Fraud Detection & Investigation Techniques

Paul e. Zikmund

Chief Resiliency Officer

Berkadia

IOFM Fall
CONFERENCE & EXPO

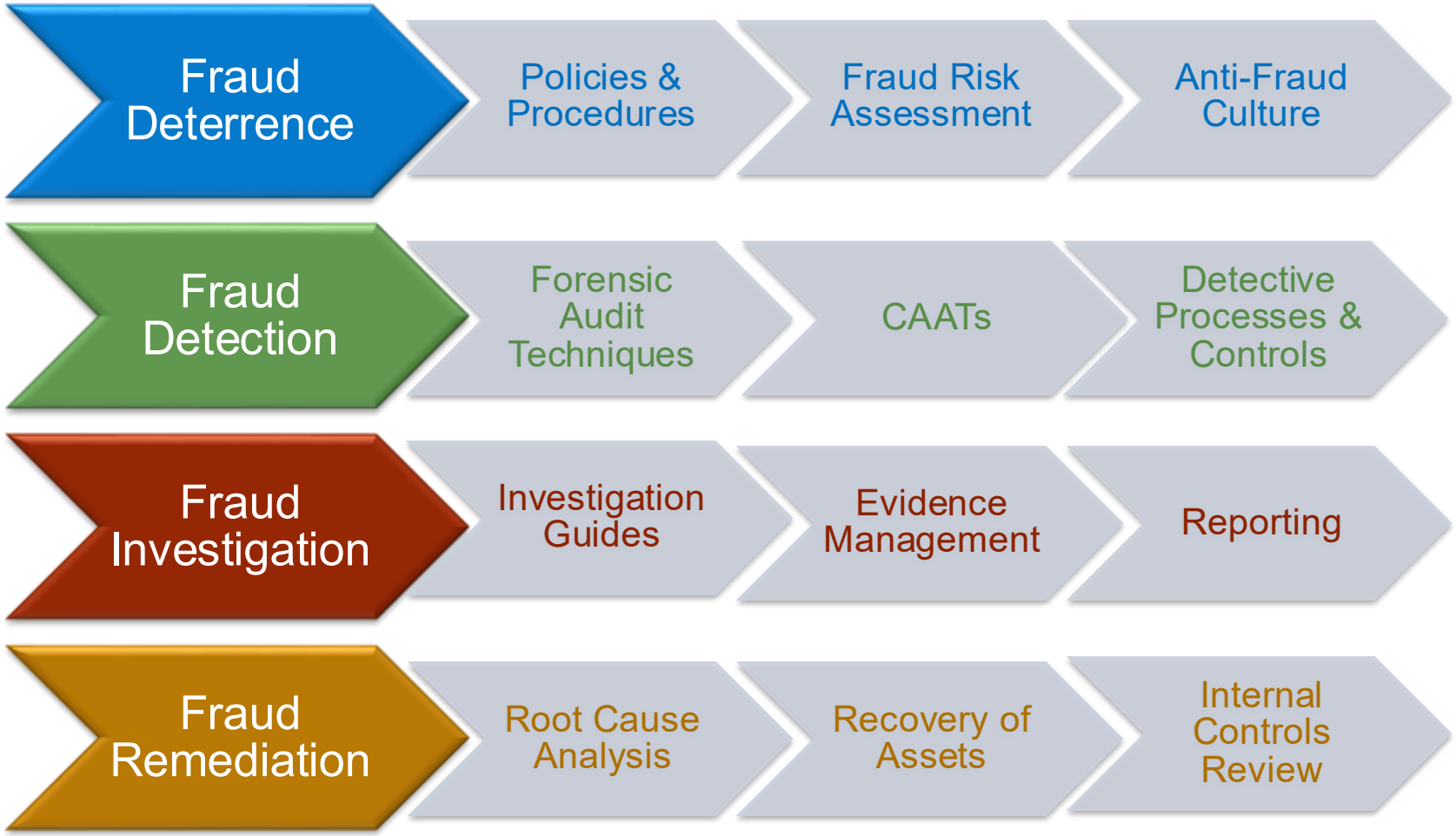
Agenda

- Understand Fraud Dynamics:
- Investigation Risks:
- Building an Internal Fraud Response Process:
- Conducting Investigations:
- Evidence:

Fraud Management Process

IOFM Fall
CONFERENCE & EXPO

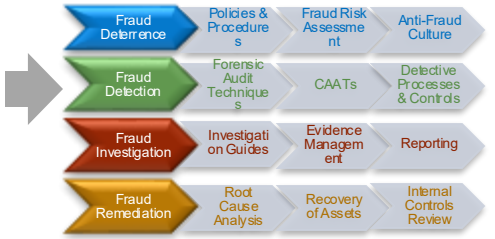
Fraud Risk Management Process



Fraud Deterrence Sub-Process

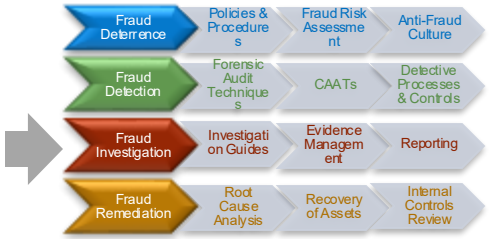
Policies & Procedures	Code of Conduct	Fraud Response Policies	Human Resources Policies
Fraud Risk Assessment	Identify Fraud Risk Factors	Define Fraud Schemes & Scenarios	Determine Residual Fraud Risk
Anti-Fraud Culture	Whistleblower Hotline	Control Environment	Employee Surveys

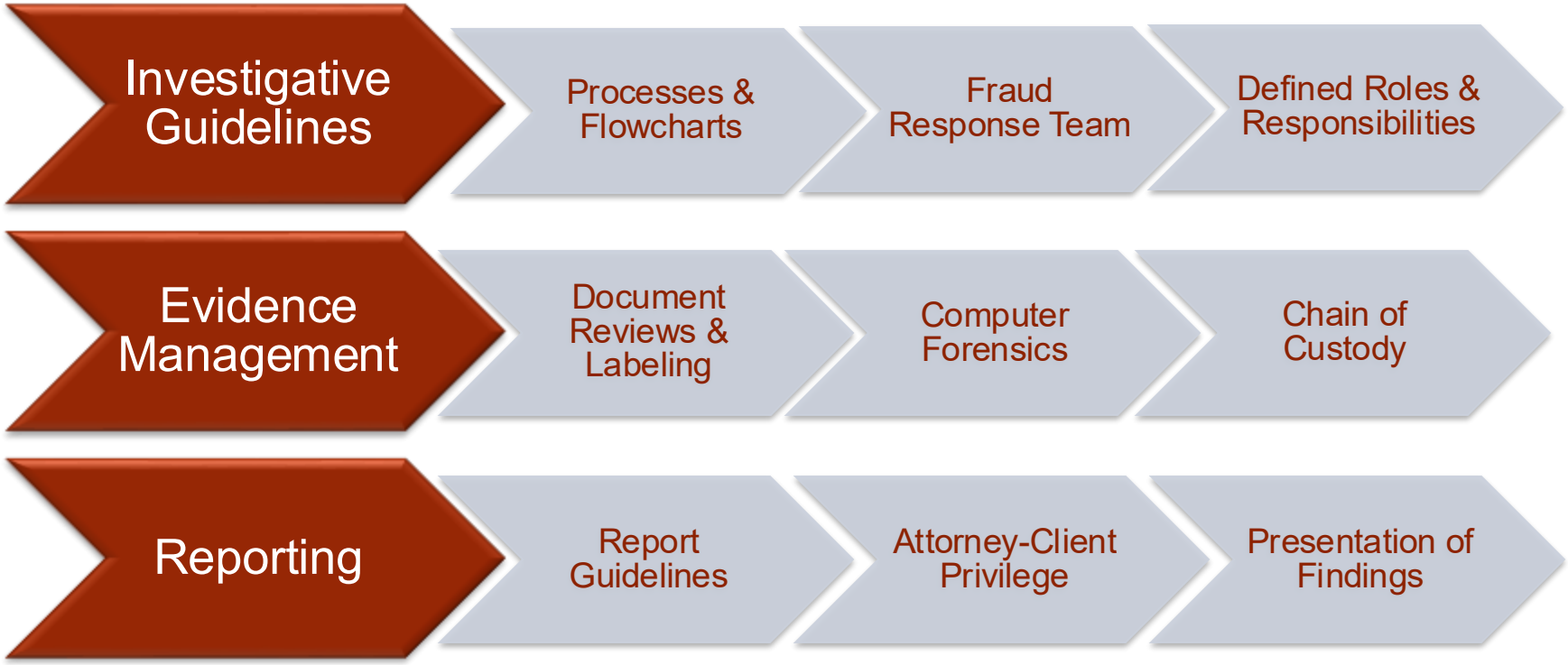
Fraud Detection Sub-Process



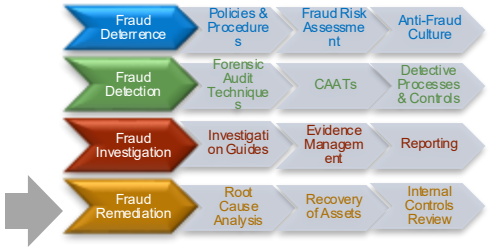
Forensic Audit Techniques	Analytical Procedures	Interviewing	Analysis of Financial Transactions
CAATs	ACL / IDEA software	Continuous Controls Monitoring	Event-Driven CAATs
Detective Controls	Segregation of Duties	Monitoring & IT Controls	Safeguarding Company Assets

Fraud Investigation Sub-Process





Fraud Remediation Sub-Process

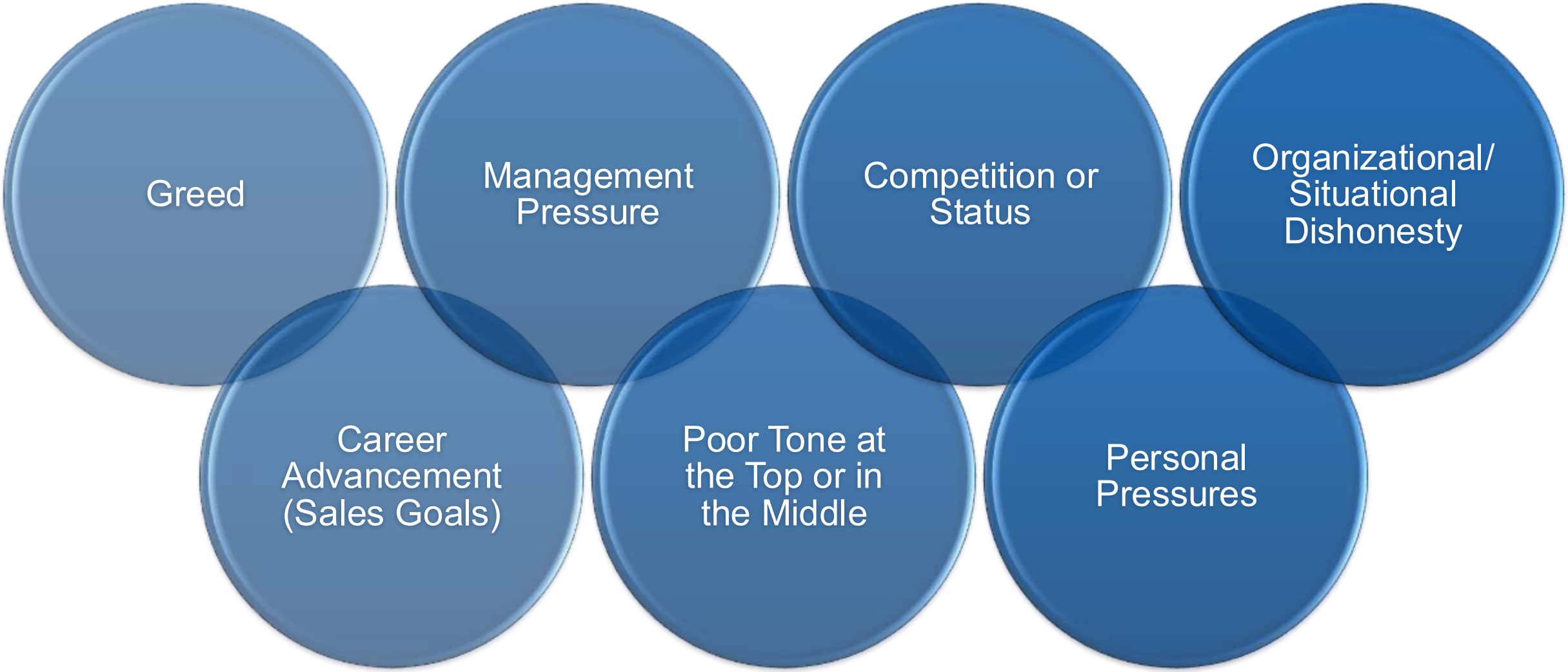


Root Cause Analysis	Internal Controls Review	Issues Tracking System	Management Accountability Program
Recovery of Assets	Civil / Criminal Action	Disciplinary Action	Insurance Claims
Information & Communication	Awareness Programs	Policy & Procedure Updates	Surveys & Certification Programs

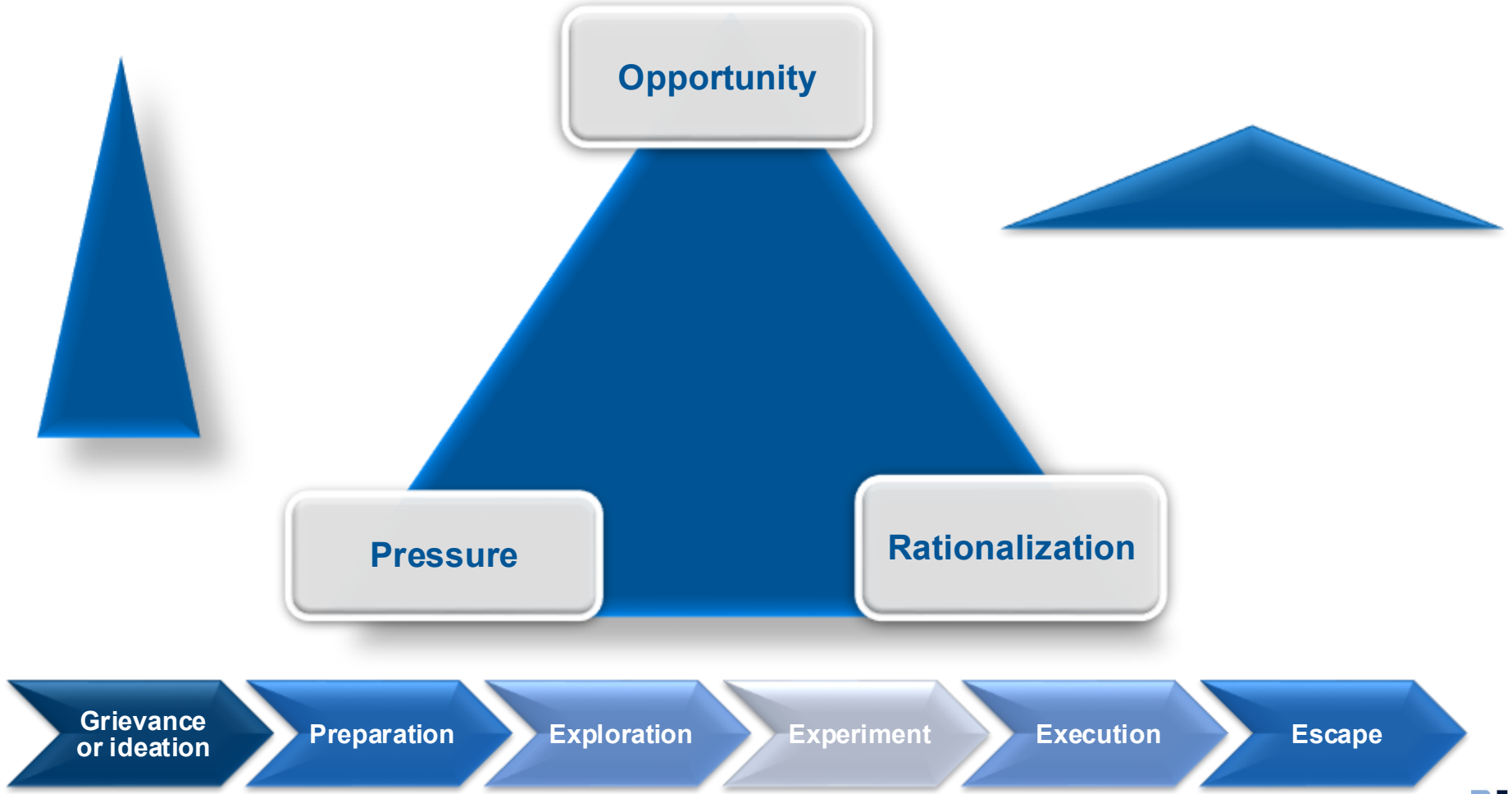
Psychology of Fraud

IOFM Fall
CONFERENCE & EXPO

What Motivates Unethical Behavior



Why People Commit Fraud – Human Factors



Type of Fraudster

Investigating Fraud

IOFM Fall
CONFERENCE & EXPO

Benefits of an Effective Investigation Process

- Obtain information quickly for decision makers
- Resolve potential Code and Legal violations systematically
- Promote a robust “Speak Up” culture
- Improve ethics and compliance program
- Reveal misconduct that violates the law and/or corporate policy
- Avoid adverse publicity
- Minimize cost of litigation
- Limit corporate, officer or director liability
- Deter incidents of future misconduct
- Avoid future loss or reputational damage
- Punish wrongdoers
- Promote achievement of company goals & objectives
- Appease company stakeholders
- Satisfy Government requirements – Yates Memo

Stakeholders

Stakeholders

Investigations Framework

Effective

Ethical

Lawful

Produces desired outcomes

Minimally disruptive to business operations

Minimize impact to the organization

Resolves allegation of misconduct and affords opportunity to remediation efforts

Value added

Inherent Risks of Investigations

- Expensive and uncertain results
- Legal liability –
  - Failure to protect privilege
  - Discrimination (employer did not conduct a proper investigation)
  - Defamation
  - Violation of privacy (Video surveillance, email reviews)
  - False imprisonment (detain against a person's free will)
  - Union requirements
- Uncover significant information
- Stimulate disgruntled employees & angst
- Adverse publicity
- Preoccupied resources
- Business disruptions

Threats to Investigations

- Rapidly changing technology
- More litigious society
- Expanded employee rights
- Increasingly sophisticated fraudsters
- Limited resources and time
- Cost
- Governmental involvement
- Inconsistent processes
- Lack of ownership by function or department
- Failing to adhere to a fact-based approach

Reducing the Risk

- Assign trained personnel
- Follow your policies and guidelines
- Know the laws and regulations
- Coordinate with other functions
- Ensure proper review of all work product and reports
- Seek experts when needed
- Continuous updates to senior management
- Communicate expectations
- Seek proper buy-in & support from executive leadership

Phases of an Investigation

Assessment

- Nature of allegation (background and understanding of issue)
- Potential criminal misconduct or violations of regulatory requirements
- Attorney client privilege?
- Company policy violation(s)
- Legal liability
- Is an investigation required?
  - Preliminary inquiry can be conducted to determine whether or not there is sufficient evidence to launch investigation.
  - The decision not to investigate should NEVER be made to avoid learning the truth
  - Outside counsel shows independence & avoids appearance of “sweeping it under the rug” if decision not to investigate is made (do not want to create future controversies)

Planning

- Establish investigation team
- Background and understanding
- Gathering information
- Resource requirements
- Coordinating team responsibilities – team lead
- Evidence requirements
  - location
  - # sites
  - type
- Identify a project manager – team leader
- Communication protocol – need to know list
- Activate fraud response plan
- Attorney client privilege ? (yes or no)
- Company policies
- Related laws and regulations
- Crisis management plan?
- Travel & logistics

Attorney Client Privilege

- Should investigation be conducted under attorney-client privilege?
  - Potential exposure and importance of investigation
  - Need to protect investigation facts from disclosure because of legal and reputational risks
- Remember waiver means waiver for all purposes (government, civil litigation)
  - Government waiver not required if facts can be provided without compromising privilege
- To Preserve…
  - If conducted internally, must be under Chief Legal Officer authorization
  - Attorney must be involved for privilege to apply – including CCing in emails, attending meetings, phone calls, etc.
- Inside/Outside counsel is easiest way to preserve privilege
  - Where involved, makes 100% clear that investigation is related to potential litigation

Reporting Obligations

Fraud Type	Internal				Neutral	External		
	Employees	Manager	Business Leaders	Exec Mgt	BOD	Auditors	SEC	DOJ
Asset Misappropriation								
Financial Statement Fraud								
Corruption								
Other Misconduct								
Compliance Issues								

The Fraud Investigations Team

Fraud examiners

Auditors

Security

Human resources personnel

Management representative

Outside consultant

Legal counsel

Information systems personnel

Fact Finding

- Document control, collection and privacy issues
- Gathering all types of evidence
- Witness and suspect interviews
- Computer forensics
- Physical/Electronic Surveillance
- Social media
- Public records
- What is the burden of proof?

Analysis

- Prove or disprove allegation (s) – Substantiated?
- Responsible parties
- Internal control failures
- Collusion
- Strength of evidence
- Criminal/civil liability or misconduct

Corrective Actions

- Identify internal control failures
- Disciplinary actions
- Crisis management
- Impact to brand/reputation
- Root cause analysis
- Determination of loss or damages
- Document reasons for decisions
- Prepare written report (yes or no)

Remediation

- Refer for prosecution
- Refer investigation findings to government agency
- Initiate civil litigation
- Remediation of internal control failures
- Training & awareness
- Recovery of loss or damages
- Rebuilding of brand/reputation
- Revise policies & procedures
- Communicate findings to appropriate persons

Investigative Techniques

IOFM Fall
CONFERENCE & EXPO

Investigative Techniques

Interviews

Document Reviews

Social Media & Public Documents

Digital & Physical Evidence

Digital & Physical Surveillance

Financial Analysis

Data Analytics

BEC Fraud Scheme

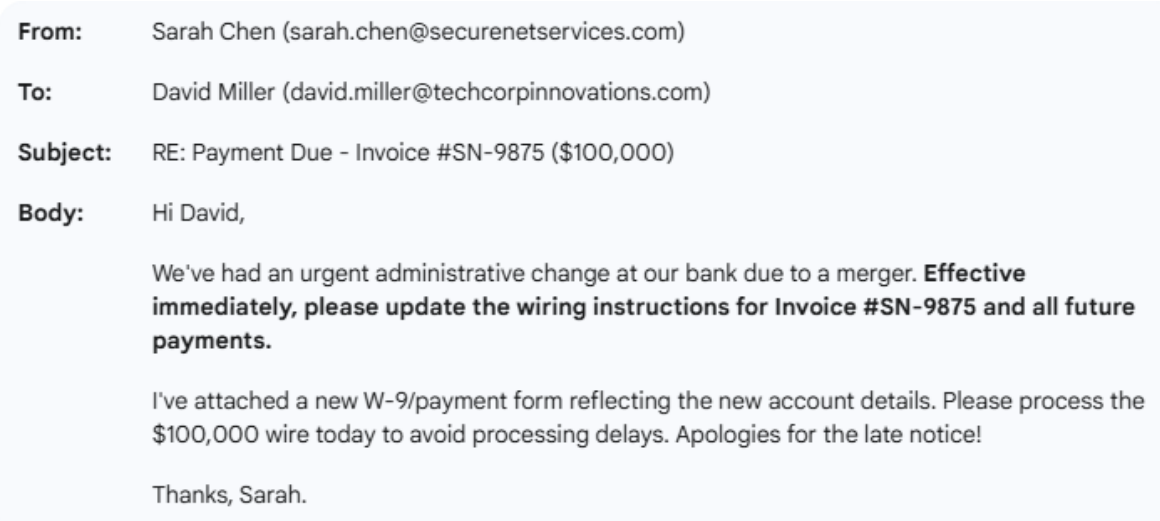
1. The Setup (Reconnaissance and Compromise)

- **Victim Company: "TechCorp Innovations"** (The paying company).
- **Legitimate Vendor: "SecureNet Services"** (The company that gets hacked).
- **The Fraudster:** An organized criminal actor.

The fraudster spends weeks conducting reconnaissance on SecureNet Services. They use phishing to compromise the email account of **Sarah Chen, SecureNet's Accounts Receivable Manager**.

- **Action:** Once inside Sarah's email, the fraudster monitors email threads, specifically looking for recent, high-value invoices sent to TechCorp Innovations and their payment schedules. They learn that TechCorp is due to pay a $100,000 invoice to SecureNet in the coming week.

BEC Fraud Scheme



From: Sarah Chen (sarah.chen@securenetservices.com)

To: David Miller (david.miller@techcorpinnovations.com)

Subject: RE: Payment Due - Invoice #SN-9875 ($100,000)

Body: Hi David,

We've had an urgent administrative change at our bank due to a merger. **Effective immediately, please update the wiring instructions for Invoice #SN-9875 and all future payments.**

I've attached a new W-9/payment form reflecting the new account details. Please process the $100,000 wire today to avoid processing delays. Apologies for the late notice!

Thanks, Sarah.

The Execution (The Fraudulent Request)

Just hours before the legitimate payment is due, the fraudster takes action from Sarah Chen's *actual, compromised email account*.

- **The Email:** The fraudster replies directly to the existing, legitimate payment thread between SecureNet and **David Miller, TechCorp's Accounts Payable Specialist**.
- **The Content:** The email is concise, uses Sarah's usual sign-off, and creates a sense of urgent, but plausible, administrative change.

BEC Scheme

The Failure of Controls (The Payment)

David Miller, under pressure to ensure the payment is on time and seeing the email come from the trusted "Sarah Chen" in the middle of a legitimate email chain, overlooks standard procedure.

- **Breach of Control:** TechCorp's official policy requires a **"Two-Factor Verification Call"** to a *pre-verified phone number* for any change in banking details. David bypasses this control, assuming the legitimate email address and urgency are sufficient.
- **The Wire:** David approves and executes a $100,000 wire transfer using the fraudulent bank details provided in the attachment.
- **The Theft:** The $100,000 is instantly wired to the fraudster's drop account and immediately transferred out, often converted into cryptocurrency or further dispersed through money mules, making recovery extremely difficult.

BEC Scheme

The Discovery (The Fallout)

- Two days later, the *real* Sarah Chen at SecureNet follows up with David, asking if the $100,000 payment has been sent.
- David confirms it was sent to the "new account."
- Sarah replies, "What new account? We never sent an update."
- **The Realization:** TechCorp realizes they have wired $100,000 to a criminal. The fraud has been confirmed.

Evidence – Fraudulent Payment Instructions

- Fraudulent Payment Instructions: The original email(s) sent from the compromised vendor's account to the company requesting the change in bank details or immediate payment (including full email headers for forensic analysis).
- Legitimate Vendor Contract/Invoice: The standing contract, last legitimate invoice, and original, verified payment instructions for the vendor to establish the baseline and contrast with the fraudulent request.
- Payment Disbursement Records: The company's internal record (e.g., wire transfer form, ACH record) showing the actual transfer of funds, including the date, amount, and the fraudulent beneficiary bank account details.
- Banking Records (Stolen Funds): Records from the bank that received the fraudulent transfer, specifically the receiving bank account number, account holder name, and all related account opening documents and transactional history to trace the funds.
- Account Statements: Relevant bank statements from the victim company showing the debit of the fraudulent payment.

Evidence – Digital Forensics & Email Information

- Full Email Headers: Raw, unaltered email headers of the fraudulent communication, which contain the Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and DMARC results, the message ID, and the Originating IP address to trace the message's true source.
- Vendor's Email Audit Logs (from the hacked vendor): Logs showing the attacker's activities within the compromised email account, including suspicious logins (IP address, geolocation), the creation of inbox rules (e.g., rules to delete/forward specific emails), and the exact time the fraudulent email was composed and sent.
- Company's Email Server Logs: Logs from the victim company showing the receipt of the fraudulent email.
- System Logs (End-User Device): Forensic images or logs from the company employee's computer who executed the fraudulent payment, showing access times, whether they clicked any links, or opened any malicious attachments (if applicable).

Evidence – Witness & Procedural Information

- Interview/Statement of the Company Employee: Statement from the employee who received the fraudulent instructions and authorized the payment, detailing the circumstances, the sense of urgency, and the steps they followed (or failed to follow).
- Interview/Statement of the Vendor Contact: Statement from the legitimate vendor contact confirming their account was compromised and confirming that the fraudulent payment instructions did not originate from them.
- Internal Control Documentation: The company's documented policies and procedures for verifying new vendor accounts or changes to payment instructions, used to determine if controls were overridden or circumvented.
- Law Enforcement and Bank Notifications: Documentation of the initial report to law enforcement (e.g., FBI IC3 report) and the immediate funds recall/clawback request sent to the financial institutions.

Proving Loss

- Direct Loss
  - Loss of funds
- Indirect Loss
  - Forensic & Investigative Costs: Fees paid to forensic accountants, Certified Fraud Examiners (CFEs), and cybersecurity experts to investigate the breach, contain the compromise, and prepare evidence.
  - Legal & Regulatory Costs: Attorney fees for recovery efforts, preparing necessary reports for regulatory bodies (if applicable), and civil litigation.
  - System Remediation Costs: Costs to harden the internal network, reset all compromised accounts, implement new security controls (like Multi-Factor Authentication), and perform employee training to prevent recurrence.
  - Lost Opportunity/Reputation: While harder to quantify, in some cases, lost contracts or damage to the company's reputation due to the incident may be claimed.

Proving Loss

Evidence Type	Purpose & Detail	Source
Transaction Confirmation	**Proof of Payment & Amount:** The immediate documentation showing the total amount wired, the date and time, and the complete **fraudulent beneficiary account details** (routing/ABA number and account number).	Victim Company's **Accounts Payable (AP) System** and **Originating Bank** records.
Bank Statements	**Proof of Debit:** Shows the stolen amount was actually withdrawn from the company's operating account.	Victim Company's **Bank Statements** (requires full period before and after the fraud).
Fraudulent Email	**Proof of Deception:** The original email (in its raw format with **full email headers**) containing the false payment instructions. This links the **deceptive act** to the **financial loss**.	Victim Company's **Email Server/Service Provider** (Digital Forensics Image).
Recall/Reversal Request	**Proof of Mitigation:** The formal request sent to the originating bank (often within hours) to initiate the recall, including the time-stamped **Hold Harmless Letter** or **Letter of Indemnity**.	Victim Company's **Financial Department** and **Originating Bank**.
Forensic and Vendor Invoices	**Proof of Consequential Loss:** Invoices and payment records for all external services hired for the investigation, including legal counsel, CFE services, and IT incident response.	Victim Company's **Internal Accounting/AP Records**.
Employee Statement	**Proof of Reliance & Cause:** A written or recorded statement from the employee who executed the payment, detailing the specific instructions they received and *why* they believed the instructions were legitimate, establishing the reliance on the false statement.	**Interview of the Employee** (documented by Legal or the CFE).

Coordination with other Functions

IOFM Fall
CONFERENCE & EXPO

Security

- Physical access documentation
- Investigative experience
- Interviewing skills
- Prior incidents
- Location background

Legal Counsel

- Legal advice
- Coordination with outside law firms/law enforcement
- Attorney-client privilege
- Review reports for language
- Communication with the Board, Audit Committee, Senior Management
- Tracking documents & investigative progress

Human Resources

- Personnel files
- Employment history
- Prior disciplinary actions – incidents
- Interviewing assistance
- Disciplinary action
- Employee assistance programs
- High risk terminations

Information Technology

- Electronic evidence collection
- Data retrieval – where/when/how
- Email reviews
- Hard drive imaging
- Internet activity
- Log in/out data

Outside Fraud Experts

- Investigative experience/expertise
- Interviewing skills
- Data mining techniques
- Computer forensics
- Report writing skills
- Forensic auditing expertise
- Expert witness – render opinions

Internal Audit

- Control weaknesses review
- Root cause analyses
- Data mining
- Document review
- Email/electronic evidence reviews

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

Fraud Detection & Investigation Techniques