

Detecting and Preventing Fraud and Embezzlement in Your Nonprofit Organization

December 6, 2011

12:30 – 2:00 pm EST

Moderator:

Jeffrey S. Tenenbaum, Esq.

Panelists:

William H. Devaney, Esq

Monica Modi Dalwadi, CPA, CIA, CFE

Maria Christofi Georges



Table of Contents

Recent Examples of Nonprofit Embezzlement	3
Why Does Employee Fraud Occur?	10
Why Are Nonprofits Frequently the Victims of Embezzlement?	13
A Note About External Audits	14
Fraud Risk Assessments	16
Strong Compliance Program	18
Preventing Embezzlement	20
Role of the Board	21
Control Measures to Consider	23
Contact Information	36



What do you think the likelihood is that your company will be a target of a fraudulent attempt in the next 12 months?

1. 0% - Not a chance!
2. Very low
3. Moderate
4. Extremely high



Recent Examples of Nonprofit Embezzlement



Discovery Counseling Center of the San Ramon Valley



- On March 11, 2011, the president and executive director of Discovery Counseling Center, a non-profit that provides counseling and other mental health services, was charged with 4 felony counts of grant theft embezzlement for stealing more than \$150,000 in funds.
- The director used a company credit/debit card linked to the centers checking account for his own daily expenses.
- The Board hired an accounting company to do an audit after receiving concerns of alleged misconduct.



Caribbean Woman's Health Association ("CWHA")



- On July 19, 2010, the former executive director of CWHA, a non-profit that provides services to low-income woman and immigrants related to HIV/AIDS prevention and maternal and child healthcare, pled guilty in Manhattan Federal Court to one count of embezzling federal funds and one count of conspiring to commit wire and bank fraud.
- The former director raised her salary without receiving CWHA Board approval.
- She embezzled \$17,500 from a 2006 grant CWHA received from NY State Department of Health NYS Aids Institute.
- She attempted to defraud FDIC-insured banks in order to procure home mortgage loans.



Kids House of Seminole

Kids House
of Seminole, Inc.

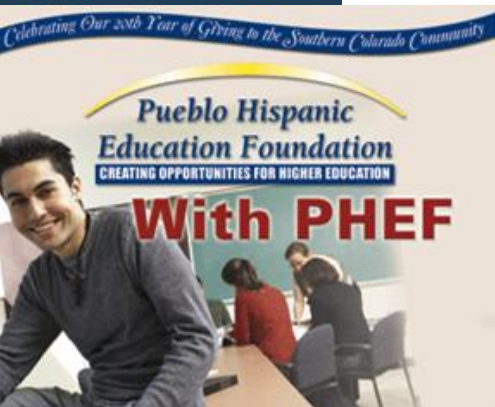


- On June 19, 2010, the former finance director of Kids House of Seminole, a nonprofit that supports children who are victims of abuse and neglect, was accused of stealing \$48,000 from the organization by writing checks from the organization to himself, then depositing the money into his personal bank account.
- The check amounts ranged from a few hundred dollars to two or three thousand dollars.
- The finance director allegedly admitted to the embezzlement and told investigators that he did it because he was a “compulsive spender.”
- The agency is reviewing its accounting system and reported that it will make any adjustments necessary.

WELLS
FARGO

 BAKER TILLY

Pueblo Hispanic Education Foundation (PHEF)



- On June 5, 2010, the director of the Pueblo Hispanic Education Foundation (PHEF), a nonprofit that helps local graduates attend college, was arrested for embezzling more than \$57,000 from the nonprofit organization.
- He was charged with two counts of theft, two counts of identity theft and 232 counts of forgery. The executive director used the foundation funds to pay for a Las Vegas trip, patio furniture and \$7,500 worth of jewelry, among other personal purchases.
- The director forged the board president's name on checks totaling \$30,143 in purchases, funneled checks destined for colleges, some that didn't even exist, into his own personal bank account, and without the 12-member foundation board knowing, he obtained a debit card and spent \$27,531 in PHEF funds for personal use.



Pueblo Hispanic Education Foundation (PHEF) – Con't.

- After the arrest, the board of directors learned that the director had pled guilty to theft in 2006 and was on probation for stealing from a Denver nonprofit, the Latin American Educational Foundation. PHEF's founder stated that the board of directors should have scrutinized the director's background much closer before hiring him.



St. Mary's Elementary School

- In November 2011, following an 18-month investigation, the former principal of St. Mary's Elementary School in Charlevoix, Michigan, was charged with 5 counts of embezzlement and 2 counts of perjury, stemming from accusations that the principal embezzled more than \$100,000 from the school over a 3 year period, by diverting school funds to her own, personal use.
- Allegedly, the principal withdrew funds from a school certificate of deposit and turned the money into cashier's checks, which she used for personal expenses.



**WELLS
FARGO**



Charleston, West Virginia Convention and Visitors Bureau

- In November 2011, the former operations Director of the Charleston, West Virginia Convention and Visitors Bureau (“CVB”) was charged with embezzling in excess of \$200,000.
- The Operations Director, described as the number two person in the organization, forged the additional required signatures on checks, including those made out to family members, and deposited funds into her personal account.



**WELLS
FARGO**



Case Study: Assistants with Access

- Evelyn Reynolds worked for Children's Education First, Inc. (CEF)*, a prestigious non-profit organization in Chicago. CEF's mission was to provide funds for underprivileged children's education expenses.
- As assistant to the Chief Operating Officer (COO), Evelyn had direct and indirect access to many facets of the business. In addition to administrative responsibilities, Evelyn had access to a variety of functions from credit card purchases to purchase order requests.
- Evelyn perpetrated a multi-faceted fraud totaling more than \$100,000 in less than ten months.

The Spoils

- Nose Job
- Recreational Vehicle
- Laptop
- Utility Bills
- Smart Phone
- Camcorder
- Vacation Packages
- Cash



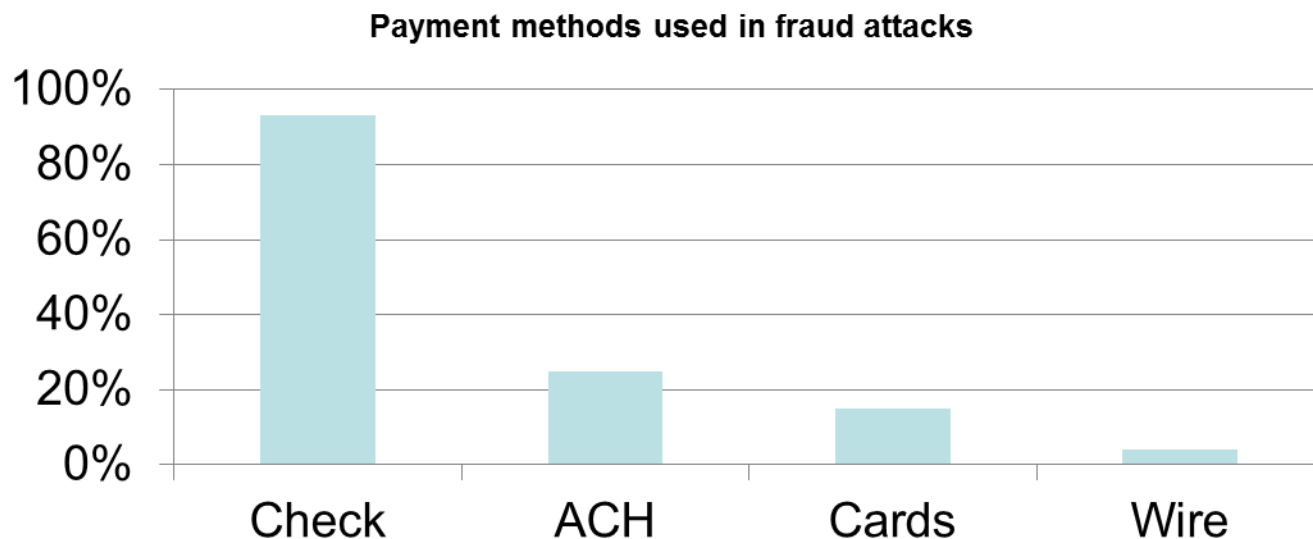
WELLS
FARGO



BAKER TILLY

Fraud Facts

- Fraud accounts for more than \$200 billion in losses each year in the U.S.¹
- 71% of organizations experienced attempted or actual payments fraud in 2010²



1. First Data Fraud Trends 2010 2. 2011 AFP Payments Fraud and Control Study



Fraud Facts

From the 2010 Global Fraud Study - ACFE

- Small organizations are disproportionately victimized by occupational fraud because they typically lack anti-fraud controls
- Anti-fraud controls appear to help reduce the cost and duration of fraud schemes
- High level perpetrators cause the greatest damage to their organizations
- Fraud perpetrators often display warning signs (living beyond their means, experiencing financial difficulties)

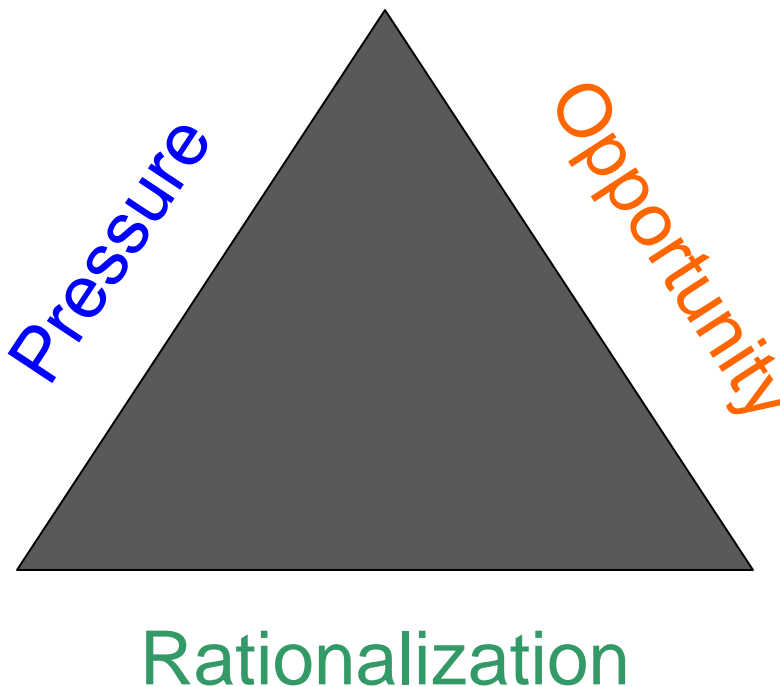


**WELLS
FARGO**



Why Does Employee Fraud Occur?

The Fraud Triangle



Why Does Employee Fraud Occur?

■ Pressure

- Economic factors such as personal financial distress, substance abuse, gambling, overspending, or other similar addictive behaviors may provide motivation.
- The current national economic recession may serve to increase the incidence of such financial motivations.

■ Opportunity

- The employee has sufficient access to assets and information that allows him or her to believe the fraud can be committed and also successfully concealed.

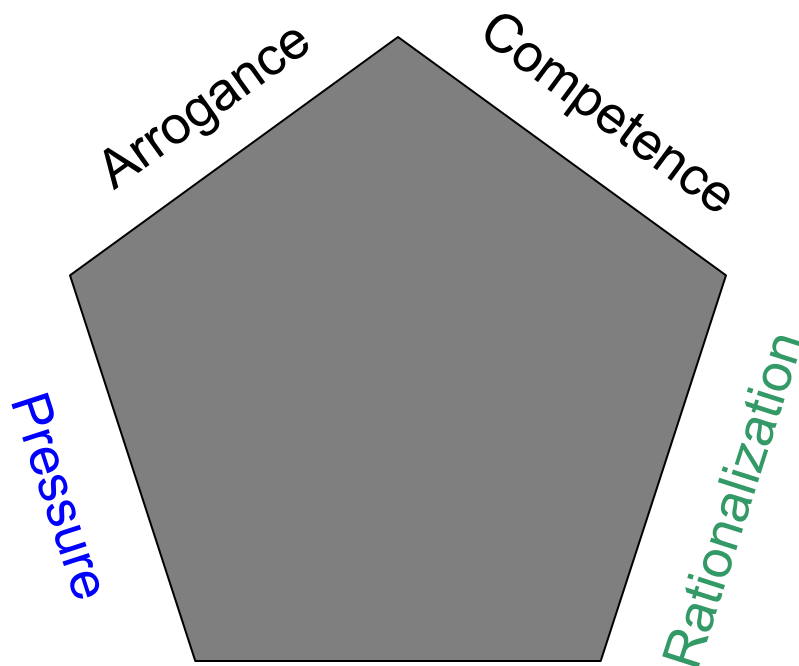
■ Rationalization

- The employee finds a way to rationalize the fraud.
- Such rationalizations can include perceived injustice in compensation as compared to their colleagues at for-profit enterprises, unhappiness over promotions, the idea that they are simply “borrowing” from the organization and fully intend to return the assets at a future date, or a belief that the organization doesn’t really “need” the assets and won’t even realize they are missing.

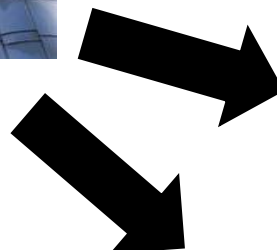


Why Does Employee Fraud Occur?

The Fraud Pentagon



Why Are Nonprofits Frequently the Victims of Embezzlement?



Management and board members are often more trusting

Leveraging operations that result in less stringent financial controls for nonprofits

Cost restrictions may result in:

- Limited or no segregation of duties due to understaffing;
- Limited resources to develop and maintain anti-fraud programs and controls; and
- Inability to maintain internal audit and/or anti-fraud departments in-house.

A belief that audits will catch any fraud



Candor. Insight. Results.

There is No “Silver Bullet”

You must employ a layered approach focused on:

- **PROTECTION** – Lowering the likelihood of successful fraud attempts
- **DETECTION** – Ensuring fraud attempts can be reliably and rapidly detected
- **RESPONSE** – Knowing what to do when you have been compromised



**WELLS
FARGO**



External Audits

- External audits can be helpful in ensuring that financial controls and fraud prevention measures are being followed and are effective.
- The standard audit, however, is not designed and should not be relied upon to detect fraud.
- The Association of Certified Fraud Examiners reports that less than 10% of frauds are discovered as a result of an audit by an independent accounting firm.
- Auditors generally only have a responsibility to give “reasonable” assurance that no material misstatements in financial statements have been made.
- While auditors are required to approach the audit with a skeptical attitude and must not overly rely on client representations (SAS 99), auditors do not have an absolute responsibility for the detection of fraud.



External Audits – Con't.

- Specific fraud audits are available and are encouraged when there is any suspicion of fraud. When fraud audits are conducted, the auditors give greater scrutiny to certain items and another auditor within the firm will often take a second look at the audit to decrease the chance that anything was missed.
- It is also a good idea to have auditors review and test your financial controls to ensure that appropriate controls are in place and working.



**WELLS
FARGO**



Fraud Risk Assessments

- The Institute of Internal Auditors (IIA) practice standard 2120.A2 states that, *the internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.*
- The purpose of a fraud risk assessment is to identify where fraud may occur within an organization and how it may be perpetrated.
- The Assessment Process:
 1. Define fraud as it pertains to the organization's industry, culture, and tolerance for risk;
 2. Determine scope (e.g., entity-wide, process-level);
 3. In collaboration with management, identify relevant fraud risks and scenarios ;
 4. Conduct facilitated brainstorming sessions to identify additional fraud risks, that include s employee participation at additional levels (e.g., process owners, staff);



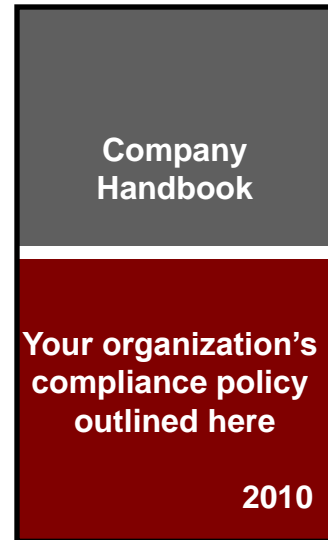
Fraud Risk Assessments – Con't.

5. Map fraud risks with their mitigating controls and identify control gaps;
 6. Measure each fraud risk based on its inherent risk (without controls) and residual risk (with controls); and
 7. Prioritize fraud risks and scenarios based on the organization's tolerance for risk.
-
- Conduct fraud risk assessment on a recurring basis (e.g., annual) as risks and controls can change based upon organizational changes, industry changes, the economy, technological advances, etc.



Strong Compliance Program

- The best way to prevent embezzlement and to protect an organization is a comprehensive and vigorous compliance program that must be more than a “mere paper program.”
- Any effective compliance program will:
 - Be tailored to the specific organization, such that the controls mitigate the risks inherent in that organization’s business and address any applicable government regulations and industry standards.
 - Include a corporate code of ethics. The organization’s commitment to ethical behavior should be clearly and concisely communicated to the board, management and employees. This commitment to the code should be affirmed by all employees on a periodic and ongoing basis.



Strong Compliance Program – Con't.

- Be owned by senior management. Management must be proactive. The Board must have ultimate oversight and control of the program.
- Provide for regular education and training for directors, management, employees, volunteers and staff.
- Be regularly monitored and audited to ensure that it is working.
- Contain effective means to report violations and concerns, such as whistleblower hotlines or other anonymous reporting mechanisms.
- Provide for meaningful discipline for violation of the policy. A reputation for aggressively investigating fraud can have a strong deterrent effect while a reputation for ignoring possible fraud is an invitation to commit fraud.
- Require that appropriate steps are taken if a crime occurs.
- Address any control weaknesses uncovered.

Company
Handbook

Your organization's
compliance policy
outlined here

2010



WELLS
FARGO

Preventing Embezzlement

Set the Tone at the Top



Role of the Board

- **Boards of Directors have a fiduciary duty to ensure:**
 - Financial decisions are made soundly and legally.
 - Individual directors and management always put the organization's financial and business interests ahead of personal financial and business interests.
 - The Board prudently manages the organization's assets in furtherance of the organization's stated purpose.

- **Business Judgment Rule protects actions taken by board members, however those actions must be taken in good-faith with that degree of diligence, care and skill which ordinary prudent people would exercise under similar circumstances.**



Role of the Board – Con't.

- Satisfying these obligations requires hands-on oversight of management.
 - Review financial and other business records
 - Question management
 - Ensure the organization's policies, procedures and mission are followed
- At least one board member should have relevant financial experience.
- At least some board members should not be current or former associates of management. Consider a seasoned lawyer as a board member, as well as members with nonprofit and sector expertise.



Control Measures to Consider

1. Double Signatures & Authorizations

- Multiple layers of approval will make it far more difficult for embezzlers to steal from your organization.
- For expenditures over a pre-determined amount, require two signatures on every check and two authorizations on every cash disbursement, written in your internal policy.
- Consider having an officer or director be the second signatory or provide authorization for smaller organizations.
- With credit cards, require prior written approval for costs estimated to exceed a certain amount.
- The person using the credit card cannot be the same person approving its use.
- Have a board member or officer review the credit card statements and expense reports of the Executive Director, CFO, CEO, etc.



Case Example

Kids House
of Seminole, Inc.



The Financial Director of Kids House of Seminole would not have been able to steal \$48,000 if the organization had implemented a control requiring that two signatures were necessary.



**WELLS
FARGO**

 **BAKER TILLY**

Control Measures to Consider

2. Require Backup Documentation

- All check and cash disbursements must be accompanied by an invoice showing that the payment is justified.
- If possible, the invoices or disbursement request should be authorized by a manager who will not be signing the check.
- Only pay from original invoices.



Control Measures to Consider

3. Never Pre-sign Checks

- Many nonprofits do this if the executive director is going on vacation.
- Keep blank checks and signature stamps locked up.

CASE EXAMPLE

An assistant to an executive director of a nursing home had the director's signature stamp locked in her drawer. She stole millions of dollars from the organization by writing checks to herself and using the director's signature stamp. The director never looked at the checks.



Control Measures to Consider

4. Segregation of Duties

- One individual should not be responsible for an entire financial transaction.
- Money Coming In: No single individual should be responsible for receiving, depositing, recording and reconciling the receipt of funds.
- Money Going Out: No one person should be responsible for authorizing payments, disbursing funds, and reconciling bank statements.
- If the organization does not have enough staff on hand to segregate these duties, a board director or officer should reconcile the bank and credit card statements.
- Require employees who hold financial positions to take an uninterrupted vacation for two weeks. Do not let them work from vacation. This permits transactions to clear properly in their absence. If you have an employee who refuses to go on vacation, that could signal a problem.



Control Measures - Case Example

- Former vice president for finance at large national nonprofit.
 - Worked there for 20 years
 - Embezzled \$11.9 million
- Wrote checks to herself, forging the signatures of the required co-signers.
 - Destroyed the canceled checks when the bank mailed them back to her.
- No one noticed because she also kept the organization's books.
- She was able to cover up for the losses by inflating the reported amount of unfulfilled pledges.
- Had someone else reconciled the bank statements, she would not have been able to destroy the checks that she had written to herself.
- Or, if someone else were responsible for unfulfilled pledges, she would not have been able to cover up the losses.



Control Measures to Consider

5. Conduct Background Checks

- Background checks on new employees and volunteers are important. Many organizations skip this basic step.
- The Association of Certified Fraud Examiners reports that 7% of embezzlers have been convicted of a previous crime.
- Background checks can reveal undisclosed criminal records and prior instances of fraud, allowing you to avoid a bad hire in the first place.
- They are also fairly inexpensive, and should be made a part of your hiring process.

CASE EXAMPLE

A thorough background investigation by the Pueblo Hispanic Education Foundation would have likely revealed that the candidate had pled guilty to embezzling money from another Nonprofit.

Control Measures to Consider

6. Fair Bidding Process

- All contracts should be subject to at least three bids, and approved by a manager uninvolved in the transaction.
- Large contracts should be reviewed and voted on by the board.

7. Fixed Asset Inventories

- Conduct a fixed asset inventory review at least once per year to ensure that no equipment (computers, printers, etc.) is missing.
- Record the serial numbers of the equipment and consider engraving an identifying mark on each item in case of theft.

8. Audits and Board Level Oversight

- Regular audits will not catch every instance of fraud, however, they are critical to prevent fraud and there should be board level review, if not oversight, of the audit.



WELLS
FARGO



BAKER TILLY

Control Measures to Consider

9. Encourage Whistleblowers

- Provide a means of anonymous communication.
- Employees may not report theft or mismanagement if they believe their job is in jeopardy.
- Employees must have a manner in which to contact a board member in the event something needs to be reported, and they do not feel comfortable reporting to management.
- Board members must be prepared to take these reports seriously, keep the reporting employee protected and contact legal counsel.



Control Measures to Consider

10. Automated Controls

- Fraud detection using system generated reports.
- Ongoing monitoring and feedback mechanisms (e.g., system generated email sent to management if individual is altering data in employee records.)
- Physical access control by security codes and badges.
- System (computer) access control by usernames, passwords, security tokens, and encryption.
- Segregation of duties by setting rights and permissions to execute various electronic tasks (e.g., entering, approving, and printing checks).
- Data mining and analysis by testing electronic data for red flags.
 - Fictitious vendors
 - Duplicate payments
- Restricting corporate credit card use by Merchant Category Code (MCC).



Control Measures to Consider

10. Automated Controls – Con't.

- **Use notification/ alert services**
 - **Sign up to receive text or e-mail notifications alerting you of electronic debits to your accounts.**
 - **Positive pay exceptions notifications**
 - **Wire notifications – incoming/outgoing**
 - **ACH Fraud Filter notifications**
 - **Balance threshold notifications**



Control Measures to Consider

11. Discuss Fraud Risk and Internal Controls by Educating Employees

- Regular (e.g., annual, quarterly) discussion of:
 - What the threats are
 - Internal control principles
 - Organizational policies and procedures
 - Incident response- what could go wrong and how to handle it in accordance with professional and legal standards – especially in “grey” areas.
- Identify key fraud risks and mitigating internal controls.
 - Develop fraud risk matrix or framework
 - Map risks and controls to identify any potential gaps
 - Update annually as part of fraud risk assessment process.
- What to do if they perceive a threat
 - Who to contact



Control Measures to Consider

12. Institute Dual Custody

- One person initiates, another approves from a different computer
 - Online payment transactions
 - ACH
 - Wire transfer
 - Self administration changes
 - Password reset
 - User enablement
 - Online payment transactions
- Be aware of collusion risks
 - Select approvers that are less likely to collude
 - Example: in different office
- Option exists to require multiple approvals



Control Measures to Consider

12. Institute Dual Custody – Con't.

- Dual custody is:
 - Free
 - Easy to implement
 - Proven to significantly reduce losses from online fraud



Control Measures to Consider

13. Use a Dedicated Computer for Online Banking

- Execute all online banking activities from a dedicated computer where email and web browsing are not possible
- Significantly reduce your exposure to malware pharming of your banking credentials

14. Use Multi-factor Authentication to Access Your Banking Portal

- A username and password do not constitute multi-factor authentication
- Add a physical security token, something in the user's possession, to provide additional protection from online threats



Control Measures to Consider

15. Update Antivirus Programs

- Install and regularly update antivirus and antispyware software
- Apply all vendor-recommended patches to
 - Company firewalls
 - Servers
 - Client applications or systems

16. Protect Your Network

- Identify trusted Web sites for your business
- Block access to any Web address not relevant to your employees' business needs:
 - Social media sites
 - Auction sites
 - Personal email accounts
 - Online chat rooms
 - Music and videos
 - Shopping

Control Measures to Consider

17. Institute Transaction and Daily Limits

- Set online wire initiation limits for each employee
 - Dollar amount
 - Account number
 - Wire type
- Review company and account limits regularly
- Evaluate averages and lower limits that are higher than necessary



Control Measures to Consider

18. Diligent User Management

- Audit users on a regular basis, especially those with transaction privileges
- Review user privileges often to ensure no one has unauthorized or unnecessary access
- Limit transaction privileges to an absolute minimum – needs only basis
- Apply separation of duties for key money movement activities



Control Measures to Consider

19. Monitor and Reconcile Accounts Daily

- One of most effective ways to catch suspicious activity as soon as possible, limiting further or substantial damage
- Establish internal processes to review key operating accounts and accounts on which you issue checks!
- Automate reconciliation function using account reconciliation services

Immediately call your financial institution if you notice anything out of the ordinary.



**WELLS
FARGO**



Control Measures to Consider

20. Appoint an Internal Audit Resource

- The Institute of Internal Auditors (IIA) defines internal auditing as :
 - *An independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.*

- Roles of the Internal Auditor:
 - Evaluate and offer recommendations on governance, risk management, and control processes, especially regarding prevention and detection of fraud.



Control Measures to Consider

20. Appoint an Internal Audit Resource – Con't.

- **Assist the organization in managing fraud risk by:**
 - **Conducting an initial or full investigation of suspected fraud**
 - **Assessing fraud risks and mitigating controls on an annual basis**
 - **Performing data analysis to identify red flags and potential indicators of fraud**
 - **Guiding implementation of anti-fraud programs and controls**



Online Fraud – The Threat is Real

■ Malware attacks explode

- Incidence of malware infections grew tenfold in 2009

Bankinfosecurity.com, “Top 8 Security Threats of 2010,” March 2010

- Number of malware-infected websites doubled from 2009 to 2010, topping 1.2 million in the third quarter

spamfighter.com

■ Phishing attacks soar

- 67,677 attacks in last half of 2010, up from 48,244 in first half

Global Phishing Survey 2H2010
Anti Phishing Working Group

■ Online fraud hits 3 out of 4 companies

- 73% of small and midsize companies experienced some form of cyber attack in 2010

Symantec State of Enterprise Security Report 2011



Online Fraud Basics

- The online fraudster's goal is simple
 - steal online banking credentials
 - set up online transactions
 - transfer money undetected
- Attacks are sophisticated, pervasive, ever changing
 - Increasingly rendering traditional prevention tactics and tools ineffective
 - Can defeat most anti-virus and anti-malware solutions
- Money is transferred to bank accounts of willing or un-witting individuals, known as “mules”, who immediately withdraw the funds and send them overseas
- Most financial institutions will never ask for confidential information through email



How can you identify a bogus site?

Wachovia Connection - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://rtewq.com/

WACHOVIA CONNECTION

WACHOVIA

CONTACT US HELP

Main Menu

System Access

Please Sign On

* User ID

* Password

Sign On

[Forgot your password?](#)

[About Wachovia Connection](#)

© Wachovia Corporation, 2004

Done Internet

Notice the URL.
Also notice there is no “s” after “http” which indicates this is not a secure site.

Notice the absence of a “padlock” symbol, indicating this is not a secure site. Wachovia’s WC+ site displays a padlock symbol.



Laws and Regulations Governing Online Fraud

- Regulation E
 - Federal law protects consumers from unauthorized electronic funds transfers (EFT)
 - Protections do not apply to wire transfers or EFTs from business accounts
- Uniform Commercial Code Article 4A
 - Governs funds transfers from a business account (ACH and wire) and wire transfers from a business or consumer account
 - Defines “ordinary care” and “commercially reasonable standards”
 - Requires notifying bank of unauthorized transactions within a “reasonable time”



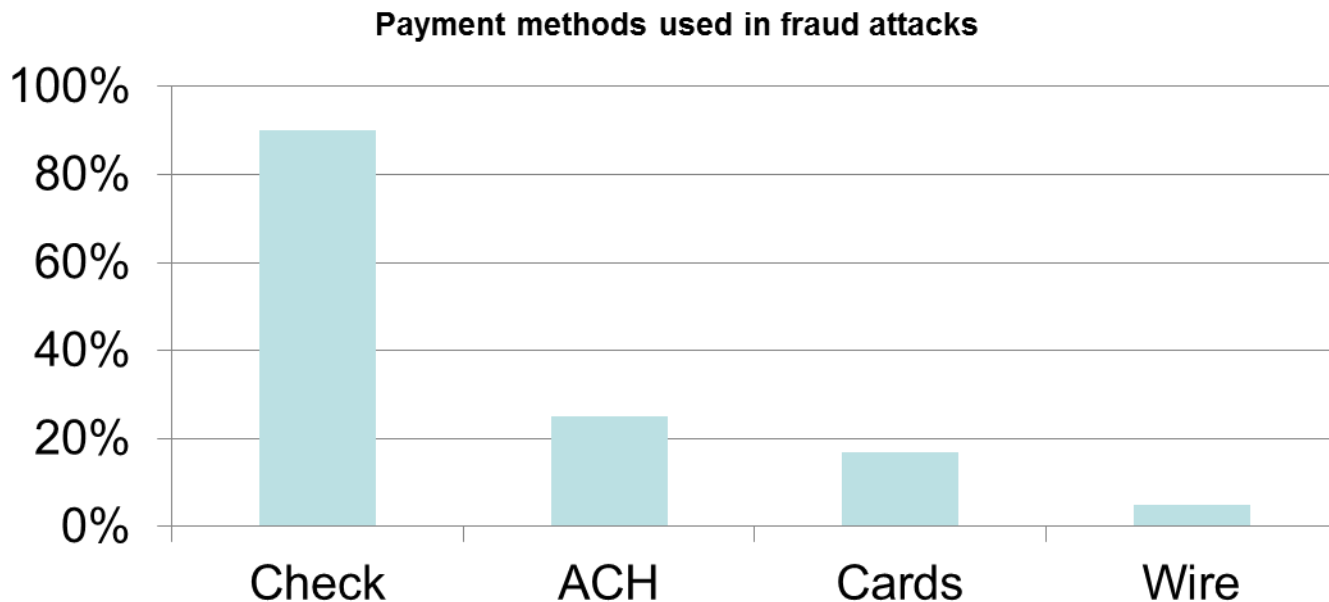
Commercial Account Agreements

- Your Bank's Commercial Account Agreement requires its customers to report unauthorized transactions within XX days of the date the Bank mails the statement that describes the unauthorized transaction



No. 1 Form of Payment Fraud: Checks

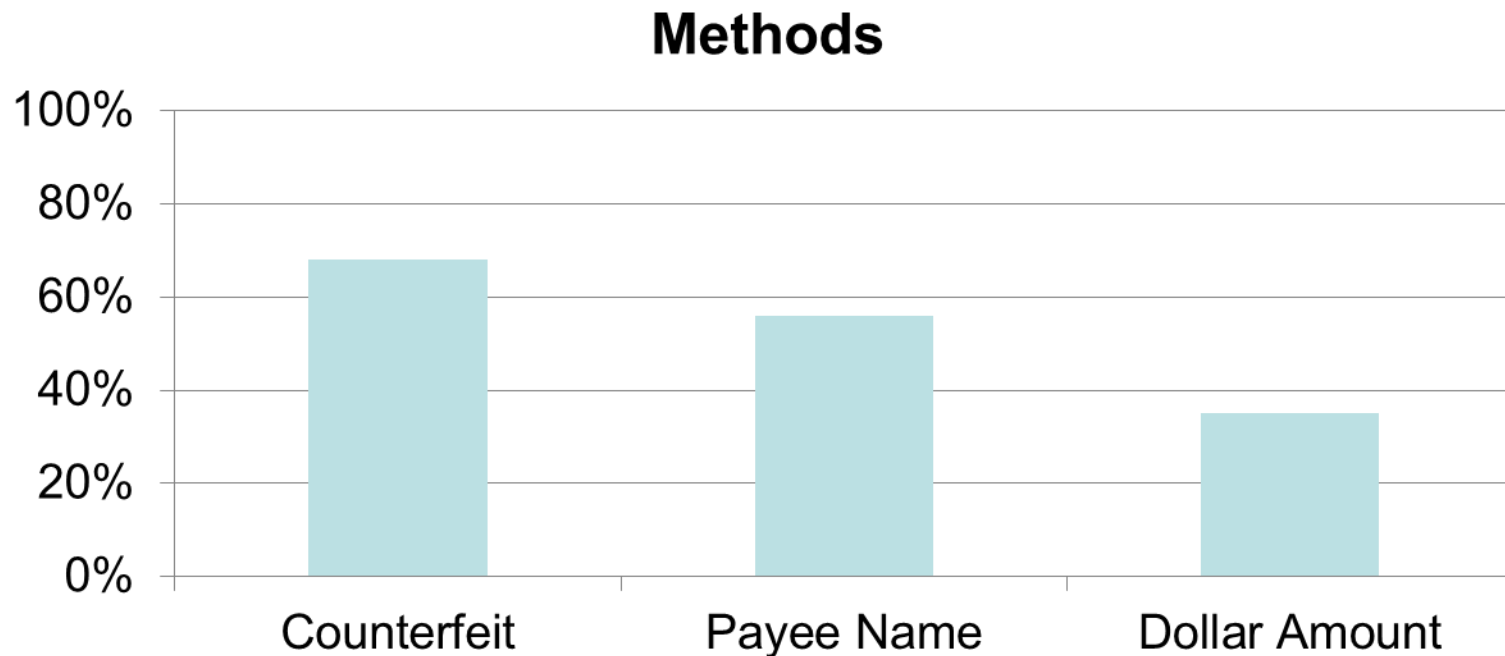
- We still write lots of checks
- Checks are touched/seen more than any other payment form – easy target



Source: 2010 AFP Payments Fraud and Control Survey



Most Common Check Fraud Methods



Source: 2011 AFP Payments Fraud and Control Survey



How to Reduce the Risk of Check Fraud

- **Don't write checks**
 - Switch to electronic payments wherever possible
 - ACH, wire, commercial card
- **Implement bank anti-fraud services**
 - Positive Pay, Reverse Positive Pay, Payee Validation, Teller Positive Pay
 - Authorization limits
 - Dual custody
- **Safeguard check stock**
- **Consider outsourcing check printing**



**WELLS
FARGO**



ACH is Not Immune to Fraud

- **Fraudulent ACH debits often originate from – a compromised check!**
- **Ways ACH fraud can impact your business**
 - **As a passive Receiver of unauthorized ACH debits against your account**
 - **As an active Originator of e-Check transaction – consumers providing fraudulent information to make purchases**
 - **Redirect vendor payments to fraudulent accounts**



Services to Protect Against ACH Fraud

- **ACH Fraud Filter:**
 - Review-service option – You review unauthorized transactions and make pay/return decisions
 - Stop-service option – All ACH transactions, except those you preauthorize, are automatically stopped and returned to originators
 - Available on most online banking systems
 - Event Messaging eligible
- **Electronic Receivables Option:**
 - Provides proxy account numbers to vendors who pay by ACH and wire
 - Keeps bank account numbers anonymous



Questions and Discussion

Venable LLP
575 7th St., NW
Washington, DC 20004
202.344.4000

JSTenenbaum@Venable.com
WHDevaney@Venable.com
monica.dalwadi@bakertilly.com
maria.georges@wellsfargo.com

To View Venable's (Searchable) Index of Articles and PowerPoint Presentations on Nonprofit Legal Topics, see www.venable.com/nonprofits/publications

