Fighting Fraud through False Positives:

a new approach to combatting insider threat

BANK OF THE WEST
BNP PARIBAS

David Pollino
2017

Introduction

- Occupational fraud involves an employee that defrauds the business they work for.
- Occupational fraud is not a new threat. It is a universal problem for all types of business that can be difficult to detect due to advances in technology and it's impact to business environments.
- Understanding the different vulnerabilities and planning is key to reducing the risk of exposure.
- A common sense approach that utilizes proactive monitoring, internal audit, and TIP hotlines can be an effective first step to deter occupational fraud.

Fraud is ubiquitous; it does not discriminate in its occurrence. And while anti-fraud controls can effectively reduce the likelihood and potential impact of fraud, the truth is that no entity is immune to this threat.

Source: ACFE – Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study

Internal Threats: Rising Security Risk

The New York Times

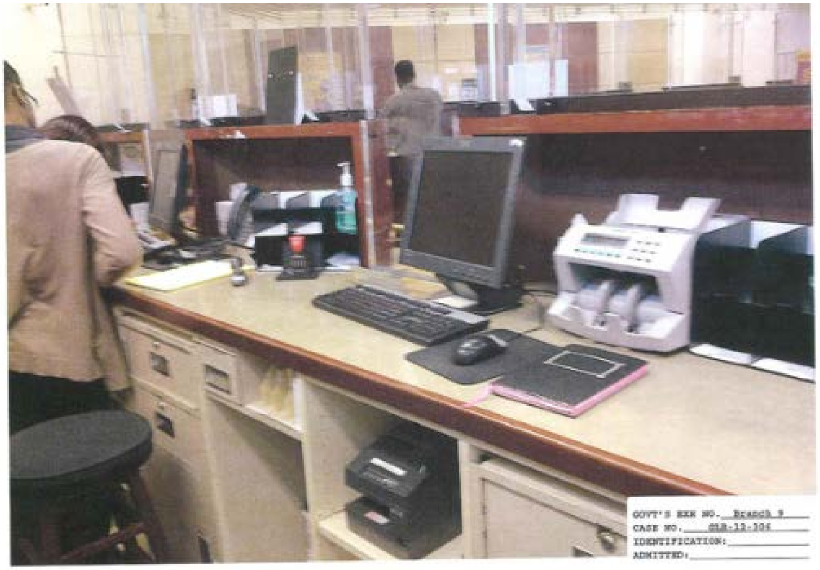
Bank Tellers, With Access to Accounts, Pose a Rising Security Risk

By STEPHANIE CLIFFORD and JESSICA SILVER-GREENBERG | FEB 1, 2016

“Bank robbers used to burst into banks brandishing guns and bearing notes demanding cash to the teller behind the window. Today, the thieves may be on the other side of the counter.”

“Though much of the focus on bank fraud has been on sophisticated hackers, it is the more prosaic figure of the teller behind the window who should worry depositors, according to prosecutors, government officials and security experts.”

“Under laws passed in the aftermath of the Sept. 11 attacks, banks are required to thoroughly vet their customers and closely monitor accounts to detect any suspicious activity. The same level of scrutiny does not always apply to the tellers, according to prosecutors. Sometimes, little more than a basic criminal-background check is performed.”



An image from the federal case of Jayad Zainab Ester Conteh, a former Capital One teller in Maryland sentenced in 2014 for gaining access to seven accounts and passing customer information to a co-conspirator who drew checks on them.

U.S. Department of Justice

BANK OF THE WEST
BNP PARIBAS

Insider Cyber Threat

Insiders Still Top Breach Threat: Experian’s Michael Bruemmer Offers 2016 Breach Forecast

- “Whether it’s a true malicious insider, or just employee negligence, 80 percent of the breaches we’ve worked so far in 2015 have been [caused by] employees”

Source: Information Security Media Group, Corp

Be Prepared

- “Organizations should consider creating an insider cyber threat program, led by a senior manager. This program would ensure that policies, resources and oversight are in place to assess and implement company controls that specifically deter, detect and mitigate the risk from *employees, contractors and business partners.”*

Source: Steven Chabinsky, Security Magazine

2015 Cyber Fraud Statistics

- 44% of adults online have been victims of cyber crimes in the last year.
- 68% of losses from cyber crime are $10,000 or more
- Of 7,818 businesses surveyed 67% had detected at least one cyber crime

Source: cybercrimestatistics.com

The Fraud Triangle

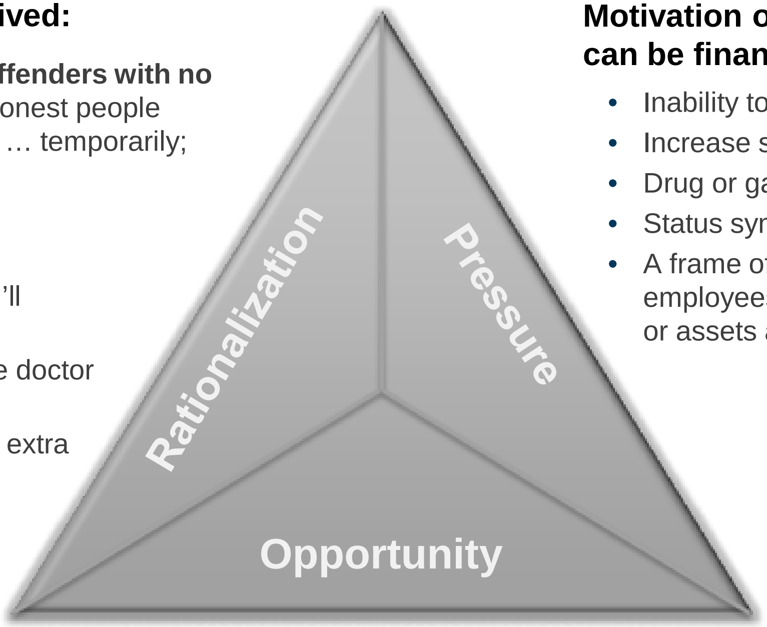
- Three components which together, lead to internal fraudulent behavior
- The component we have the most control over is Opportunity
- The best way to eliminate “perceived opportunity” is through Detection and Monitoring

Rationalization - Real or Perceived:

Vast majority (95%) are first-time offenders with no criminal past, view themselves as “honest people caught between a rock and hard spot … temporarily; not as a criminal

Personal

- I am only borrowing the money, I’ll return it next week
- I had no choice, I have to pay the doctor bill
- My employer owes me for all the extra hard work



Motivation or pressure to commit the crime can be financial or non financial:

- Inability to pay one’s bills
- Increase sales or other productivity targets
- Drug or gambling addictions
- Status symbol driven
- A frame of mind or ethical character that allows employees to intentionally misappropriate cash or assets and justify their dishonest actions

Possible when employees have access to assets and information that allow them to commit and conceal fraud

- A belief that their activities will not be detected
- There must be a way for the person to use or abuse their position of trust
- Preferred approach is “low and slow” where detection is delayed and more damage can be done
- Opportunity is created by weak internal controls, poor oversight and/or through use of ones position and authority

Accidental Fraudster vs Career Criminal

Accidental Fraudsters

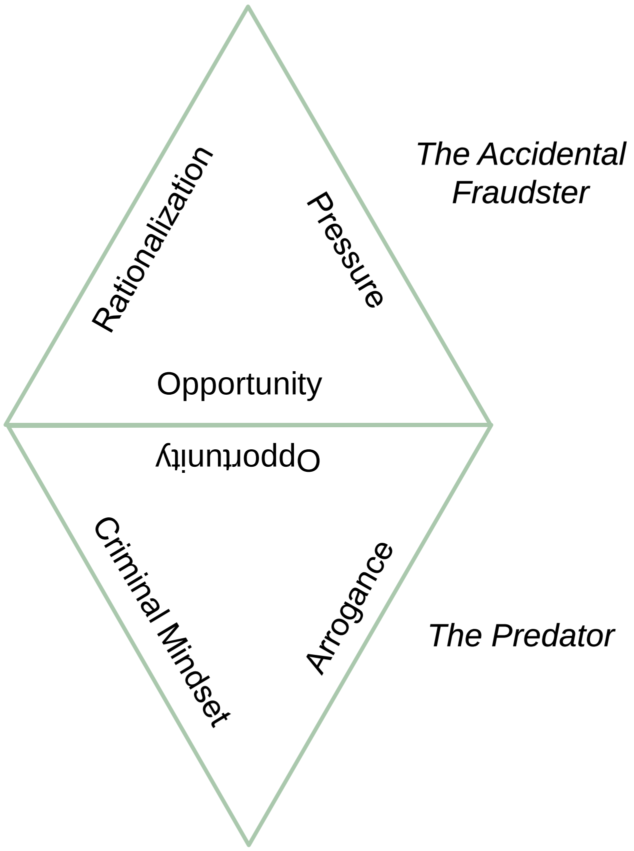
- Law-biding individual who never thought of committing fraud, break serious law and harm people
- Usually first time offender and the reason they commit fraud is because of non-sharable problem that can only be solved with money
- Rationalize actions aligned with opportunity

Predators

- Often start out as an accidental fraudster
- Look for target organization where they can commit crime
- Harder to detect because their fraud schemes are usually better organized

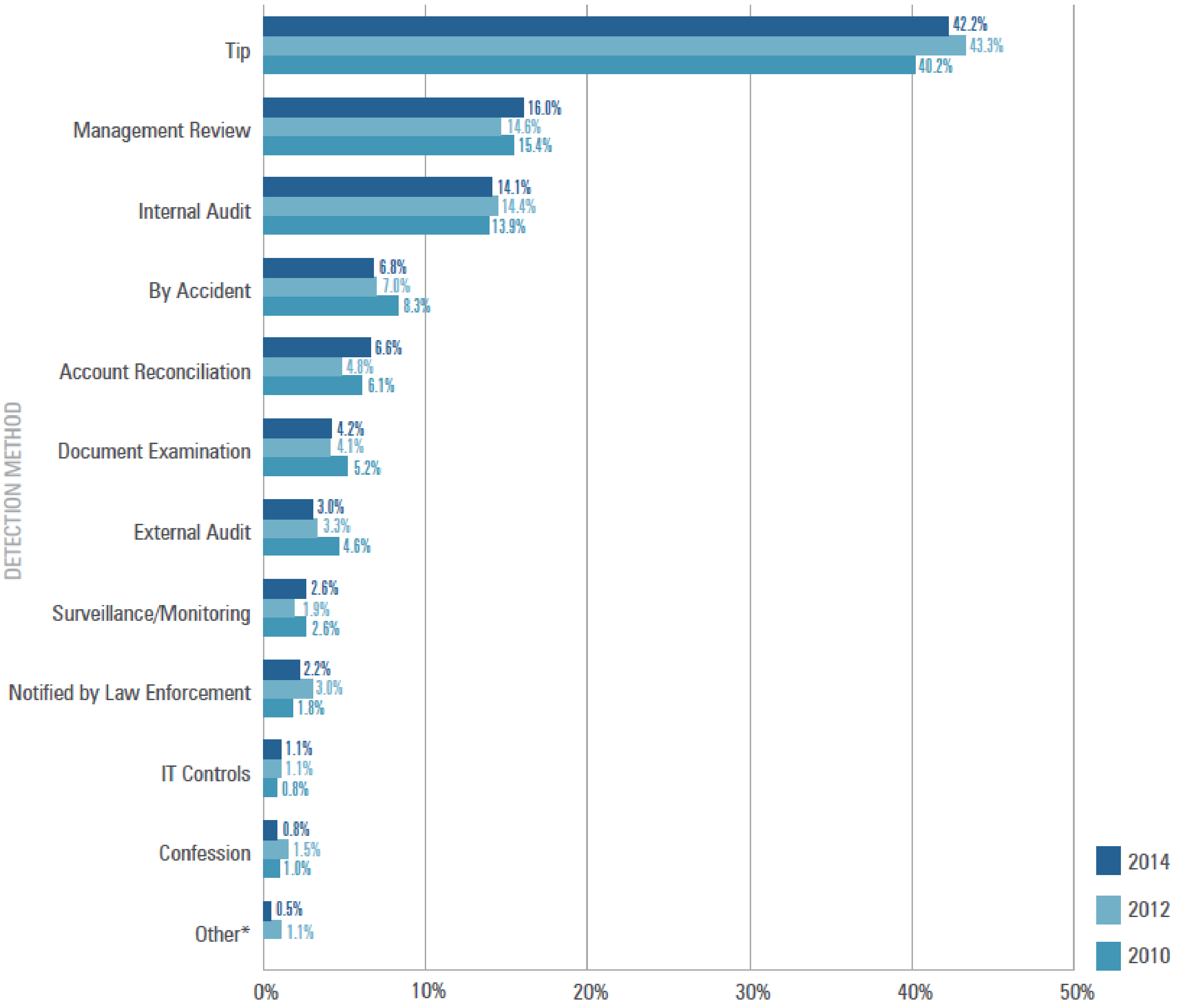
Source: Chegg, Forensic Accounting and Fraud Examination study aids

THE FRAUD DIAMOND



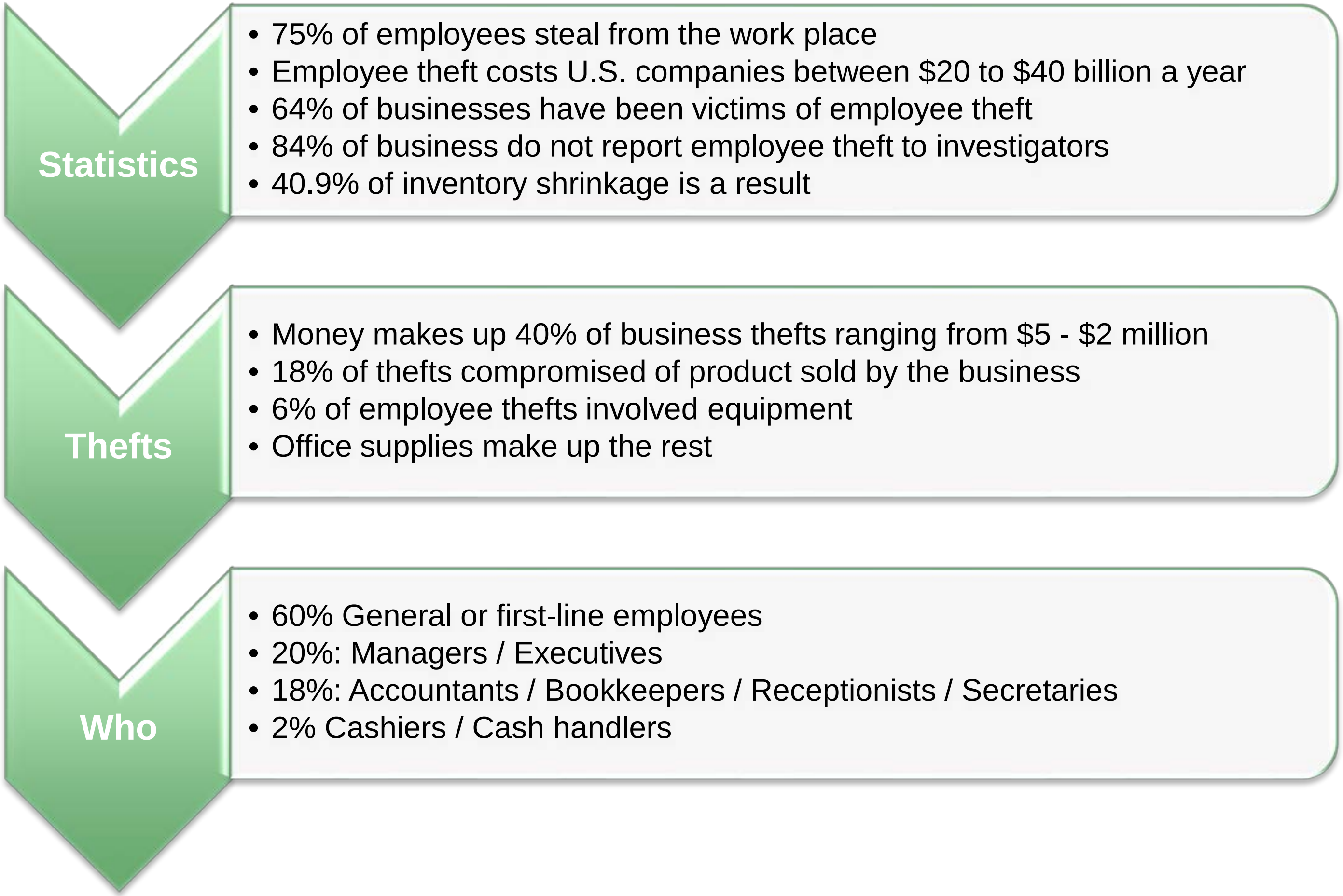
Source: ACFE, Bill Blend, MSL

Initial Detection of Occupation Fraud



Source: ACFE – Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study

Anatomy of Employee Theft



Statistics

- 75% of employees steal from the work place
- Employee theft costs U.S. companies between $20 to $40 billion a year
- 64% of businesses have been victims of employee theft
- 84% of business do not report employee theft to investigators
- 40.9% of inventory shrinkage is a result

Thefts

- Money makes up 40% of business thefts ranging from $5 - $2 million
- 18% of thefts compromised of product sold by the business
- 6% of employee thefts involved equipment
- Office supplies make up the rest

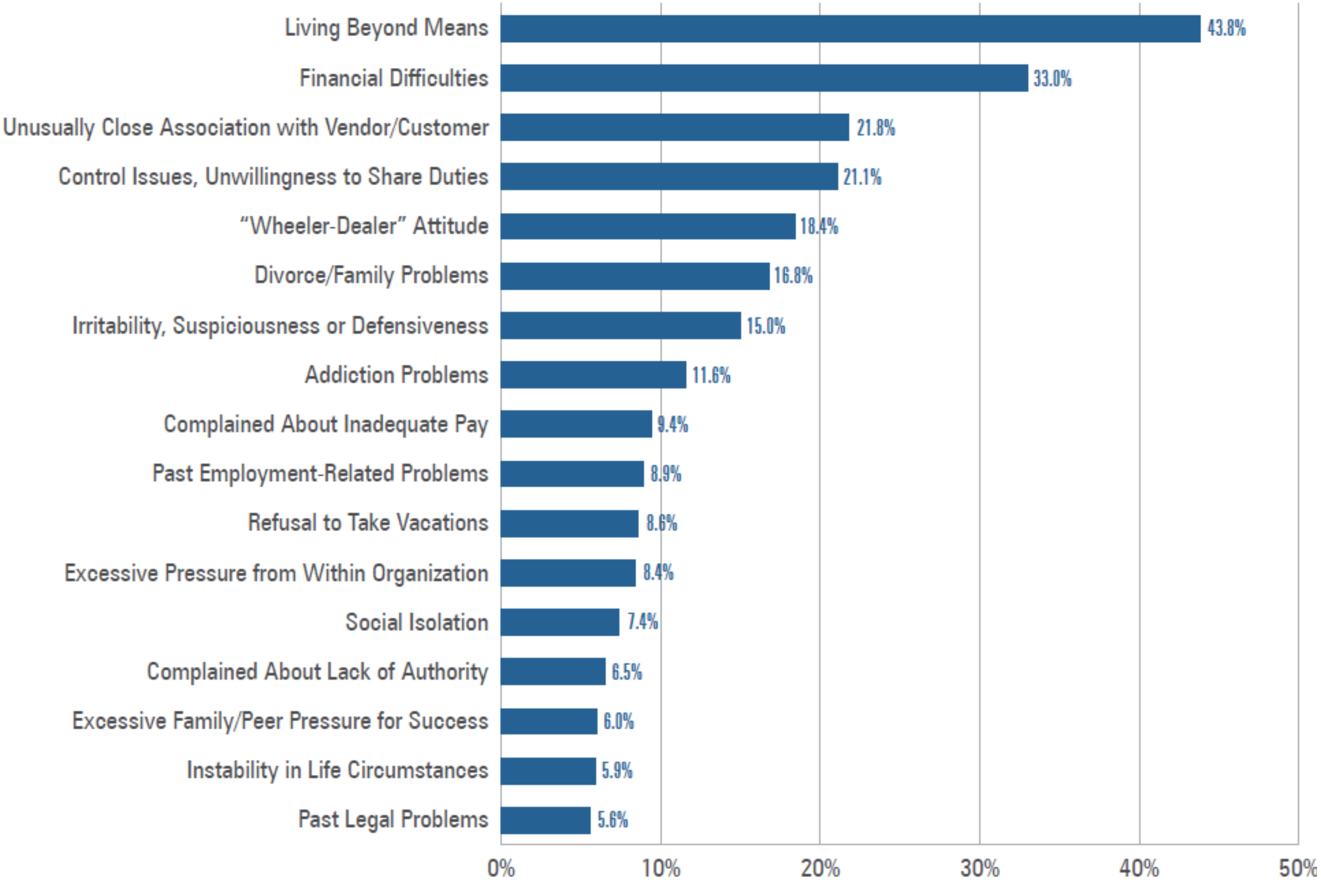
Who

- 60% General or first-line employees
- 20%: Managers / Executives
- 18%: Accountants / Bookkeepers / Receptionists / Secretaries
- 2% Cashiers / Cash handlers

Source: https://www.tycois.com/insights-and-opinions/infographics/anatomy-of-employee-theft

Behavioral Red Flags

Occupational fraudsters exhibit certain behavioral traits or characteristics while committing crimes. In 92% of the cases analyzed by the Association of Certified Fraud Examiners (ACFE), the fraudster displayed at least one of these red flags, and in 64% of cases, multiple red flags were observed before the fraud was detected.



Other Common Red Flags:

- Unusually close association with a vendor or customer (22%)
- Displaying control issues or an unwillingness to share duties (21%)
- General "wheeler-dealer" attitude involving shrewd or unscrupulous behavior (18%)
- Recent divorce or family problems (17%).

Source: http://www.acfe.com/rttn-red-flags.aspx

Insider Cyber Threat

Insiders Still Top Breach Threat: Experian's Michael Bruemmer Offers 2016 Breach Forecast

- "Whether it's a true malicious insider, or just employee negligence, 80 percent of the breaches we've worked so far in 2015 have been [caused by] employees"

Source: Information Security Media Group, Corp

Be Prepared

- "Organizations should consider creating an insider cyber threat program, led by a senior manager. This program would ensure that policies, resources and oversight are in place to assess and implement company controls that specifically deter, detect and mitigate the risk from *employees, contractors and business partners."*

Source: Steven Chabinsky, Security Magazine

2015 Cyber Fraud Statistics

- 44% of adults online have been victims of cyber crimes in the last year.
- 68% of losses from cyber crime are $10,000 or more
- Of 7,818 businesses surveyed 67% had detected at least one cyber crime

Source: cybercrimestatistics.com

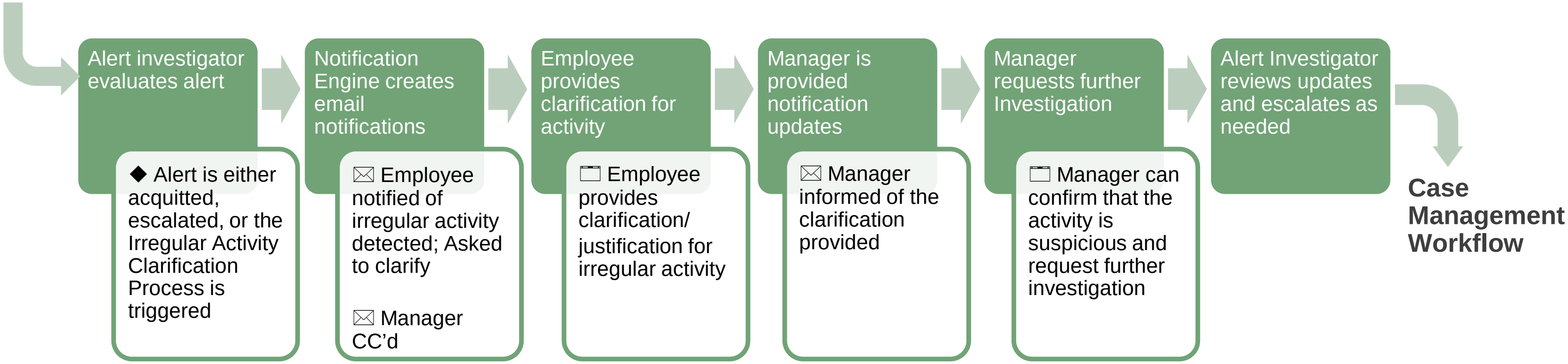
Be Purposefully Noisy

As appropriate, internal fraud alerts are routed to employees and managers for the purpose of:

- Gathering additional information for investigators
- Reinforcing the awareness of suspicious activity monitoring

Irregular Activity Clarification Process

Internal Fraud Alerts



Alert investigator evaluates alert

◆ Alert is either acquitted, escalated, or the Irregular Activity Clarification Process is triggered

Notification Engine creates email notifications

✉ Employee notified of irregular activity detected; Asked to clarify

✉ Manager CC'd

Employee provides clarification for activity

🗔 Employee provides clarification/ justification for irregular activity

Manager is provided notification updates

✉ Manager informed of the clarification provided

Manager requests further Investigation

🗔 Manager can confirm that the activity is suspicious and request further investigation

Alert Investigator reviews updates and escalates as needed

Case Management Workflow

Internal Threat Deterrence: Communications & Controls

COMMUNICATIONS

Standards and Policies

- Ethical Conduct Policy
- Standard Operating Procedures
- Employment Contracts
- Privacy Policy

Organizational Culture

- “No Jerks Rule”
- Management Tone
- Word of Mouth
- Signage

Training and Testing

- Onboarding Training
- Manager Kits
- Risk Assessments and Testing

Tipline / Ethics hotline

- Phone | Email | Web
- Feedback Loop / Continuous Improvement

CONTROLS

Employee Screening Controls

- Background Checks
- Reference Checks
- Social Media Searches
- Early Warning -Internal Fraud Prevention Service

Operational Controls

- Segregation of Duties
- Transactional Parameters Screening
- Employee Self-Dealing Monitoring
- Error Resolution Process
- Quality Control Process
- Reconciliation Process
- Accounts Payable Fraud Analysis
- Internal Audits
- Surprise Audits
- Customer Returns

Physical Security Controls

- Building Access
- Equipment Access
- Equipment/Property Passes
- Guards
- Cameras
- Inventory handing and tracking

Information Security Controls

- Network Access
- Logical Access
- System Access
- Permissions/Accessibility
- Application Access
- Computer activity monitoring
- Web Monitoring
- Data Loss Prevention

Insider Threat Mitigation Best Practices

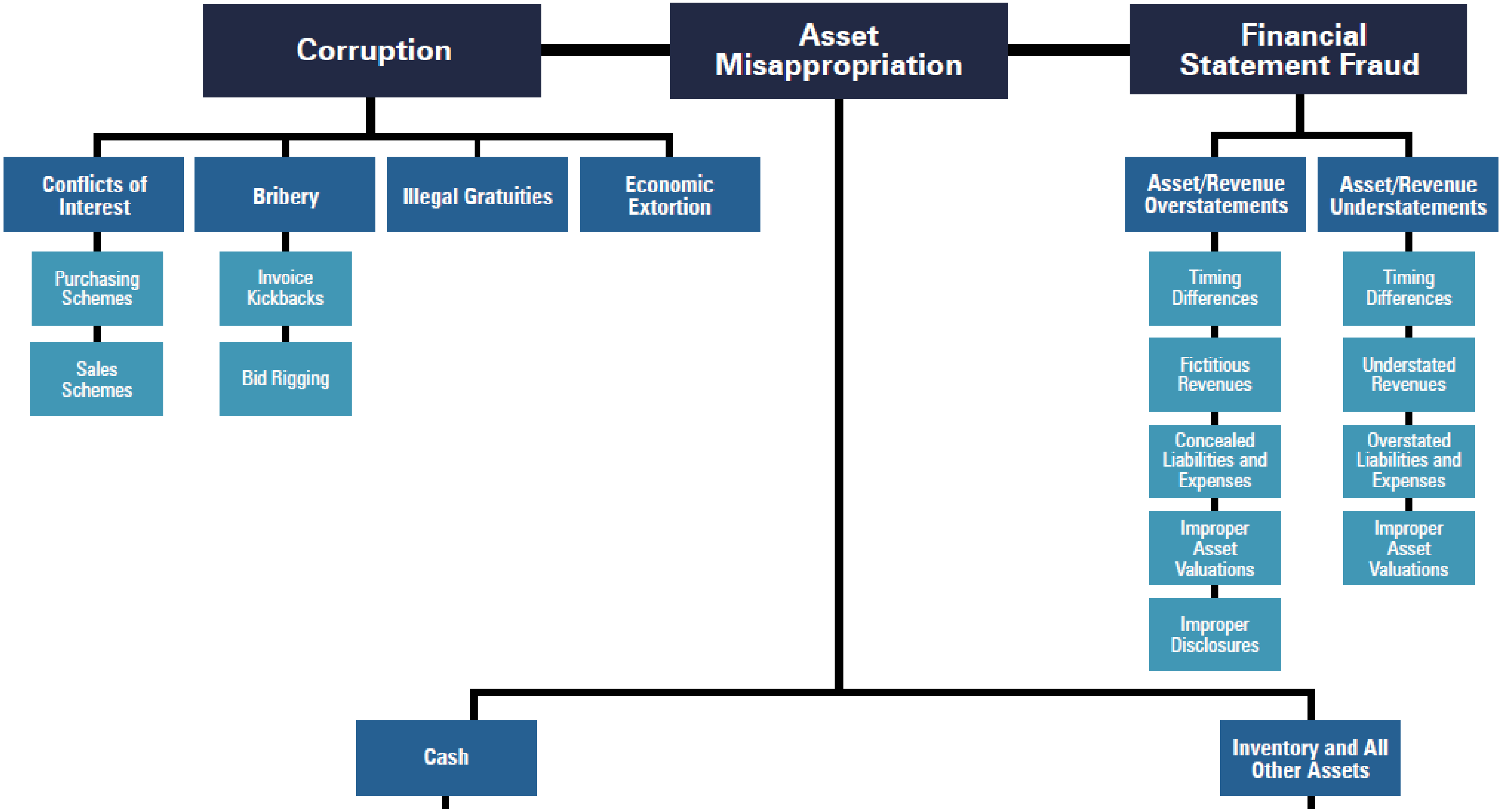
- Consider threats from insiders and business partners in enterprise-wide risk assessments.
- Clearly document and consistently enforce policies and controls.
- Incorporate insider threat awareness into periodic security training for all employees.
- Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
- Anticipate and manage negative issues in the work environment.
- Know your assets
- Implement strict password and account management policies and practices
- Enforce separation of duties and least privilege
- Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
- Institute stringent access controls and monitoring policies on privileged users
- Institutionalize system change controls
- Use a log correlation engine or security information and event management (SEIM) system to log, monitor, and audit employee actions
- Monitor and control remote access from all end points, including mobile devices
- Develop a comprehensive employee termination process
- Implement secure backup and recovery processes
- Develop a formalized insider threat program
- Establish a baseline of normal network device behavior
- Be especially vigilant regarding social media
- Close the doors to unauthorized data exfiltration

Software Engineering Institute Carnegie Mellon

Source: "Common Sense Guide to Mitigating Insider Threats, 4th Edition" **CERT**®

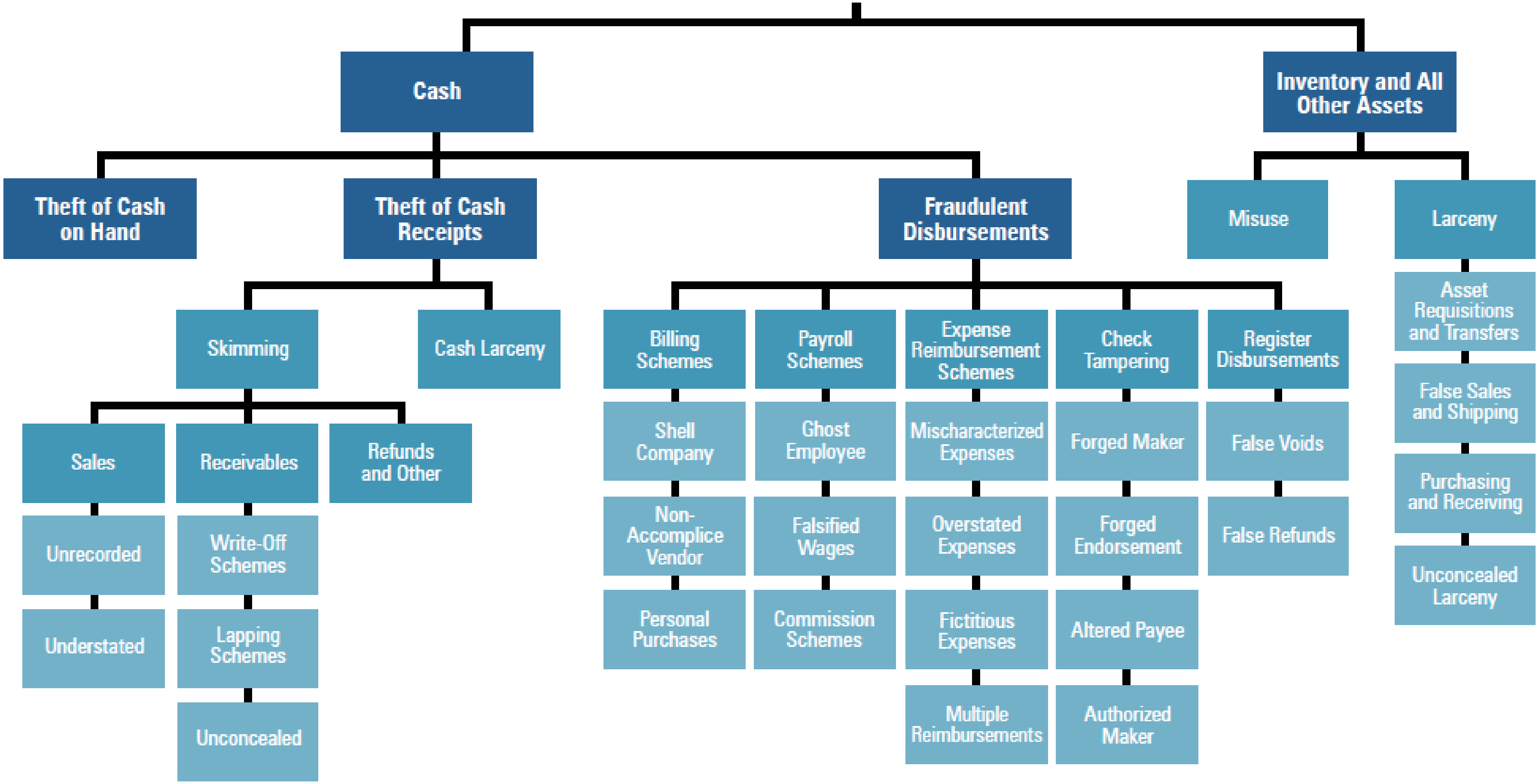
Appendix

Fraud Tree – Classification



Source: ACFE – Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study

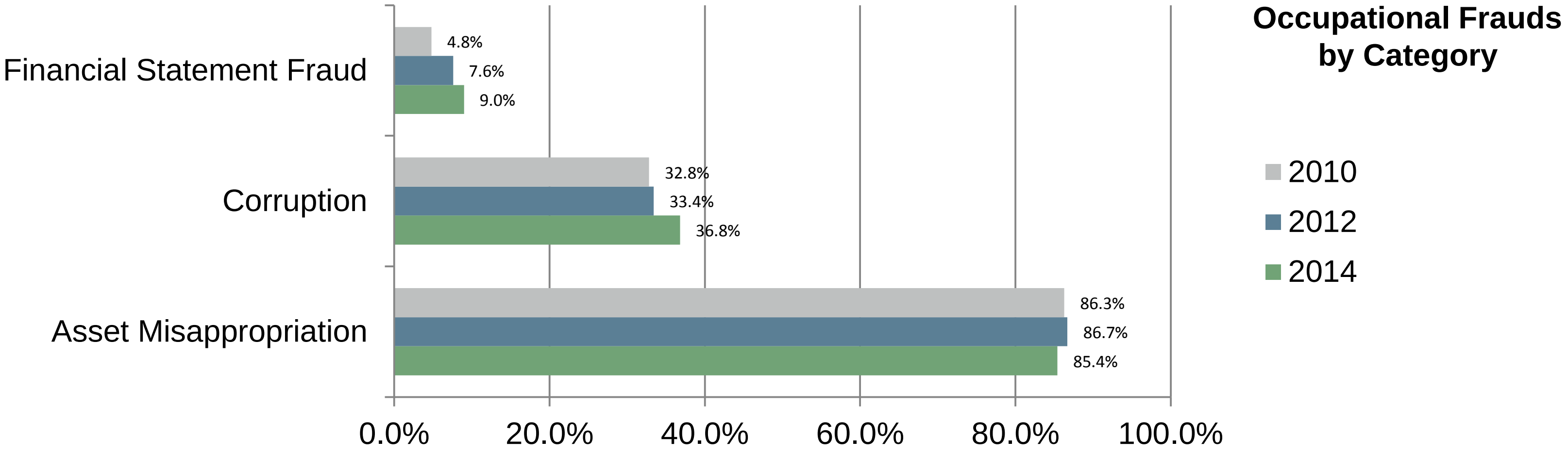
Fraud Tree – Classification

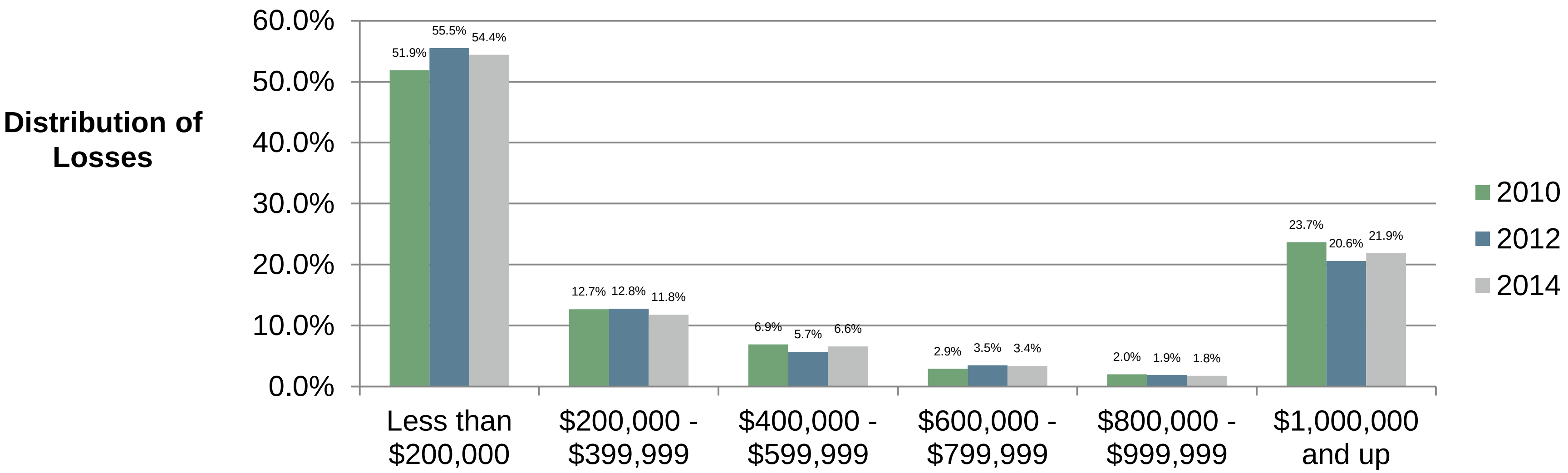


- Cash
  - Theft of Cash on Hand
  - Theft of Cash Receipts
    - Skimming
      - Sales
        - Unrecorded
        - Understated
      - Receivables
        - Write-Off Schemes
        - Lapping Schemes
        - Unconcealed
      - Refunds and Other
    - Cash Larceny
  - Fraudulent Disbursements
    - Billing Schemes
      - Shell Company
      - Non-Accomplice Vendor
      - Personal Purchases
    - Payroll Schemes
      - Ghost Employee
      - Falsified Wages
      - Commission Schemes
    - Expense Reimbursement Schemes
      - Mischaracterized Expenses
      - Overstated Expenses
      - Fictitious Expenses
      - Multiple Reimbursements
    - Check Tampering
      - Forged Maker
      - Forged Endorsement
      - Altered Payee
      - Authorized Maker
    - Register Disbursements
      - False Voids
      - False Refunds
- Inventory and All Other Assets
  - Misuse
  - Larceny
    - Asset Requisitions and Transfers
    - False Sales and Shipping
    - Purchasing and Receiving
    - Unconcealed Larceny

Source: ACFE – Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study

Losses & Frequency


Occupational Frauds by Category


Distribution of Losses

Source: ACFE – Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study

THANK YOU

Bank of the West

David Pollino

13505 California St.
Omaha, NE 68154

David.Pollino@bankofthewest.com