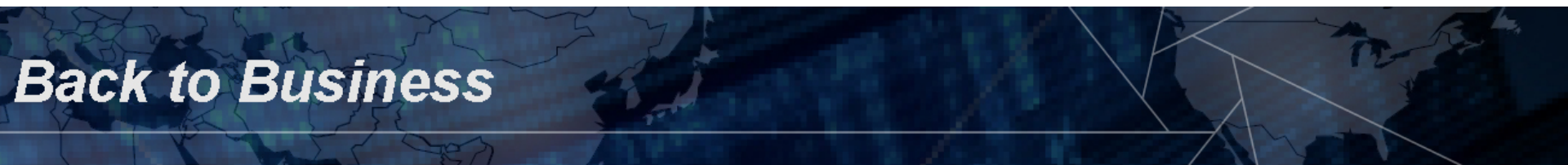




Identifying and Mitigating the Risks of Occupational Fraud and Identity Theft

Presented by Quinn Sawyer, CFE, CAMS



Back to Business

Contents

- Occupational fraud statistics
- Types of occupational fraud
- Understanding internal fraud drivers
- Warning signs and perpetrator profile
- Detection channels and best practices
- Case studies
- Managing internal fraud risks
- Identity theft threats and prevention measures

Occupational Fraud Statistics

5%

\$160,000

18 months

90%

Data from the 2010 Report to the Nations on Occupational Fraud and Abuse prepared by ACAMS

More Statistics

**Banking/
Financial
Services**

Manufacturing

**Government/
Public
Administration**

Accounting

Operations

Sales

Executive/
Upper
Management

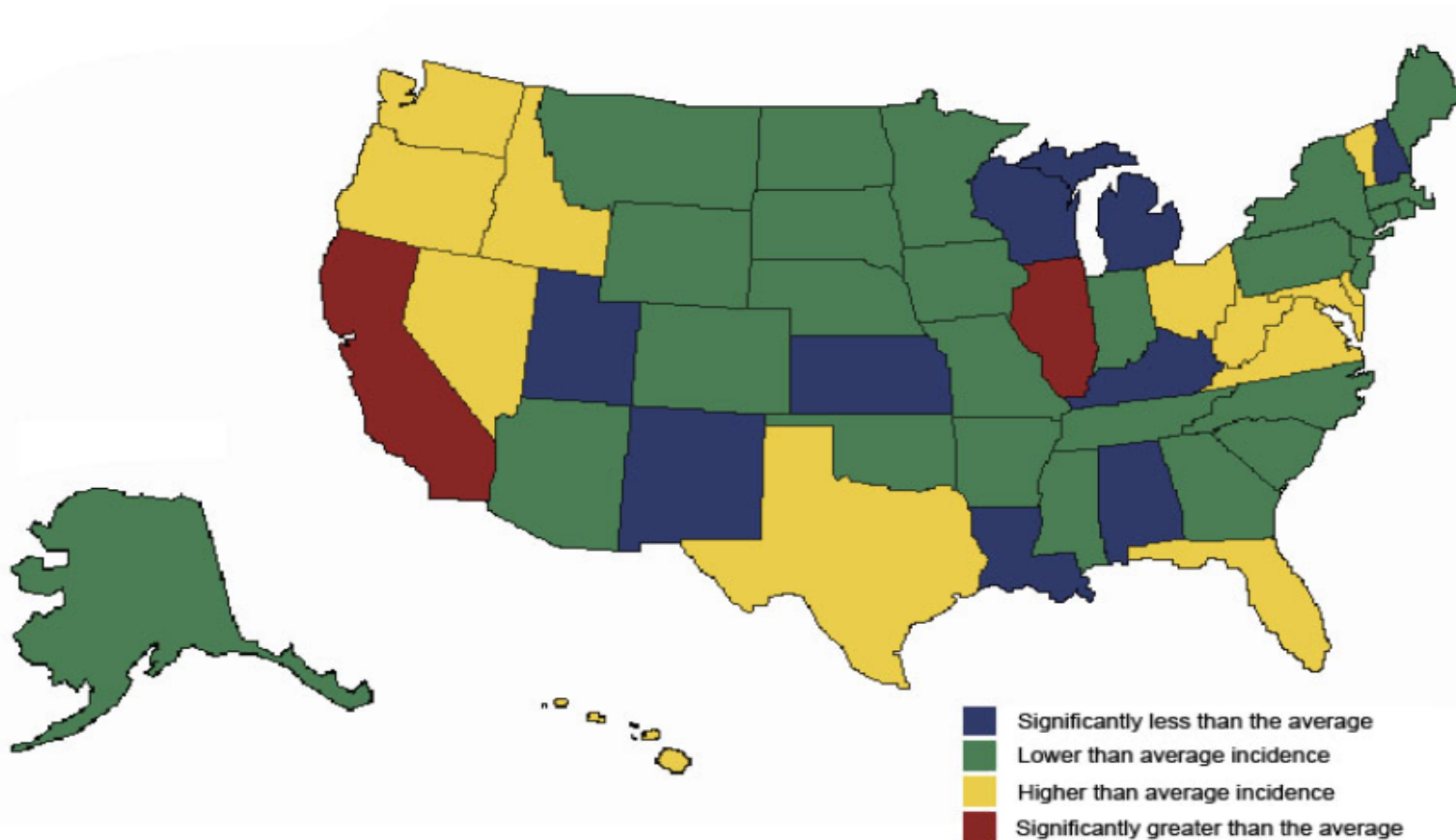
Customer
Service

Purchasing

Data from the 2010 Report to the Nations on Occupational Fraud and Abuse prepared by ACAMS

Geography of Fraud

Figure 7: U.S. Fraud Incidence Rates by State, Averaged Over Three Years



© 2009 Javelin Strategy & Research

Definition

Internal / Insider / Staff / Occupational Fraud / Abuse

The use of one's occupation for personal enrichment through the deliberate misuse or misappropriation of the employing organization's resources or assets

Categories

Corruption

22% of all frauds
Avg loss \$250,000 per case*

Bribes

Kickbacks

Conflict of Interest

Asset Misappropriation

90% of all frauds
Avg loss \$135,000 per case*

Larceny

Skimming

Misuse of Assets

Fraudulent Disbursements

Fraudulent Financial Statements

4% of all frauds
Avg loss \$4 million per case*

Fictitious Revenues

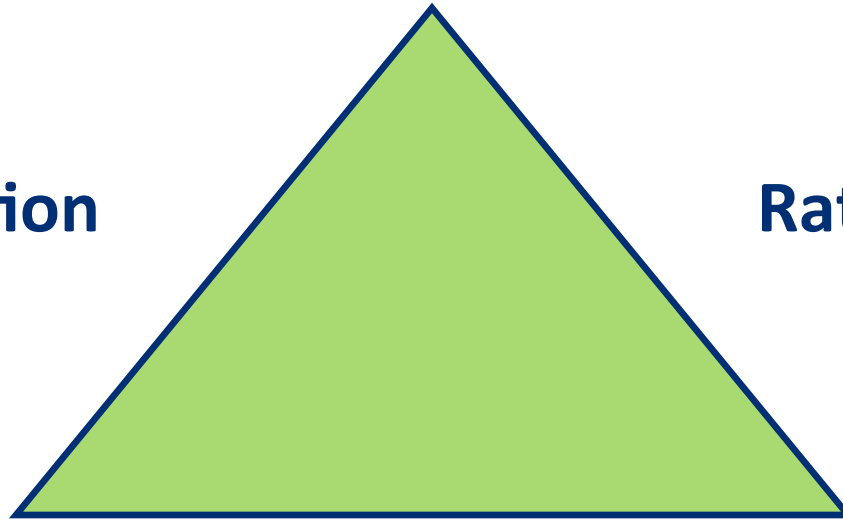
Concealed Liabilities & Expenses

*Data from ACFE's 2010 Report to the Nations on Occupational Fraud and Abuse. The sum of percentages exceeds 100% because several cases involved schemes from more than one category.

What Motivates Fraud?

Motivation

Rationalization



Opportunity

Opportunity

- **Company assets are valuable and relatively easy to access due to:**
 - Weak security
 - Loose organizational controls
 - Poor management oversight
 - Lack of segregation of duties
 - Loose monitoring of accounting anomalies
 - Misplaced trust
 - Business climate
- **Current trend:**
Internal controls weakened by staff reductions and expenditure cuts

Motivation

- **Pressures that cause an employee to commit fraud:**
 - Personal needs and debts
 - Excessive gambling habit
 - Alcohol or drug problems
 - Too onerous targets & pressure to achieve them
 - Management incentive
 - Unethical tone at the top
 - Belief the employee won't get caught
 - Enigmatic human nature...
- **Current trend:**

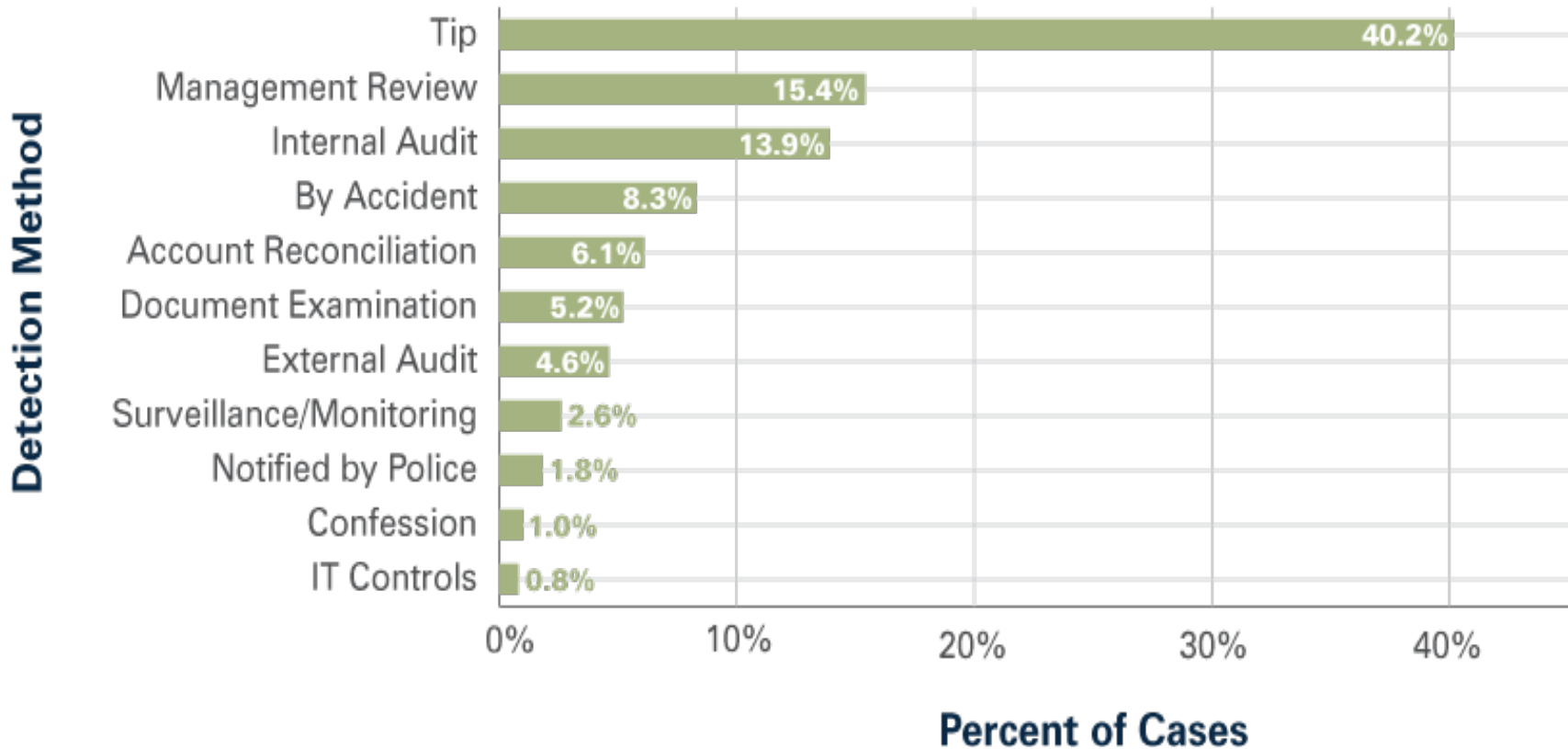
The fraudster is motivated not only by financial pressure but also by the sense of alienation and disaffection

Rationalization

- Reconciling personal behavior with commonly accepted notions of decency and trust:
 - “I don’t get paid enough for the work I do”
 - “I need to look after myself because I can’t trust them to be fair”
 - “I am doing it to save my family/home/car”
 - “I am just borrowing this money for a few days and I will return it next week. It is not stealing”
 - “There is no one to help me. I am on my own”
- Current trend:

Employees use struggling economy and growing financial pressures as moral justification of their behavior

Detection Channels Statistics



From the 2010 Report to the Nations on Occupational Fraud and Abuse prepared by ACAMS

Red Flags

Behavioral Changes

Living beyond apparent means

Bragging about new purchases

Not taking vacation/sick time

Working unsupervised after hours

Not allowing others access to area of responsibility

Personality Traits

Displaying strong desire for personal gain

Displaying a wheeler/dealer attitude

Having self-control issues

Being domineering and unable to relax

Not allowing other people review their work

Life Events

Experiencing financial difficulties

Going through a divorce

Starting a new business/struggling with current business

Experiencing medical problems (especially for a loved one)

Developing drug, alcohol, or gambling addiction

Perpetrator Profile

Middle-aged male member of middle to senior management who has worked in an organization for many years and is considered trustworthy

- Male
- 36 to 45 years old
- Commits fraud against his own employer
- Works in the finance function or in a finance-related role
- Holds a senior management position
- Employed by the company for more than 10 years

- Works in collusion with another perpetrator

Driven by personal greed or pressures to reach tough profit and budget goals

Back to Business

Citi, Banking

Gary Foster, 35

Midlevel accountant in the internal treasury finance department, 10.5 years with Citi

- Transferred \$19.2 million from various Citigroup corporate accounts to Citigroup main cash account, then wired the funds to his personal account at JP Morgan Chase in 8 separate transactions
- Fraud was detected by internal audit
- Red flag: luxurious lifestyle

July 2010

December 2010

\$19.2 million

Bank of America, Banking

BofA employee with access to accountholder information and member of a criminal ring

- Sold personally identifiable information such as names, addresses, Social Security numbers, bank balances, and driver's license numbers to a ring of criminals
- The fraudsters used that information to commit a variety of Identity Theft crimes.

Unknown



2010

\$10 million

Bathgate, Wegener & Wolf, Real Estate

Kathleen Baker, 54

Office manager, 30 years with the company

- Created a fictitious company (aka “straw man” company) called “Corporate Solutions,” and directed funds to a bank account under its name from a real estate account for which she was a signatory
- The money was subsequently used to pay off her credit card bills and personal debts
- Red flag: large credit card debts

June 2003



June 2009

\$1.14 million

Marriott, Hospitality

Tia McNeill, 34

Sales manager at Tinicum Township Renaissance Hotel

- Created six fake accounts in the Marriott Rewards loyalty program and gave herself points to purchase goods from the SkyMall airline catalog to be later sold for cash
- Illegally obtained over \$30K worth of Marriott Visa cards

October 2010



December 2010

\$130,000

Children's Hospital of Philadelphia, Healthcare

Roosevelt Hairston Jr., 46

General counsel and executive vice president, longtime top executive

- Created dozens of false invoices for shell companies
- Used the money to buy real estate, a luxury yacht with a captain, and high-end cars
- Red flag: lavish lifestyle

1999



February 2011

\$1.7 million

Bank of New York Mellon, Banking

Adeniyi Adeyemi, 27

Computer Technician in the IT department

- Stole identities of over 150 BONY employees and opened over 30 dummy brokerage accounts in their names
- Funneled over \$1.1 million from charities and non-profits into the dummy accounts
- Withdrew the funds or transferred them to a second layer of dummy accounts

November 2001

April 2009

\$1.1 million

E-Trade and Charles Schwab, Financial Services

Michael Largent, 23

- Wrote a fake script that opened over 58,000 online brokerage accounts in the names of cartoon characters
- Profited by test micro-deposits ranging \$0.01 - \$1.00
- Deposits added up to \$50,000

November 2007



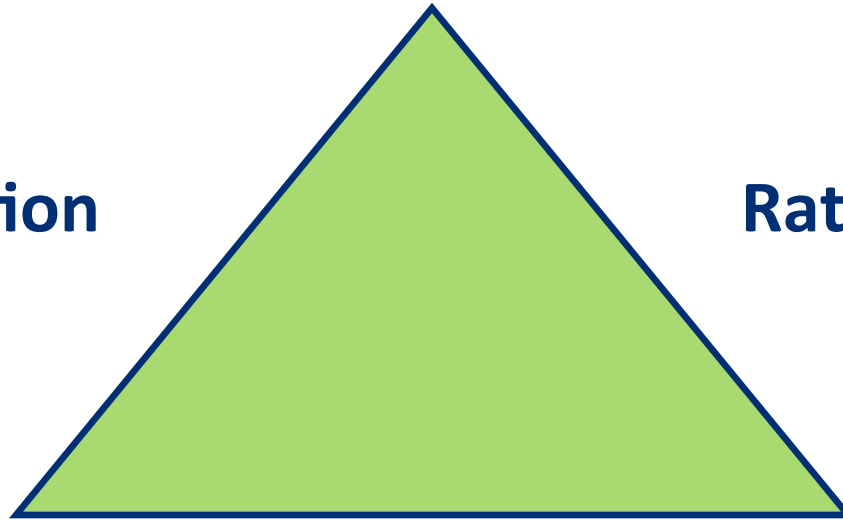
May 2008

\$50,000

Prevention

Motivation

Rationalization

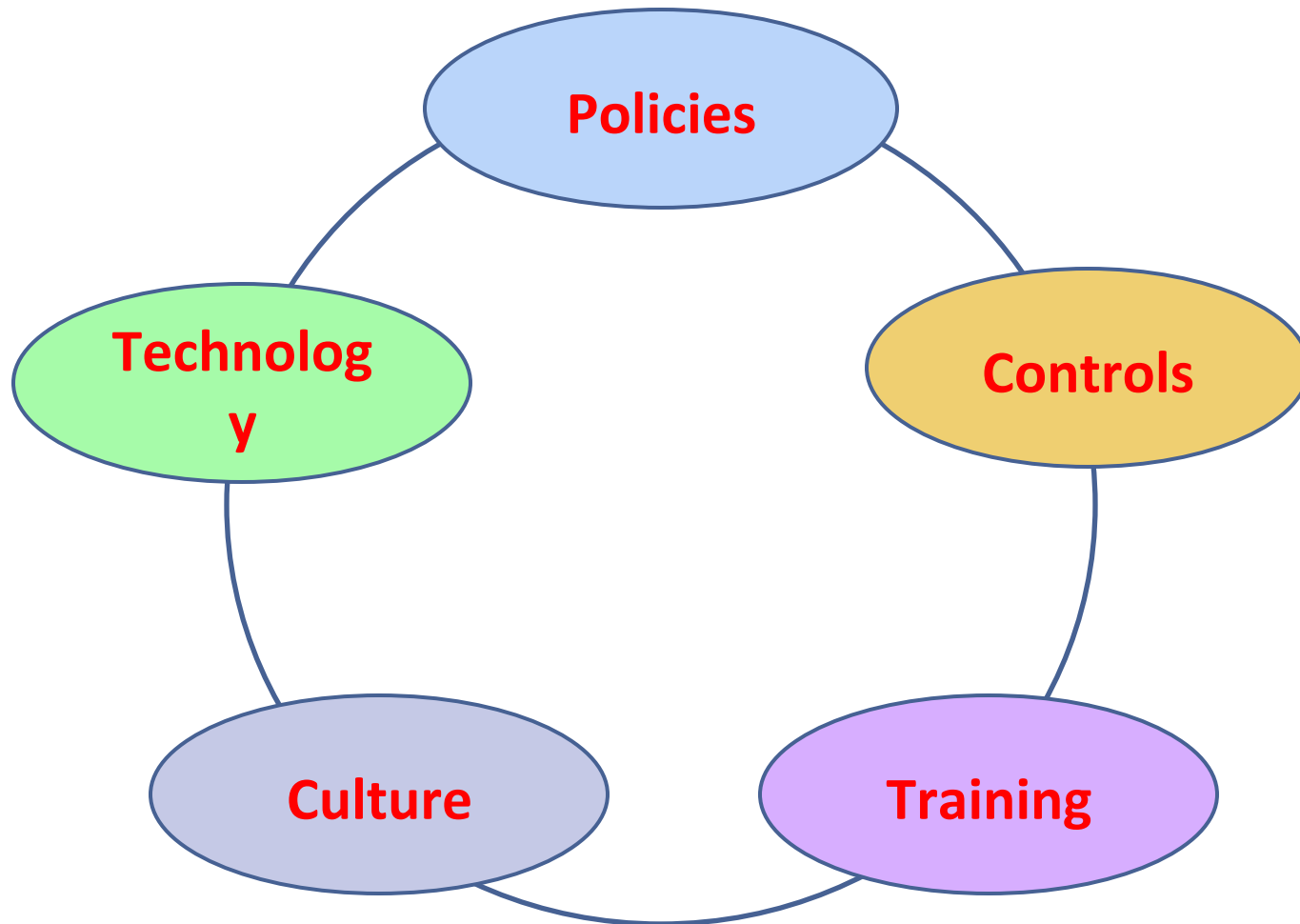


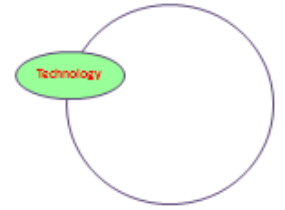
Opportunity

Strategic Responses

- Be proactive
- Manage risk holistically
- Standardize business processes
- Improve security measures
- Enforce controls
- Deploy technology
- Respond to identified fraud
- Raise fraud awareness
- Encourage culture of open communication
- Have a plan
- Trust your instincts...

Prevention Measures



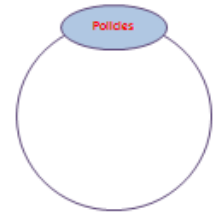


Technology

- Security in computer systems
- Platform and network access control (including remote access)
- Immediate deactivation of computer access upon termination
- Access to sensitive information through mobile devices
- Deployment of a monitoring and alerting software
- Data analysis

Best practices:

- Use technology to track internal fraud cases and uncover systemic issues that expose the organization to further internal attacks



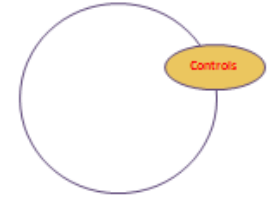
Policies

- Job rotation/mandatory vacation
- Segregation of duties
- Limited access to sensitive areas
- Proper approvals
- Redundant transaction authorization
- Timely reconciliation of statements
- Reporting of irregularities

Best practices:

- Incorporate ethics compliance and fraud prevention goals into the performance measures against which managers are evaluated

Controls



- Bookkeeping monitoring
- Supervisory review of employees work
- Physical inventories
- Surprise cash and other asset counts
- Independent validation of department/employee operations - audit

Best practices:

- Pay attention to travel reimbursement claims to ensure they are reasonable and properly supported by receipts, and are not in disagreement with the “footprints” of employees presence in the office

Training

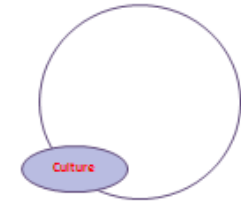


- Precise and clear code of conduct
- Training on code of conduct and fraud reporting to all new employees upon hiring
- Ongoing fraud awareness training for continuing employees
- Education on fraud red flags
- Education on penalties for defying the policies

Best practices:

- Training must cover employees at all levels of the organization – including senior managers and executives
- New employees should receive and sign statements that delineate what they can and can't do

Culture



- Careful selection of employees
- Setting the tone at the top
- Zero tolerance to fraud
- No-fear climate
- Employee support programs
- Make example of offenders

Best practices:

- Create a system for employees to anonymously report illegal or unethical actions they have witnessed or suspect. Hotlines are most effective.
- Perception of detection is the best deterrent.

Common Misconceptions About the Role of Audit

- It is auditors' responsibility to determine if there is employee fraud in the organization
- Auditors will uncover fraud, if any
- Auditors can stop fraud
- Audit is reactive
- Successfully passed audit means there is no internal fraud

Internal Fraud Takeaways

- Open communication culture facilitates tipping that leads to internal fraud detection
- Perception of detection is the easiest and less costly internal fraud deterrent
- Auditors can aid in detecting internal fraud but can't be held solely responsible for its detection. Creating and maintaining an ethical environment is everyone's responsibility.

Internal Fraud Essential Reading

- “2010 Report to the Nations on Occupational Fraud and Abuse” by ACFE
- “Who is the Typical Fraudster?” by KPMG
- “ACFE Fraud Prevention Check-up” by ACFE
- “The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risks” by PWC
- “Red Flags for Fraud” by Thomas DiNapoli
- “Trust and Occupational Fraud” by Grant Thornton
- “Monitoring, Detecting and Preventing Insider Fraud and Abuse” by Dan Sullivan

Identity Theft Definition

Identity Theft / ID Fraud

The fraudulent acquisition and use of a person's private identifying information, usually for financial gain

True Name

Account Takeover

Medical

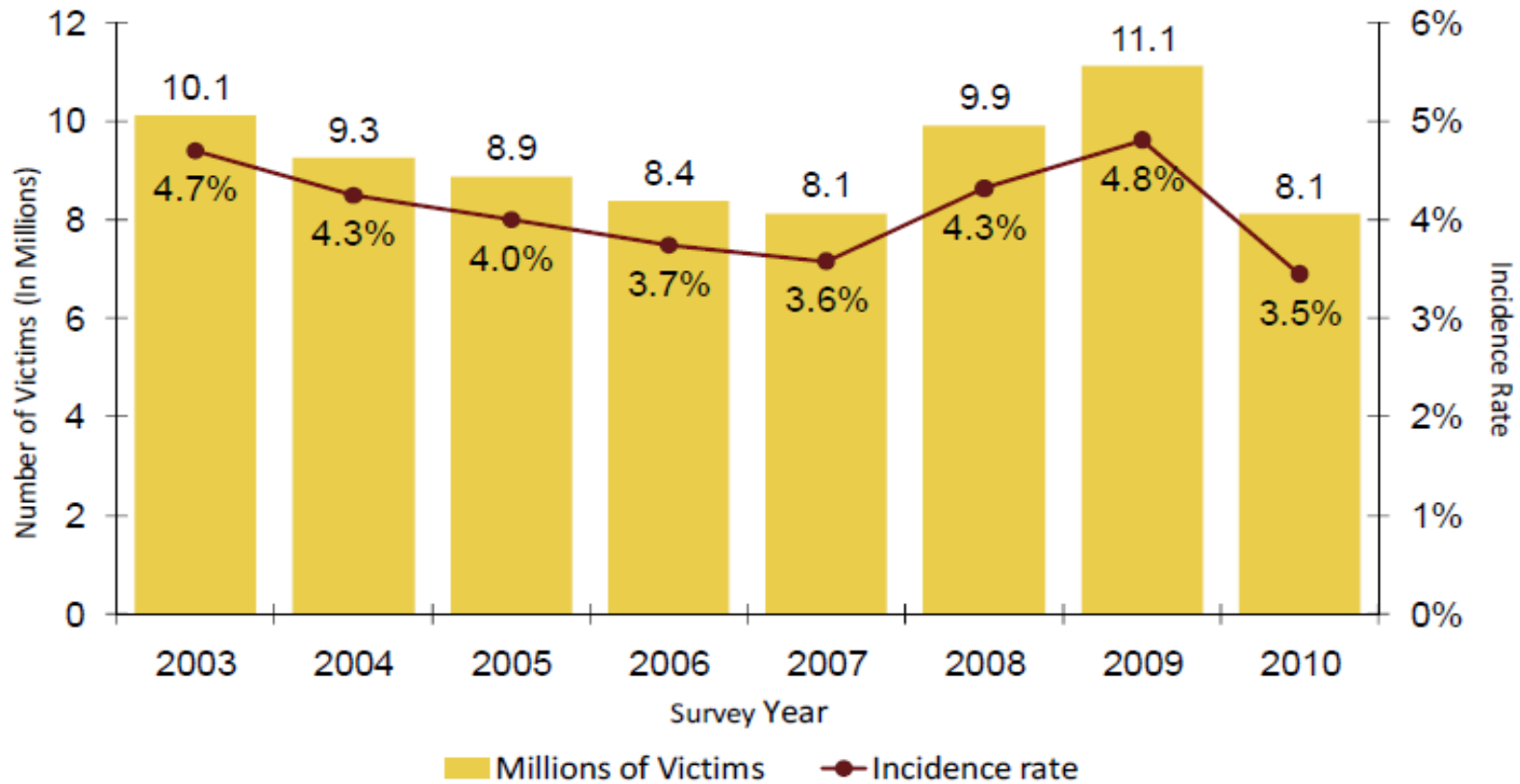
Criminal

Child IT

Identity Cloning

Identity Theft Statistics

Figure 2: Number of Victims and Incidence Rates of Identity Fraud, 2003–2010



© 2011 Javelin Strategy & Research

Identity Theft Threats

Common threats:

- Malware
- Phishing scams
- Mobile security threats
- Social networking

Evolving threats:

- Instant messaging
- Copiers
- Electronic health records

Case Study: Facebook & Identity Theft (Aug 2011)

Iain Woods used his neighbors' identities to steal from their bank accounts using their social networking info

- Amount: £35,000
- Duration: over 2 years
- How:
 - intercepted neighbors' mail
 - spent 18 hours a day on the computer looking for their personal information on social networking sites
 - accessed their online accounts and said he could not remember the password to be asked security questions about dates of birth and mother's maiden names
- Jailed for 15 months

Black Market

- About 5,000 fresh credit cards are up for sale at any given time
- Pricing :
 - credit card number from 50¢
 - complete identity (“fullz”) from \$14
 - Discover & AmEx numbers sold at a premium
 - European cards are twice as expensive as US cards
- Added-value offerings: reliable drop addresses and cash out services
- Communication channels: instant messaging services such as ICQ, MSN and Jabber plus Internet Relay Chat
- Payment methods: Liberty Reserve, WebMoney or Western Union

Search fullsS

Bins:

bin(+0.2)

Country:

Bank:

Type:

State:

City:

Zip Code:

Base:

Card type

With phone no

With DOB

Load Banks

(+0.2)

type1(+0.2)-type2(+0.3)

Load States

Load Cities

Search

Total Items: 0

Total Price: \$0



How to use search

Welcome to Our Service , Happy carding

Payments: We currently accepting Libertyreserve/ Western Union payments, for any other payments mode contact ICQ : 645305363

Prices may vary up or down depend on base validity. Base Valid rate 95 %

Replacment Policy:

- Approval fulls , cant be replaced.
- To check/refund bad credit cards go to orders page and click check (note, you have only 30 min to check your cards).
- Any attempt to cheat will be followed by an automatic ban!

Base information:

If you can provide quality fulls, you might become a reseller.

ICQ SUPPORT : [645305363](#)

Order details

Card details with id: 139617

Bin: 474478 Base: base1 Price: \$2.5 Refunded: **No** [Check](#)

Name: **ANDREA BOLZ**

CCN: 4744788888139617

Expire: 0213

CCV: 259

Address: 4500 CORNING DR APT 505

City: **ANNANDALE**

State: **VA**

Zip code: 22003

Country: **UNITED STATES**

Phone: 703-555-1234

Bank: **BANK OF AMERICA, NATIONAL ASSOCIATION**

Type 1: **DEBIT**

Type 2: **PLATINUM**

Copy whole order :

4744788888139617;0213;259;ANDREA BOLZ;4500 CORNING DR APT 505;VA;ANNANDA

Order details

Order ID: 47821

Cards: 1

Price: \$2.5

Refunded cards: 0

Info

Select the order you want to check its details inside.

You may request to manually check any card within **30 min**, it will be automatic refunded.

If the card checked was invalid it will be automatic refunded without any charging for check.

If cards are approved your balance will be decreased by 0.3 \$.

USER MENU

- » Home page
- » Buy Cvv
- » Buy Fullz
- » Billing
- » Your Cvv
- » Your Fullz
- » Support
- » Terms and conditions
- » Code Merchant
- » Our Formats
- » FAQ
- » Your info
- » Change your pass
- » Logout

SEARCH CVV

VISA | Mastercard | Discovery (+0.3\$) | AmEx (+0.3\$)

BIN (+0.5\$):

Country:

State (+0.3\$):

City (+0.3\$):

with DoB only

Search

CART

0 items

Total cost \$0,00

Your balance \$0,60

OUR PRICES

Cvv	Country	Fulls
\$4,00	United Kingdom	N/A
\$1,50	United Stats	N/A

BALANCE REFUNDING POLICY

💰 — if country have such marker then we are returning money for invalid cards (if you use checker ofcourse)

💰 — we does not return moneys if cards of this country are invalid

SEARCH RESULTS

Country: United Stats. State: VA (+0.3\$). City: McLean (+0.3\$).

Search cost: 0.6\$.

Search cost will be added to the cards cost when you will add them to your cart and will be taken from your balance when you will buy items from your cart.

Card number	Country	Location	DoB	Cost	<input type="checkbox"/>
5519*****	🇺🇸 United Stats	State: VA City: McLean ZIP: 22101	N/A	1.50+0.6\$	<input type="checkbox"/>

Card Check



Has your credit card number been STOLEN on the Internet?

card number

/

expires

Check It



Prevention Measures

- Lock sensitive information
- Invest in a paper shredder
- Exercise care on social networking sites
- Use unique passwords
- Think before giving your info to petitioners
- Install anti-virus and anti-malware software
- Use your credit, not debit, card for online purchases

Identity Theft Takeaways

- ID theft fraud is pervasive, spanning far beyond stealing and using just financial information
- ID theft fraud evolves rapidly as organized criminals move into the mass-market
- Although there is no guaranteed protection against ID theft, the easiest way to stay in control is by regularly checking bank statements and shredding your mail

Identity Theft Essential Reading

- “2011 Identity Fraud Survey Report” by Javelin
- “The Cyber-Crime Black Market: Uncovered” by Panda Security
- “Online Identity Theft: Changing the Game” by Microsoft
- “Electronic Health Information at Risk: A Study of IT Practitioners” by Ponemon Institute
- “Protecting Personal Information: A Guide for Business” by Federal Trade Commission

Contact Info

Quinn Sawyer

415-705-7395

Quinn.Sawyer@unionbank.com

Questions?

Thank you!