

The background of the slide is a solid dark brown color with a pattern of lighter brown, stylized autumn leaves scattered across it. The leaves have prominent veins and are oriented in various directions, creating a textured, organic feel.

Fraud

By

Marshall Romney, PhD, CFE

Brigham Young University

Business Trip to Louisiana

A Wisconsin businessman went to Louisiana. When he arrived he sent a short E-mail to his wife, Jennifer Johnson, whose address is JennJohnson@world.net. The return address was Your Loving Husband.

In his haste, he mistyped a letter. The E-mail went to JeanJohnson@world.net, the address of Jean Johnson, the wife of a preacher who had passed away and was buried that very day.

After all her funeral guests had left she realized it had been a few days since she checked her email. When she saw the one from "Your Loving Husband" she eagerly opened it. The preacher's wife took one look at the E-mail and promptly fainted.

It read: "Arrived safely, but it sure is hot down here!"

Fraud Estimates

- ACFE: U.S. business loses \$994 billion/yr (7% revenues)
 - Small business (< 100 emp) had largest median loss: \$200,000
 - Sizable increase from 2006 survey: 5%, or \$652 billion,
- Fraud represents 10% of the nation's health care bill
 - Costs between \$75 and \$130 billion/year
- Tax gap (Owed - paid) exceeds \$290 billion/yr
- 60% of Americans have shoplifted
 - 200 million incidents/yr: costs \$12 billion, \$150 per family/year
- 30% of all business failures are caused by fraud
- 13% of credit card sales result in fraud loss
- 67% of executives expect insider crime to rise in next 2 yrs
- Employees taking office supplies cost business \$120 billion/yr
- 44% of restaurant/fast-food employees steal cash or merchandise

HONESTY ESTIMATES

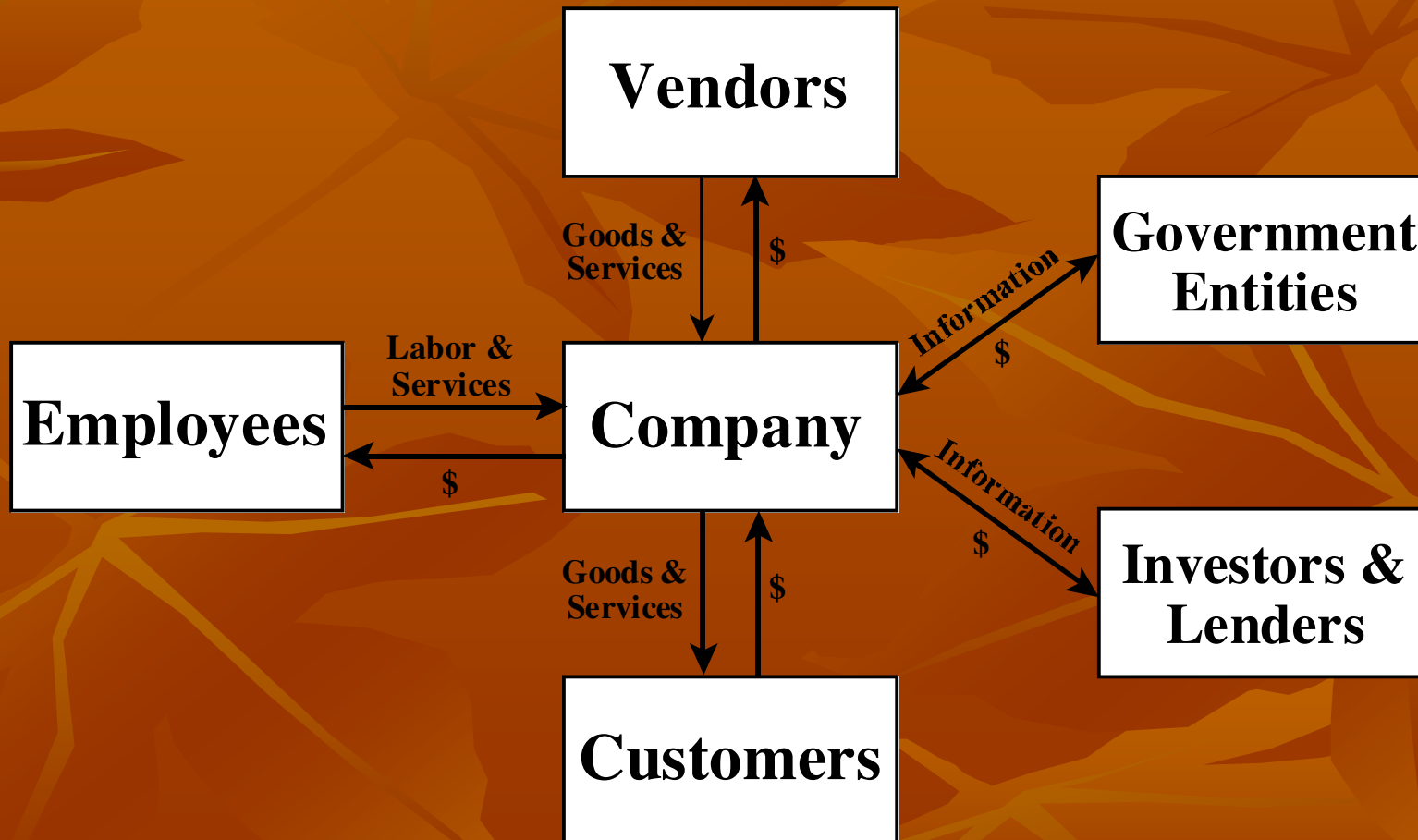
- Director of fraud prevention for a large consulting firm said that of every 10 employees
 - ___ look for a way to steal
 - ___ would steal if given an opportunity
 - ___ would usually be honest
- 2 of 3 college students admit cheating on an exam
- Institute of Management study found
 - 87% of managers will defraud to make organization look better
- Study of 400 people: How many would understate write-offs that decrease company profits?
 - 47% of top executives
 - 41% of controllers
 - 76% of graduate business students

Types of Fraud

Many ways a person can defraud another:

- Financial Statement
- Employee (Misappropriation of assets)
- Investment
- Consumer
- Identity
- Customer/vendor

COMPANIES: PERPETRATORS AND VICTIMS



Fraudulent Financial Reporting (FFR)

➤ Intentional or reckless conduct, by act or omission, that results in materially misleading financial statements.

Usually

- Committed on behalf of company
- Involves overriding Internal Controls or overstating revenues/assets

➤ May involve:

- Manipulation, falsification, or alteration of accounting records or supporting documents used to prepare Financial Statements
- Misrepresentation in, or intentional omission from, the financial statements of events, transactions, or other significant information.
- Intentional misapplication of accounting principles relating to amounts, classification, manner of presentation, or disclosure.

FINANCIAL STATEMENT FRAUD SCHEMES

1. Record unearned, fictitious, or misclassified revenue
2. Recognize genuine transactions at the wrong time (Timing)
3. Bill customers for items not shipped
4. Overstate assets, such as inventory or accounts receivable
5. Fail to disclose material financial statements facts
6. Capitalize, conceal, misclassify, depreciate, amortize, defer, or fabricate expenses
7. Conceal or understate liabilities and losses
8. Deal with related parties (companies you own or control), allowing you to be both buyer and seller
9. Record excess, one-time reserves and restructuring charges and later inflate profits by using the excess reserves
10. Back date Stock Options
11. Record “favorable” errors up to the limits of materiality

Financial Statement Fraud Examples

- Enron
- Worldcom
- Adelphia
- Tyco
- Pharmalot
- Phar-Mor
- Crazy Eddie
- Many, many more

Employee Fraud

- Employee theft or misappropriation of assets
 - Usually for personal gain
- Most frequently stolen asset is cash
 - Easy to spend
 - Easy to take large amounts
 - Does not have to be sold

Types of Employee Fraud

➤ Theft of Asset Inflows

- Steal cash at point-of-sale or received in the mail
- Steal assets shipped to company

➤ Theft of Assets

- Cash
- Inventory, supplies, equipment
- Information
- Unauthorized use of assets

➤ Theft of Outflows

- Fictitious vendors/invoices
- Payroll fraud (ghost employees, pad hours)
- Reimbursement/refund
- Credit card (paying personal expenses with company funds)
- False cash register disbursement
- Loan frauds (fictitious borrowers, inflated amounts)
- Theft of assets shipped by company

Employee Fraud Examples

- Bad economic times can bring out worst in some employees
 - "I could get laid off anytime; I might as well dip while the getting's good."
- A company used expense report software to search for fishy activity
 - Rounded-up numbers, travel upgrades, meal expensed by two colleagues
 - Nailed employees upping car mileage, inflating tips, duplicate reports
- Prized software company employee resigned, reported laptop stolen
 - Using the Web, IT guys traced laptop to his house.
 - Using company methodology, system design, technology to help competitor
- Maryland man swiped 32 laptops from nonprofit employer
 - Sold them on eBay
- CFO changed type color on spreadsheet data (black to white)
 - Hid fake numbers that boosted the totals and his bonus.
- Regional VP charged \$4,000 for Victoria's Secret lingerie to corporate card – was not given to his wife
- Muffler man

INVESTMENT FRAUD

- Persuading individuals or organizations, usually through deception, to invest money in a real or fictitious business or investment, then diverting the money to personal use or to fund the fraud scheme.
- Successful investment swindlers use every trick in the book to get their victims to part with their money and line their pockets
 - They target the most vulnerable citizens
 - They use increasingly sophisticated tools
- Many easily elude law enforcement as they pick victims' pockets
- Many Internet scams originate overseas; hard to trace perpetrators
- There is an almost unlimited number of investment fraud schemes
- Must take three steps to minimize investment fraud losses
 - Carefully check out the person and firm you invest with
 - Take a close and cautious look at the investment offer itself
 - Continue to monitor an investment

U.S. Investment Fraud Statistics

- \$400 billion = estimated annual securities & commodities fraud
- 11.2% = Percent of Americans scammed every year
- 25 million = number of adults scammed yearly
- 431,118 = number of fraud complaints FTC received in 2005, an all-time high
- Majority of victims are between the ages of 25 and 44
 - Next biggest group is baby boomers
- Victims likely to be financially educated, have high incomes, be deep in debt
- How victims found out about scams:
 - 33 % via print advertising (newspapers, magazines, direct mail, catalogs)
 - 17% via telemarketing
 - 14% via the Internet
 - 10.5% via television or radio advertising



Bernard Madoff

Arrested December 11, 2008

EXTENT OF FRAUD

- Largest Ponzi scheme in history
 - Exceeded \$50 billion in losses
 - Five times larger than the financial statement fraud that bankrupted the telecom company WorldCom in 2002
- Madoff ran the fraud scheme for at least two decades
 - Some people claim the fraud started as far back as the 1970s
- Many investors lost their life savings
- Many charities shut their doors or were severely damaged when donors had to take back their pledges

VICTIMS

- Over 13,000 names and addresses listed on official victim list
- French financier committed suicide
- Spain's Grupo Santander
- France's BNP Paribas
- Norman Braman, former owner of Philadelphia Eagles
- Fred Wilpon, owner of the New York Mets
- J. Ezra Merkin of GMAC
- Zsa Zsa Gabor, actress
- Elie Wiesel Foundation
- Spielberg charity
- Fairfield Greenwich Group
- Carl Shapiro of Kay Windsor Inc.
- Leonard Feinstein of Bed, Bath, & Beyond
- Maxam Capital Management, LLC.

HOW DID HE HIDE IT FOR SO LONG

- Great reputation on Wall Street
- Friendly personality
- Explained his methods of generating profit in terms that made sense to his clients and that had basis in legitimate money-managing strategies
- Appealed to investors because of its steady returns
- Claimed that his business was closed and that he was not taking any new money
- Kept his business secretive, making those who were able to invest with him feel privileged

Lessons Learned

- Diversification of assets
- Perform your own due diligence
- Greed cannot rule investments
- If the returns seem too good to be true, they probably are
- Nobody beats the market

Infallible Forecaster

- Perpetrator emails soccer fans
 - Acknowledges they do not know him or have a basis to trust him
 - He wants to demonstrate his soccer knowledge and research skill
 - Predicts a soccer team will win its next game
- Team wins; second email predicts another team will win
 - No solicitation: forecasts help you decide if want trust his knowledge
- Third and fourth contact is made – all predictions are correct
 - Recipient believes and wants to buy his predictions
- Recipient does not know perpetrator began with 2000 people
 - First call, 1000 told Team A would win, 1000 told team B would win
 - Second call to 1000 given correct forecast – 500 told A, 500 told B
 - Third call and fourth call reduces pool to 125 people eager to buy predictions as perpetrator had been right 4 straight times
- Lose big when they use info to place bets, perpetrator disappears

Rare Cigars

A Charlotte, North Carolina man, having purchased a case of 24 rare, and very expensive cigars, insured them against...get this ...fire.

Within a month, having smoked his entire stockpile of fabulous cigars, and having yet to make a single premium payment on the policy, the man filed a claim against the insurance company.

In his claim, the man stated that he had lost the cigars in "a series of small fires." The insurance company refused to pay, citing the obvious reason that the man had consumed the cigars in a normal fashion. The man sued... and won!

In delivering his ruling, the judge stated that since the man held a policy from the company in which it had warranted that the cigars were insurable, and also guaranteed that it would insure the cigars against fire, without defining what it considered to be "unacceptable fire," it was obligated to compensate the insured for his loss.

Rather than endure a lengthy and costly appeal process, the insurance company accepted the judge's ruling and paid the man \$15,000 for the rare cigars he lost in "the fires."

After the man cashed his check, however, the insurance company had him arrested...on 24 counts of arson!

With his own insurance claim and testimony from the previous case being used as evidence against him, the man was convicted of intentionally burning the rare cigars and sentenced to 24 consecutive one-year prison terms!

CONSUMER FRAUD

Nearly all consumer scams operate on the basis of offering consumers something for nothing, such as a major win in a lottery or prize draw (even though you have never entered), an exclusive entry to a scheme, or a way to earn easy money.

To get this easy money, they usually ask you to send money up front.

Prize or Lottery Scams

- **BAIT:** You won a Canadian or European lottery, prize drawing, or sweepstakes
- **CATCH:** To claim, must pay taxes, insurance, fees
- **CON:** Of course, the prize doesn't exist
- Many scams deceptively use the name of a real lottery
- Elderly and young particularly susceptible to the scheme
 - Hard to convince someone they are victim of a scam, especially when con artist has made numerous phone calls and formed a bond with the victim
- Over 400 New Yorkers, in first 7 months of 2006, lost up to \$35,000 each. Elderly Kansas man lost over \$300,000.
- Multiple cash demands, claiming even more money needed
- **Remember:**
 - No legitimate contest makes you pay a fee to collect a prize
 - You cannot win a contest you did not enter

Bad Check Scam

- **BAIT:** Tenant sends landlord an expense check from employer for rent and deposit
- **CATCH:** Landlord cashes the check, deducts the rent, sends the rest back to the renter
- **BAIT:** Online job seekers offered lucrative courier job
- **CATCH:** For huge fee, receive & deposit large checks in personal accounts, wire it (less fee) to a foreign account
- **CON:** Bad check bounces **AFTER** the victim refunds the overage or wires the money

REMEMBER:

- Never send (return) money until the check to you has cleared
- Be wary of an unsolicited, online employment offer where there is no interview, especially if the job offer is not related to your experience or qualifications

GARDEN EQUIPMENT

The mule an old man had been using for years to work his large garden finally died. The only mule he could afford was one almost as old as himself.

When the old man returned to pick up the mule, the mule dealer said, " Jim, that old mule died last night. I am real sorry; I know you were counting on it for your spring planting. Hold on while I get your money."

"No, I bought it and you were just holding him as a favor. It's my loss, not yours."

Jim loaded the mule and drove off. A couple of weeks later the mule dealer saw Jim working his garden on a new \$10,000 garden tractor. He asks Jim how he could afford the tractor when a couple of weeks before all he could afford was an very old mule.

"Well, after leaving with the mule, I had this idea and I stopped at the local print shop and had 2,000 \$5 raffle tickets printed up. Grand prize...Gardening Equipment. Then I sold all the raffle tickets to people around town."

"But where did you get the gardening equipment"

"From you"

"But, all you got from me was a dead mule."

"I know, that's what I raffled off."

"My Goodness, Jim! You raffled off a dead mule? I'll bet it really made a lot of people mad when they found out about it."

"Naw, not really. The only one really ticked off was the winner, and I gave him his 5 bucks back."

IDENTITY THEFT (FRAUD)

- Michelle Brown's life changed when she filled out a rental application
 - It was stolen by Heddi Ille, the landlord's friend
 - Heddi rented property, purchased vehicles, got cosmetic surgery, and set up telephone service in Michelle's name
 - Heddi got a driver's license with her picture, Michelle's name
 - Identified herself as Michelle when arrested for drug smuggling
 - Heddi was booked and prosecuted as Michelle Brown
 - The real Michelle Brown spent years and thousands of dollars trying to clear her name and reestablish her credit
- A felon incurred \$100,000 in credit card debt; got a home loan; and bought homes, vehicles, and handguns in his victim's name
 - He called and taunted the victim, stating identity fraud was not a federal crime and he could continue the fraud indefinitely
 - He served a brief sentence for making a false statement to obtain a firearm
 - He paid no restitution to the victim

IDENTITY THEFT

- **Identity theft is obtaining and using another's personal data to defraud or deceive, usually for financial gain**
 - Congress made identity theft a federal crime in 1998
- **Plagues every age, race, gender, economic status, educational background**
 - 10 million victims per year, or 19 people every minute
 - Actual numbers likely much higher, as many do not report the crime
 - It has passed up drug trafficking as the #1 crime in the nation
 - Cost U.S. \$56.6 billion in 2005
- **Majority of ID thieves are repeat offenders, with other convictions**
- **Also affects business community**
 - \$2.5 million in lost business
 - Losing a laptop can cost \$90,000
 - Avg cost of info loss: \$182/compromised record, \$660,000/company
 - Expenses: fines, investigative time, notifying customers, credit monitoring for victims, damage control, legal expenses, customer turnover, hotline, auditing programs, remediation policies

IDENTITY THIEF PROFILE

- Difficult for law enforcement, researchers to profile
- 75% of info used in identity fraud is stolen offline
- Yet, high-tech cyber crimes receive most media attention
 - Past, most cyber identity thieves worked alone
 - Changing to sophisticated cyber-crime rings
- Most identity thieves are never caught
 - Nature of crime, international locations of perpetrators
- Among known perpetrators, the most likely to commit:
 - Family member, roommate, neighbor, business associate
- Average Identity fraud
 - By person known to victim - \$15,607
 - By person not known to perpetrator - \$2,320

Desired Information

- Name and address
- Date of birth
- Social Security and driver's license numbers
- Mother's maiden name
- Account numbers
- Card expiration dates
- Personal Identification Numbers (PIN)
- User IDs and passwords
- Credit card numbers
- Security numbers from back of credit, debit cards

Who Commits Fraud

DUMB CRIMINALS

A man, wanting to rob a downtown Bank of America, walked into the branch and wrote "this iz a stikkup. put all your muny in this bag."

While standing in line, waiting to give his note to the teller, he began to worry that someone had seen him write the note and might call the police before he reached the teller window.

So he left the Bank of America and crossed the street to Wells Fargo. After waiting a few minutes in line, he handed his note to the Wells Fargo teller.

She read it and, surmising from his spelling errors that he was not the brightest light in the harbor, told him that she could not accept his stickup note because it was written on a Bank of America deposit slip and that he would either have to fill out a Wells Fargo deposit slip or go back to Bank of America.

Looking somewhat defeated, the man said "OK" and left.

The Wells Fargo teller then called the police who arrested the man a few minutes later, as he was waiting in line back at Bank of America.

ANOTHER DUMB CRIMINAL

A man walked into a little corner store with a shot gun and demanded all the cash from the cash drawer. After the cashier put the cash in a bag, the robber saw a bottle of scotch that he wanted behind the counter on the shelf.

He told the cashier to put it in the bag as well, but he refused and said "Because I don't believe you are over 21." The robber said he was, but the clerk still refused to give it to him because he didn't believe him.

At this point the robber took his drivers license out of his wallet and gave it to the clerk. The clerk looked it over, and agreed that the man was in fact over 21 and he put the scotch in the bag. The robber then ran from the store with his loot.

The cashier promptly called the police and gave the name and address of the robber that he got off the license.

They arrested the robber two hours later.

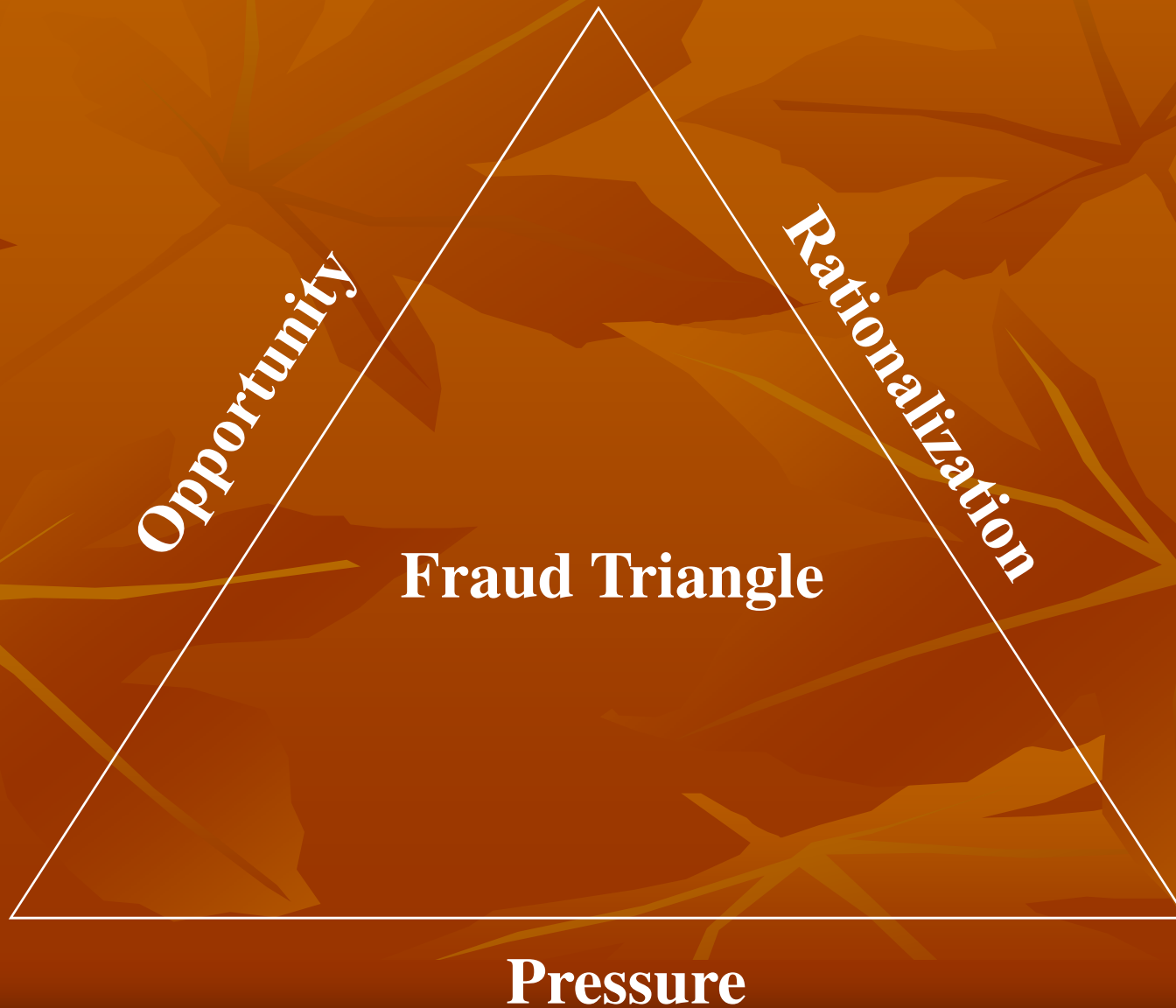
SMART LAWYER

A lawyer defended a man accused of burglary with:
"My client merely inserted his arm into the window and removed a few trifling articles. His arm is not himself, and I fail to see how you can punish the whole individual for an offense committed by his limb."

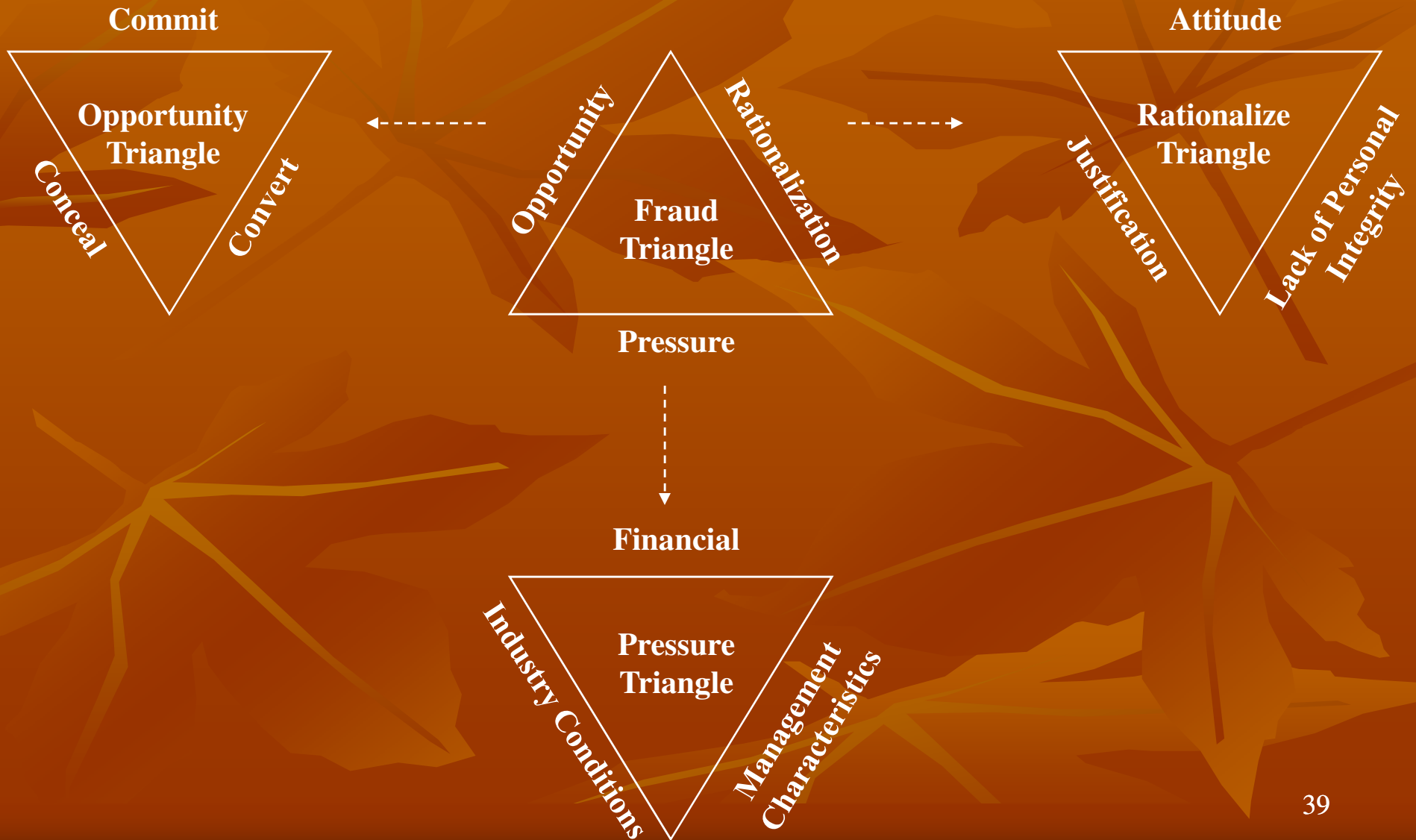
"Well put," the judge replied. "Using your logic, I sentence the defendant's arm to one year's imprisonment. He can accompany it or not, as he chooses."

The defendant smiled. With his lawyer's assistance he detached his artificial limb, laid it on the bench, and walked out.

Why Does Fraud Occur



Why Does Fraud Occur



RATIONALIZATION TRIANGLE

➤ **Justification**

- Reason or excuse why actions are not wrong or dishonest or why they are more important than honesty and integrity

➤ **Attitude**

- Allows perpetrators to violate position of trust and still consider themselves honest people.

➤ **Lack of personal integrity**

- Usually not concerned with what is fair and just
- Choose what is expedient or advantageous at moment, with little regard to consequences
- Consistently value money or profit above ethics, honesty, morality and other ideals
- One of best personality predictors of fraud perpetrators
- As individuals adopt and internalize high integrity, the probability they will commit fraud is reduced

Farmer Joe

Farmer Joe was in an accident and decided to take the trucking company responsible for the accident to court. In court the trucking company's fancy lawyer was questioning farmer Joe.

Didn't you say, at the accident scene, I'm fine,' asked the lawyer.

Farmer Joe responded, "Well. I had just loaded my favorite mule Bessie into the...

"I didn't ask for details," the lawyer interrupted, "just answer the question. Didn't you say, at the scene of the accident, 'I'm fine!'"

Farmer Joe said, "Well, I got Bessie into the trailer and was driving down the road..."

The lawyer interrupted and said, "Judge, I am trying to establish the fact that, at the scene of the accident, this man told the Highway Patrol that he was fine. Now he is suing my client. I believe he is a fraud. Please tell him to answer the question.

Judge: "I'd like to hear what he has to say."

Joe: "Well, this huge truck ran a stop sign and crashed into my truck. I was thrown into one ditch and Bessie into the other. Shortly after the accident a Highway Patrolman arrived. He could hear 'ol Bessie moaning and groaning so he went over to her. After looking at her he took out his gun and shot her between the eyes.

Then the Patrolman came across the road, with his gun still in his hand, and said to me. "Your mule was in such bad shape I had to shoot her.

How are you feeling?"

The 5 C's of Fraud

To prevent fraud you need to know how people:

- **Commit** the fraud
- **Conceal** the fraud
- **Convert** fraud to personal gain
 - At each step, perpetrator actions can be detected because it results in one or more red flags

Management must:

- **Catch** (detect) each fraud scheme
- **Control** (prevent) the fraud
 - Companies can implement controls to prevent fraud

Dr. Brian Lee

- Brian Lee was a very successful plastic surgeon in a large, physician-owned clinic in the Southwest. Dr. Lee was the clinic's top producer, in most years billing more than \$1 million annually. His take home salary and bonus ranged from \$300,000 to \$800,000 a year. Unfortunately, that wasn't enough for Brian, a 42-year-old bachelor. He wanted more, much more. Brian was part of an ultra-successful family where wealth was the family obsession. Brian, his father, and his brother had a very serious family competition: one-upmanship with respect to who had the latest and greatest material possessions. When Brian could not compete on his salary from the clinic, he risked everything he had and began skimming revenue from the clinic. Over a four year period, he defrauded fellow doctors of hundreds of thousands of dollars.
- Doctors in the clinic were free to run their offices as autonomous units. Dr. Lee, like most plastic surgeons, provided potential patients with a free, and confidential, consultation. After examining the patient, Dr. Lee would explain the patient's options, the expected results, his fee, and payment options. Like most plastic surgeons, Dr. Lee did not accept credit card payments; all payments had to be in cash or by check. If the surgery was covered by insurance, the patient had to pay the deductible before the surgery was performed. If the surgery was cosmetic or not covered by insurance, the patient had to pay in full prior to the surgery or other treatment.

- Dr. Lee's fraud was very simple, yet effective. Instead of having his patients check in at the clinic reception area, he had them come to his office, check in with his staff, and pay them or him. That way, the staff at the clinic were unaware of the patient's appointment or surgery. He then operated on them in one of the clinic's operating rooms and updated the patient's medical files. The secretary attached the payment and a copy of the receipt to the appropriate procedure form and recorded the transaction in a daily report. At the end of each day, Dr. Lee or one of his staff forwarded the paperwork and the payments to the clinic cashier.
- To perpetrate the fraud, Dr. Lee simply pocketed a patient's payment and tore up the receipt that accompanied the payments. He only took payments from patients undergoing elective surgery, meaning they had to pay for the surgery themselves. He avoided patients covered by insurance, as insurance providers might request additional documentation from the clinic that would uncover the fraud. When he took checks, usually made out to Dr. Lee, he often kept them in his desk for a few weeks before cashing them or depositing them into a personal bank account. Dr. Lee's staff had no idea that he was not forwarding the patient's payments to the clinic's office
- This went on for four years. Then Rita Mae Givens, a rhinoplasty patient, noticed that her insurance company would, under certain circumstances, cover rhinoplasty, or at least count it toward meeting the policy's yearly deductible. A requirement of the insurance claim was that a billing statement from the Doctor or clinic be attached to the claim. Since she had never received a bill, she went to the clinic and requested a copy.

- The cashier at the clinic found her file, but it did not show a bill for surgery. When Givens insisted surgery had been performed and paid for with a personal check, the cashier asked the office manager and then the clinic administrator for help. Neither could find the bill.
- Stymied, the administrator checked the doctor's surgery log and verified that Dr. Lee performed the surgery on the date and at the time Givens provided. However, Dr. Lee had never submitted the payment to the head cashier. In fact, the copy of the canceled check that Givens provided to prove she paid for the surgery was endorsed and deposited in Dr. Lee's personal bank account.
- The administrator presented the information to Dr. Lee and he confessed. The administrator immediately alerted the board. When the physician-shareholders on the clinic's board of directors found out that Dr. Lee was skimming funds, they had their law firm hire Doug Leclaire, a certified fraud examiner, to investigate.
- Dr. Lee cooperated fully with Leclaire during the weeks it took to investigate the fraud. Dr. Lee did not try to hide anything and made available all his records and bank statements. This enabled Leclaire to accurately calculate the total amount of the fraud: about \$200,000.
- Leclaire presented his results to the board. During the meeting two main issues arose. The most important was the clinic's income tax liability. Leclaire, a former IRS agent, assured them they had no liability for uncollected revenue, though taxes would be due when Dr. Lee paid back the funds he had stolen. The second: whether to terminate or retain Dr. Lee. Some board members wanted Dr. Lee terminated immediately, while others were willing to work with him.

Questions

- What motivated Dr Lee's fraud?
- How did Dr Lee commit, conceal and convert?
- How could the clinic have detected the fraud?
- What controls should the clinic implement to improve payment controls?
- Should the clinic terminate Dr Lee or retain him and "work" with him?