Federal government-related fraud issues: Prevention and detection

Jesse Morton

KPMG's Federal Advisory Practice, Director, Fraud Risk Management

May 18, 2016

Agenda

- Introduction to fraud
- Fraud risk assessments
- Government-related fraud statistics
- Government-related fraud “hot topics”
- Fraud investigation techniques and tools

KPMG

Introduction to fraud

Introduction to fraud

Definitions

— Fraud is “a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment” per Black’s Law Dictionary.

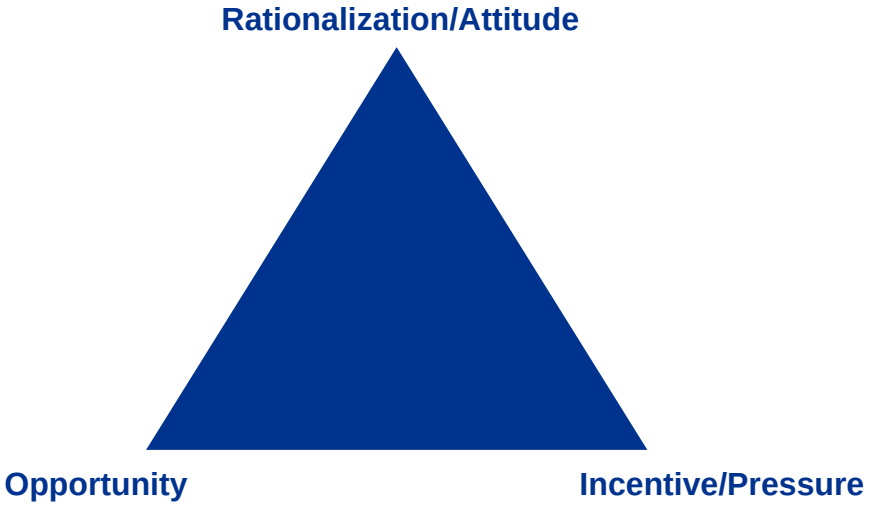
— Determining whether fraud occurred is a legal question, forensic accountants investigate and report on the facts.

Types of Fraud per the Association of Certified Fraud Examiners (ACFE):

— Financial statement fraud

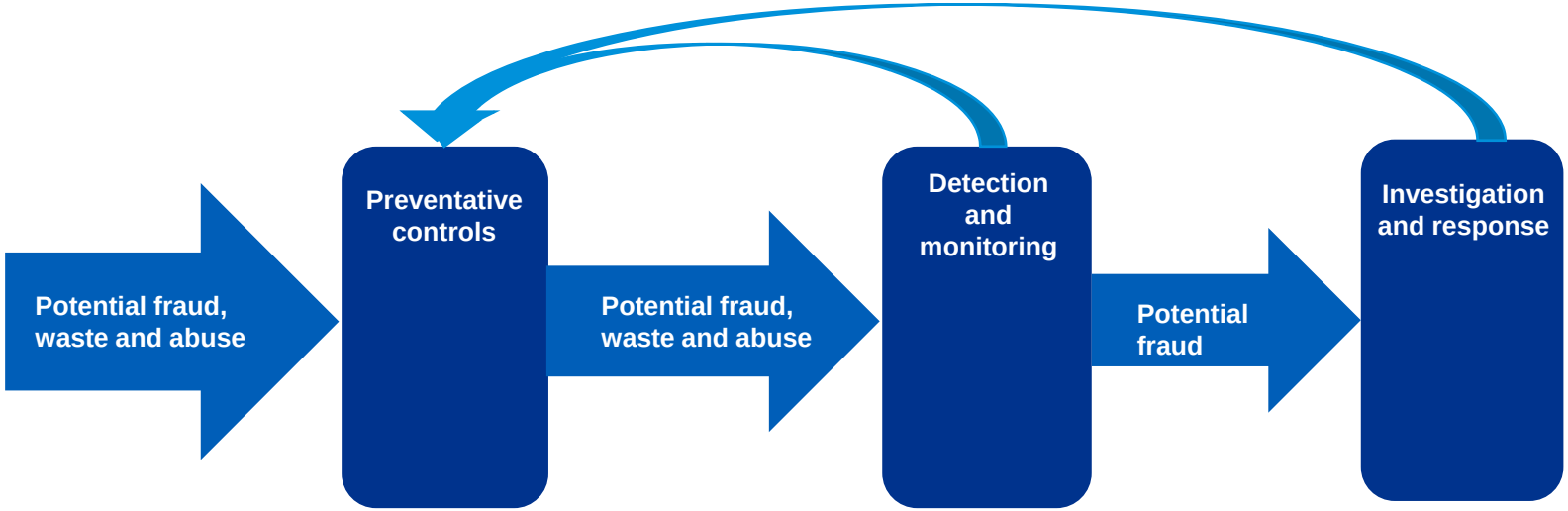
— Asset misappropriation

— Corruption (including conflict of interest and bribery) and other regulatory violations



Fraud control activities

Lessons learned influence future use of preventative controls



- Fraud and misconduct risk assessment
- Code of conduct and related standards
- Employee and third-party due diligence
- Communication and training
- Process-specific fraud risk controls
- Proactive forensic data analysis

- Hotlines and whistle-blower mechanisms
- Auditing and monitoring
- Retrospective forensic data analysis

- Internal investigation protocols
- Enforcement and accountability protocols
- Disclosure protocols
- Remedial action protocols

Source: U.S. Government Accountability Office, *Framework for Fraud Prevention, Detection, and Prosecution*, Jul. 12, 2006.

GAO's Fraud Risk Management Framework

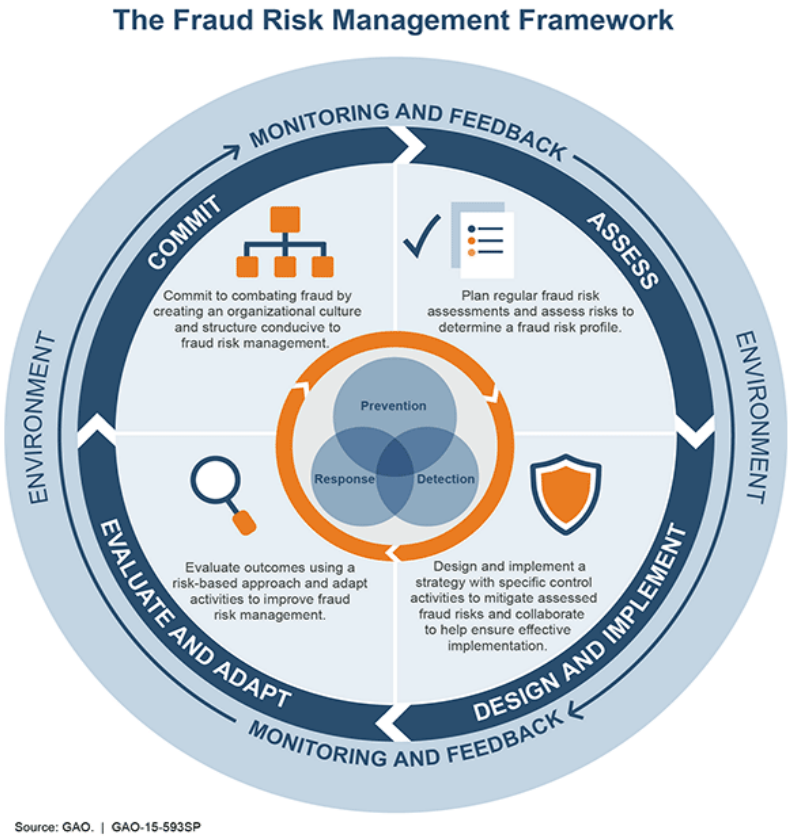
GAO Leading Practice

Commit – Commit to combating fraud by creating an organizational culture and structure conducive to FRM.

- Demonstrate a senior-level commitment to combat fraud and involve all levels of the program in setting an antifraud tone.
- Designate an entity within the program office to lead FRM activities.
- Ensure the entity has defined responsibilities and the necessary authority to serve in its role.

Assess – Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.

- Tailor the fraud risk assessment to the program, conduct assessments at regular intervals, identify specific tools, methods, and sources for gathering information about fraud risks, and involve relevant stakeholders in the assessment process.
- Identify the population of relevant fraud risks, assess the likelihood and impact of those risks, and determine risk tolerance.
- Examine the suitability of existing controls, prioritize residual risks, and document a fraud risk profile.



Source: U.S. Government Accountability Office, *A Framework for Managing Fraud Risks in Federal Programs*, Jul. 28, 2015.

GAO's Fraud Risk Management Framework

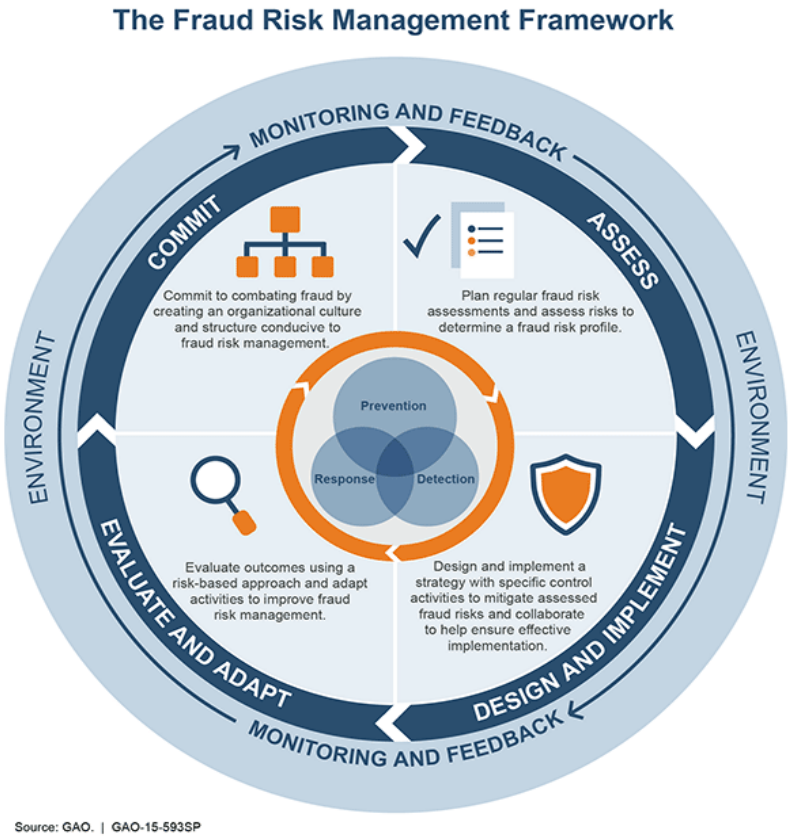
GAO Leading Practice

Design and Implement – Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.

- Develop, document, and communicate an antifraud strategy, focusing on preventive control activities.
- Consider the benefits and costs of controls to prevent and detect potential fraud, and develop a fraud response plan.
- Establish collaborative relationships with stakeholders and create incentives to help ensure effective implementation of the antifraud strategy.

Evaluate and Adapt – Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.

- Conduct risk-based monitoring and evaluation of fraud risk management activities with a focus on outcomes measurement.
- Collect and analyze data from reporting mechanisms and instances of detected fraud for real-time monitoring of fraud trends.
- Use the results of monitoring, evaluations, and investigations to improve fraud prevention, detection, and response.



Source: U.S. Government Accountability Office, *A Framework for Managing Fraud Risks in Federal Programs*, Jul. 28, 2015.

KPMG

Fraud risk assessments

Conducting a fraud risk assessment - Purpose

- A process for identifying the quantitative and qualitative nature of potential integrity and/or internal control breakdowns
- Identifies the pressures and incentives that give rise to some of the most salient integrity-related risks
- Basis for mitigating fraud and misconduct risk
- Performing a fraud risk assessment is a good way to fulfill the auditor's fraud identification requirements (Circular A-123)
- Improve communication and fraud awareness
- Identify potential vulnerabilities
- Develop ways to investigate and determine if fraud has occurred
- Assess internal controls
- Comply with regulations and professional standards

Conducting a fraud risk assessment – Key points for a successful fraud risk assessment

- Collaborative effort of management and auditors
- Right sponsor
- Independence/Objectivity of people leading and conducting the work
- Good working knowledge of the business
- Access to people at all levels of the organization
- Ability to “think outside the box” and think the “unthinkable”
- Refresh the assessment regularly and treat as an ongoing exercise

Fraud risk assessment: Four fundamental steps

Step #1: Identify units, locations, or processes to assess

Step #2: Inventory and categorize fraud and misconduct risks

Step #3: Rate risks based on the likelihood and significance of occurrence

Step #4: Remediate risks

Step #1: Identify units, locations, or processes to assess

- What aspects or parts of the organization will be subject to the risk assessment?
  - Entity Level
  - Unit Level
  - Program Level
  - Geography
- What organizational and reporting structures can be significant in understanding the pressures, incentives and opportunities for fraud and misconduct to occur?
- What are the significant accounts and classes of transactions?
- Are there complex transactions?

Step #2: Inventory and categorize fraud and misconduct risks

- Fraud triangle
- Fraud risk factors include:
  - Known instances or allegations of fraud
  - Complexity of the risk
  - Complexity of the entity or program
  - Visibility associated with the risk
  - Instances and occurrences of fraud in other agencies
  - Fraud trends in the commercial industry
- Inventory common frauds specific to organization
- Analysis

Step #2: Inventory and categorize fraud and misconduct risks

— Other input:

- Market research
- Media reports
- Internal reports
- IG reports
- GAO and Congressional hearings
- Interviews with key program and oversight personnel
- Documentation review (code of conduct, policies and procedures, reported instances of fraud and misconduct, etc.)
- Focus groups
- Workshops
- Surveys
- Watchdog findings

Step #3: Rate risks based on the likelihood and significance of occurrence – An example

Inherent likelihood factors	Rating
Known instances/allegations Previous history	**High/Probable (Score = 7–9)**
Pervasiveness of the risk across operations Complexity of the risk Results of surveys and focus groups	**Medium/Reasonably possible (Score = 4–6)**
Industry trends Criticisms by the media or NGOs Findings of the IG or watchdog Other internal considerations	**Low/Remote (Score = 1–3)**

Quantitative factors:

— Potential monetary loss to the organization including loss of inventory, cash or fixed assets or fines, settlements and judgments

Qualitative factors:

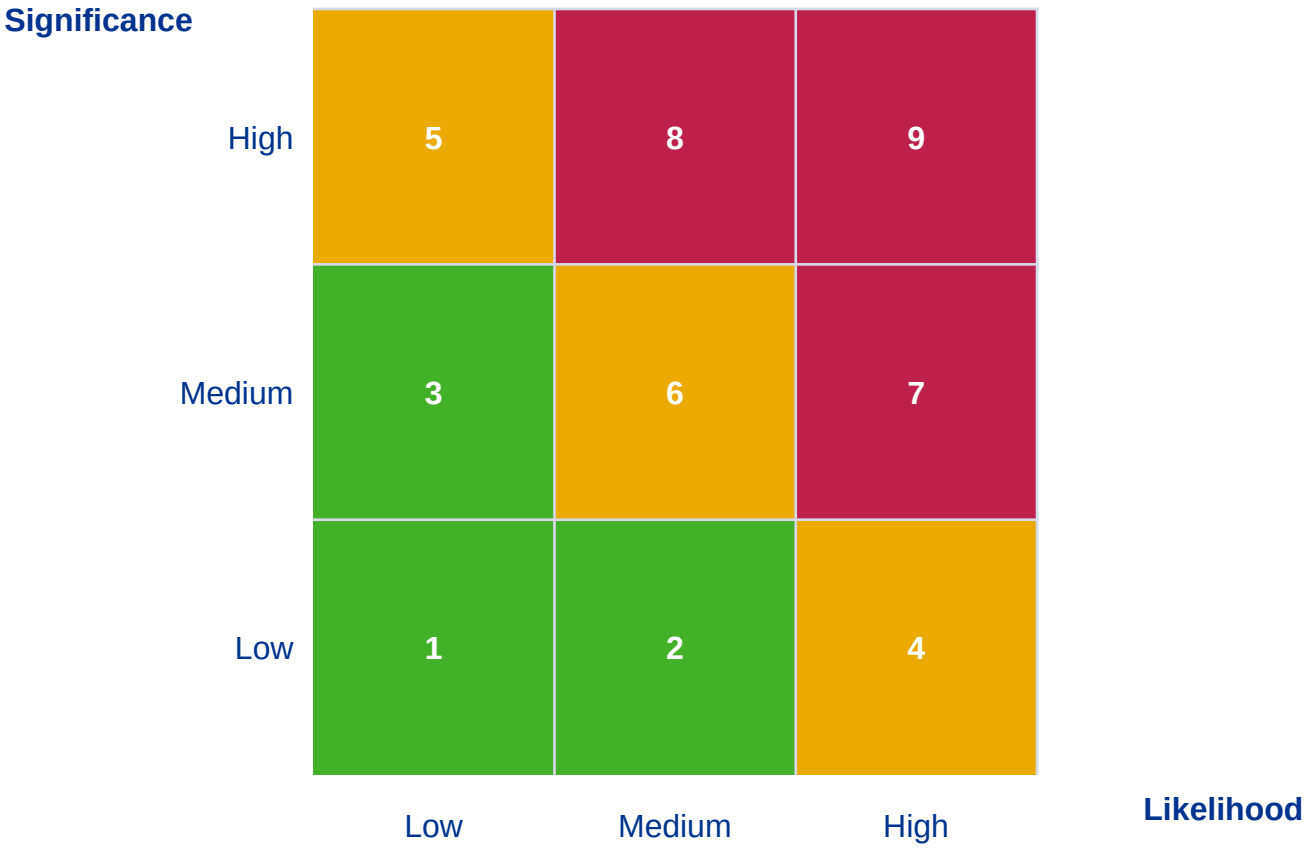
— Negative media attention, reputational damage, scrutiny from Congress

Step #3: Rate risks based on the likelihood and significance of occurrence – An example (continued)

Financial Significance	Nonfinancial Significance	Rating
Significant	Criminal investigation Major change to program National media attention Financial restatement Systemic fraud and/or misconduct in program Congressional scrutiny Resignations or loss of confidence	**High/Material (Score = 7–9)**
Material	Regional/trade media attention Negative findings from an OIG audit Negative findings from external auditor Scrutiny from watchdog	**Medium/More than Inconsequential (Score = 4–6)**
Immaterial	Minor program losses identified Major change to program strategy	**Low/Inconsequential (Score = 1–3)**

Step #3: Rate Risks Based on the Likelihood and Significance of occurrence

Using a heat map to identify inherent risk



Step #3: Rate Risks Based on the Likelihood and Significance

Consider existence of mitigating controls, residual risk, and prioritize risks

— Existence of mitigating controls:
  - Entity-level and process-level controls designed to help ensure that operations are efficient, that financial statements are accurate, and that programmatic requirements are met
  - Evaluate effectiveness
  - Understand the primary purpose of controls
  - Avoid overstating the effectiveness
  - Use previous control evaluations performed by management

— Residual risk:
  - The remaining exposure the organization faces after controls have been put into place to mitigate the risk
  - Assists management in prioritizing risks and devoting the right amount of resources to mitigating the salient fraud risks that still face the organization

— Prioritize risks

Step #4: Remediate risks

- Focus on strengthening controls for insufficiently mitigated fraud and misconduct risks
- Identify additional improvement opportunities
- Identify individual with responsibility for helping to ensure that the control environment is improved
- Link specific controls, policies, and procedures to the identified risks
- Determine if additional resources should be committed to enhance existing controls or to design and implement new programs and controls

KPMG

Government-related fraud statistics

2016 ACFE Report to the Nations on Occupational Fraud and Abuse - Government Related Fraud Statistics

- Asset misappropriation is the most common type of fraud scheme
- Tips are by far the most common type of detection method, followed by internal audit and management review
- The government was the victim organization in 10.5% of cases analyzed (2nd highest), behind only banking and financial services
- The median loss was $194K for schemes where the federal government was the victim organization, and $100K for schemes where state governments were the victim organization
- The most common type of misconduct is corruption, followed by billing and expense reimbursement schemes
- The most common type of internal controls weakness cited as causing the scheme was lack of internal controls, followed by lack of management review, override of existing controls, and poor tone at the top

Source: Association of Certified Fraud Examiners, *2016 Report to the Nations on Occupational Fraud and Abuse*

Common "red flags": Organizational

- Lack of segregation of duties
- Management override or dominance
- High employee turnover
- Siloed or overly complex structure
- Lack of proper documentation
- Unusually high success rate on project bids
- Lack of training program
- Low number of and/or underqualified accounting/financial reporting employees based on size and/or complexity of organization

Common "red flags": Organizational

- Poor IT controls
- "Do whatever it takes" attitude
- History of illegal and/or unethical behavior
- "Aggressive" management estimates
- Offline accounting records or use of spreadsheets
- Use of intermediaries
- Concentration of ownership
- Significant number of related-party transactions

2016 ACFE Report to the Nations on Occupational Fraud and Abuse – Perpetrator Fraud Statistics

- Managers and above most frequently commit fraud, and frauds committed by these level perpetrators have the highest median losses
- Perpetrators most often have a tenure with the victim organization of 6+ years
- Perpetrators are most often in the accounting and operations departments
- Perpetrators are overwhelmingly male (69%)
- The majority of perpetrators are over the age of 40, and over 20% are over the age of 60
- The vast majority of perpetrators have a university degree and/or postgraduate degree, and nearly 45% have postgraduate degrees
- The vast majority of schemes are perpetrated by multiple individuals, and over 50% of the schemes were committed by five or more perpetrators
- Over 88% of the perpetrators have no prior criminal history, and over 82% of the perpetrators have never been fired/terminated from a position
- The most common behavioral red flags cited as being displayed by the perpetrators were living beyond means, followed by financial difficulties, unusually close relationship with customer/vendor, and control issues/unwilling to share responsibilities

Source: Association of Certified Fraud Examiners, *2016 Report to the Nations on Occupational Fraud and Abuse*

Common "red flags": Individual

- Lavish lifestyle and/or living beyond one's means
- Substance abuse and/or gambling problems
- Poor job performance
- Employee does not take vacation/sick leave
- Employee has interest in related outside business(es)
- Employee secretive and/or protective about work responsibilities

KPMG

Government-related fraud "hot topics"

Common federal statutes use to prosecute fraud

1. Mail & Wire Fraud (18 U.S.C. 1341 & 1343)
2. Embezzlement and Theft of Federal Money or Property (18 U.S.C. 641) – criminalizes intentional and unauthorized taking, destruction, or use of government money, property, or records and prohibits receiving or concealing such property or records.
3. Interstate Transportation of Stolen Property (18 U.S.C. 2314) – often used in conjunction with mail and wire fraud statutes.
4. Racketeer Influenced and Corrupt Organizations (18 U.S.C. 1961 et. seq.) – prohibits the investment of ill-gotten gains in another enterprise, using deceptive or coercive acts to acquire an interest in an enterprise, and conducting business through such acts.
5. Conspiracy to Defraud the Federal Government with False Claims (18 U.S.C. 286) – makes it a crime for two or more persons to agree to conspire to defraud the United States by obtaining or aiding in obtaining payment or allowance of any false, fictitious, or fraudulent claim.
6. False, Fictitious, or Fraudulent Claims (18 U.S.C. 287) – criminal False Claims Act., makes it illegal to present or make false, fictitious, or fraudulent claims against any agency or department of the United States
7. Civil False Claims Act (31 U.S.C. 3729)
8. Bribery of Public Officials and Witnesses (18 U.S.C. 201) –principal federal corruption statute applies to any U.S. official, juror, or witness.
9. "Honest Services" Fraud (18 U.S.C. 1346) – the payment or receipt of bribes deprive the public of its right to honest and unbiased services of public servants.
10. Bribery of a Bank Examiner (18 U.S.C. 212-213)
11. Anti-Kickback Act (41 U.S.C. 51) – outlaws the giving or receiving anything of value for the purpose of improperly obtaining or receiving favorable treatment in connection with a government contract.

Source: Association of Certified Fraud Examiners, *2015 Fraud Examination Manual*

What is bribery?

Bribery is a form of corruption that may be defined as the offering, giving, receiving, or soliciting of anything of value to influence an act or decision.

Official bribery refers to the corruption of a public official to influence an official act of government. Illegal payments to public officials can be prosecuted as official bribery, and they can give rise to stiff criminal penalties. The elements of official bribery generally include:

— The defendant gave or received (offered or solicited)

— A thing of value

— The recipient was (or was selected to be) a public official

— The defendant acted with corrupt intent

— The scheme was designed to influence an official act or duty of the recipient.

Illegal gratuity is similar to bribery schemes, except gratuity often occurs after the recipient has made the decision. Illegal gratuity is often a lesser-included offense to official bribery.

Source: Association of Certified Fraud Examiners, *2015 Fraud Examination Manual*

Today's hot topics in the government sector

Topic	Example	Type
Asset Misappropriation	Collusion Procurement Fraud Credit Card Fraud Check Tampering Payroll/Expense Reimbursement Schemes	Asset misappropriation
Conflicts of interest	Navy/Fat Leonard Scandal	Corruption
Bribery/Corruption	Navy/Fat Leonard Scandal	Corruption
Cybercrime	OPM records breach	Asset misappropriation
Insider threat	Snowden/Manning Ft. Hood: Major Nadal Hassan	Asset misappropriation/ Other
Bribery/Corruption (domestic)	Fat Leonard scandal VA Former-Governor Bob McDonnell	Corruption
Claims fraud	HHS/CMS HUD/FHA FSA, DHS/FEMA, IRS/EITC	Asset misappropriation
Improper payments	HHS/CMS DHS/FEMA	Asset misappropriation
Supply chain risk: Third-Party due diligence	Navy/Fat Leonard scandal	Asset misappropriation/ Corruption
Whistleblower retaliation	Veteran's Affairs	Corruption

Procurement Fraud - Example

— Air Force

- "Mark J. Krenik, a former civilian employee of the Air Force, 7th Communications Group, who was convicted of stealing over $500,000 from the Air Force by submitting false invoices and fictitious receiving reports for contractor services and materials"
- "Mr. Krenik successfully encouraged certain Hughes STX employees to prebill the government over $300,000 for services that were not rendered"
- Mr. Krenik "then attempted to obtain these funds by directing Hughes STX employees to bill the government for consulting services from a nonexistent subcontractor by using a bogus subcontractor invoice that he supplied"
- Had Mr. Krenik's scheme worked, "the government would have paid Hughes STX for work performed by the fictitious subcontractor; and Hughes STX would have reimbursed the subcontractor by sending the money to a post office box controlled by Mr. Krenik"
- Discovered when Hughes STX contract team learned of employee involvement in the scheme and opened an internal investigation; also when employees at Mr. Krenik's bank became suspicious of unusually large transactions

Source: U.S. Government Accountability Office, *Fraud by an Air Force Contracting Official*, Sept. 23, 1998

Conflicts of interest, Bribery & Corruption - Example

— U.S. Department of Defense, Department of the Navy, “Fat Leonard” Scandal

- “The bribery scandal involves a Singapore-based naval company run by Leonard Glenn Francis, which provided various logistical and port-related services for American military vessels operating in Asia.”
- “Francis received confidential ship schedules for the Navy’s 7th Fleet, along with pricing information about bids submitted by competitors," Weirick recounts. He used this information to snag additional contracts for Glenn Defense Marine Asia and overcharge US taxpayers by some $20 million — although "Fat Leonard" and his company had to forfeit $35 million after the fraud was exposed.”
- “The scandal implicated some of the highest-ranking officials in the Navy — including the former superintendent of the US Naval Academy in Annapolis, a vice admiral who received a censure after admitting to accepting bribes from ‘Fat Leonard.’ According to Defense News, as many as ‘three-dozen flag officers’ were under federal investigation for their connections to the scandal”

Source: Business Insider, *The Navy’s bribery and prostitution scandal is even worse than it looks*, Apr. 20, 2015

Cybercrime - Example

— U.S. Office of Personnel Management Records Breach

- After an "interagency forensics investigation" revealed a massive cyber breach "affecting background investigation records of current, former, and prospective Federal employees and contractors"
- "OPM has determined that the types of information in these records include identification details such as Social Security Numbers; residency and educational history; employment history; information about immediate family and other personal and business acquaintances; health, criminal and financial history; and other details. Some records also include findings from interviews conducted by background investigators and fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen."
- "The team has now concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases. This includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, predominantly spouses or co-habitants of applicants. As noted above, some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints."

Source: U.S. Office of Personnel Management Press Release, *OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats*, Jul. 9, 2015

Insider Threat - Example

— U.S. National Security Agency, Edward Snowden

- "Edward Joseph Snowden (born June 21, 1983) is an American computer professional, former Central Intelligence Agency (CIA) employee, and former contractor for the United States government who copied and leaked classified information from the National Security Agency (NSA) in 2013 without prior authorization"
- "On May 20, 2013, Snowden flew to Hong Kong after leaving his job at an NSA facility in Hawaii and in early June he revealed thousands of classified NSA documents to [several] journalists"
- "On June 21, 2013, the U.S. Department of Justice unsealed charges against Snowden of two counts of violating the Espionage Act of 1917 and theft of government property."

Source: Wikipedia, *Edward Snowden*

Improper Payments - Example

— U.S. Government Accountability Office, 2014 GAO Report

- "Federal agencies across the board are continuing to waste tens of billions of taxpayer dollars on duplicative spending efforts, even after Congress' official watchdog has made hundreds of recommendations for cutting back. The spending issues, ranging from Medicare and Medicaid mismanagement to transportation programs to weapon systems acquisitions, cost taxpayers $125 billion in improper payments in 2014 alone, as highlighted in a new report from the Government Accountability Office."
- "Over the last five years, the GAO said it has made 440 recommendations across 180 areas where federal agencies can cut back on fragmented, overlapping and duplicative spending programs, but as of November 2014, only 29 percent of the actions were fully addressed, according to the report."
- "According to GAO, the federal government made about $125 billion in improper payments in 2014 alone. Solving that would give you enough money to kill the death tax, repeal the federal gas tax and airline ticket tax, end all federal excise taxes on alcohol and tobacco and remove all federal taxes on phone and Internet bills. . . . After that, there would still be enough money left over to give everyone in America a tax cut of $60 just for having a pulse."

Source: Washington Times, *GAO reports federal government wasted $125 billion in 2014 alone*, Mar. 5, 2014

Whistleblower Retaliation - Example

— U.S. Department of Veterans Affairs

- "After a food services manager with the Department of Veterans Affairs in Philadelphia blew the whistle on faulty sanitation practices, his supervisors attempted to fire him for eating four old sandwiches worth a total of $5. Yet the concerns he raised about a fly infestation were not investigated, investigators said. He was also reassigned to clean a morgue."
- "'This is a pattern where whistleblowers who disclose wrongdoing often face trumped-up charges but where employees who put vets' health at risk or engage in misconduct that endangers vets are going unpunished,' Lerner said. 'The bottom line is, you can't discipline whistleblowers for coming forward but not discipline those who have done wrong.'"
- "'The lack of accountability in these cases stands in stark contrast to disciplinary actions taken against VA whistleblowers,' Lerner said in the letter. 'The VA has attempted to fire or suspend whistleblowers for minor indiscretions, and often for activity directly related to the employee's whistleblowing.'"
- "VA said in a statement that they were 'committed to creating a work environment in which *all* employees – from front-line staff through lower-level supervisors to senior managers and top VA officials – feel safe sharing what they know, whether good news or bad, for the benefit of Veterans, without fear of reprisal."

Source: Washington Post, *He blew the whistle on the VA — and then was almost sacked for eating stale sandwiches*, Sept. 21, 2015

Public corruption - Example

— Virginia Former-Governor Bob McDonnell

- "On January 21, 2014, McDonnell and his wife were indicted on federal corruption charges. The charges followed a months-long federal investigation into gifts McDonnell received from a political donor. They were charged with fourteen different counts, relating to their acceptance of more than $135,000 in gifts, loans, trips and other items from Jonnie Williams Sr., former CEO of Star Scientific, a company developing a compound called anatabine as a dietary supplement and as a drug. In 2013, McDonnell repaid more than $120,000 to Williams and apologized for bringing 'embarrassment' to the state. McDonnell insisted he did not break the law and vowed to fight 'these false allegations.' He became the first Governor of Virginia to be indicted for actions committed during his tenure. In July and August 2014, Williams testified at McDonnell's federal corruption trial."
- "After a five-week trial and three days of jury deliberations in the United States District Court for the Eastern District of Virginia, McDonnell and his wife were found guilty of public corruption charges on September 4, 2014. He was convicted of honest services wire fraud, obtaining property under color of official right, and extortion under color of official right. His wife was convicted of honest services wire fraud, obtaining property under color of official right, extortion under color of official right, and obstruction of a federal proceeding."

Source: Wikipedia, *Bob McDonnell*

KPMG

Fraud investigation techniques and tools

Data analytics

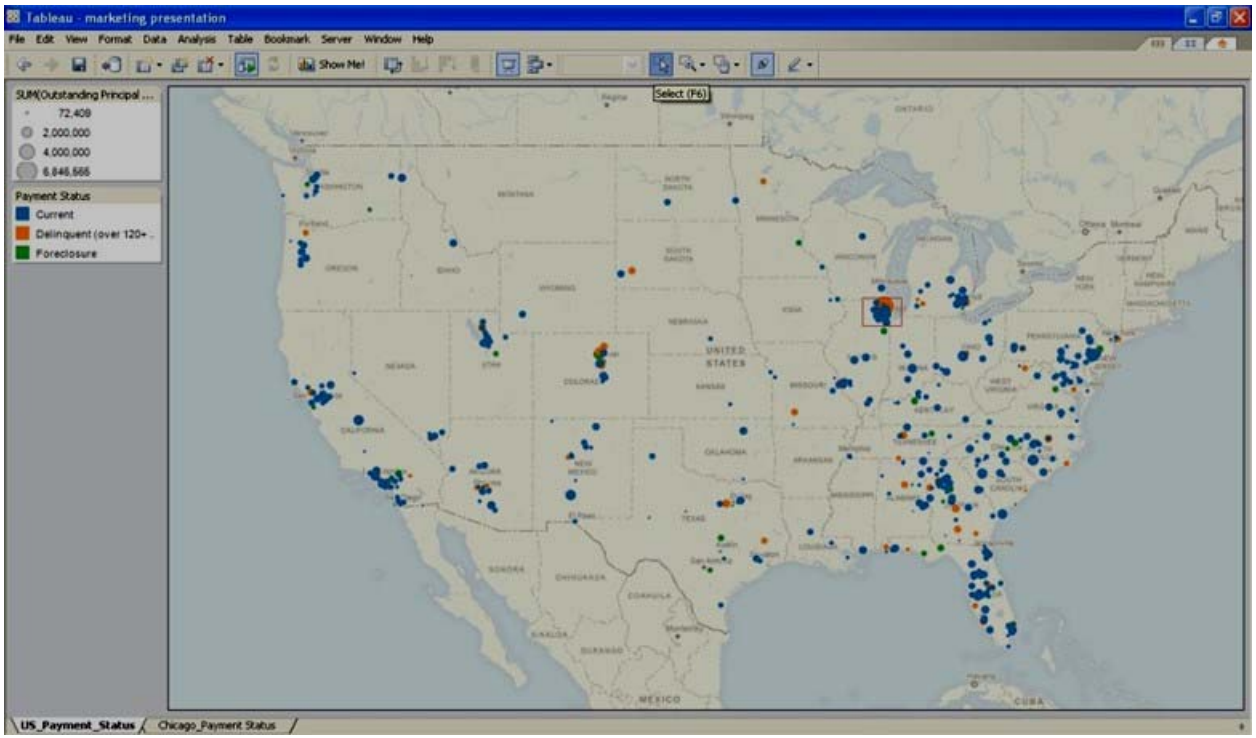
— Data visualization tools – Expense analysis

— Benford's Analysis
— Duplicate payments
— Trends/Outliers
— Risk ranking

Data analytics

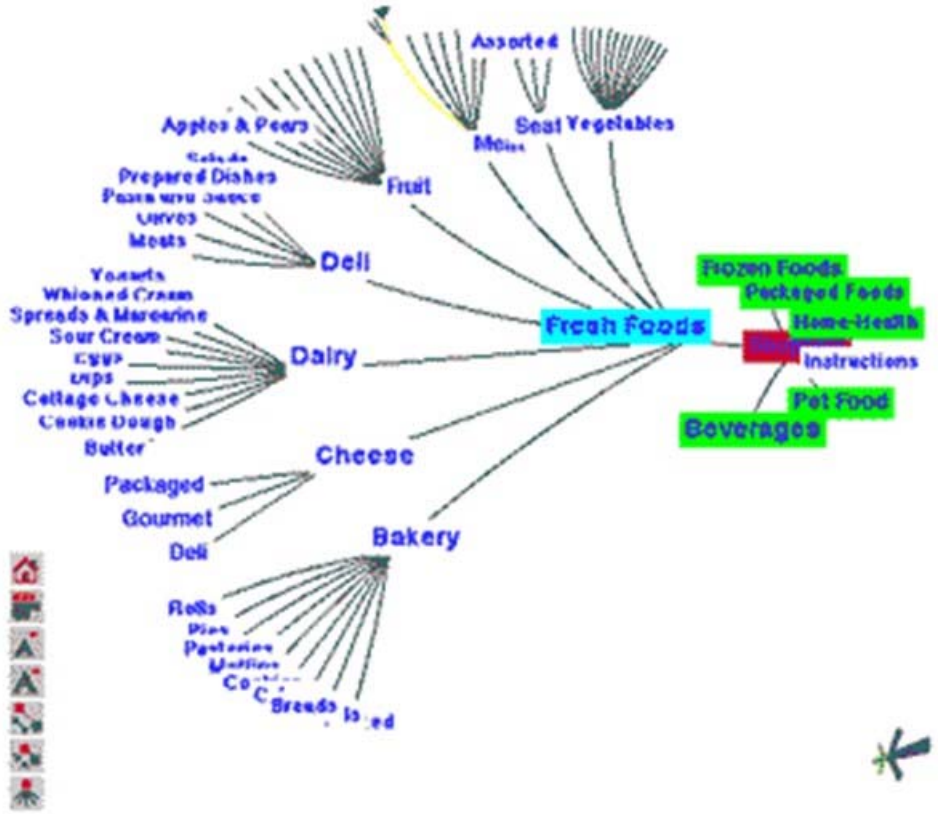
— Data visualization tools – presents data in a form that allows the user to identify anomalies in a data set

- Geospatial mapping (“heat map”) (e.g., high concentration of defaulted loans in a specific geographic location)



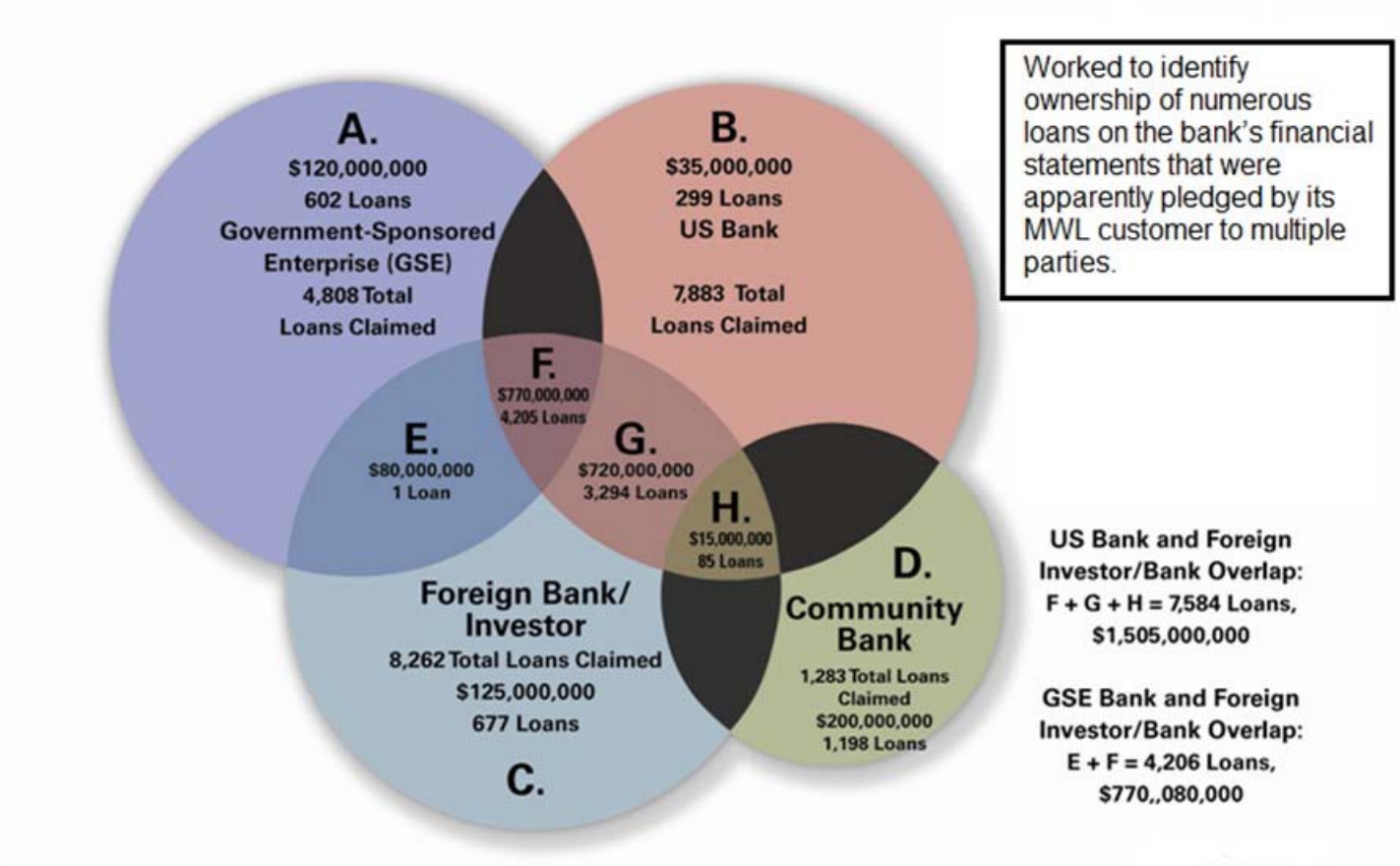
Data analytics

— Hyperbolic tree (e.g., counterparty with unusually high number of related parties)



Data analytics

— Venn diagram – Used to identify overlapping or duplicative transactions



Fraud investigation techniques and tools

Corporate intelligence

When do you perform corporate intelligence?

— Integrity due diligence – the process of mitigating risk arising from association with a third party who may be or may have been engaged in unethical or illegal practices
  - Internal resources (i.e., employees and contractors)
  - Third-party intermediaries (e.g., suppliers, vendors, customers)

— Investigations support
  - Financial services/mortgages
  - Healthcare
  - AML/Threat Finance

— Litigation support

Corporate intelligence

Examples:

- Review counterparty qualifications and assertions
- Public records searches (e.g., Secretary of State Web sites, LexisNexis, Westlaw, criminal records, UCC filings, etc.)
- News stories and other media (e.g., Google, Google Maps)
- Public filings (e.g., SEC filings)
- Social media (e.g., Facebook, LinkedIn, Twitter)
- Background checks
- Litigation history
- Regulatory compliance history
- Interview related parties
- Verify licensing compliance

E-mail reviews

Actual examples from an e-mail review:

— "We have [the auditors] coming on Monday. I need u to get [these accounts] looking spotless…I don't care how…loans can't be on ther [sic] longer than 120 days…"

— "The auditors are going to look specifically at [these accounts]…this needs to get cleaned up, even if just for a day or two….PLEASE…..URGENT…."

— "when I get an adjoining suite with martha stewart, it will be worse. I never should have used that money in the first place."

— "Can we change the date of the advance so they won't look so old for the auditors?"

— "Can we go over this and discuss? … we need you guys to look like a normal customer!"

Interviewing tips

BE LOUD & CLEAR:

L isten for content and detail.

O bserve nonverbal behavior throughout the interview.

U se silence to gather further information.

D on not interrupt or complete interviewees sentence.

A void personal and environmental distractions.

N od and use positive verbal and nonverbal gestures.

D on not make assumptions and presumptions.

C losed minds can miss important information.

L isten completely, not selectively.

E mpathy and patience are important.

A sk questions to clarify.

R epeat or summarize key points.

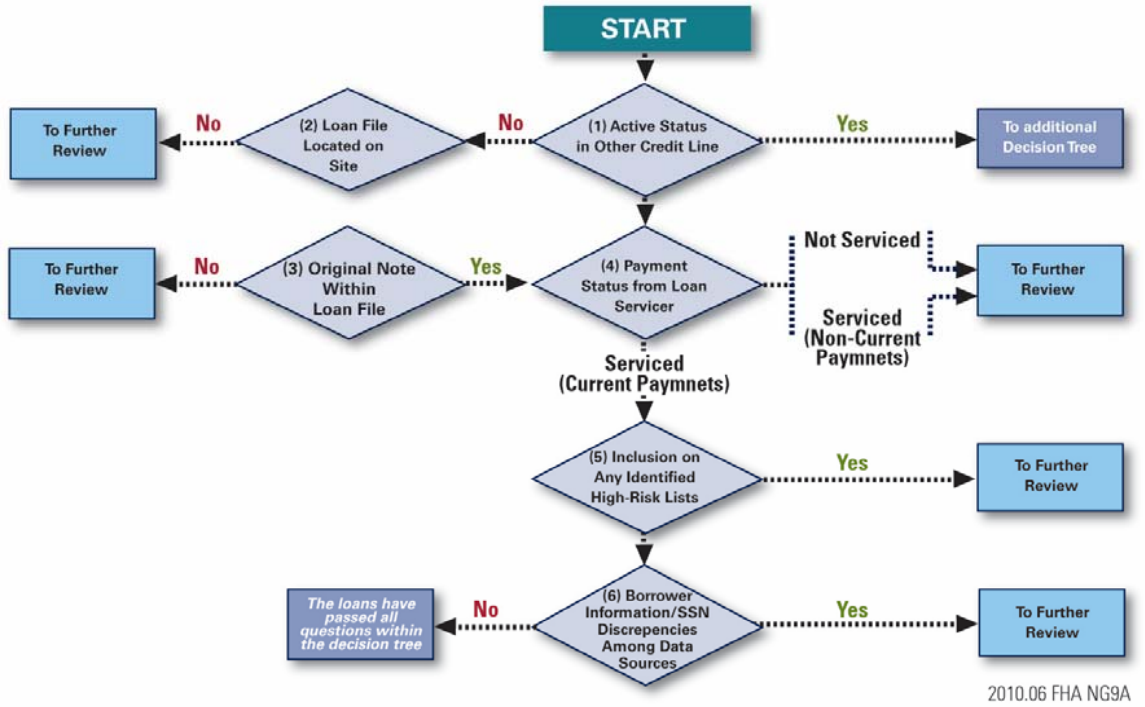
Other tools

- Review whistleblower/hotline contacts
- Analyze source documentation:
  - Identify forgeries
  - Identify counterfeit documents
  - Identify altered documents
- Develop relationship charts and/or time lines
- Funds tracing:
  - Trace source document through accounting/recording process
  - Vouch a financial statement line item and/or journal entries to source documentation
- Review non-system generated reports and/or accounting records:
  - Spreadsheets
  - Databases
- Analytical procedures:
  - Horizontal analysis
  - Vertical analysis

Other tools (continued)

— Decision tree analysis

- Used to systematically analyze source documentation that should have similar or identical characteristics (e.g., residential loan application)



KPMG

Questions?

Contact us

Jesse Morton
Director
Federal Forensic

KPMG LLP
1676 International Drive

Tyson’s Corner, VA 22102

jrmorton@kpmg.com

Tel 404 221 2368
Fax 202 478 0895
Cell 202 550 5058

kpmg.com/socialmedia