

Risk Management in an Increasingly Risky World

Susan E. Flad, CTP

Wells Fargo Bank

Together we'll go far



Agenda

- What is it?
- Impact of not Managing Risk
- Questions to Ask
- Best Practices

What is it?

- **Anything that can negatively impact your ability to do business**
 - Theft
 - Outside – Thieves, virtual and In-person
 - Inside – employees, vendors or customers
 - Environmental “Incidents”

Impact of not Managing Risk

- \$\$ Loss
- Reputation Risk – do you want to be the poster child?
- Impact to your customer
- Inability to run your business

How does it happen?

- Overt – theft or lack of oversight/controls
 - Recent article in Treasury & Risk predicts increase in internal fraud in the face of “challenging” economy.
 - “We’ve never had check fraud” mentality
 - Thieves are becoming more technologically savvy
- Unforeseen – power outage, flood, pandemic
 - Lack of preparation for the “what if?”

And the survey says....

- 2009 AFP Fraud and Control survey
 - Over **70%** Of organizations surveyed experienced **attempted or actual payments fraud in 2008.**
 - **30%** of survey respondents report that incidents of fraud **increased** in 2008 compared to 2007. Further, nearly **40%** of organizations experienced **increased** fraud activity during the second half of 2008 as economic conditions worsened in the U.S.

Questions to ask?

- Do you have **full and immediate visibility** into all of your cash, who is touching and what they can do with it? Who is responsible for controlling access? Who controls their access?
- Do you have **dual controls** and **separation of duties** for all key money movement activities?
- If there were a **pandemic** tomorrow and your physical offices were inaccessible, would it be business as usual or business in trouble?

Tools for Managing Payment Fraud

- Positive Pay w/ Payee Validation
 - 59% of check fraud involved altered payee name*
- ACH Fraud Filter and Debit Blocks
- Merchant Category Code (MCC) blocks and timely statement reviews – P-Cards
- PCI compliance and full use of fraud prevention tools (e.g. CVV – Card Value Verification)
- Account Masking

** 2009 AFP Fraud and Control survey*

Going Electronic

- Providing your account number to facilitate ACH payments – how do you know who is really asking? How do you know what they're doing with that number? Is it any different than writing a check?
 - Know your customer!
- Remote Deposit Capture – why do we suggest you shred the checks?
 - Those are LIVE account numbers.... **your customer's** account number!

You want to send more ACH...

- How do you know that the account number you've been given is really your vendor's? And not one of their disgruntled employees? How do you validate?
 - Callbacks. Invoice is a good start. An independent source (e.g. Google) is helpful.
 - Request a voided check
 - Request a letter from the vendor's bank w/ account number.
 - Cumbersome vs. Expensive. Which do you prefer?

Accepting cards

- Secure the Payment Environment
 - Eliminate Storage of Prohibited Data
 - PCI DSS – Merchant Compliance
 - Payment Application Best Practices
- What exactly is PCI DSS?
 - Payment Card Industry Data Security Standard
 - A common set of industry tools and measurements to help ensure the safe handling of sensitive information.
 - Applies to all merchants and third party service providers that store, process and transmit card holder data

Additional options

- Periodically run vendor lists to identify duplicate payee information. Same vendor, but with different account numbers or addresses? Slightly different name spellings? Review and confirm with the vendor.
- Outsource check printing to the Bank.
 - No more check stock to maintain.
 - Still need dual control!
- Migrate to more ACH origination
 - Reduce check fraud and need for positive pay

Sample Phishing E-mail

From: Wachovia Connection banking Consumer support [mailto:support@wachovia.com]
Sent: Wednesday, March 19, 2008 6:28 AM
To:
Subject: Wachovia Connection network security plan

Dear Wachovia Connection Bank Customer:

Due to the emergency situation with our server room and the closing of the New Orleans Branch of the Federal Reserve, Wachovia Connection Bank is presently unable to process wire transfers. Therefore we are asking that customers please refrain from initiating wire transfer requests through Wachovia Connection until further notice. All wires initiated before 12:30 PM CDT will be processed; however, there may be significant delays in doing so.

IMPORTANT: All customers must validate personal information.

VERIFICATION LINK: <https://wc.wachovia.com>

This situation involves circumstances outside of our control, so we ask for your patience. We will keep you advised as the situation changes.

With Best Regards,
Wachovia Connection Bank Operations team.

Wachovia Corporation, 2004

ForwardSourceID: NT00112362
ForwardSourceID: NT0005B1F2

Phishing Do's and Don'ts

- Common sense –
 - Don't Click
 - Don't respond with your sign on information
- Delete suspicious e-mails
- Use Dual Controls
- Not sure? Pick up the phone and call someone!

Back to the pandemic...

- What would happen to your Treasury if there were a pandemic tomorrow and nobody could get to the office? What if just you could not get to the office?
- Business as usual?
- Do you have policies/procedures?
- Have you tested them? Really tested them? When were they last updated?
- Laptop policy? Token policy? Use of handheld devices?

Keep Your Treasury Healthy

- No organization is immune from risk, but you can immunize.
- Plan for tomorrow today.
- Prevention is the best medicine. Use prevention tools **AND** strong policies and processes.

Questions?

- Thank you!

Appendix

- Link to AFP Payments Fraud Survey:

http://www.afponline.org/pub/pdf/2009_Payments_Fraud_Survey.pdf