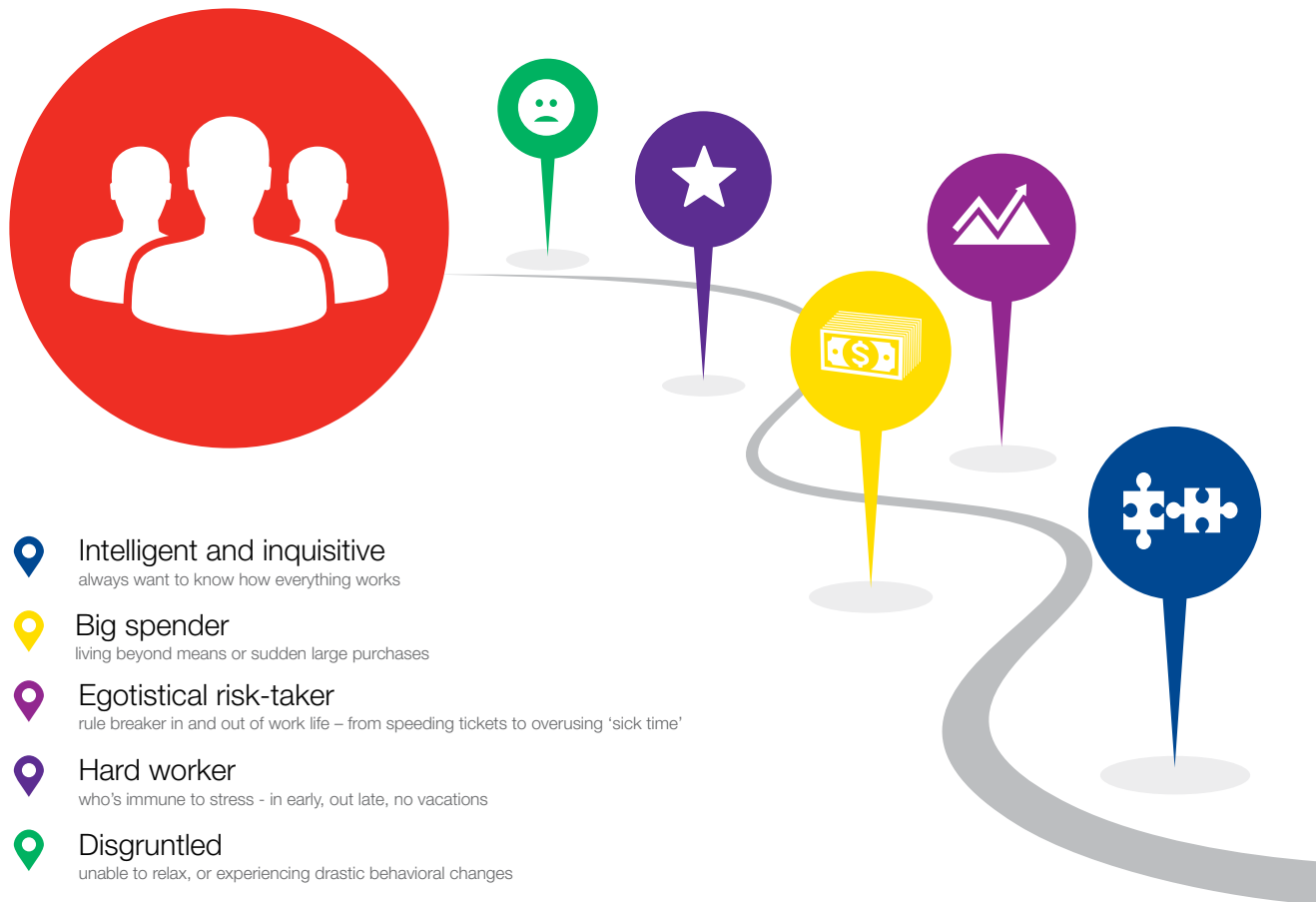
Could lower salaries for those who handle your money contribute to rationalizing embezzlement?<sup>2</sup>

Position	Median annual salary	Percentage of cases
Bookkeeping, accounting, and auditing clerks	\$37,250	11%
Office and administrative support	\$33,200	5%
Office clerks	\$29,580	5%
Tellers	\$26,410	4%

<sup>2</sup> Occupational Employment Statistics. May 2015. [http://www.bls.gov/oes/current/oes\\_nat.htm](http://www.bls.gov/oes/current/oes_nat.htm)

# Warning signs of an embezzler

Embezzlers may possess one or many of the following attributes.



## All about access

Those with the most access to and control over the money take the most. The positions with the highest frequency of embezzlement are made up of employees with the access to money or more tenured managers who oversee the financial controls.

### Median loss by position

Position	Median loss	% of sample
Controller/Comptroller	\$1,215,562	5%
CFO/CEO/COO	\$966,257	6%
Office Manager	\$529,666	4%
Teller	\$500,000	4%
Accounting/AP/AR	\$390,156	5%
Manager	\$370,000	10%
Bookkeeping	\$307,472	11%
Director	\$300,000	9%
Administrative	\$218,484	4%
Treasurer/Tax Collector	\$138,658	7%
President	\$110,000	5%
Employee	\$14,699	8%



# Every company is vulnerable

---

The majority of employee thefts occur in organizations with 150 employees or less, though the size and type of theft scheme vary by industry and region.

## Size matters

Year over year, our research suggests a connection between the size of an organization and its tendency for embezzlement.

Among small and medium-sized enterprises (SME's), organizations with fewer than 150 employees are particularly at risk with 82% of all embezzlement cases. Though it may seem counter-intuitive, smaller organizations with tight-knit workforces are particularly vulnerable precisely because employees are trusted and empowered.

82%

of cases in research took place in organizations with fewer than 150 employees



### % losses in sample by employee size

	2015	2014
1-150	82%	87%
151-250	11%	7%
251-500	7%	6%

# Different industries, different opportunities

The type of fraud embezzlers can commit varies by industry. What doesn't change, however, is the need for access to funds. In the majority of cases we studied, managers were more likely than employees to steal. **So who's guarding the guardians?**



## FINANCIAL SERVICES

- Remains the industry with the highest number of cases (17%) for the second year in a row
- One of three industries where more employees than managers were perpetrators of theft
- 80% of cases had fewer than 150 employees.



## NON-PROFITS

- Second-highest number of cases (16%)
- Over 50% of perpetrators were managers
- Over 80% of cases were at organizations with fewer than 150 employees
- Almost 50% of fraud cases were funds theft.



## LABOR UNIONS

- Over 90% of cases occurred in organizations of fewer than 150 people
- Check fraud and credit card fraud made up 67% of the cases.



## REAL ESTATE/ CONSTRUCTION

- The only industry with multiple cases perpetrated by company owners. Owners were responsible for 11% of cases with a median loss of nearly \$350,000
- Nearly all cases at companies with fewer than 150 employees.



## MUNICIPALITY

- More managers (63%) than employees (38%) embezzled, but the median loss for schemes perpetrated by managers was nearly three times as high
- Nearly 85% of cases had fewer than 150 employees
- Second most frequent industry for check fraud.



## HEALTHCARE

- Highest percentage of managers who embezzled with 65% of fraud cases perpetrated by those in a management position
- All cases were at companies with under 250 employees.



## PROFESSIONAL SERVICES


- 63% of perpetrators were employees
- Over 80% of cases were at companies with fewer than 150 employees.



## RETAIL

- Over 50% of embezzlers were managers
- Lowest number of cases at just 5%, but high median loss at \$475,876
- Likely to be underreported. Some estimates put losses from retail theft by employees at \$18 billion per year.



	SECTOR	MEDIAN LOSS	PERCENT OF SAMPLE	PERCENT OF MANAGEMENT PERPETRATORS
	Professional Services	\$615,101	5%	38%
	Healthcare	\$600,000	6%	65%
	Retail	\$475,876	5%	53%
	Real Estate/ Construction	\$416,000	9%	60%
	Financial Services	\$308,162	17%	33%
	Non-Profit	\$274,846	16%	58%
	Municipalities	\$218,874	9%	54%
	Labor Unions	\$79,389	10%	60%

In 75% of  
the industries  
studied,  
managers  
embezzled  
more  
often than  
employees.

## In real life

A woman who worked as a bookkeeper in Maryland stole over \$1.3 million from four different non-profit organizations. She took money that was intended to provide services for disadvantaged children and homeless families.



## Largest scheme by region

### MIDWEST **\$8.7 million**

The controller at a manufacturer in Cincinnati stole \$8.7 million over 11 years through fraudulent checks.

### WEST **\$4 million**

A Utah insurance agency owner embezzled \$4 million over two years by diverting funds from an escrow account to his own personal account.

### NORTHEAST **\$9 million**

The controller of a Connecticut hedge fund embezzled more than \$9 million over 9 years by transferring money from his employer to accounts he controlled.

### SOUTH **\$16.7 million**

A Texas bakery executive and his wife stole almost \$17 million over 15 years through paying personal expenses with company checks.








## In real life

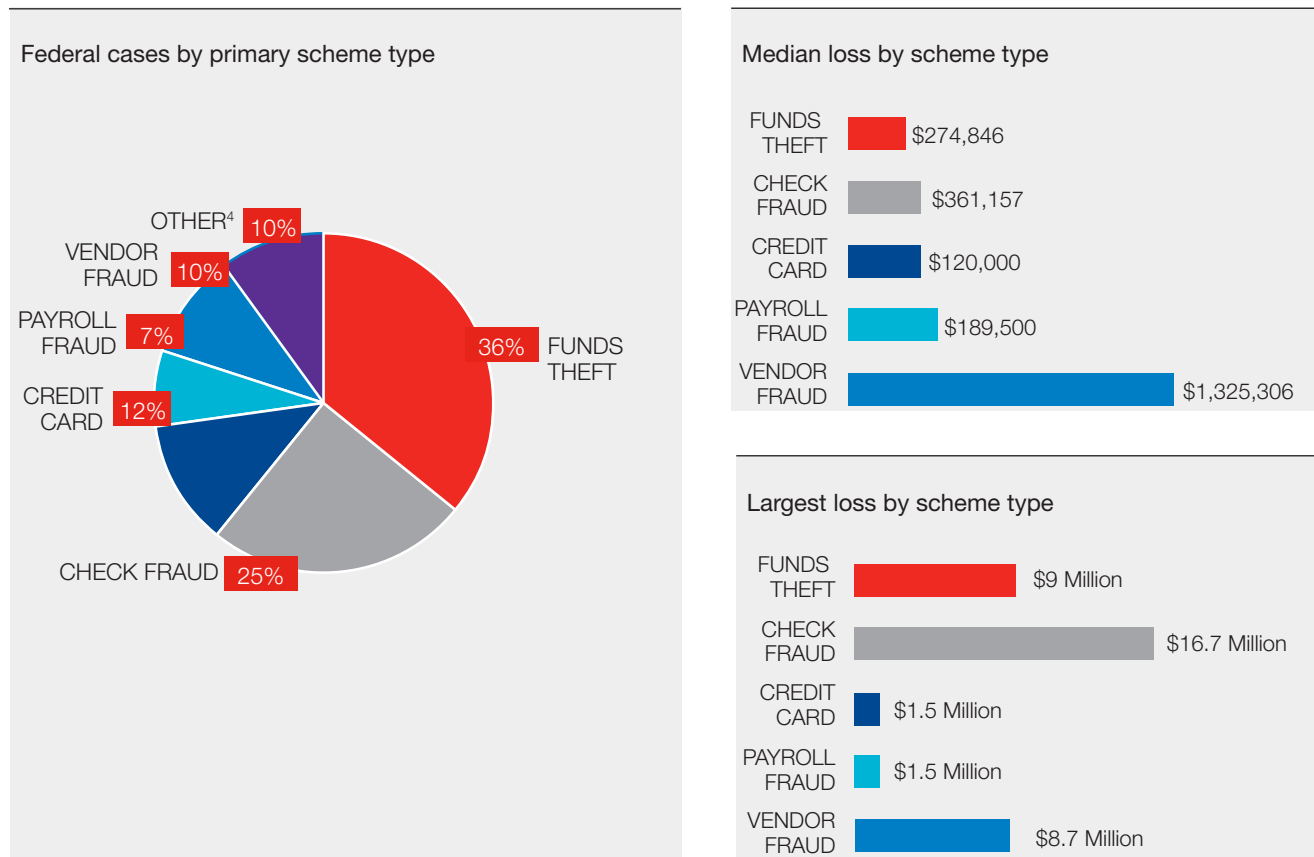
A 46-year-old bookkeeper embezzled \$155,460 from a nursing center in Kansas. When she was caught, it was found she'd also stolen from several other employers as well. Her job as a bookkeeper was a violation of her parole on previous fraud charges.

# Common themes, common schemes

Embezzlement schemes possess commonalities and are often intertwined. Perpetrators may use more than one to help cover their tracks. Recognizing these schemes is the first step towards prevention.

Scheme	What is it?	How it is done	How to prevent it
 <p><b>Outright Funds Theft</b> (36% of cases)</p>	Involves taking cash or bank deposits, or transferring funds to an account controlled by perpetrator.	A CFO embezzled \$2.1 million over 4 years by using company funds to pay his AMEX bill.	Set separated duties for making payments and reconciling accounts between two or more individuals.
 <p><b>Check Fraud</b> (26% of cases)</p>	Involves altering or forging checks, or making checks payable to themselves.	Corporate Controller stole \$16 million over 9 years by printing checks to their credit card company, then voiding the checks. Issued vendor checks for the same amount, but never mailed.	Split responsibility for payable function between at least two employees.
 <p><b>Credit Card Fraud</b> (12% of cases)</p>	Includes fraudulent use, authorization, or creation of an employer's credit or debit cards.	Over \$200,000 stolen when woman opened credit card in own name but linked to business owner's account. Statements went to her address instead of company.	Send company credit card statements and bank statements to the home address of the owner of the company, rather than business address, for review prior to reconciliation.
 <p><b>Vendor Invoicing &amp; False Billing</b> (10% of cases)</p>	Involves using fictitious invoices from made-up companies, or trumped-up invoices from actual vendors.	Hospitality facility manager and accomplices invoiced \$500,000 for equipment rentals that never took place. Invoices paid to conspirators' 'companies'.	Ensure different people approve and vet the selection of vendor and the authorization of payments. Conduct background checks on all vendors you're doing business with.
 <p><b>Payroll Fraud</b> (7% of cases)</p>	Occurs when an employee uses payroll system to divert funds to themselves or family members.	Hospital payroll director stole \$480,000 over three years by 'paying' salaries and vacation time to terminated employees.	Regular review of payroll records. Functions for issuing payroll checks or deposits and reconciling deposits should be separate. Changes should require approval from multiple levels of management.

## How the data breaks down



## Schemes by company size

Scheme	1-150 employees	151-250 employees	251-500 employees
Funds theft	83.2%	8.4%	8.4%
Check fraud	93.2%	6.8%	0%
Credit card fraud	79.4%	2.9%	17.6%
Payroll fraud	88.2%	11.8%	0%
Vendor invoices and false billing	60.7%	21.4%	17.9%

# How companies protect themselves

---

Losses due to embezzlement are often never recovered, so prevention is critical. Understanding the perpetrator, prevalence, and method is the first step, but enacting and enforcing controls can be the single most important step to minimizing the loss to a victim organization.



## Don't

- Give end-to-end responsibilities for accounting
- Send bank financial statements directly to the accounting department. *Have someone outside the department review them first.*
- Assume long term employees are incapable of embezzlement
- Stop at a criminal and credit checks for employees who will be handling money. *Continue to run background checks even after the hire date*
- Allow embezzlers to leave your employment without pursuing a conviction.



## Do

- Implement checks and balances
- Send bank statements to business owners home
- Pay attention to employee lifestyles and extreme changes to them
- Promote a culture of trustworthiness and integrity
- Talk with all employees about fraud detection and internal controls. Have them sign a code of ethics
- Complete background and credit checks on employees who will be handling money
- Review cancelled checks that come directly from the bank.

# Cyber deception – a new kind of fraud

---

Cyber Deception is a growing form of fraud committed by external parties with the assistance of unsuspecting company employees. FBI reports over \$2.3 billion embezzled this way between October 2013 and February 2016.

## What is it?

- Also known as ‘business email compromise’ (BEC)
- Scam involving corrupting legitimate business email accounts through social engineering or computer intrusion to commit fraud
- Targets businesses that work with foreign suppliers or commonly use wire transfer payments.

## What are the methods?

- Bogus email, purportedly from a legitimate vendor, requesting funds be sent to an alternate account
- Email appearing to come from a company executive requesting a wire transfer to a new account  
Email often refers to a ‘secret project’ or an ‘emergency’ requiring immediate action
- Email account of an employer hacked and used to request invoice payments directed to hacker’s account.

## How do you protect against it?

- ✓ Technology — DKIM, SPF, and other technologies can prevent phishing techniques from taking
- ✓ Education — train employees on what to look out for
- ✓ Control — create multiple levels of signoff, two employees to approve any wire transfer, call back procedures at previously established contact details before changing payment information / accounting information
- ✓ Exposure — understand your average funds transfer and establish more stringent controls over anything outside that window; transfers to foreign countries, particularly Asia, Middle East, Russia are more likely.



## In real life

A real estate investment and development firm lost over \$1 million after cyber thieves drained bank funds. Attackers gained access to the owner’s email, established correspondence with his bookkeeper and convinced the bookkeeper to wire money from the firm’s accounts to their own in China.



# 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, company websites and common news aggregators. These cases, almost 425 in total, either became publicly known or were active in the federal system during calendar year 2015, 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 2015, 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.

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.

Hiscox  
520 Madison Avenue  
32nd floor  
New York  
NY 10022

T 646 442 8322  
[www.hiscoxbroker.com](http://www.hiscoxbroker.com)

**Doug Karpp**

SVP, National Product Head — Crime and Fidelity  
[doug.karpp@hiscox.com](mailto:doug.karpp@hiscox.com)  
+1 213 412 1223

