

Identifying Your Vulnerabilities: How to Mitigate Fraud

Presented by: Paul Zikmund

Do you need NASBA CPE credits?

- Navigate to website: iofm.cnf.io
or scan the QR code →
- Check-in and check-out of your sessions to track your attendance for NASBA CPEs
- Certified with IOFM? No need to check-in and out of sessions. Self-report CEUs on IOFM.com instead after the event!



Objectives

01

Understand the current fraud landscape and identify emerging threats in accounts payable

02

Learn advanced techniques and best practices for detecting and preventing fraud.

03

Develop strategies to enhance internal controls and improve fraud detection capabilities.

04

Explore the role of technology and data analytics in strengthening fraud prevention efforts.

Risk Landscape

Risk Landscape



AP Department as a High-Value Target: AP teams handle the payments and confidential vendor banking details that cybercriminals actively seek.



Unrelenting Phishing Epidemic: Phishing, especially sophisticated Business Email Compromise (BEC), remains the primary gateway for vendor data theft and financial fraud.



Vendor Impersonation: The Most Damaging Deception: Fraudsters exploit the trust between your company and its suppliers to change payment information and steal funds.



AI-Powered Threat Evolution: Generative AI is making phishing and impersonation attacks more convincing, personalized, and harder to detect than ever before.



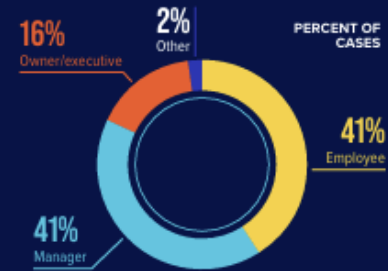
Vendor Data is the New Gold: Protecting critical PII (Personally Identifiable Information) and banking data is no longer just an IT issue—it's a massive financial and reputational risk for the entire organization.

ACFE 2026 Fraud Statistics

PROFILE OF A FRAUDSTER

LEVEL OF AUTHORITY

Most fraudsters were employees or managers, but **FRAUDS PERPETRATED BY OWNERS AND EXECUTIVES WERE THE COSTLIEST.**



TENURE

THE LONGER a fraudster has worked for an organization, **THE MORE COSTLY** their fraud.



GENDER

WOMEN committed fewer frauds and caused lower losses.



COLLUSION

FRAUDSTERS WHO COLLUDED with others caused median losses **MORE THAN 4X AS HIGH** as those who acted alone.

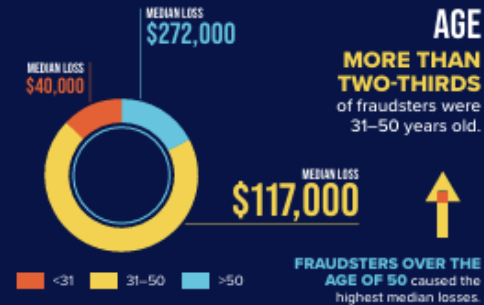


EDUCATION

MORE THAN 60% of occupational fraudsters **HAD A UNIVERSITY DEGREE OR HIGHER.**



Fraudsters **WITHOUT A DEGREE** caused **LOWER LOSSES.**

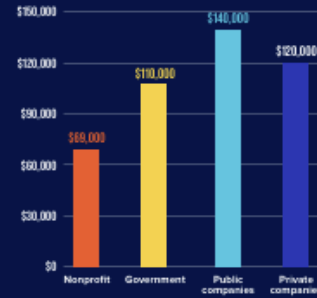


ACFE 2026 Fraud Statistics

KEY FINDINGS

VICTIM ORGANIZATIONS

MEDIAN LOSS BY ORGANIZATION TYPE

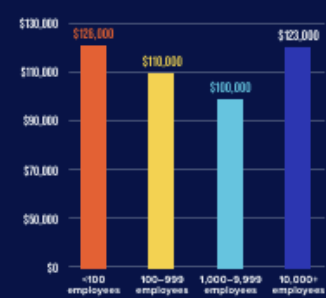


NONPROFIT ORGANIZATIONS EXPERIENCE THE **LOWEST MEDIAN LOSSES** OF ALL ORGANIZATION TYPES.



SMALL BUSINESSES EXPERIENCE THE **HIGHEST MEDIAN LOSSES** OF ALL ORGANIZATION TYPES.

MEDIAN LOSS BY ORGANIZATION SIZE



PERPETRATORS

Median losses for frauds by owners/executives were more than **9X GREATER** than those carried out by employees.



Frauds carried out by **THREE OR MORE** perpetrators caused median losses almost **6X GREATER** than those carried out by a single perpetrator.



MORE THAN HALF of all cases came from these five departments:



THE LONGER a fraudster has worked for an organization, **THE MORE COSTLY** their fraud.



84% of fraudsters displayed at least **ONE BEHAVIORAL RED FLAG**.



ANTI-FRAUD CONTROLS

The presence of anti-fraud controls is associated with

LOWER fraud losses AND **QUICKER** fraud detection



80% of victim organizations **MODIFIED** their anti-fraud controls following the fraud.

MORE THAN HALF of occupational frauds occurred due to a lack of internal controls or an override of existing internal controls.

CASE RESULTS

68% of perpetrators were terminated by their employers.

54% of cases were referred to **LAW ENFORCEMENT**.

72% of those referrals resulted in a **CONVICTION**.

Of organizations that did not refer to law enforcement:

51% cited **INTERNAL DISCIPLINE** as a reason.

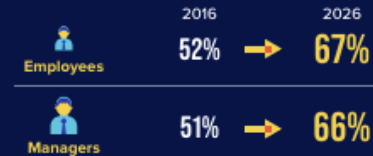
35% cited fear of **BAD PUBLICITY** as a reason.

ACFE 2026 Fraud Statistics

THE EFFECTIVENESS OF PROVIDING FRAUD AWARENESS TRAINING

Providing fraud awareness training to employees at all levels of an organization is an important component of a comprehensive fraud risk management program. Our study highlights how this type of training can help organizations detect frauds faster and reduce fraud losses.

A growing percentage of organizations are providing **FRAUD AWARENESS TRAINING** for their staff.



Organizations that have **FRAUD AWARENESS TRAINING** have lower median losses.

Training both staff-level employees and management
\$84,000 MEDIAN LOSS

Training neither
\$150,000 MEDIAN LOSS

OVER 2X MORE TIPS

Employees whose organizations provided fraud awareness training to employees were **MORE THAN 2X** as likely to submit a tip that resulted in the detection of fraud.

Employee tips with and without **FRAUD AWARENESS TRAINING**

71%
Employee whistleblowers had fraud awareness training



29%
Employee whistleblowers did not have fraud awareness training

THE IMPACT OF FRAUD AWARENESS TRAINING AT PRIVATELY HELD COMPANIES

ONLY 47% of private organizations train employees on fraud awareness.



Key Findings – 2026 AFP Report

KEY FINDINGS

Adoption of AI for fraud prevention remains limited, despite recognized benefits



Few organizations (17%) report using AI to combat payments fraud. While adoption is higher among large organizations – i.e., those with annual revenue of at least \$1 billion – most respondents cite immaturity of technology, cost and reliance on existing controls or banking partners as reasons for limited use, despite reported benefits such as improved detection and efficiency.

Business email compromise (BEC) is the most prevalent fraud vector



BEC affected 74% of organizations in 2025, representing a significant increase from 2023 and 2024. Fraudsters primarily impersonate vendors or executives to request changes to payment instructions, making email the dominant channel for payments fraud regardless of organization size. Additionally, 39% of organizations continue to receive genuine emails that have been intercepted by fraudsters.

Checks continue to be the payment method most frequently impacted by fraud



Despite declining fraud activity via their use, checks continue to be the most-often targeted method for fraud, reported by 58% of organizations in 2025 – outpacing fraud via ACH debits (30%) and wire transfers (25%). Check usage continues to be widespread; 68% of companies use checks for vendor payments because vendors require payment via checks. That is a 16% increase from 2024. Nearly three-quarters (72%) of organizations plan to continue using checks for the foreseeable future.

Treasury plays a central role in payments fraud detection, reporting and recovery



Treasury is most frequently cited as the business unit discovering both attempted fraud (83%) and actual fraud (55%), underscoring its critical risk management role in monitoring bank activity, managing controls and coordinating recovery efforts – often in close collaboration with Accounts Payable and banking/vendor partners.

Payments fraud remains widespread; over three-quarters of surveyed organizations experienced either attempted or actual fraud attacks in 2025



Payments fraud remains widespread; over three-quarters of surveyed organizations experienced either attempted or actual fraud attacks in 2025



Payments fraud impacts U.S. businesses of all revenue categories with varying consequences

Nearly half of organizations (48%) with annual revenue less than \$1 billion that experienced payments fraud in 2025 incurred a loss, and 24% of these companies were unsuccessful in recouping any funds lost. Two-thirds (66%) of larger organizations with annual revenue of at least \$1 billion faced a financial loss due to fraud, and 19% were unable to recoup funds lost.

Smaller organizations experience payments fraud less frequently, but when fraud succeeds, they are far more likely to absorb the full financial loss. While larger organizations face more frequent attacks, they recover those losses more effectively due to stronger detection, escalation and recovery infrastructure.

FBI IC3 Reports

2024

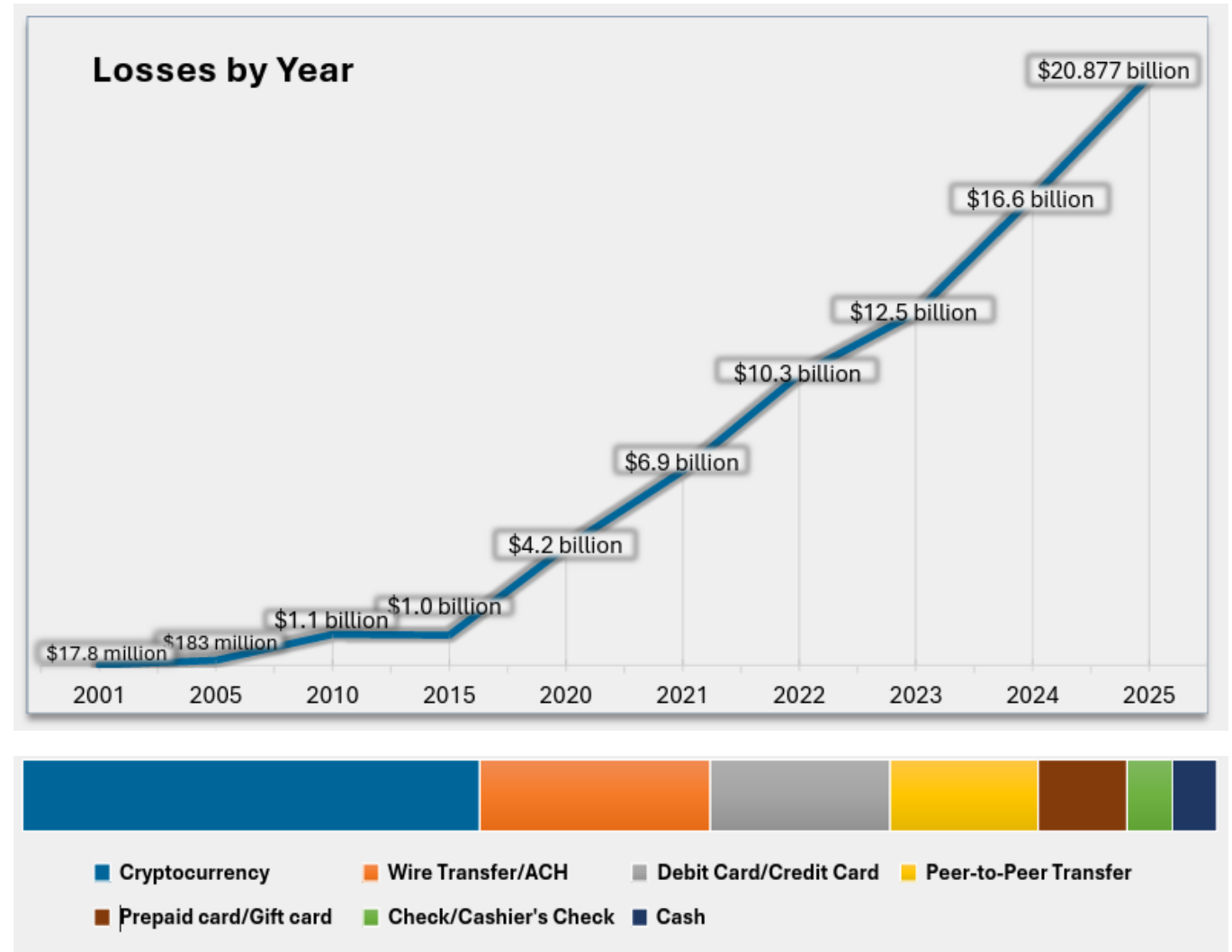


2025

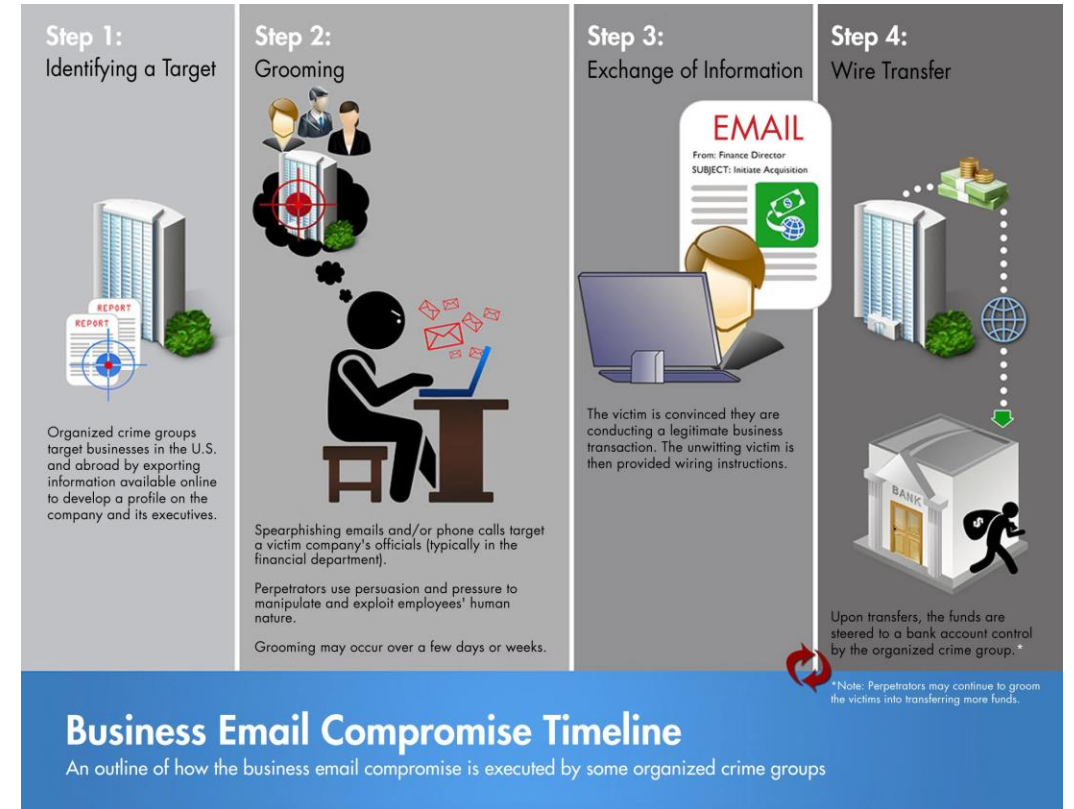


FBI 2025 IC3 Report

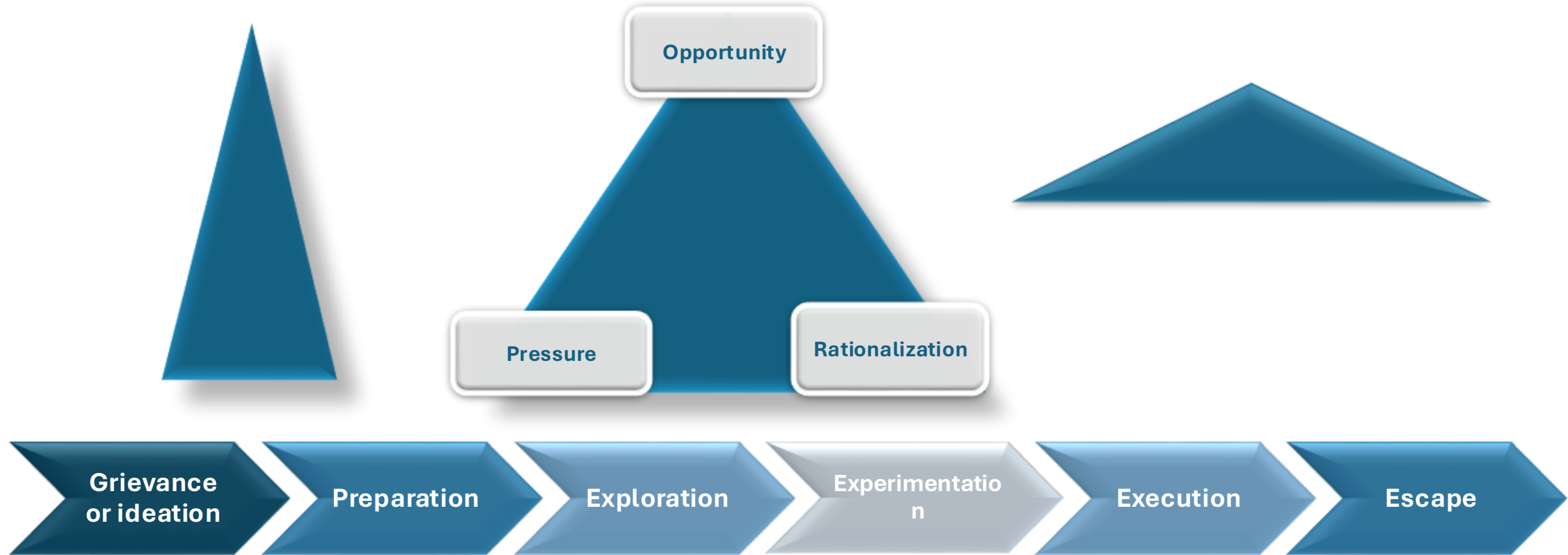
- Complaints exceeded 1 million for the first time.
- Phishing #1 ranked complaint (192,000)
- Total BEC Loss: Close to \$3.0 billion.
- Number of BEC Complaints: 24,768.
- Ranking: BEC was the second costliest cybercrime category overall in 2024.
- Included a dedicated reporting category for AI-enabled scams for the first time.
- Logged more than 22,000 AI-related complaints.
- Adjusted losses tied to AI-driven fraud surpassed \$893 million.
- Seniors (Ages 60+): Filed 201,266 complaints with losses reaching \$7.7 billion.



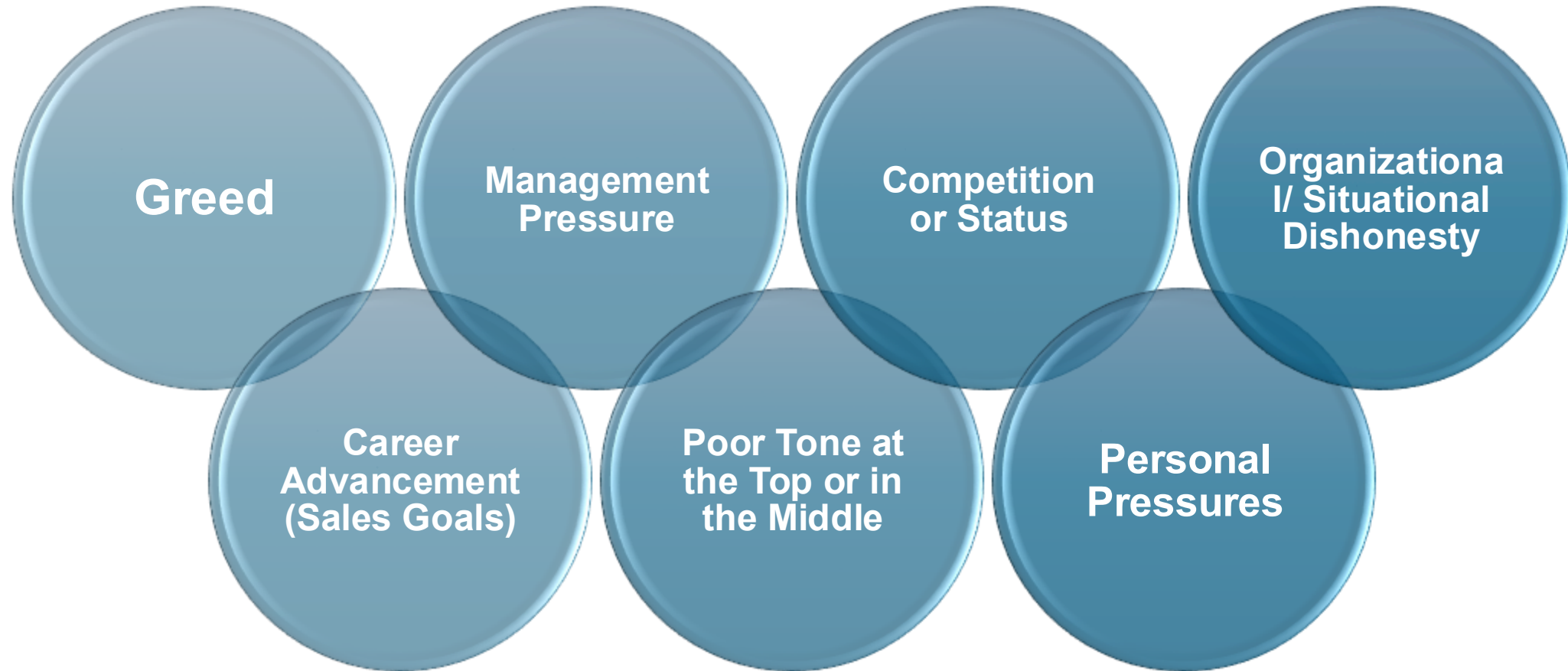
Evolution of Fraud Schemes



Why People Commit Fraud – Human Factors



What Motivates Unethical Behavior





Accounts Payable Fraud Resiliency Lifecycle

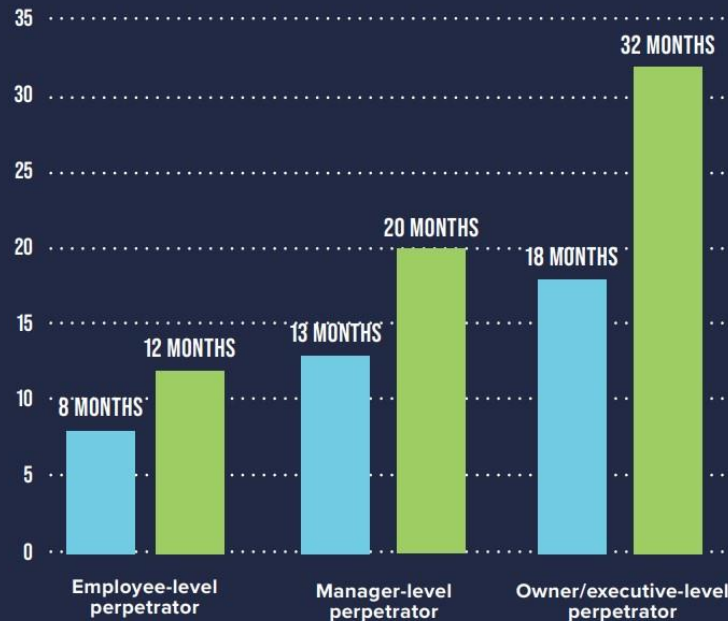
November 2026 | JW Marriott Austin | Austin, TX



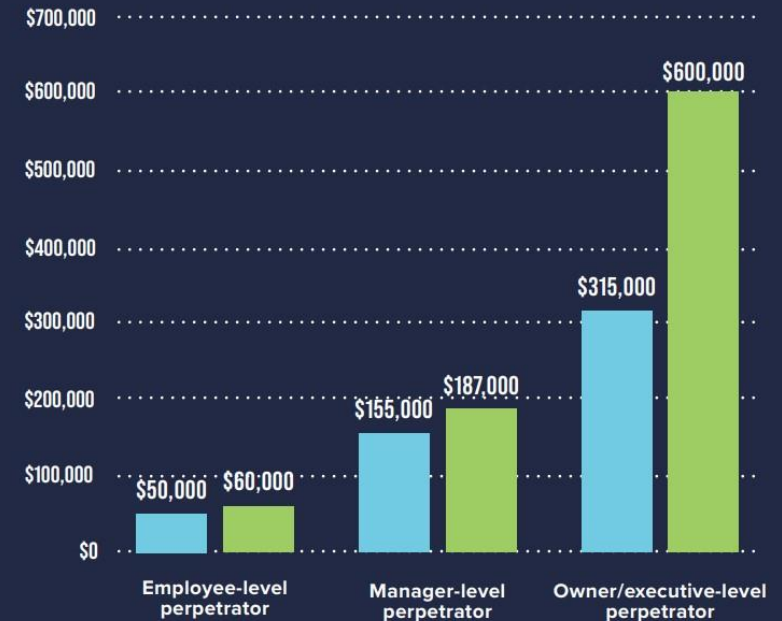
Importance of Training & Awareness Programs

Fraud awareness training for managers and executives is associated with **FASTER DETECTION AND LOWER LOSSES** in general, but the benefit is most seen when the perpetrator is at the owner/executive level

DURATION OF FRAUD WITH AND WITHOUT FRAUD AWARENESS TRAINING FOR MANAGERS/EXECUTIVES

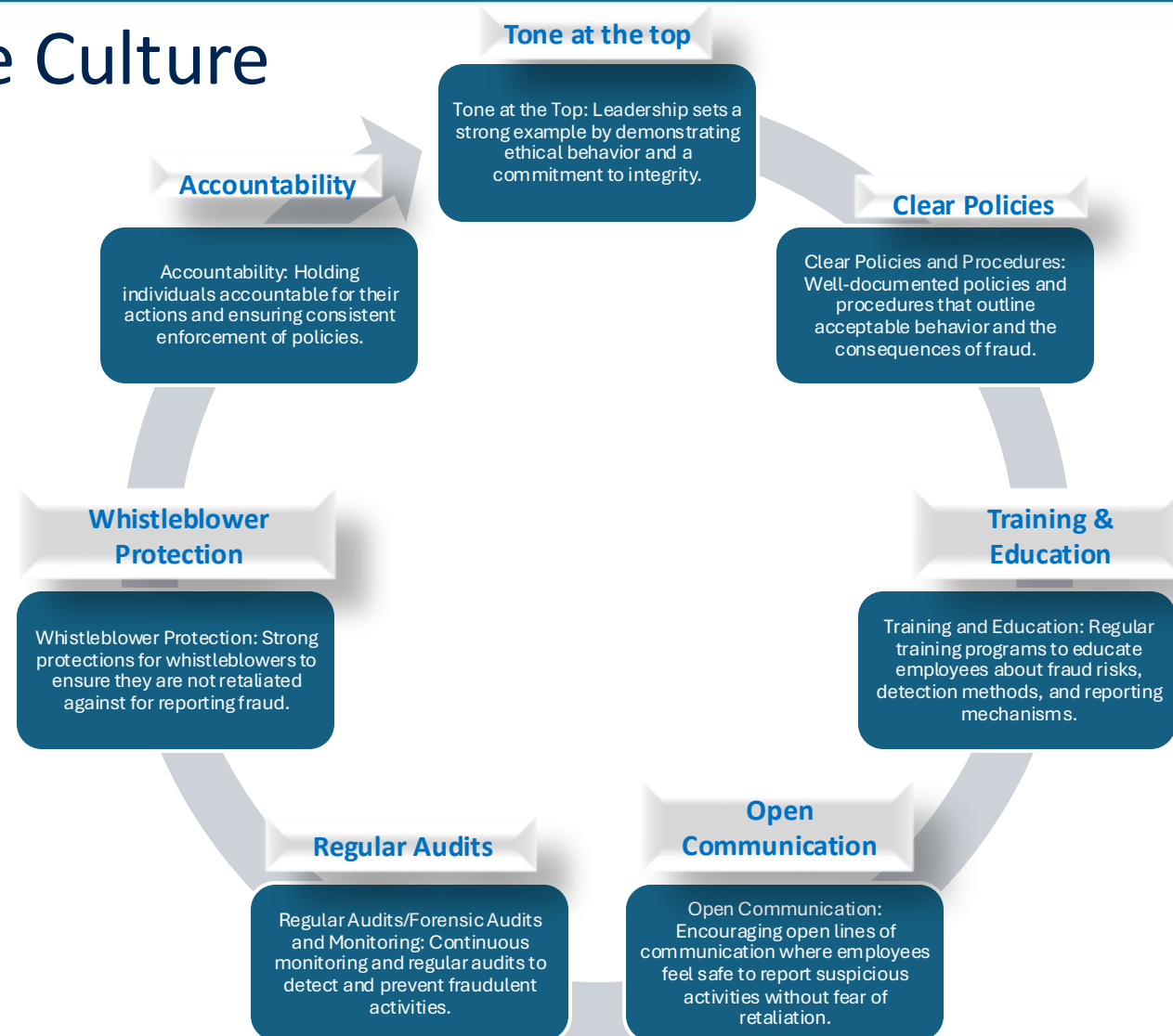


MEDIAN LOSS WITH AND WITHOUT FRAUD AWARENESS TRAINING FOR MANAGERS/EXECUTIVES

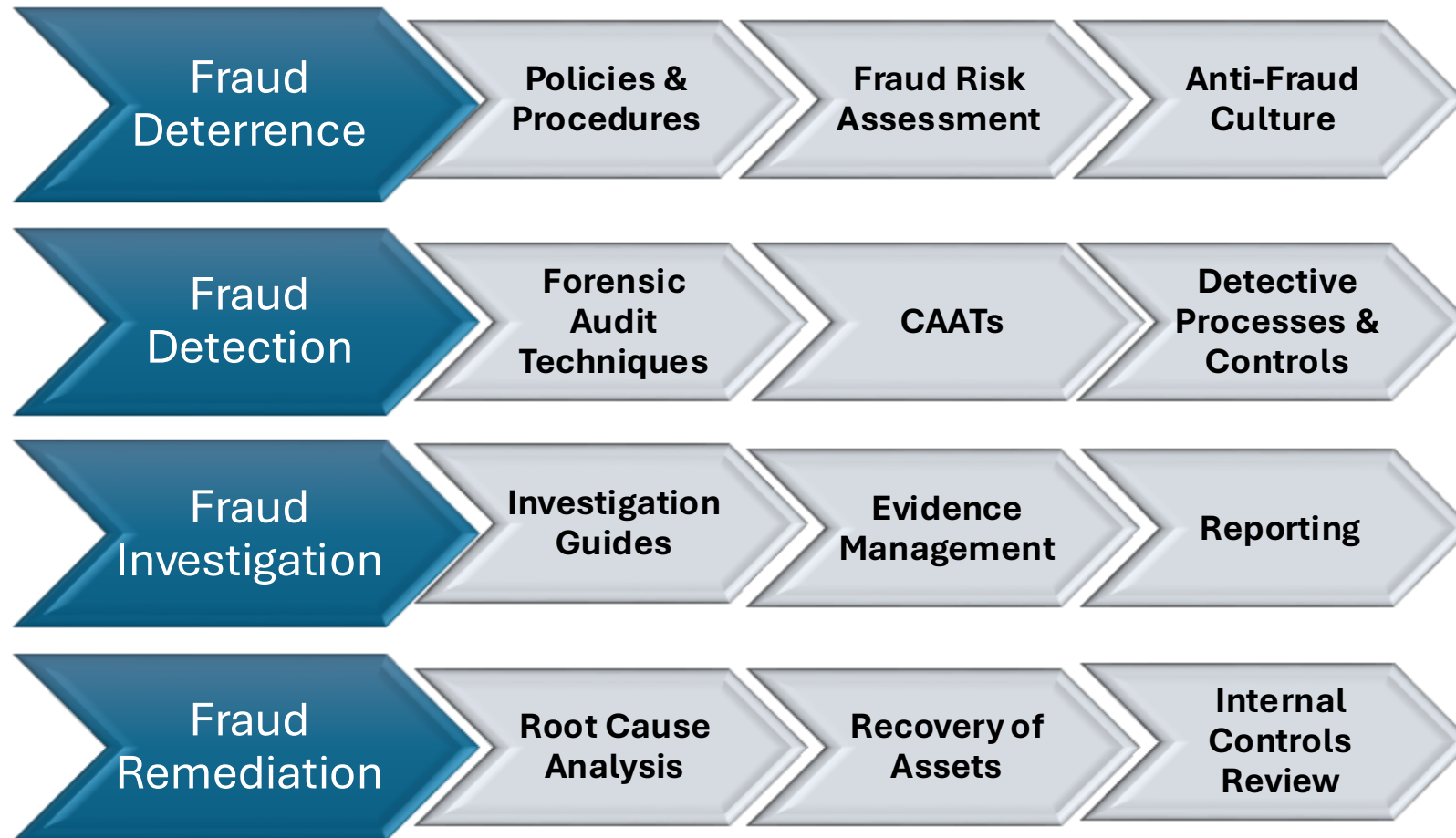


ACFE 2024 Annual Fraud Report to the Nation

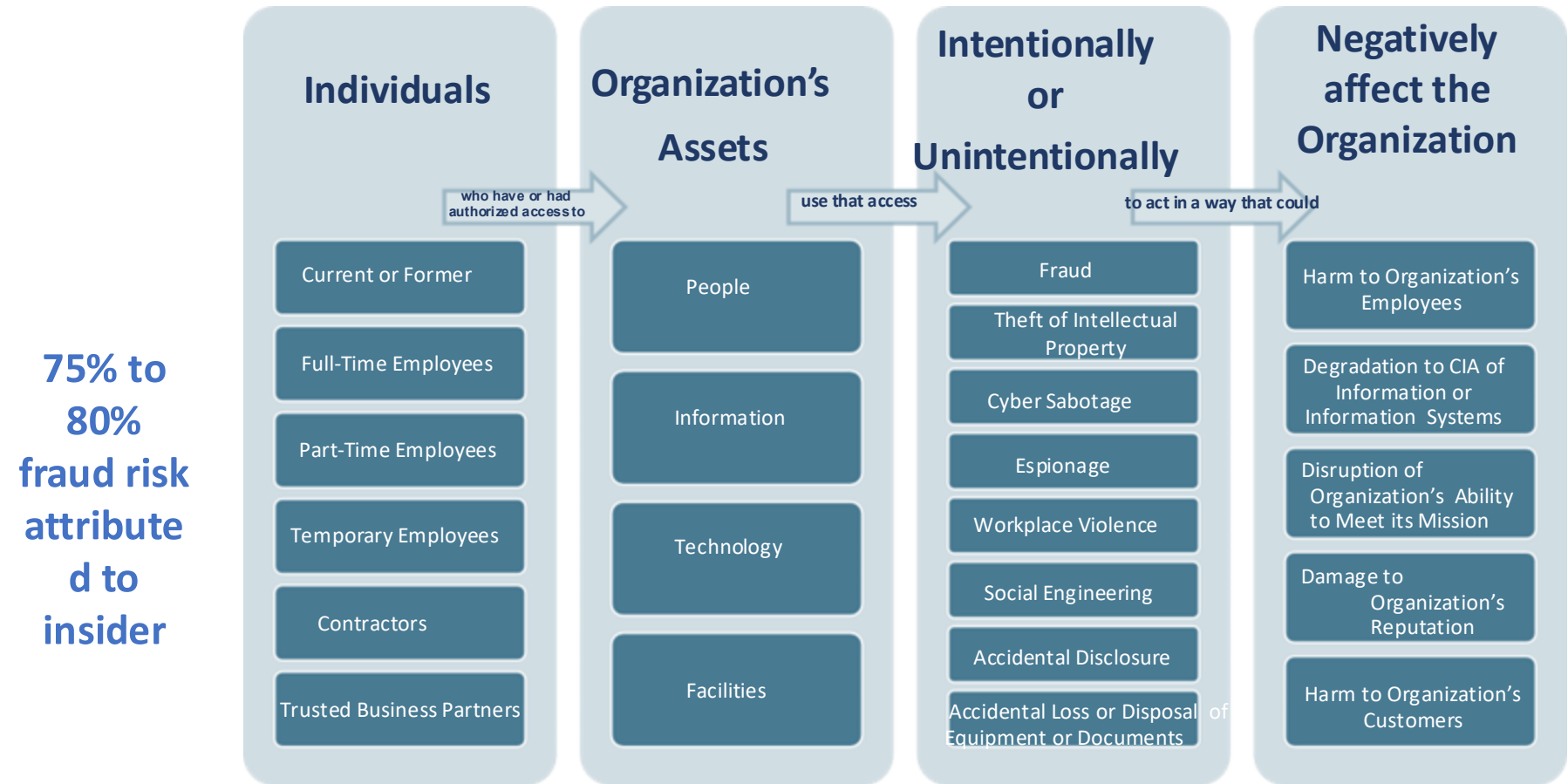
Building Fraud Aware Culture



Fraud Risk Management Programs & Controls



Insider Threat



Accounts Payable Risk Landscape

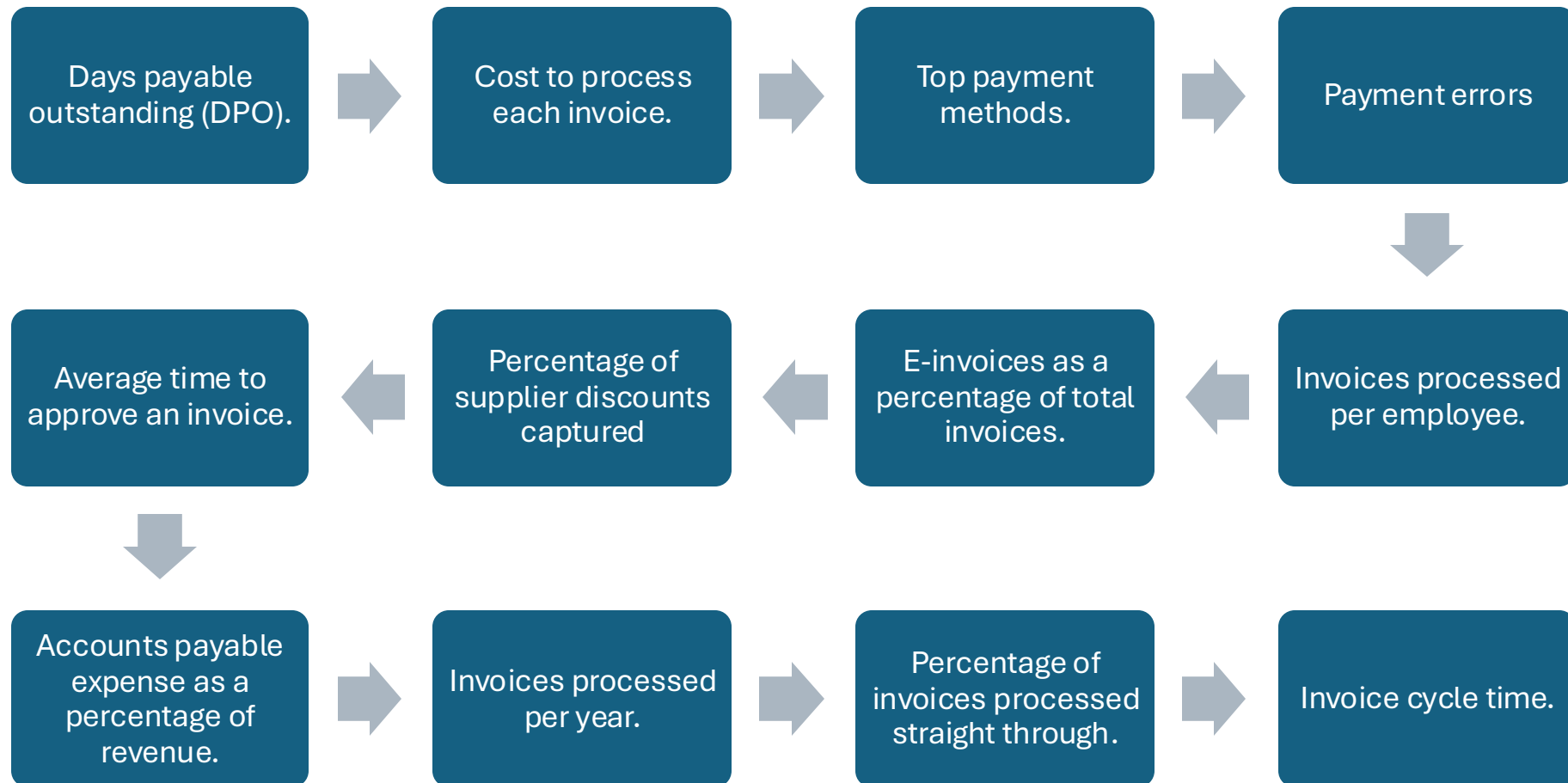
Account Payable Lifecycle



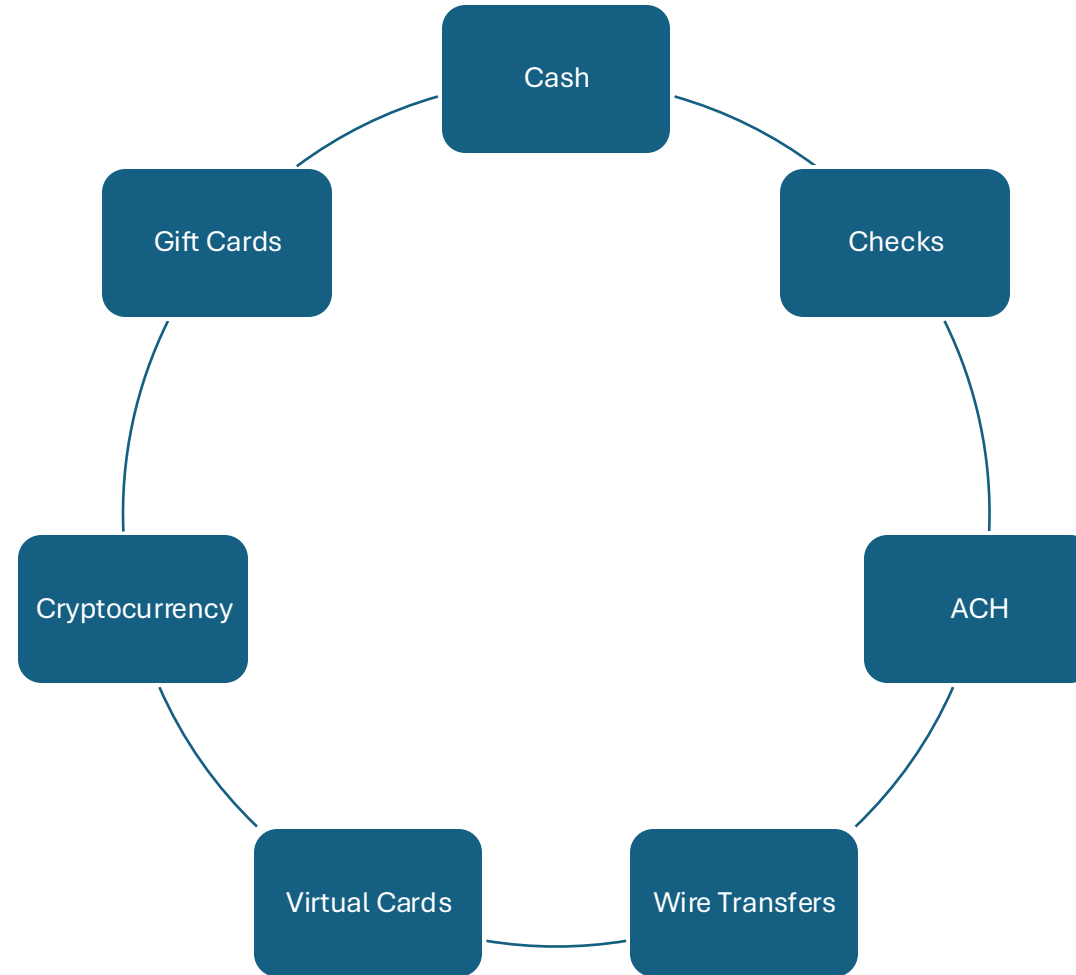
$$\text{Risk} = \text{Vulnerability} \times \text{Threat}$$



Top Accounts Payable KPIs

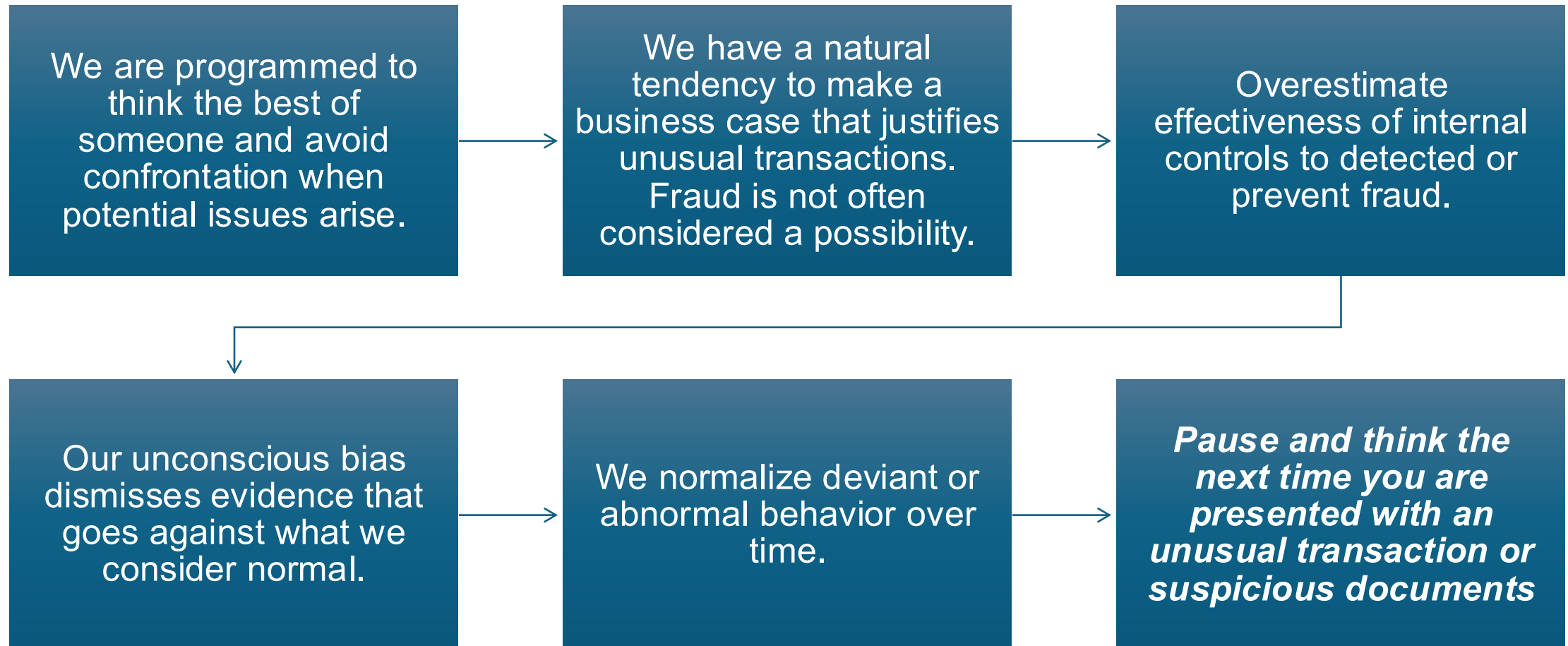


Payment Methods

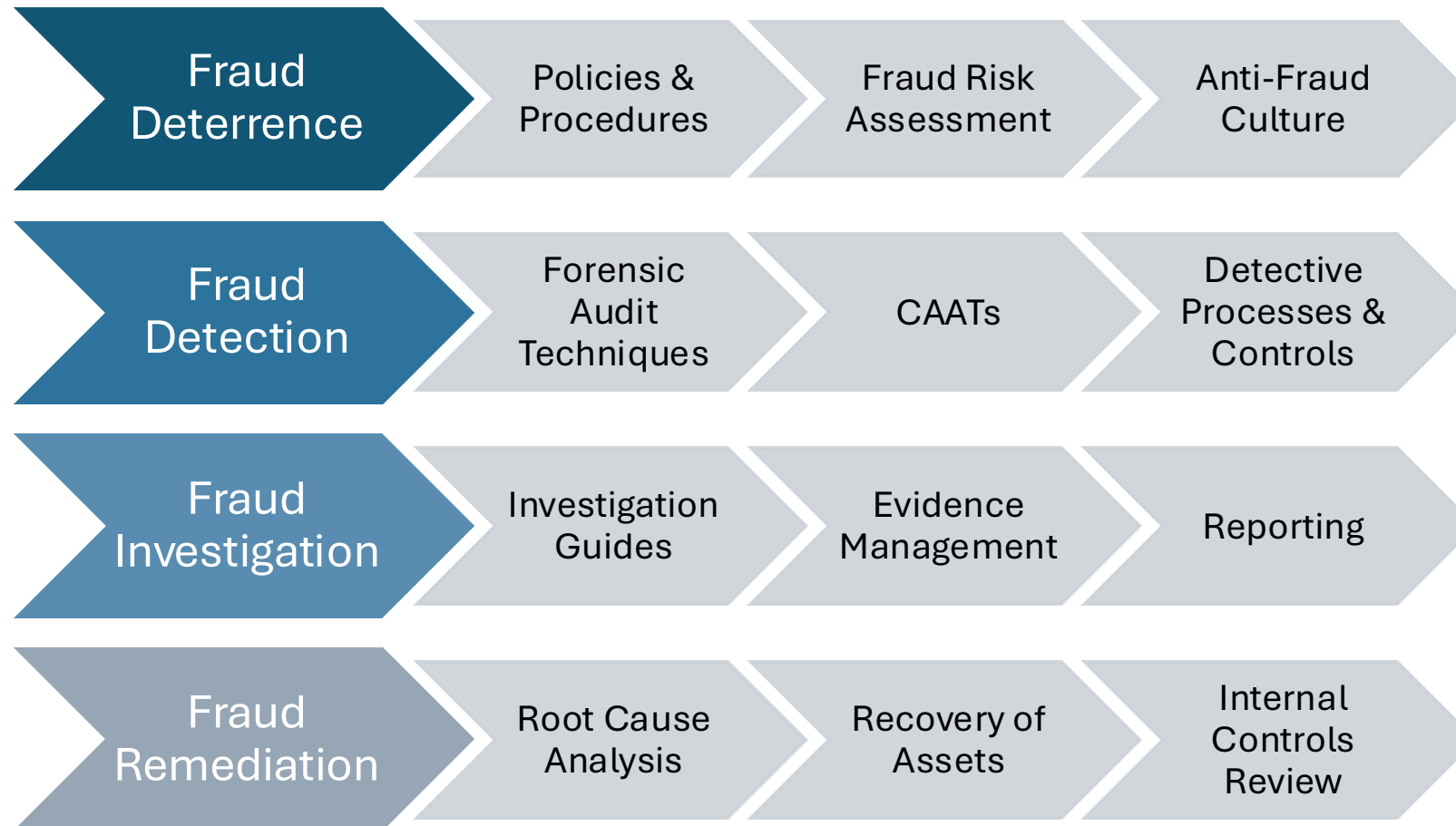


November 2026 | JW Marriott Austin | Austin, TX

Fraud Awareness and Mindset



Fraud Risk Management Process



Fraud Schemes

Accounts Payable Fraud

Internal

Overbilling or duplicate payments

Paying for goods/services not received

Fictitious vendors

Personal or disguised purchases

Financial statement fraud

Kickbacks

External

Vendor fraud

Corruption schemes

Cyber fraud

BEC schemes

Conflicts of interest

Incomplete/inferior goods or services

Accounts Payable Fraud Red Flags

Unexplained variances (increase in payables to existing or new vendors/budget variances)

Vendor complaints of non or insufficient payment

Unusual payment requests

Unfamiliar vendors

Missing or falsified documentation

Inconsistent invoices

Unusual employee behavior

Unexpected or increasing write-offs

Large one-time payment

Billing Schemes

Most common type of fraud perpetrated by the accounting department in ACFE's 2024 study. Billing schemes can take on a few different forms, including:

Setting up a shell company for which the employee can generate false invoices and cut checks. Fraudulent invoices for services companies are most common because there is no physical inventory to account for.

Pass-through schemes, in which an employee who approves invoices and authorizes payments sets up a shell company that orders things the company legitimately gets from another supplier. These items are then marked up and sold to the business through the shell company, and the employee keeps the profit.

Generating invoices from inactive suppliers in the vendor master file and writing checks to vendors the company no longer does business with.

Check Fraud - Prevention

Positive Pay:	• Implement a positive pay system where the company provides the bank with a list of checks issued.
Segregation of Duties:	• Ensure that different employees are responsible for issuing checks, reconciling bank statements, and authorizing payments to prevent any single person from having too much control.
Check Security Features:	• Use checks with advanced security features such as watermarks, microprinting, and holograms to make them harder to counterfeit.
Controlled Check Stock:	• Store blank check stock in a secure location and limit access to authorized personnel only.
Dual Signatures:	• Require dual signatures for checks above a certain amount to add an extra layer of authorization.
Regular Audits:	• Conduct regular internal and external audits to review check issuance and reconciliation processes.
Vendor Verification:	• Verify the authenticity of vendors and their banking details before issuing checks to prevent payments to fraudulent entities.
Electronic Payments:	• Encourage the use of electronic payment methods such as ACH transfers, which are generally more secure than paper checks.

Check Fraud - Detection

Bank Reconciliation:

- Perform timely and regular bank reconciliations to identify discrepancies between the company's records and the bank's records.

Check Monitoring:

- Use automated systems to monitor check activity and flag unusual transactions, such as checks issued out of sequence or to unfamiliar payees.

Fraud Detection Software:

- Implement fraud detection software that uses algorithms to identify patterns indicative of check fraud.

Employee Training:

- Train employees to recognize signs of check fraud and encourage them to report suspicious activities.

Review Check Endorsements:

- Regularly review check endorsements to ensure they match the intended payee.

Bank Alerts:

- Set up alerts with your bank for any large or unusual check transactions.

Duplicate Check Numbers:

- Monitor for duplicate check numbers, which can indicate that checks are being reused fraudulently.

Physical Inspection:

- Periodically inspect physical checks for signs of tampering, such as alterations in the payee name or amount.

ACH Fraud - Prevention

- ☐ **Dual Authorization:** Require dual authorization for initiating and approving ACH transactions, ensuring that no single individual has complete control over the process.
- ☐ **Segregation of Duties:** Separate responsibilities among different employees for initiating, approving, and reconciling ACH transactions to reduce the risk of internal fraud.
- ☐ **Vendor Verification:** Verify the authenticity of vendors and their banking details before setting up ACH payments to prevent payments to fraudulent entities.
- ☐ **ACH Blocks and Filters:** Use ACH blocks and filters to control which transactions are allowed to debit your accounts. Blocks can prevent all ACH debits, while filters allow only pre-approved transactions.
- ☐ **Secure Banking Platforms:** Use secure, encrypted banking platforms for initiating ACH transactions to protect against cyber threats.
- ☐ **Employee Training:** Train employees on the risks of ACH fraud and best practices for secure transaction processing, including recognizing phishing attempts and other social engineering tactics.
- ☐ **Strong Password Policies:** Implement strong password policies and multi-factor authentication (MFA) for accessing banking systems to prevent unauthorized access.
- ☐ **Regular Audits:** Conduct regular internal and external audits of ACH processes and transactions to identify and address vulnerabilities.

ACH Fraud - Detection

Transaction Monitoring:

- Use automated systems to monitor ACH transactions in real-time and flag unusual or suspicious activities, such as transactions to new or unrecognized accounts.

Daily Reconciliation:

- Perform daily reconciliations of ACH transactions to quickly identify and investigate discrepancies between the company's records and bank statements.

Bank Alerts:

- Set up alerts with your bank for any large or unusual ACH transactions, including notifications for transactions above a certain threshold.

Fraud Detection Software:

- Implement fraud detection software that uses algorithms to identify patterns indicative of ACH fraud.

Review ACH Reports:

- Regularly review ACH transaction reports provided by your bank to ensure all transactions are legitimate and authorized.

Account Activity Review:

- Periodically review account activity for any unauthorized or unusual transactions, especially those involving new or infrequent payees.

Positive Pay for ACH:

- Use ACH positive pay services where the company provides the bank with a list of authorized ACH transactions, and the bank matches incoming transactions against this list.

Vendor and Employee Education:

- Educate vendors and employees about ACH fraud risks and encourage them to report any suspicious activities or requests for banking information.

Weaponization of AI

76% of Organizations: According to the 2026 AFP Payments Fraud and Control Survey, over three-quarters of U.S. firms experienced attempted or actual payments fraud in 2025.

The Median Loss: Recent data from Q1 2026 shows that the median loss for a single digital fraud incident has climbed to \$2,307, though Business Email Compromise (BEC) events in the enterprise space often average \$120,000+ per successful heist.

Volume Spike: Phishing attacks reached a record high in early 2025 driven largely by automated AI tools.

184-Day Dwell Time: Fraudsters now remain undetected in standard AP systems for over 6 months, using that time to map out executive approval patterns before striking.

61% Mid-Market Targeting: Smaller and mid-sized firms are increasingly the primary targets due to a perceived "Security Maturity Gap" compared to large enterprises.

90% of Attacks: Cyber-defense data confirms that approximately 90% of successful breaches begin with AI-enhanced phishing or spoofing.

The Sophistication Gap: Fraudsters are now using Generative AI to create "Synthetic Invoices" and Deepfake audio overrides. 1 in 6 consumers and businesses reported losing money to these increasingly precise, AI-driven scams in the past year.

Speed of Attack: Criminals can now generate thousands of unique, personalized fraudulent emails in seconds—a task that previously took weeks of manual "social engineering."

Fraud Detection with AI



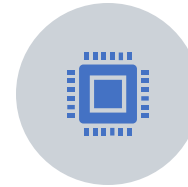
Anomaly detection: AI can analyze large volumes of transaction data to identify unusual patterns or anomalies that may indicate fraudulent activity such as duplicate payments, payments to unknown vendors, or transactions that deviate from the norm



Predictive analytics: machine learning algorithms can predict potential fraud by learning from historical data and identifying risk factors.



Automated invoice processing: AI can automate the verification of invoices against purchase orders and receiving reports, reducing the risk of human error and fraud.



Real-time monitoring: AI systems can provide real-time monitoring and alerts for suspicious transactions or changes to vendor details, enabling immediate investigation and response.



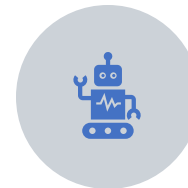
Behavioral analysis: AI can track and analyze user behavior to detect deviations from normal activity, which may signal fraudulent intent such as unusual access to financial systems or irregularities in transaction approvals



Natural language processing (NLP): NLP can be used to analyze email communications and detect phishing attempts or fraudulent requests.



Fraud scoring: AI can assign fraud risk scores to transactions based on various factors, helping prioritize investigations.



Continuous learning: AI systems can continuously learn and adapt to new fraud tactics, improving their detection capabilities over time.

Detecting Accounts Payable Fraud

Anomalies such as invoice cloning, approval threshold manipulation, and vendor impersonation

- Model used fuzzy matching to compare invoice metadata (amount, vendor, line items) and detect duplicates or near-duplicates.
- Historical data trained the algorithm to understand normal vs. suspicious submission patterns.
- Invoices from the same vendor with nearly identical line items but different invoice numbers.
- Invoices submitted at irregular times (e.g., weekends or holidays).
- Same invoice amounts appearing across different business units.

Approval threshold manipulation

- Models trained to understand standard invoice patterns and detect repeated sub-threshold amounts submitted within a short time frame.
- Time-series analysis applied to track when multiple low-value invoices were submitted from the same vendor.
- Multiple invoices just below a key threshold (e.g., \$9,950 when approval is needed for \$10,000+).
- Several low-value invoices submitted within days of each other for the same project or purchase order.
- Invoices approved by the same employee without escalating to a second approver.

Vendor Behavior Analysis

Profile vendor behavior
(e.g., frequency of
invoicing, invoice size,
delivery timing)

Detect anomalies like
abrupt cost increases,
duplicate charges, or
invoice splitting

Assign dynamic fraud
risk scores to each
vendor

Vendor invoice trends
and compare them to
historical norms

Changes in vendor data
like bank accounts or
service types

Patterns in timing (e.g.,
end-of-quarter invoice
spikes)

Monitor vendor
behavioral shifts (new
banking info, abrupt
cost changes)

Detect deviations in
invoice frequency and
category

Build vendor risk
profiles based on
historical behavior and
contract delivery
patterns

Flag suspicious
activities like repeated
change orders, billing
above market rates, and
vendor clustering

Monitor for deviations
from expected invoice
timing, pricing, and
volume

Detect relationships
between vendors and
internal staff (conflict of
interest)

Alert finance teams to
high-risk vendor
behavior in real time

Tools

Spend Auditor

- Tool: AppZen
- The AI Edge: It uses Computer Vision and NLP to "read" an invoice like a human would, but at scale. It doesn't just look at the numbers; it checks the vendor's website, regulatory filings, and even news reports to see if the company is legitimate.
- ROI Factor: Drastic reduction in "Audit Cycle Time." Instead of humans auditing 10% of invoices, the AI audits 100% in seconds, allowing the team to only touch the "high-risk" 1%.

Fraud Prevention

- Tool: Tipalti
- The AI Edge: It specializes in Payee Intelligence. Before a payment is even processed, its AI checks the recipient against 26,000+ global watchlists (OFAC, SDN, etc.) and uses "Frictionless Onboarding" to validate bank details in real-time.
- ROI Factor: Avoidance of massive regulatory fines and "payment error" losses that occur when dealing with complex international currency and tax regulations.

Tools

Behavioral Analyst

- Tool: Oversight Systems
- The AI Edge: This tool looks for Collusion Patterns. It analyzes the relationship between the person who created the vendor, the person who approved the invoice, and the person who authorized the payment. It flags "Split Purchases" (breaking a \$10k invoice into four \$2,500 chunks to avoid approval workflows).
- ROI Factor: Detecting "Theft of Opportunity" by employees and high-risk vendors that traditional systems ignore.

Duplicate Detective

- Tool: FISPLAN or Directly Integrated ERP AI (e.g., SAP Cash Application)
- The AI Edge: It catches "Fuzzy Duplicates." A rule-based system catches Invoice #123 and Invoice #123. AI catches Invoice #123-A, Invoice #l23 (using an 'l' instead of '1'), and the same invoice submitted twice with slightly different dates.
- ROI Factor: Direct "Hard Dollar" recovery. For a company with \$500M in spend, even a 0.1% duplicate rate is \$500,000 in found cash.

Challenges

High volume: "we have too many invoices to look at."

Global complexity: "we pay people in 20 countries and it's a mess."

Accuracy/duplicate issues: "we keep paying the same thing twice."

Compliance/audit: "our internal auditors are always finding errors after the fact."

Data management: "our data is everywhere and we cannot get IT to assist us."

Knowledge gap: "we do not have the required SMEs to implement AI solutions"

ROI: "we have not been able to demonstrate the ROI for these investments in AI"

Data overload: "we are unable to effectively manage the overwhelming number of alerts"

Applications

Fraud Prevention and Anomaly Detection

- Traditional systems look for exact duplicates. AI looks for behavioral anomalies.
- Example: An AI system flags a sudden change in a long-term vendor's bank account details. It cross-references this with global databases to determine if the change matches known "business email compromise" patterns before the payment is processed.

Dynamic Approval Routing

- Instead of rigid "if-then" rules, AI learns the organizational structure and behavior.
- Example: If an invoice is coded to "Marketing" but exceeds a specific budget threshold for that quarter, the AI automatically reroutes the approval to the CFO instead of the Department Manager, proactively enforcing compliance.

Global Compliance (E-Invoicing)

- With 2026 seeing a surge in global e-invoicing mandates (like ViDA in Europe), AI is used as a "compliance gatekeeper."
- Example: A company operating in France or Poland uses AI to automatically format and validate outgoing and incoming invoices to ensure they meet specific government XML standards (e.g., Peppol), avoiding heavy non-compliance fines.

Supplier Sentiment and Inquiry Management

- Example: Using Generative AI, companies like Adyen or Billerud have implemented AI "agents" that monitor AP email inboxes. These agents answer 80% of supplier questions regarding "When will I be paid?" by looking up the real-time status in the ERP and responding in natural language.

Red Team/Blue Team Exercise

- Your group is a sophisticated criminal syndicate. You have three pieces of information: the name of a real vendor your company uses, the name of your Controller, and the fact that your company is currently undergoing a busy software migration. How do you steal \$50,000 without triggering a basic 'rules-based' alert?
- Scenarios to Consider:
 - The Velocity Attack: Submitting 20 small invoices just under the approval threshold.
 - The Identity Pivot: Sending a bank change request from a domain that is one letter off (e.g., @vendor-inc.com vs. @vend0r-inc.com).
 - The Social Engineer: Using a Deepfake audio clip or "Urgent" email from an executive to bypass standard PO matching.
 - Other examples

Preventing Fraud

Segregation of Duties:

Ensure that different employees handle invoice approval, payment processing, and account reconciliation.

Vendor Management:

Maintain a vetted and approved vendor list, and regularly review and update vendor information.

Authentication, Validation and Management**Invoice Verification:**

Implement a three-way match process to verify that purchase orders, receiving reports, and vendor invoices align before payment.

Approval Workflows:

Establish clear approval hierarchies and require multiple levels of authorization for large or unusual transactions.

Regular Audits: Conduct periodic internal and external audits to identify and address discrepancies or irregularities.

Automated Systems: Use accounts payable automation software to enhance accuracy, track transactions, and flag suspicious activities.

Employee Training:

Educate employees on fraud risks and detection techniques, and encourage them to report suspicious activities.

Fraud Detection Tools:

Implement data analytics and monitoring tools to detect patterns indicative of fraud.

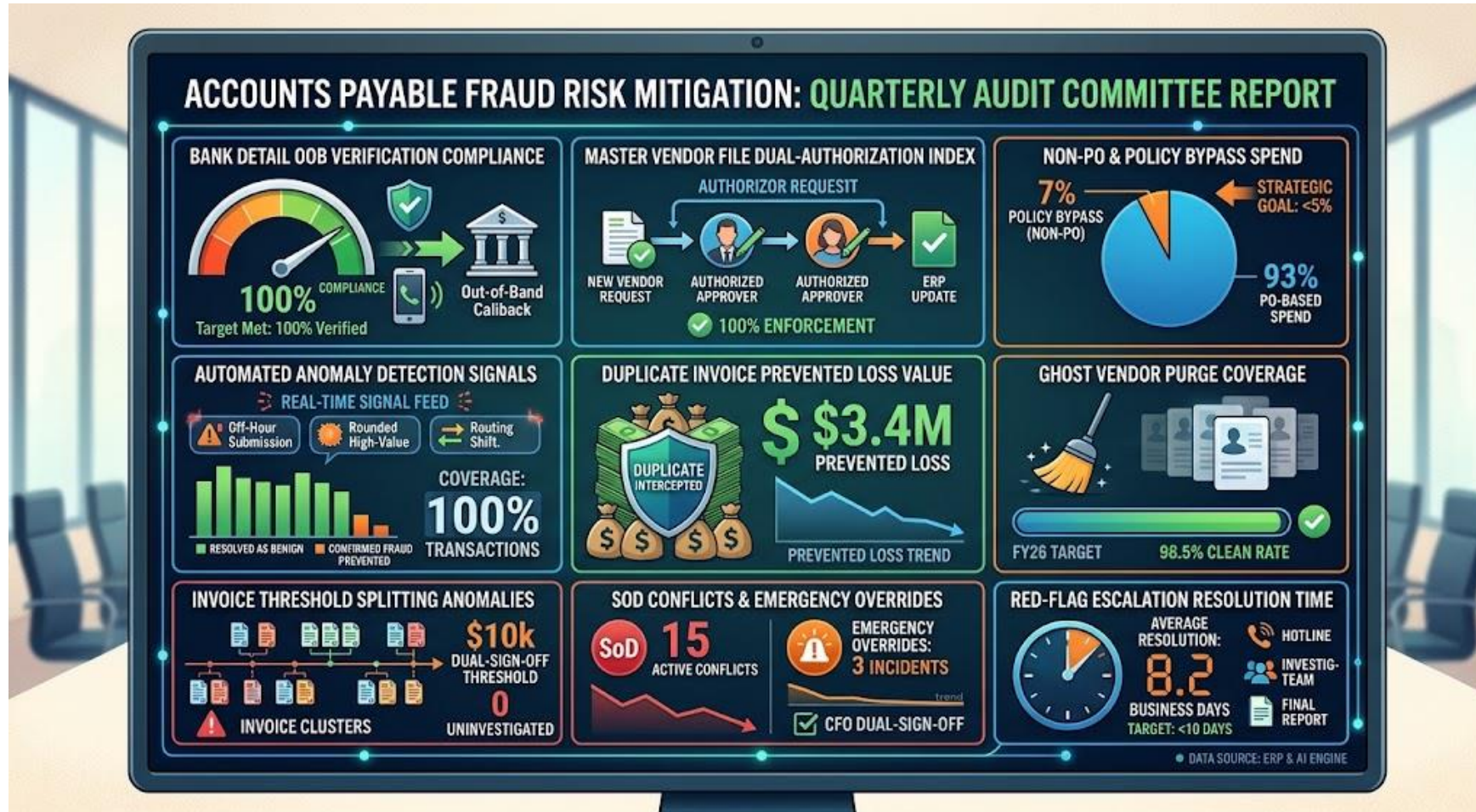
Whistleblower Hotline:

Provide a confidential reporting mechanism for employees to report suspected fraud without fear of retaliation.

Policy Enforcement:

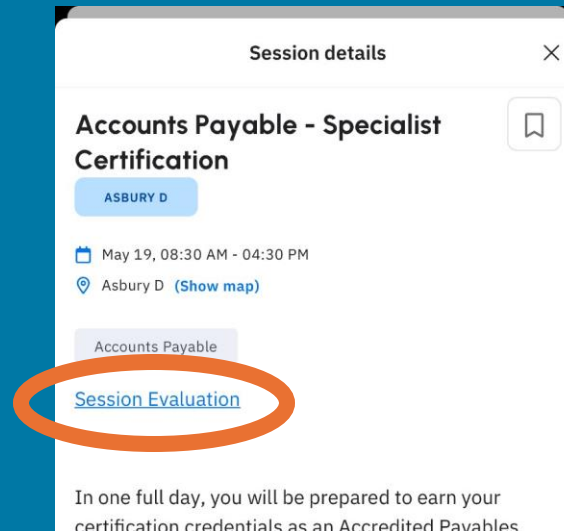
Develop and enforce comprehensive policies and procedures for accounts payable processes.

Management Reporting



Please tell us what you think!

- Please scan this QR code using your mobile to access a short feedback survey →
- Also accessible via the mobile app



QUESTIONS?

Paul Zikmund

REMINDER!

If you checked in for NASBA CPE credit, check out at iofm.cnf.io