# Non-Profit Collaborative
# How to Protect your Non-Profit from Fraud and Embezzlement

May 22, 2018

**Michael Gallagher**
Chief Risk Officer, EVP

**Meaghan Lally-McGurl**
Senior Risk Management Manager, SVP

Enterprise Bank
Member FDIC
CREATE SUCCESS

# Disclaimer

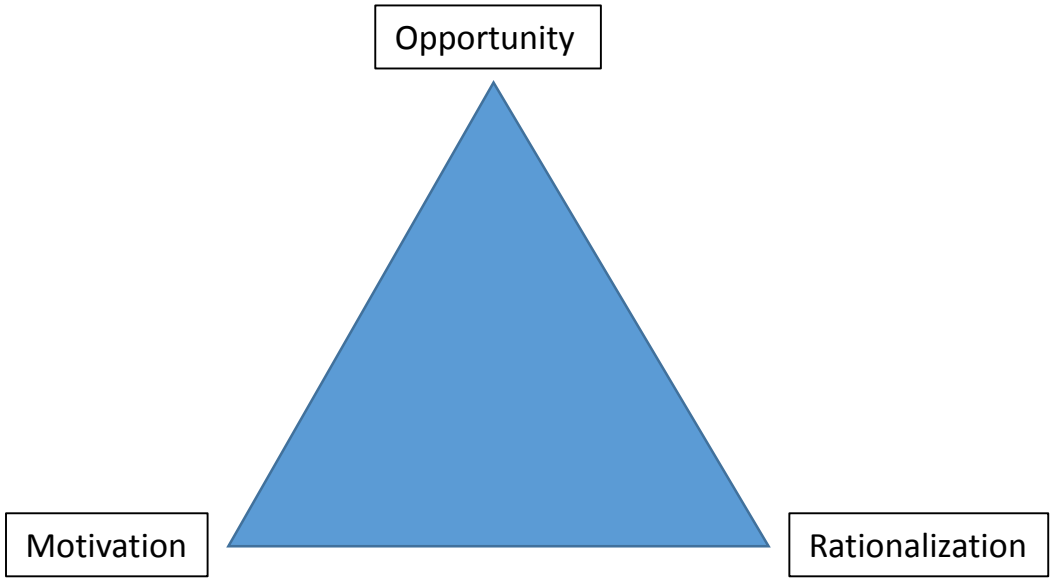
The information contained in this presentation as well as the comments by the presenters do not necessarily represent the views, positions, or opinions of Enterprise Bank. The information is for educational purposes only and does not constitute accounting or legal advice.

# Today's Agenda

- What is Fraud?
- Internal Threats
- External Threats
- Prevent
- Identify
- Recover
- Conclusion

# What is Fraud?

Fraud - Wrongful or criminal deception intended to result in financial or personal gain



# 2,690
real cases of occupational fraud

from

# 125 countries

in

# 23 industry categories

# $7 BILLION+
**IN TOTAL LOSSES**

# $130,000
**MEDIAN LOSS PER CASE**

# 22%
**OF CASES CAUSED LOSSES OF**
# $1 MILLION+

Median duration of a fraud scheme

# 16
# MONTHS

## CORRUPTION
was the most common scheme in every global region

## SMALL BUSINESSES LOST ALMOST TWICE AS MUCH PER SCHEME TO FRAUD

**$104,000**
MEDIAN LOSS
100+ EMPLOYEES

**$200,000**
MEDIAN LOSS
<100 EMPLOYEES

# Current Statistics

- Internal Control weaknesses were responsible for nearly 50% of cases.
- Over 40% of all cases were detected by a tip (more than twice the rate of any other detection method).
- For non profits, the median loss is $75,000 and is 9% of the total fraud ($7 billion) reported.
- If fraud is caused by an individual, the median loss is $74,000, if two people commit the fraud together, the loss increased to $150,000, and if three or more people work together, the loss increased to $339,000.
- Most common fraud schemes for non-profits include billings, corruption, expense reimbursements, cash, and payroll.

*Statistics from the ACFE's Report to the Nations

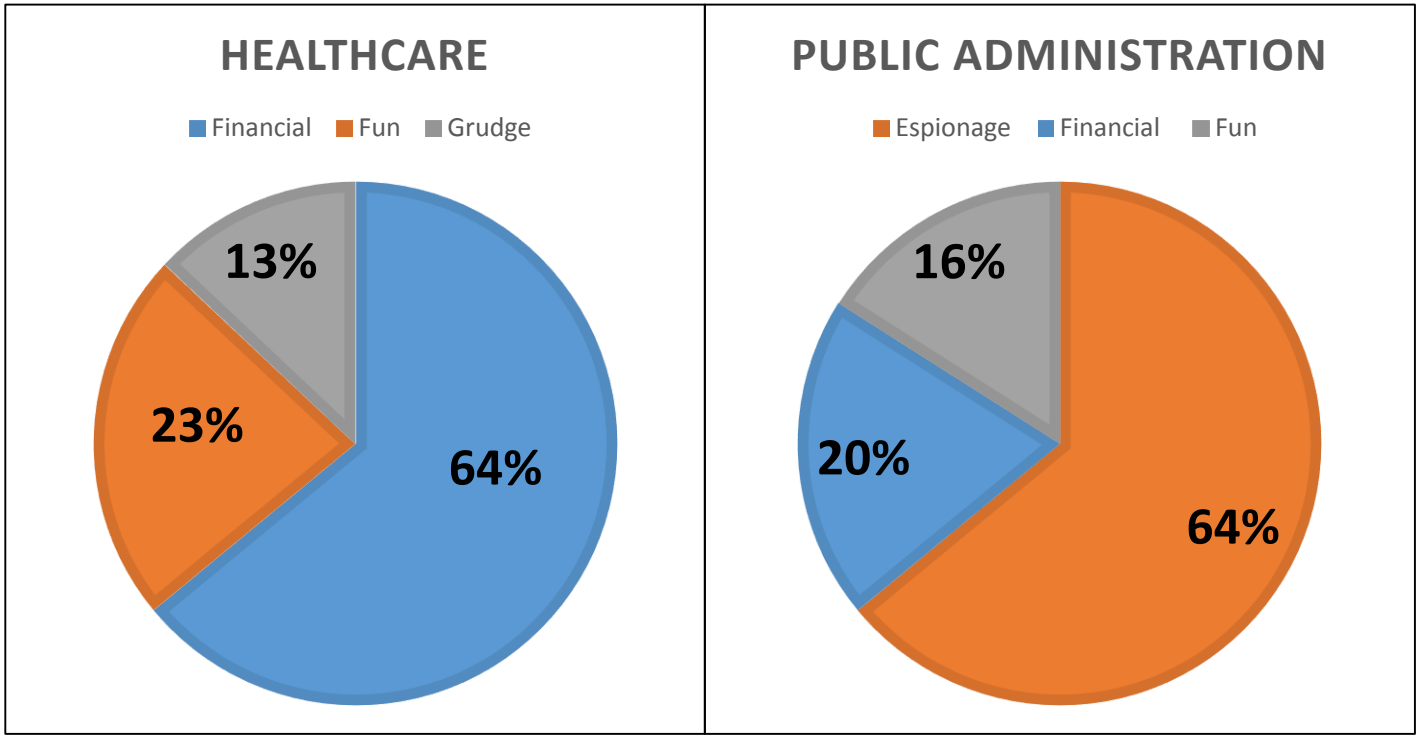
# Impact of Fraud

- Financial Losses
- Reputational Impact
  - Loss of Trust of a Funder
- Lower Employee Morale
- Potential lawsuits
  - Personal liability or jail time
- Closing of Non Profit

# Types of Fraud

| Internal | External |
|---|---|
| Accounts Payable/Purchasing | Check Fraud and Petty Cash |
| Financial Statement Fraud | Corporate Account Takeover |
| Bribery/Corruption/Kickbacks | Debit Card/Credit Card Fraud |
| Expense Reimbursements | Third parties |
| Business Assets for Personal Use | Fictitious employees |

# Why Do They Do It?

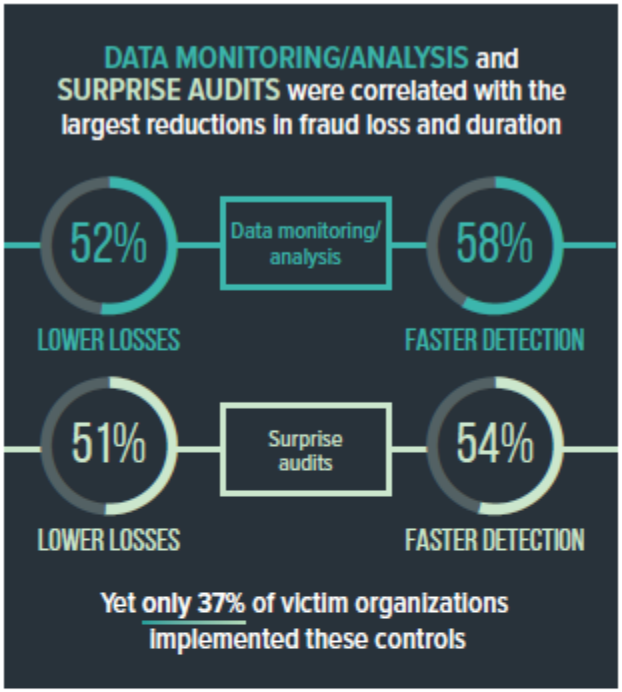


# Internal Threats

- Our people and providing the opportunity and motivation
- Poor physical controls
  - Data Centers
  - Negotiable Instruments
  - Access After Hours
  - Alarms
- Granting too much access to confidential information
  - Financial Data (Insider Trading)
  - Unlimited Authorization/User Access Rights
  - Customer and Employee Data
  - Information Databases
  - Trade Secrets

# Internal Threats

- Social Engineering
- Lack of monitoring
  - Reconciliations of Bank and General Ledger Accts.
    - Unusual amounts
    - Stale dated items
  - User activity
    - Access attempts
    - Hours of access
    - What are they getting into?
  - Financial transactions
  - Unusual variances
  - Expense growth
  - Cash transactions




85% OF FRAUDSTERS DISPLAYED AT LEAST ONE BEHAVIORAL RED FLAG OF FRAUD

## FRAUDSTERS WHO HAD BEEN WITH THEIR COMPANY LONGER STOLE TWICE AS MUCH

MORE THAN 5 YEARS' TENURE
$200,000
MEDIAN LOSS

LESS THAN 5 YEARS' TENURE
$100,000
MEDIAN LOSS

## OVER THE PAST 10 YEARS, OCCUPATIONAL FRAUD REFERRALS TO PROSECUTION DECLINED 16%


## ONLY 4% OF PERPETRATORS HAD A PRIOR FRAUD CONVICTION

A MAJORITY OF THE VICTIMS RECOVERED NOTHING

# Why Do They Do It?

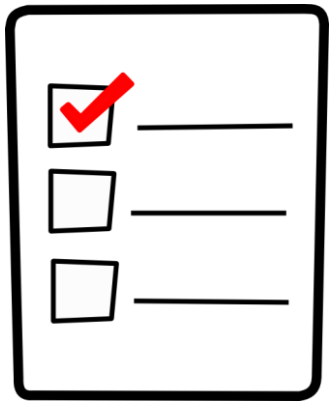
- Undefined roles and responsibilities
  - Create job descriptions
- Improper tone from the top
  - Create core values and Code of Ethics
- Collaboration amongst employees
  - Circumvention of controls
- Loss of customer data or a data breach
  - Third party access
  - Training and awareness
  - Incident response

# Why Do They Do It?

- Lack of understanding of technology
  - System configuration
  - Software limitations
  - Electronic security needs
  - Virus and malware detection
  - Patching
  - Penetration and vulnerability testing
- Convenience is our greatest threat

# External Threats

- Relationships with third parties
  - Risk rate your vendors
  - What standards should they comply with?
  - Read the fine print in contracts
  - Conduct a Google search of the vendor
  - Perform background checks
  - Collect data
  - Review information security programs



# External Threats

- Pressure to commit fraud
  - Spouse and family
  - Financial commitments
  - Addictions:  drugs, gambling, etc.
- Copy cats that see an opportunity
- Complexities of doing business
  - Understand what data you collect
  - Where is data stored?
  - Who has access to the data?
  - How long is it retained?

# External Threats

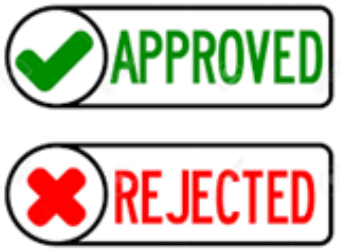
- Loss of a third party
- Loss of utility services, internet, etc.
- Electronic threats
  - Viruses and sleepers
  - Malware
  - Skimming devices
  - Denial of service attacks

# External Threats

- Customer threats
  - Identity theft
  - Corporate account takeover
  - Stolen cards and checks
  - Social engineering
  - Improperly identifying a customer
- The Internet and Social Media
  - The internet of things
  - This is where it all begins…..

# Preventing Fraud

- Establish written policies and procedures
- Rotate roles periodically
- Authorization limits
  - Contracts
  - Wages
  - Credit Cards (who has access to #?)
  - Check signing authority
  - Loans
  - Accounts Payable; vendors and invoices
  - Wires, ach, and any electronic money transfers



# Protecting Electronic Data

- Protect and dispose of physical and electronic files properly
- Properly install new technologies and communication channels (wifi and remote access)
- Check security standards and don't use factory defaults
- Periodically have your system tested; penetration and vulnerability
- Know your third parties and what they do with data
- Business continuity and disaster recovery
- Have an Incident Response Program

# Employee/Volunteer Focus

**Personnel Controls:**

- Observe employee behaviors
- Test knowledge and review policies
- Perform due diligence when hiring new employees or temporary workers
  - Background check
  - Credit check
  - Check references

# THE RED FLAGS OF FRAUD

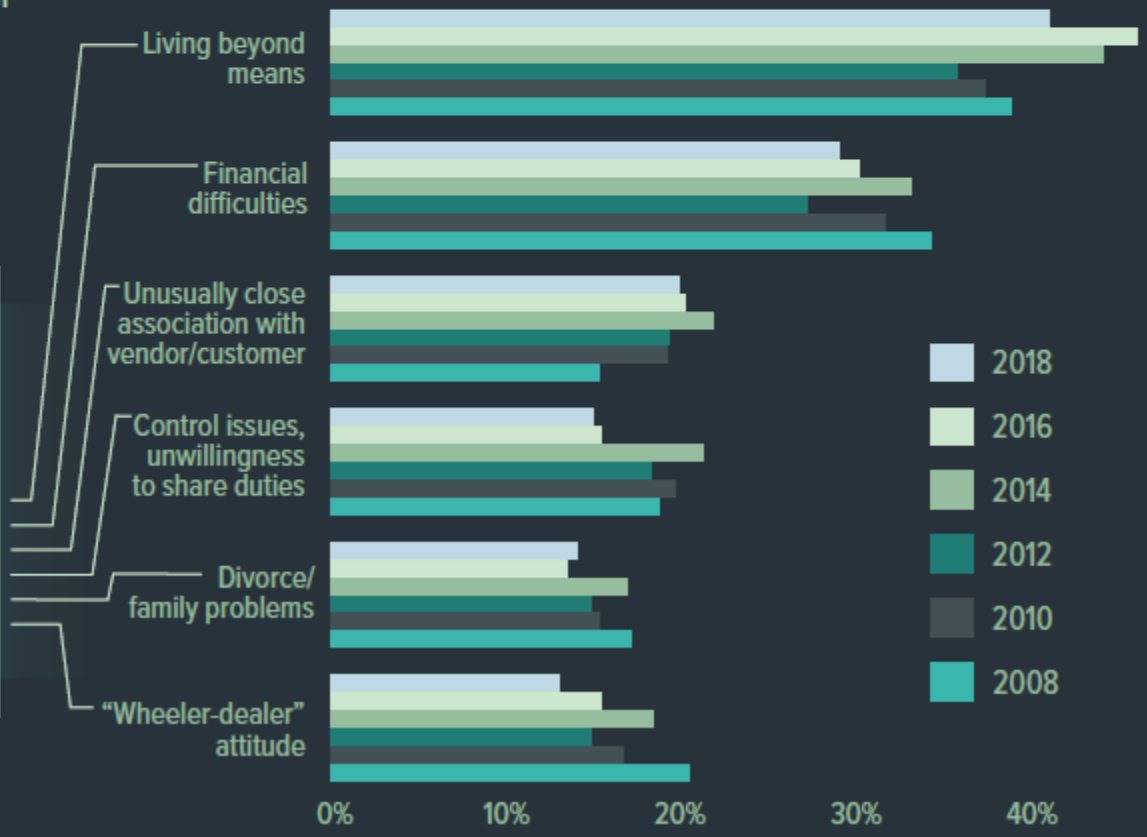
Understanding and recognizing the behavioral red flags displayed by fraud perpetrators can help organizations detect fraud and mitigate losses.

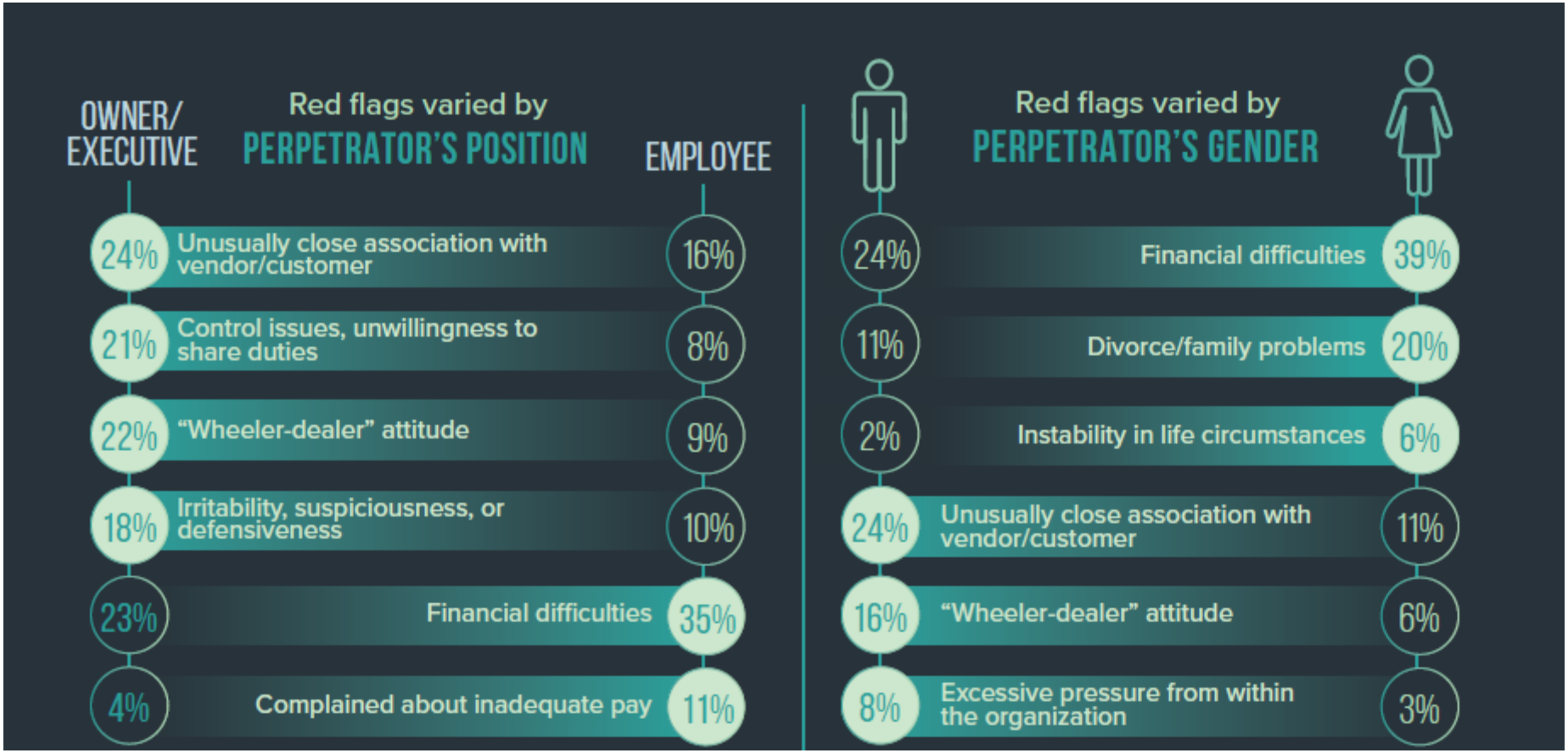
IN **85%** OF CASES FRAUDSTERS DISPLAYED AT LEAST ONE BEHAVIORAL RED FLAG

AND IN

**50%** OF CASES THEY EXHIBITED MULTIPLE RED FLAGS

These **6 BEHAVIORAL RED FLAGS** have been the most common in every one of our studies dating back to 2008, with a remarkably consistent distribution




OWNER/ EXECUTIVE
Red flags varied by
PERPETRATOR'S POSITION
EMPLOYEE
24% Unusually close association with vendor/customer 16%
21% Control issues, unwillingness to share duties 8%
22% "Wheeler-dealer" attitude 9%
18% Irritability, suspiciousness, or defensiveness 10%
23% Financial difficulties 35%
4% Complained about inadequate pay 11%
Red flags varied by
PERPETRATOR'S GENDER
24% Financial difficulties 39%
11% Divorce/family problems 20%
2% Instability in life circumstances 6%
24% Unusually close association with vendor/customer 11%
16% "Wheeler-dealer" attitude 6%
8% Excessive pressure from within the organization 3%

# Preventing Fraud

**Establish strong policies and procedures:**

- Conduct new employee orientation
- Implement a Whistleblower Policy
  - A way to report suspected activity
  - Anonymous method
  - No retaliation
- Establish a Code of Ethics
  - Conflicts of interest
  - Gifting policy
  - Expected behaviors and values
- Create record retention guidelines
- Have an employee handbook
  - Accountability
  - Document a process for violating the rules

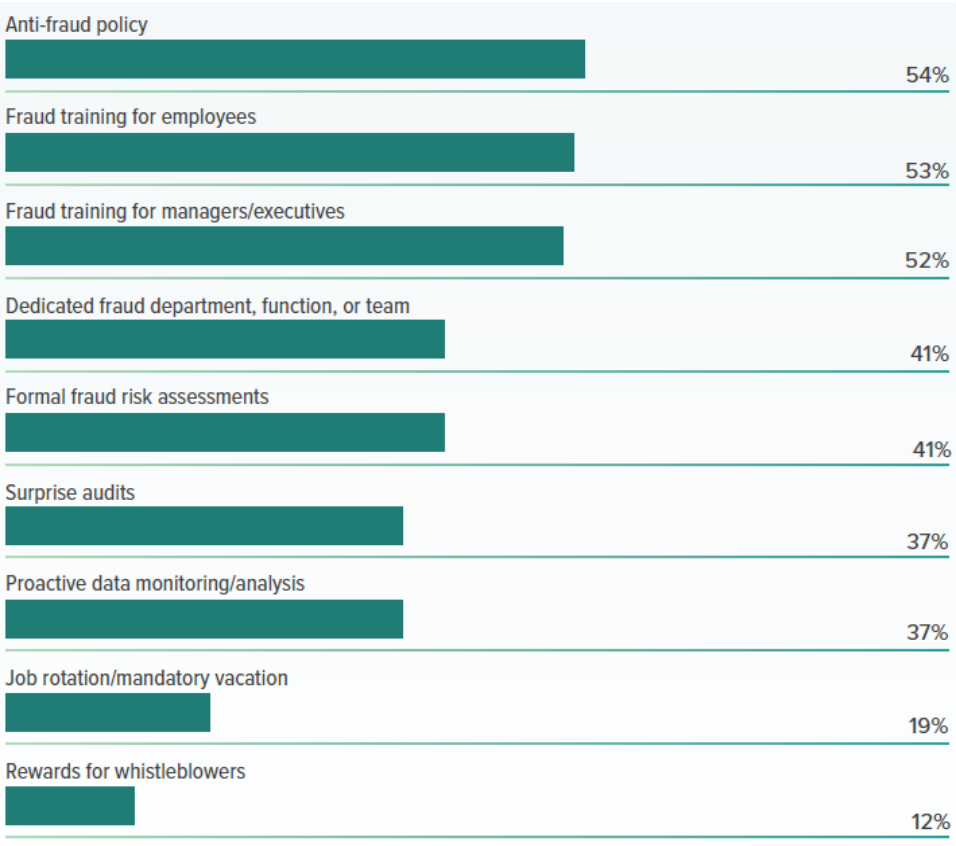
# Protecting Data

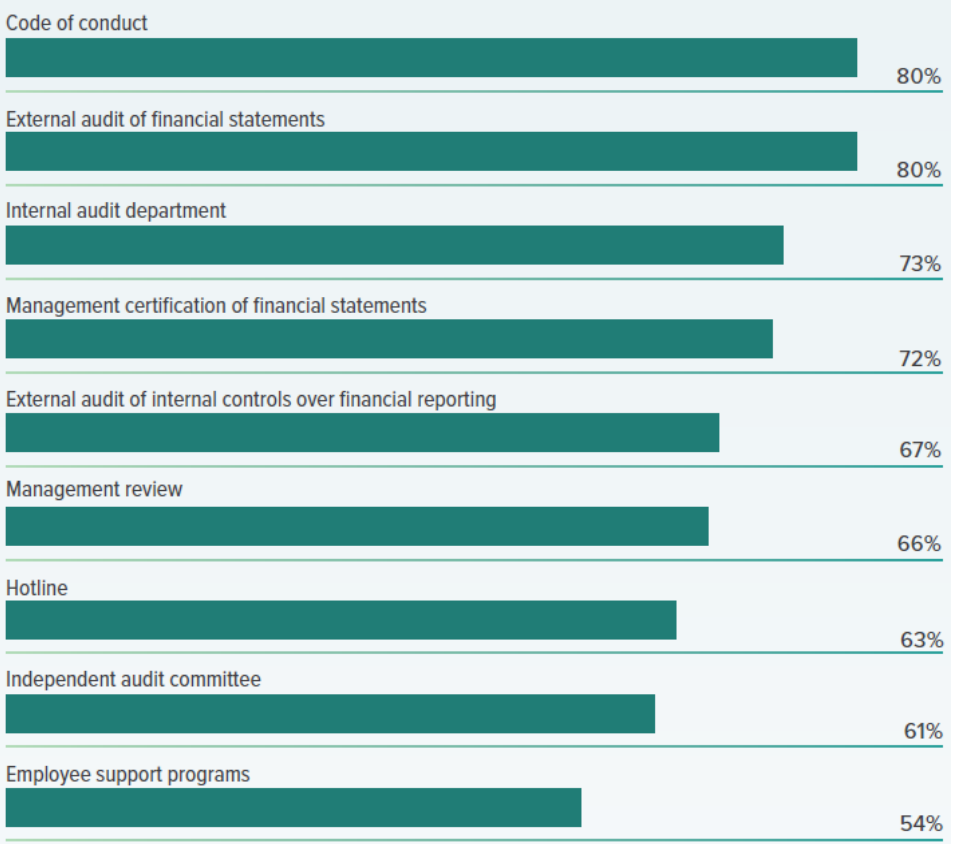
- Utilize complex passwords
- Provide user access based on job responsibilities
- Implement patches and upgrades
- Truncate account numbers and personal information
- Don’t store credit card data
- Back up programs and data regularly
- Apply patches when released
- Look for end of life or unsupported systems
- Perform network scans
- Review firewall configuration

# Preventing Fraud

- Physical Controls
  - Negotiable instruments
  - Cash and records
  - Dual controls
- Physical security
  - Alarms
  - Access Controls
  - Video surveillance

# Most Common




# Anti-Fraud Controls

Enterprise Bank
CREATE SUCCESS

# Identifying Fraud

**Financial Controls:**

- Conduct annual reviews or audits of financial records
  - Compilations, reviews and audits
- Regularly conduct account reconciliations
  - Review stale activity
  - Segregation of duties
  - Delivery of bank statements
- Review budget-to-actual projections
  - Identify unusual fluctuations and variances

# Identifying Fraud

**Observations:**

- Employees that take vacation or never take vacation
  - > 5 years tenure = $200,000 while <5 years = $100,000
- Phone Calls or mail for unrelated people or businesses sent to your non-profit
- Access logs
- Management reviews
- New vendors set up for accounts payable

# Insurance as a Control

Insurance is not a control, but it can save your entity

- Directors and Officers Insurance
- Employment practices policy (payroll)
- Bond or General Liability policy
  - Actions of employees
- Interruption of Services or Cyber insurance
- Property insurance
- Review your deductibles
- Assess your coverage periodically

# Recover from a Fraud

- Notify the appropriate agencies (law enforcement, Attorney General, Consumer Affairs, etc.)
- Notify your insurance agency, financial institutions, and CPA firm.
- Remediation of computer equipment
  - Change passwords
  - Change accounts
  - Change user name
  - Restore from backups
- Retain documentation;
  The Devil is in the Details

# Conclusion

- Fraud is everywhere
- Establish a system of checks and balances
- Monitor activity
- Protect your physical environment
- Review and understand financial results
- Know where your data is, and who has access to it
- Understand and utilize technology
- Review relationships with third parties
- Know your employees
- Educate your employees
- Be observant and practice professional skepticism

# References

- Association of Certified Fraud Examiners – http://www.acfe.com/
- 2018 Report to the Nations - http://www.acfe.com/report-to-the-nations/2018/
- MA Data Breach Requirements - https://www.mass.gov/service-details/requirements-for-data-breach-notificationsInternet Crime Complaint Center – www.ic3.gov
- Federal Bureau of Investigation - https://www.fbi.gov/investigate/cyber
- Department of Homeland Security - https://www.dhs.gov/topic/combating-cyber-crime
- Verizon Data Breach Report - http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
- Federal Trade Commission – https://www.ftc.gov/

# Questions?

**Michael Gallagher**
Chief Risk Officer, EVP
(978) 656-5611
michael.gallagher@ebtc.com

**Meaghan Lally-McGurl**
Senior Risk Management Manager, SVP
(978) 656-5692
Meaghan.Lally-McGurl@ebtc.com