



Computer Fraud & Security

Chapter 5



Fraud & Computer Fraud

- The definition of fraud has nothing to do with the technology used to commit it. Fraud is fraud.



FRAUD

- Fraud** is any and every act or omission intended to gain an unfair advantage or cause injury to another.
- Legally, to be considered fraud, the act must involve:
 - A false statement or omission
 - About a material fact
 - Intent to deceive
 - A victim relies on the statement
 - And suffers injury or loss as a result

The definition is the same whether it is a criminal or civil fraud case.

The only difference is the burden of proof required.

- Criminal case:** Beyond a reasonable doubt.
- Civil case:** Preponderance of the evidence OR clear and convincing evidence.

Classic Fraud Techniques

- What is LAPPING?
 - Cash collections scheme that allows the perpetrator to, at least temporarily, steal company money.
 - Usually done by a cash collections clerk.

Lapping

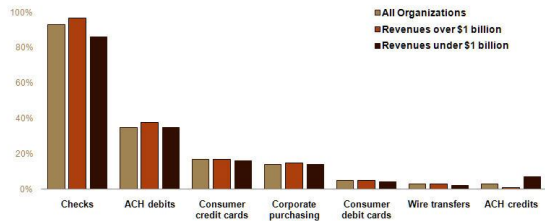
Sales on A/R	Cash Collections
1/15 \$200	2/15 \$200 (STOLEN)
1/20 \$200	2/18 \$200
1/23 \$500	2/21 \$500
<u>- 300</u>	
\$200	

Classic Fraud Techniques

- What is KITING?
 - In a kiting scheme, the perpetrator covers up a theft by creating cash through the transfer of money between banks.

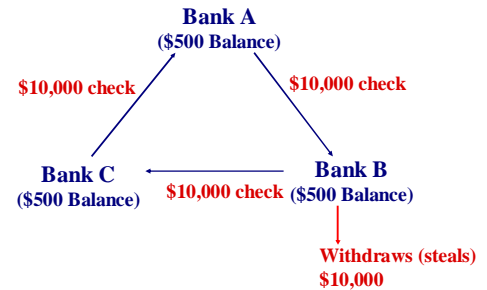
Kiting – a kind of check fraud

Payment Methods Subject to Fraud in 2006



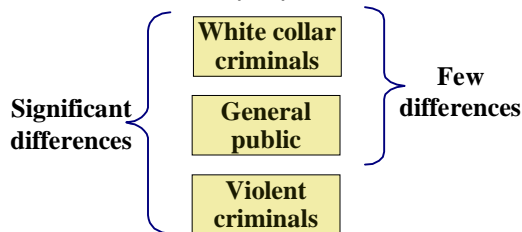
Kiting

Example: 3 bank accounts at 3 banks, \$500 in each account



Why Fraud Occurs

Researchers have compared the psychological and demographic characteristics of three groups of people:



Why Fraud Occurs

- Three conditions are necessary for fraud to occur:
 - 1 A pressure or motive
 - 2 An opportunity
 - 3 A rationalization (integrity)

Pressures

- What are some *financial* pressures?
 - Living beyond means
 - High personal debt
 - “Inadequate” income
 - Poor credit ratings
 - Heavy financial losses
 - Large gambling debts

Pressures

- What are some *work-related* pressures?
 - Low salary
 - Non-recognition of performance
 - Job dissatisfaction
 - Fear of losing job
 - Overaggressive bonus plans

Pressures

- What are *other* pressures?
 - Challenge
 - Family/peer pressure
 - Emotional instability
 - Need for power or control
 - Excessive pride or ambition

Opportunities

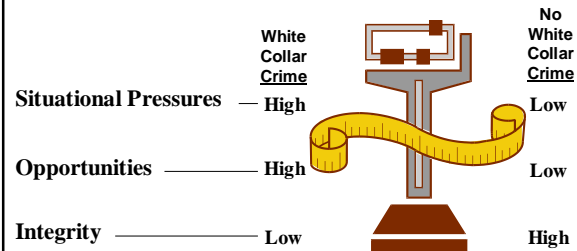
- An *opportunity* is the condition or situation that allows a person to commit and conceal a dishonest act.
- Opportunities often stem from a *lack of internal controls*.
- However, the most prevalent opportunity for fraud results from a company's failure to *enforce* its system of internal controls.

Rationalizations

- Most perpetrators have an excuse or a rationalization that allows them to justify their illegal behavior.
- What are some rationalizations?
 - The perpetrator is just "borrowing" the stolen assets.
 - The perpetrator is not hurting a real person, just a computer system, or an organization.
 - The perpetrator is redressing an injustice.

Fraud or Honesty?

Decision determined by interaction of three forces:



A Fraud Example

Julia Sweeney

- Saturday Night Live 1990-1994
- Grand Larceny



July 23, 1999 Program
"Allure of Crime"



Julia Sweeney
Alec Baldwin
Chris Farley

Why Fraud Occurs

- What are some common characteristics of fraud perpetrators?
 - Most spend their illegal income rather than invest or save it.
 - Once they begin the fraud, it is very hard for them to stop.
 - They usually begin to rely on the extra income.
 - Sometimes they get hooked or addicted to the thrill of fraud

Why Fraud Occurs

- Perpetrators of **computer fraud** tend to be younger and possess more computer knowledge, experience, and skills
- Want to “beat the system”
- Others commit fraud to gain stature among others in the computer community

Types of Frauds

- Three types of occupational fraud:
 - Misappropriation of assets
 - Corruption
 - Fraudulent statements

Types of Frauds

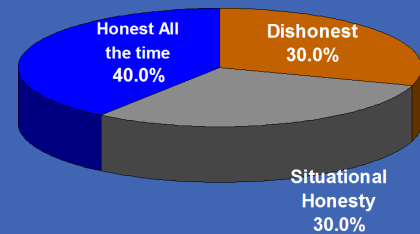
OCCUPATIONAL

- **Fraudulent Statements**
 - Financial
 - Non-financial
- **Asset Misappropriation**
 - Theft of Cash
 - Fraudulent disbursements
 - Inventory and other assets
- **Bribery and Corruption**
 - Bribery
 - Illegal gratuities
 - Economic extortion
 - Conflict of interest

OTHER

- Intellectual property theft
- Financial institution fraud
- Check and credit card fraud
- Insurance fraud
- Healthcare fraud
- Bankruptcy fraud
- Tax fraud
- Securities fraud
- Money laundering
- Consumer fraud
- Computer and Internet fraud

Honesty testing firms have established....



Anti-Fraud Regulations

1987 The Treadway Commission focused on Financial Statement Fraud

The commission determined that financial statements are falsified to:

- Deceive investors and creditors
- Cause a company's stock price to rise
- Meet cash flow needs
- Hide company losses and problems

Anti-Fraud Regulations

- Sarbanes-Oxley Act (2002)
- Statement of Auditing Standards (SAS) No.99

Anti-Fraud Regulations

SAS 99: The Auditor's Responsibility to Detect Fraud Understand fraud

- Discuss the risks of material fraudulent misstatements ("Brainstorming instruction")
- Obtain information
- Identify, assess, and respond to risks
- Evaluate the results of their audit tests
- Communicate findings
- Document their audit work
- Incorporate a technology focus

Computer Fraud

The U.S. Department of Justice definition:
"any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution."

Computer Fraud

What are examples of computer fraud?

- Theft of money by altering computer records or the theft of computer time
- Unauthorized use, access, modification, copying, and destruction of software or data
- Theft or destruction of computer hardware
- Use or the conspiracy to use computer resources to commit a felony

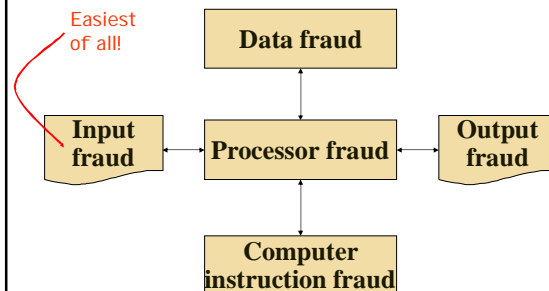
The Rise in Computer Fraud

- Organizations that track computer fraud estimate that 80% of U.S. businesses have been victimized by at least one incident of computer fraud.
- However, no one knows for sure exactly how much companies lose to computer fraud.
- Why?

The Rise in Computer Fraud

- There is disagreement on what computer fraud is.
- Many computer frauds go undetected, or unreported.
- Most networks have a low level of security.
- Many Internet pages give instructions on how to perpetrate computer crimes.
- Law enforcement is unable to keep up with fraud.

Computer Fraud Classifications





Computer Fraud and Abuse Techniques

- What are some of the more common techniques to commit computer fraud?
- Hacking (cracking)
- data diddling
- data leakage
- denial of service attack
- eavesdropping
- e-mail forgery and threats



Computer Fraud and Abuse Techniques

- hacking
- internet misinformation and terrorism
- logic time bomb
- masquerading or impersonation
- password cracking
- piggybacking
- round-down
- salami technique

Computer Fraud and Abuse Techniques

- software piracy
- scavenging
- social engineering
- superzapping
- trap door
- Trojan horse
- virus
- worm

Preventing and Detecting Computer Fraud

5 ways to decrease the potential of fraud

- 1 **Make fraud less likely to occur.**
- 2 **Increase the difficulty of committing fraud.**
- 3 **Improve detection methods.**
- 4 **Reduce fraud losses.**
- 5 **Prosecute and incarcerate fraud perpetrators.**

Preventing and Detecting Computer Fraud

- 1 ***Make fraud less likely to occur:***
 - Use proper hiring and firing practices.
 - Manage disgruntled employees.
 - Train employees in security and fraud prevention.
 - Manage and track software licenses.
 - Require signed confidentiality agreements.

Preventing and Detecting Computer Fraud

2 **Increase the difficulty of committing fraud:**

- Develop a strong system of internal controls.
- Segregate duties.
- Require vacations and rotate duties.
- Restrict access to computer equipment and data files.
- Encrypt data and programs.

Preventing and Detecting Computer Fraud

3 **Improve detection methods:**

- Protect telephone lines and the system from viruses.
- Control sensitive data.
- Control laptop computers.
- Monitor hacker information.



Preventing and Detecting Computer Fraud

4 **Reduce fraud losses:**

- Maintain adequate insurance.
- Store backup copies of programs and data files in a secure, off-site location.
- Develop a contingency plan for fraud occurrences.
- Use software to monitor system activity and recover from fraud.

Preventing and Detecting Computer Fraud

5 **Prosecute and incarcerate fraud perpetrators:**

- Most fraud cases go unreported and unprosecuted. Why?
 - Fraud not detected.
 - Companies are reluctant to report computer crimes.
 - Law enforcement officials, lawyers, and judges lack the computer skills
 - Expense

END

Chapter 5