



Psychology of Fraud - Insights from a Fraud Investigator

Shauna Woody-Coussens, CFE

Managing Director, Public Sector Advisory Services National
Practice Leader

Doug Manhart, CFE

Director, Forensic & Valuation Services

BKD



WHAT WE WILL COVER TODAY

- The psychology of fraud perpetrators
- Common occupational frauds perpetrated against gov't entities
- Cost effective internal controls

EVOD

PSYCHOLOGY OF FRAUD

Everyone needs a trusted advisor. Who's yours?

BKD

WHO PERPETRATES FRAUD?

FIG. 24 How does the perpetrator's level of authority relate to occupational fraud?





WHY DO EMPLOYEES STEAL?

- Legitimate financial need is rare anymore
- Other basic reasons employees steal
 - Low morale
 - Feel employer has mistreated or “wronged” them
 - Feel underpaid and/or under appreciated
 - Consequences of theft are minimal
 - Lack of preventative measures

WHY DO OWNERS/EXECUTIVES STEAL?

- Same reasons generally apply to owners/executives, but there are others
 - Greed – many risk more than they stand to gain
 - Arrogance – power and money lead to feeling of invincibility
 - Personality Disorder – lack of empathy, denial even in face of overwhelming evidence of guilt

CASE STUDY - SCOTT TUCKER

- ▶▶ \$3.5 billion payday loan business
- ▶▶ 1997-2013
- ▶▶ More than 4.5 million borrowers impacted



PAYDAY LOAN BUSINESS MODEL

- Customers are high-risk (previous history of non-payment)
- Only 7 out of 10 will repay, and there is virtually no recourse
- Pricing is about \$30 for every \$100 advanced. Loan maturities are approximately 14 days
 - Tenure at job
 - Claimed regular income
 - Established bank account

PAYDAY LOAN BUSINESS MODEL

- Scaled from \$300,000 initial investment in a single store front in 1997 and used Internet to speed things up and make them more convenient and efficient through use of online lending software
- Could approve loans in 3/10ths of a second
- Use of Internet allowed companies to make loans to borrowers in states where they did not have a physical presence and that did not allow Payday lending. So, in 2003, a couple of states sued

TRIBAL SOVEREIGN IMMUNITY

- Tucker entered into business relationships with three Native American tribes to gain the protection of “tribal sovereign immunity”
- State supreme courts in the states that sued ruled that this was permissible
- In a subsequent suit brought by the FTC, it was found that Native American tribes are subject to the FTC Act and that Tucker’s companies violated the Act

RELATIONSHIPS WITH NATIVE AMERICAN TRIBES

- The processing center operations were located in Overland Park, not OK or NE where the tribes are located. However, employees were told to lie and say they were located in OK or NE if asked
- Tribes received approximately 1%-2% of AMG's revenue, while 99%-98% was retained by Tucker's companies
- At least \$400 million went directly to Tucker, in part through personal expense and purchases paid out of the tribal entity bank accounts



SCOTT TUCKER'S \$400 MILLION

- Money went to support Tucker's lifestyle:
 - Level 5 Racing Team - 4 Porsche and 6 Ferrari automobiles and related racing team assets (\$60 million)
 - Learjet (\$14 million)
 - High-priced jewelry
 - Aspen home (\$8 million) and a Leawood, KS home (\$1.8 million)
 - Over \$200+ million sitting in various bank accounts

FRAUD: WHERE DID TUCKER'S COMPANIES GO WRONG

- Lending website informed borrower of amount they could borrow based on their claimed income and employment
- Borrowers had to electronically indicate that they had read certain documents online and to preauthorize electronic funds withdrawals from their accounts to repay the loans
- The loan principal was made available the next day via electronic deposit into the borrower's bank account

FRAUD: DECEPTIVE AND MISLEADING TILA DISCLOSURES

- The Loan Note and Disclosure had to include the TILA box to disclose the cost of the loan in clear and simple terms
- For a \$500 loan, the TILA box would indicate finance charges of \$150 and a total of payments of \$650. The loans were for 14 days, so the stated APR on this loan would be 782.14%

FRAUD: DECEPTIVE AND MISLEADING TILA DISCLOSURES

- However, the actual repayment schedule was as follows:
 - On the borrower's payday, the entire amount of the finance charge was withdrawn, but none was applied to principal unless borrower arranged to pay-off the loan
 - This would occur for four more paydays
 - On the fifth payday, the lender would begin to withdraw an additional \$50 to apply to the principal balance of the loan

ACTUAL AMOUNT PAID ON \$500 LOAN WAS \$1,925

Pmt #5 would often result in a call from the borrower

Payday	Withdrawal	Amount Applied to Finance Charge	Amount Applied to Principal	Principal Balance Remaining
1	\$ 150	\$ 150	\$ -	\$ 500
2	150	150	0	500
3	150	150	0	500
4	150	150	0	500
5	200	150	50	450
6	185	135	50	400
7	170	120	50	350
8	155	105	50	300
9	140	90	50	250
10	125	75	50	200
11	110	60	50	150
12	95	45	50	100
13	80	30	50	50
14	65	15	50	0
	\$ 1,925	\$ 1,425	\$ 500	

These figures were not provided to the borrower in any of the documentation



BORROWER HARM

- Borrower's were cash-strapped to begin with
- Unauthorized withdrawals would keep them from paying other obligations and resulted in overdrafts and NSF fees
- Some borrowers actually had to take out additional payday loans to cover their other obligations, worsening their situation

CONVICTIONS & JUDGEMENTS

- Criminal case (2013-2018): 16 years 8 months in federal prison and potential \$3.5 billion judgement
 - Part of reason for length of prison term was his absolute lack of remorse
 - This will be Tucker's second stint in prison. He spent a year in prison related to a bank fraud scheme and was released in 1992
- He also has a \$1.3 billion judgement against him arising from a civil case brought by the FTC. His wife has a \$30 million judgement
- Tucker has been charged in Kansas for filing a false tax return that did not reflect more than \$100 million that he made through his businesses



BEHAVIORAL PROFILING

- For fraud offenders in management, the same characteristics that serve as behavioral traits that serve as fraud offender risk factors are at times the same traits they are rewarded for in organizations
 - Entitled (access to resources regardless of impact)
 - Exploitative
 - Prone to rule breaking
 - Machiavellian (ends justifies the means)



HOW TUCKER SAW HIMSELF

- Was Tucker remorseful?
- In a letter to the court, Tucker defended his business practices and implied he was misunderstood
 - “Although I saw myself as being an entrepreneur, a jobs provider, and a contributor to the American economy, I’ve learned that others view me through a different lens. I am very sorry that our leaders castigate me as a villain or some type of predator.”



HOW OTHERS MAY SEE TUCKER

- In the Netflix series “Dirty Money”
 - Tucker comes across as arrogant and completely rejects the thought that what he was involved in was wrong. His position was “It was just a business. There was demand, and consumers and the business was built around that.”
 - He was asked “Do you think you are a moral person?” After a pause he answered “I’m a business person”

TUCKER SEEMS TO BLAME THE JUDGE

- Jury was tired by end of trial (Judge let trial go on too long)
- Judge sent the case to the jury on a Friday, and there was usually no court on Friday
- Judge started the day at 8:30am rather than the normal 10:00am
- Judge did not let the jury go out to lunch as was the norm; the judge had lunch brought in
- SO, the jury was disgruntled and we couldn't catch a break. They came back with a guilty verdict a little before 5:00pm that day. Jury took the easy way out and found for guilty

COMMON FRAUD THEORY

THE FRAUD TRIANGLE

Pressure
Motivation or Incentive to
Commit Fraud

Rationalization
Justification of Dishonest
Actions

FRAUD

Opportunity
The Knowledge and Ability
to Carry Out Fraud

COMMON ELEMENTS OF PRESSURE

- Financial strain, but subjectively applied
 - Above-average affluence may feel economically deprived in comparison to their perceived relative standard
 - “Keeping up with the Jones”-true financial deprivation does not exist, its about ego
 - Threat of loss of something currently owned
 - Adverse business conditions threaten current standard of living– not only potential loss of material possessions, but also of power

COMMON ELEMENTS OF PRESSURE

- Financial strain, but subjectively applied
 - Lifestyle choices
 - Compulsive gambling or other addictive behaviors
 - Relationship breakdowns
 - Divorce settlements, custody or maintenance battles
 - True financial need
 - Often will see some repayment in the early periods of the fraudulent activity



COMMON ELEMENTS OF PRESSURE

- Not all pressures are financial
 - Ego/power
 - Power over people
 - Mastery of a situation generates a needed thrill
 - Revenge
 - A common motivation for fraud perpetrated by employees
 - May not be about the money

HOWEVER, NOT ALL FRAUD IS MEANT TO LEAD TO MONEY

TOMMY ELROD AND “WAKEY LEAKS”

- ▶▶ Player and long-time assistant at Wake Forest University
- ▶▶ Accused of providing Demon Deacon game plans to opposing coaches
- ▶▶ Financial gain? \$0





BUT PRESSURE NEEDS MOTIVATION

- Motivation is a combination of an individual's personality and the circumstances in which they find themselves
- Psychological factors will influence the way a person interprets the circumstances they are in, and this, in turn, will influence the action they **choose** to take
- This is why not everyone with a pressure and an opportunity will commit fraud



RATIONALIZATION

- Reduces the fraudster's inhibitions
- Nullifies internal objections
- Extenuating circumstances that remove the perception of criminality, at least from the perpetrator's point of view
 - "They can afford it..."
 - "They did me wrong..."
 - "Everyone is doing it..."



TOP OCCUPATIONAL FRAUD SCHEMES AND WHAT TO DO ABOUT THEM

COMMON OCCUPATIONAL FRAUDS AT GOV'T ENTITIES

- #1 Corruption
- #2 Billing
- #3 Expense Reimbursement/P-Cards



CORRUPTION



CORRUPTION

- An **employee misuses his or her influence** in a business transaction in a way that violates his or her duty to the employer **in order to gain a direct or indirect benefit**
- In most businesses, the most common form of corruption is the payment of **kickbacks related to purchases**

COUNTY IT DIRECTOR EMBEZZLED \$1.8M

- County IT Director hired his former employer, a tech company, to provide services to the County
- The tech company was required to subcontract 100% of the services to the County IT Director's daughter's tech company
- County IT Director approved above market payments for tech services, which were split between the two tech companies
- Both companies sent cashier's checks to County IT Director, which he deposited into his personal account

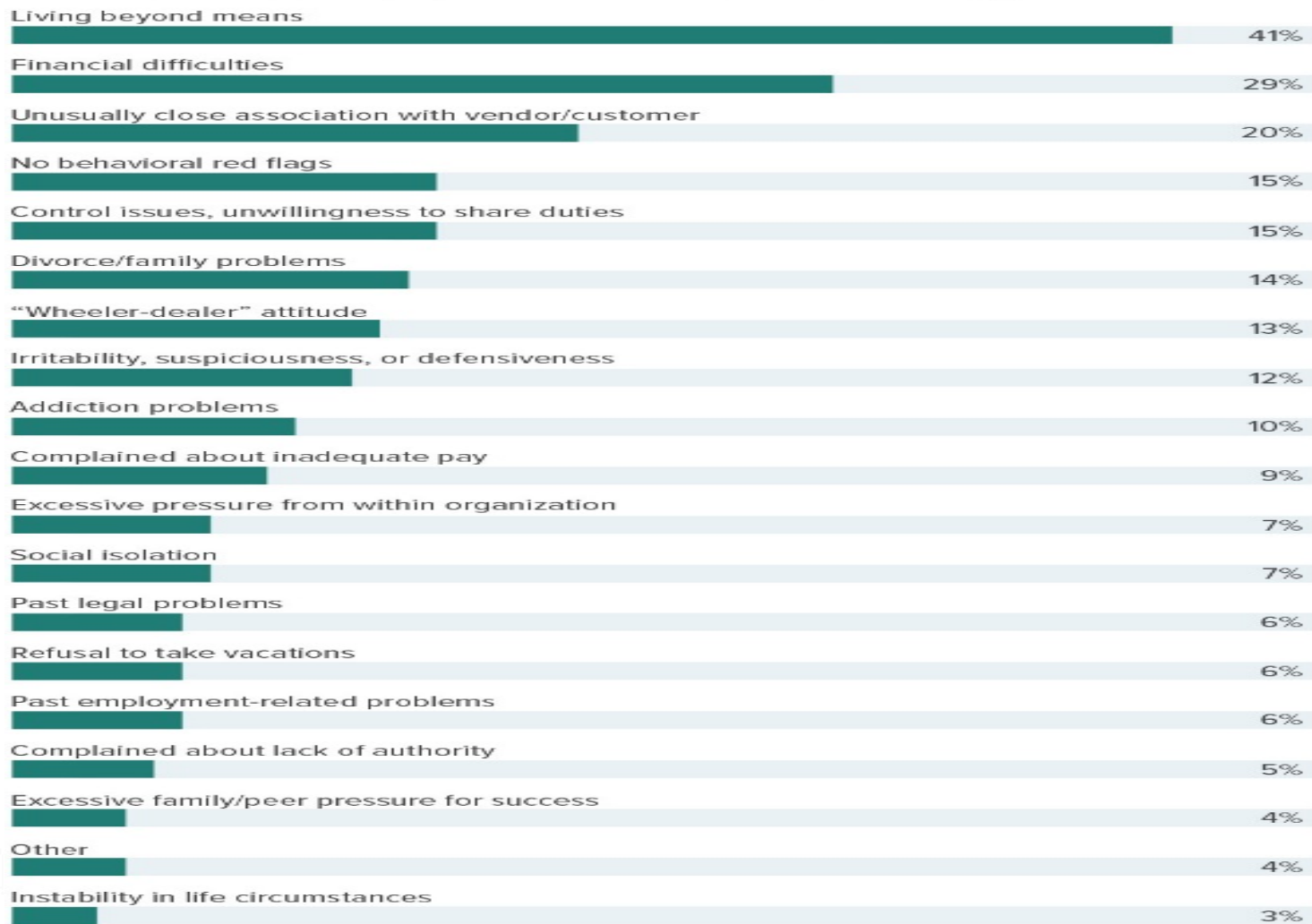


RED FLAGS FOR CORRUPTION

- **Off-book fraud**, so very hard to detect
 - Payments often do not go through the organization's accounting records
 - Payments often paid in cash
- **Look for “behavioral” red flags**
 - Rapidly increasing purchases from one vendor
 - Excessive purchases of goods and services
 - Too close of a relationship with a vendor

BEHAVIORAL RED FLAGS

FIG. 38 How often do perpetrators exhibit behavioral red flags?



ANTI-FRAUD CONTROLS FOR CORRUPTION

- Publicize your **fraud/ethics hotline**
- Implement a strong **ethics and conflicts of interest policy**
- Require **annual disclosure/reporting** of potential conflicts of interest
- **Limit gifts** from vendors and contractors
- Develop/follow a well defined **procurement process**
- Rotate buyers
- Conduct contract audits

DATA ANALYTICS FOR CORRUPTION

- Overpaid purchase orders
- Invoices greater than goods receipt
 - Compare quantities ordered and received
- Compare order quantity to optimal reorder quantity
- Compare purchase volumes/prices from like vendors
- Split transactions



BILLING SCHEMES



BILLING SCHEMES

- Fraudster **creates false support for a fraudulent purchase**, causing the company to pay for goods or services that are nonexistent, overpriced or unnecessary
 - Invoicing via shell company
 - Invoicing via an existing vendor
 - False invoicing for non-accomplice vendors
 - Pay-and-return schemes
 - Personal purchases with company's funds

\$2.2 MILLION FICTITIOUS VENDOR FRAUD

- Supervisor inquires about “emergency purchases” from two unfamiliar vendors
- Requested report of purchases under sole authority for previous 2-year period
- Two fictitious vendors
 - Used his own cell phone number and a PO Box
- Pressure was a significant gambling addiction

POTENTIAL RED FLAGS FOR BILLING SCHEMES

- Invoices for **unspecified consulting** or other service
- **Unfamiliar** vendors
- Vendors with **PO boxes**
- Vendor name consisting of **initials**
- Rapid increases in purchases
- Employee/vendor **address match**
- **Consecutively numbered** invoices from a vendor
- Repeated requests to expedite payments to particular vendors
- Invoice for **round dollar amounts**

ANTI-FRAUD CONTROLS FOR BILLING SCHEMES

- Prior to authorizing payment, **verify validity** of vendor, **receipt** of goods/services, and **accuracy** of pricing
- Prior to processing payment, check invoice for **proper authorization**
- Strictly **control access** to the Vendor Master file
- Implement a **mandatory approved vendor lists**

ANTI-FRAUD CONTROLS FOR BILLING SCHEMES

- **Control over selection** of new vendors
 - Who can select them? How are they selected?
- **Due diligence** performed on new vendors
 - Is vendor real? Is pricing reasonable? Periodically reassess vendor relationships
- **Minimize or eliminate conflicts of interest**
 - Is vendor related to an employee?

DATA ANALYTICS FOR BILLING SCHEMES

- Vendor attribute analysis
- Trending of vendor payments
- Identification of high risk payments

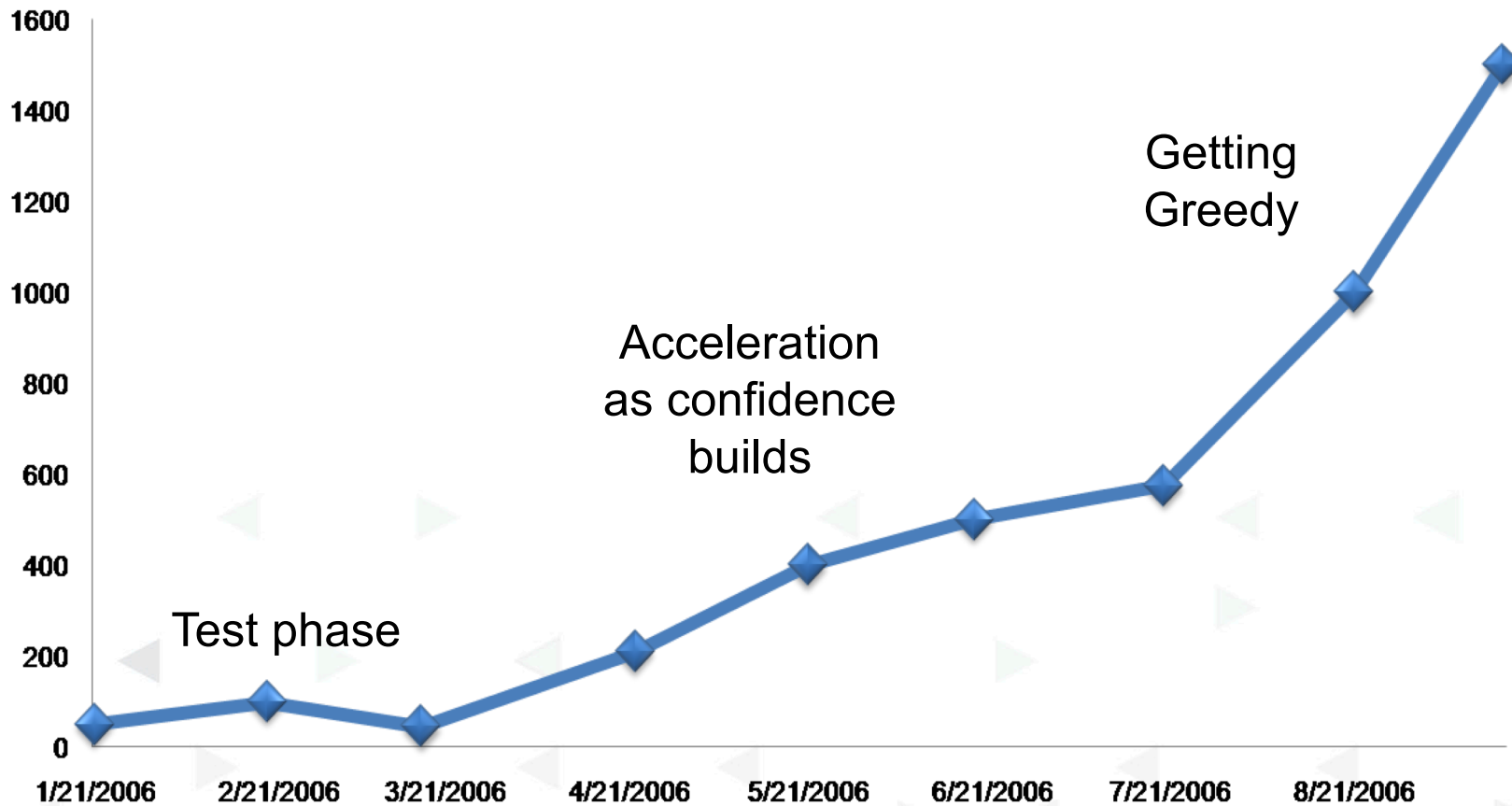
VENDOR ATTRIBUTE ANALYSIS EMPLOYEE/VENDOR MATCHING

Vendor Information							Employee Information	
Vendor TIN	Vendor nu	Name	City	Total Amount Paid from January 04 to July 2005	Street	Region	NAME	ADDRESS1
227620426	454385	JPS		no activity	605 HIGHLAND AVE SW			605 Highland Ave Sw
241720797	437069	L&L LANDSCAPING		\$ 3,786.00	3139 BECKS CHURCH RD			3139 Becks Church Rd.
243464534	509775	RIDGECREST INVESTMENTS LLC		\$167,708.00	315 RIDGECREST DRIVE			315 Rigdecrest Dr.
250085378	434913	KELLY MARKETING		no activity	436 EAST TIERRA DR			436 E. Tierra
255398736	497638	EDGE INTERACTIVE GRAPHICS		\$ 1,748.00	1247 DEE KENNEDY RD			1247 Deen Kennedy Rd
259869739	525761	SIMS JANITORIAL SERVICES		\$ 70.00	1510 LITTLE RIVER DRIVE			1510 Littlriver Dr
260159762	443860	ALLGOODS LAWN CARE		\$ 13,042.00	151 MONTGOMERY RD			151 Montgomery Road
265960806	445631	MORRIS PHOTOGRAPHY		\$ 2,472.00	1204 FIR STREET			1204 Fir Street
292649087	496812	AJ'S LAWN CARE SERVICES		\$ 225.00				P.O. Box 141
294847554	473441	DEBBIE ENGEN		no activity	5825 CROSSINGS BLVD #216			680 Lake Terrace Drive
319729230	424820	SERVICE PLUS		\$ 920.00	876 LIBERTY STREET			612 California Avenue

Vendor addresses match employee addresses

TRENDING OF VENDOR PAYMENTS

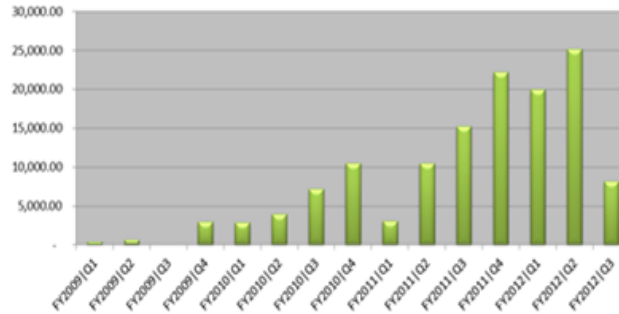
Vendor: JLM Plumbing Authorized: Janice L. McPhearson



VENDOR PAYMENTS- TIME SERIES ANALYSIS

Acceleration Patterns:

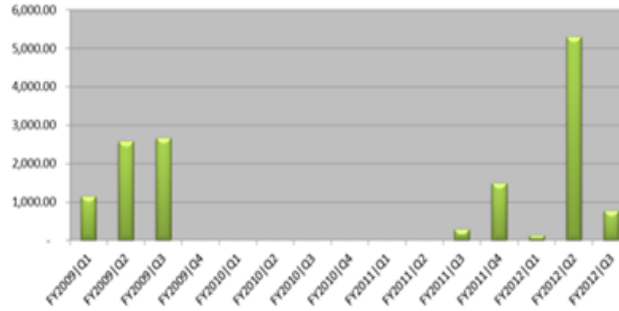
Vendors exhibiting a pattern of increased activity over multiple consecutive periods.



Possible fictitious vendor

Valley Patterns:

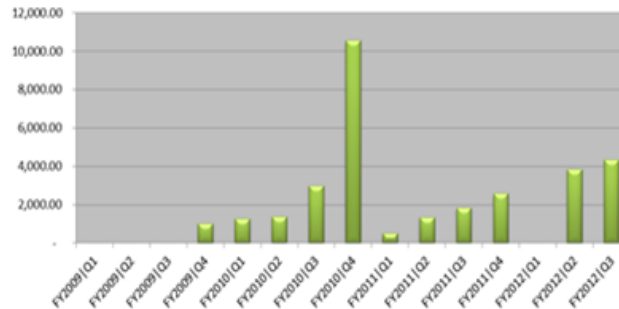
Vendors exhibiting a pattern of activity characterized by long periods of inactivity between periods of activity.



Possible abuse of dormant legitimate vendor

Spike Patterns:

Vendors exhibiting a pattern of activity characterized by unusually high payments in a single period.



Possible abuse of active legitimate vendor

IDENTIFICATION OF HIGH RISK PAYMENTS – MAIL DROPS

Vendor Information							Total	Business Name
Vendor ID	Name	Address 1	Address 2	City	State	Zip	Payments	
109					MS		70,512.70	UPS STORE
3126					MS		6,790.00	UPS STORE
3145					MS		1,705.00	UPS STORE
3189					TX		600.00	POSTNET

Mail Drop – an address used only to receive letters and packages to be picked up later

IDENTIFICATION OF HIGH RISK PAYMENTS – PROXIMITY ANALYSIS

Vendor (A)

Shauna's Design Company, 123 5th Street
Anytown, MO (Total Payments = \$84,337)

Employee (B)

Shauna Woody, 4300 Oak Street
Anytown, MO





EXPENSE REIMBURSEMENT/P-CARD FRAUD

EXPENSE REIMBURSEMENT/P-CARD FRAUD

- Any scheme in which an employee makes a **claim for reimbursement** of fictitious or inflated business expenses
 - Employee files fraudulent expense report, claiming personal travel, nonexistent meals, etc. , as incurred business expenses
 - Employee purchases personal items and requests reimbursement from the employer

\$25,000 TRAVEL REIMBURSEMENT FRAUD

- Three employees of a state Department of Human Services were charged with submitting false reimbursement requests to the state agency
- A supervisor had submitted fraudulent travel reimbursement requests and collected more than \$25,000 for mileage for driving to and from work over a nearly three year period
- The director of the field operations division had allowed for the travel reimbursements, and the county director had approved the reimbursements

RED FLAGS FOR EXPENSE REIMBURSEMENT/P-CARD SCHEMES

- Photocopies of the receipts are provided instead of originals
- Overall expenses for the organization are **considerably over budget** compared to other years
- Expense reimbursement amounts are regularly **just below the threshold for review**
- **Excessive or unusual reimbursements** to one employee compared to other employees in the organization
- A lack of supporting documents

RED FLAGS FOR EXPENSE REIMBURSEMENT/P-CARD SCHEMES

- Employee/manager **becomes defensive** when asked to provide supporting documents
- Purchases appear to be for **non-business** products or services
- Parts of the dates or amounts on receipts appear to be **altered or missing**
- Submitted receipts are **consecutively numbered**
- Expenses in **round dollar amounts**
- Expensive business lunch/dinner expenses **without names/organizations of attendees and business purpose** noted

ANTI-FRAUD CONTROLS FOR EXPENSE REIMBURSEMENT/P-CARD SCHEMES

- Get supporting documentation for purchases
 - **Original itemized receipts** – not just credit card statement
- Address possible **weaknesses in review process**
 - No review/weak review
 - Wrong person doing the review
- Question any potentially **inappropriate purchases**
- **Strengthen** your expense/purchase **related policies**
- **Do not allow personal purchases on organization credit cards/p-cards as a standard practice**

DATA ANALYTICS FOR EXPENSE REIMBURSEMENT/P-CARD SCHEMES

- Identify transactions on **weekends, holidays or while employee is on vacation**
- Identify **split transactions** in which a large purchase are split into smaller transactions just under approval threshold
- Identify **unusually high or frequent** expense reimbursement/p-card usage
- Identify expenses in **round dollar amounts**
- If utilizing “bankcard” electronic data, ask for **Level 3 data**



One CFE's Opinion of the:

TOP 20 COST EFFECTIVE INTERNAL CONTROLS

BKD

THE IMPACT OF ANTI-FRAUD CONTROLS

- Will never be completely fraud-proof
- Can take preventative anti-fraud actions
- Decrease duration of schemes that occur
- Decrease dollar amount of losses
- Insurance as a backstop

1. CREATE THE RIGHT CULTURE

- Tone at the top
- Positive workplace environment
- Culture of honesty & high ethics
- Emphasis on doing the right thing
- Management must walk the talk
- Code of ethics & fraud policy
 - Annual acknowledgement & disclosure

2. FRAUD AWARENESS TRAINING

- Targeted training for employees & managers
- Cannot solve fraud from the accounting or internal audit department
- Organization-wide awareness is critical
- Lower losses & shorter duration can be correlated to awareness training for employees

“At a minimum, staff members should be educated regarding what actions constitute fraud, how fraud harms everyone in the organization & how to report questionable activity.”

--Association of Certified Fraud Examiners

3. CONFIDENTIAL HOTLINES

- Single most cost effective anti-fraud action
- Tips are number one way that frauds are detected
- Most tips come from employees
- Both a deterrent & a detection method
- Lower losses are observed where a hotline is present
- Puts employees on notice that you want to know

“Providing individuals a means to report suspicious activity is a critical part of an anti-fraud program.”

--Association of Certified Fraud Examiners

4. APPROPRIATE BANK STATEMENT REVIEW

- Statements should be reviewed by management before giving them to the person responsible for the bank reconciliation or management should frequently review online statements
- Where possible, cancelled checks (or images) sent with bank statements
 - **Review them!**
- Management should get familiar with reoccurring ACHs/EFTs
 - **Review them!**

5. GOOD CONTROLS AROUND ACH & WIRES

- Follow the controls religiously
- Train employees to protect log-in credentials
- If you are not sure your controls are good enough in this area, have an assessment done
- Account takeover has become a big problem
- Many mistakes being made in this area

6. PERIODICALLY “AUDIT” YOUR BANK ACCOUNTS

- Make sure you know how many bank accounts you have and what they are used for



7. SEGREGATION OF DUTIES

- Custody vs. Authorization vs. Recordkeeping
- Objective is more than one pair of eyes
- Oversight & monitoring
- A few to focus on (there are many more)
 - Separate purchasing from payables
 - Never allow the same person to:
 - open the mail,
 - record payments,
 - prepare the bank deposits



8. KNOW YOUR VENDORS

- Clean up the Vendor Master File
 - Delete or inactivate old vendors
 - Complete information for all
 - Address
 - Phone number
 - EIN
- Restrict who is able to add a new vendor
 - Scrutinize new vendors
- Know relationships between employees and vendors

9. REQUIRE BACK-UP DOCUMENTATION

- All checks & cash disbursements **MUST** be accompanied by an invoice showing the payment is justified
- Only pay from **original invoices**
- Require itemized bills – especially for meals
 - Review the bills (alcohol/too many attendees)
- Do not reimburse employees until you have **ALL** receipts
- Purchasing cards- have consequences for not providing all receipts
- **Push back on things that seem unusual**
- **Don't make exceptions!**

10. 2nd LAYER OF APPROVAL & MAKE IT A REAL CONTROL

- Require two signatures on checks
 - Consider having an officer/director be the secondary signatory
 - Provide back-up documentation (invoice/receipt)
- Second person often signs off based on trust & does not actually review the transaction
 - Train employees to understand before they sign off & make this control more effective
- **Never (ever) pre-sign checks**
- **PITCH THAT SIGNATURE STAMP**

11. PHYSICALLY SECURE THE ORGANIZATION'S PREMISES AND ASSETS

- Restrict after hours access
- Lock assets up
- Set alarms
- Consider video surveillance system
- Conduct a fixed asset inventory review once a year
 - Ensures no equipment, printers, etc. are missing

12. SOLID BUDGET-TO-ACTUAL PROCESS

- Reliable budget
- Examine variances monthly
- Understand what is REALLY causing variances
- Identify & follow up on any unusual trends

13. LOG CITIZEN COMPLAINTS

- Complaints about payments, timeliness of posting, statements, etc.
- Often complaints are directed to perpetrator
 - Allows scheme to continue
- Patterns in complaints are seldom recognized until it is too late
- A lot can be learned by knowing about complaints

14. GOOD HR PRACTICES

- Background checks
- Credit checks
- Performance evaluation processes
- Exit interviews

15. MANDATORY VACATIONS

- Someone must fill in for employee on vacation & perform their duties
- Job rotation can also be used
- Many problems are identified during perpetrator vacations



16. DATA MINING

- Pattern recognition
- Identify patterns indicative of fraud schemes
- Find things you will never find by looking at documents
 - Employee – Vendor matches
 - Time series analysis
 - Weekend or holiday transaction dates
 - Transactions processed at unusual hours
 - High volume of transactions ending in 0 or 5

17. BE AWARE OF BEHAVIORAL RED FLAGS

- Rarely takes vacation
- Does not/will not produce records/information voluntarily or on request
- Tends to shift blame and responsibility for errors
- Surrounded by “favorites” or people who do not challenge them
- Rumors/indications of personal bad habits/addictions/vices
- Bullies or intimidates colleagues
- Vendors/suppliers will only deal with this individual
- Lifestyle seems excessive for income
- Is suspected to have over-extended personal finances
- Cuts corners and bends rules
- Micromanages some employees; keeps others at arm’s length

18. GIVE YOUR ORGANIZATION A CHECKUP

- When was the last time you reviewed your internal controls?
- Do you have a fraud policy statement in place?
- Are all appropriate employees bonded?
- Do your employees know what is expected of them ethically?
- Do you keep an eye out for unusual employee behavior?
- Do you have clear written policies and procedures for each staff position?

19. DO NOT FORGET ABOUT THESE

- Accounts payable
 - Fake vendors
 - Kickbacks
 - Fraudulent disbursements
- Expense reimbursement & corporate credit cards
 - Policies – “business purpose” not good enough
 - Get the support for transactions
 - Solid review process



20. PROSECUTE

- If you are a victim, please prosecute
- Huge deterrent impact
- Criminal record for perpetrator
- Lack of enforcement undermines all your anti-fraud efforts

Questions?

Thank You!



Shauna Woody-Coussens

National Practice Leader, Public Sector Advisory Services
816.701.0250
swoodycoussens@bkd.com



Doug Manhart

Director, Forensics & Valuation Services
972-702-8262
dmanhart@bkd.com