April 2014

Fighting Fraud
Risks, Solutions and Best Practices

Tammy Ledet, Treasury Management Sales Advisor
Government Banking – Louisiana/Texas

Debbie K. Nolan, CTP, VP
Louisiana Sales Manager – Treasury Management

Capital One

Agenda

- Recent Payments and Fraud Statistics
- Who's Liable for Fraud?
- Fraud Risks
- Products and Services to Help Mitigate Fraud Risk
  - Dual Control Authorization
  - ACH Debit Protection/ACH Positive Pay
  - Positive Pay/Reverse Positive Pay
  - Account Reconciliation
  - Commercial Card Program Controls
- Best Practices
- Conclusion

Capital One

2013 AFP Electronic Payments Survey Overview

- The typical organization makes 50 percent of its B2B payments by check, down from 74 percent in 2007 and 57 percent in 2010
  - For payments to major suppliers, organizations make an average of 43 percent of their payments by check; 31 percent by ACH credit and 16 percent by wire transfer
- One in five organizations makes a majority of their payments through electronic means. Just under half of the survey respondents indicate that their organization is very likely to convert the majority of its B2B payments to major suppliers from checks to electronic payments in the next three years. 40 percent of financial professionals cite fraud control as a benefit for their organization's increased use of electronic payments
- Today, paper-based checks continue to be the payment type most likely to be targeted, even as their use decreases with the introduction of electronic solutions

Capital One

•Source: 2013 AFP Electronic Payments Survey

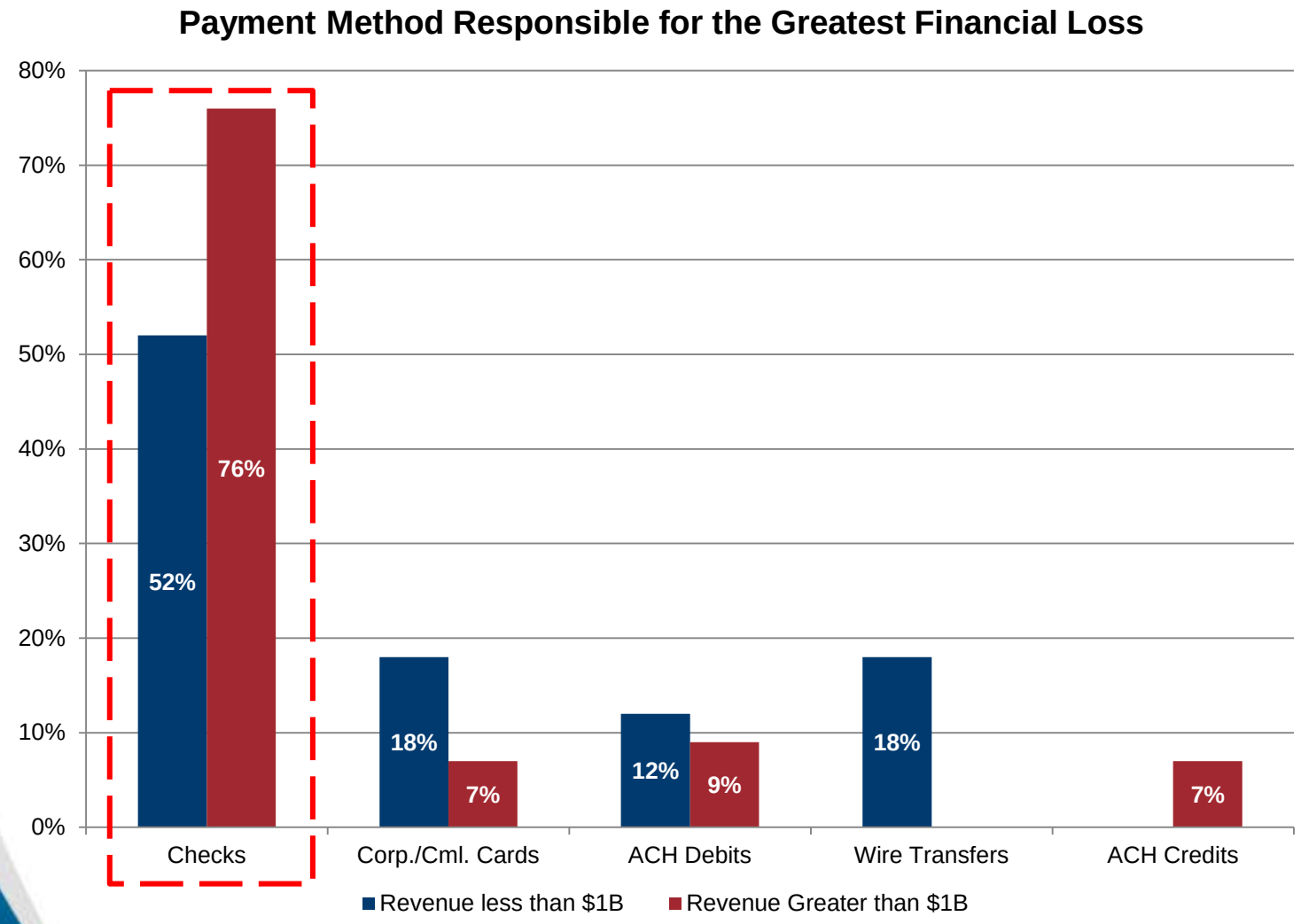
Payments Fraud Rages On

According to the 2013 AFP Payments Fraud and Control Survey, the level of fraudulent activity remains high.

- Of those surveyed, **61 percent** of organizations said they'd experienced actual or attempted payments fraud.
- The majority of those – **87 percent** – reported that checks in particular were targeted.
- Of those affected, 29 percent reported that Commercial Cards were targeted.
- Typical losses due to payments fraud was **$20,300**.

•Source: 2013 AFP Payments Fraud and Control Survey

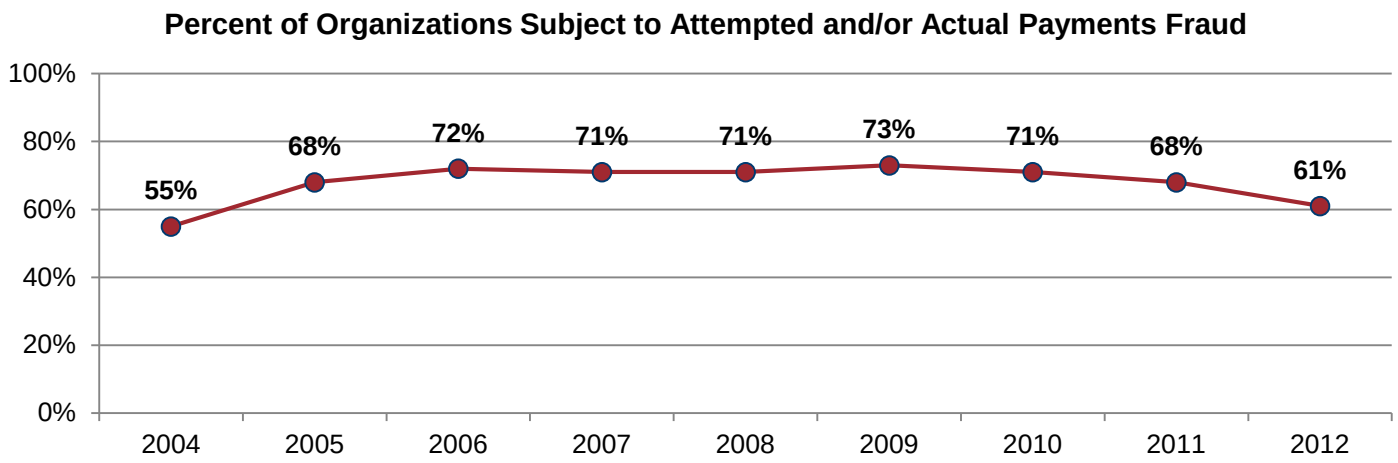
Checks are also the payment method responsible for the greatest financial loss



•Source: 2013 AFP Payments Fraud and Control Survey

Fraud Impacts the Majority of Organizations

- Although the percent of organizations subject to fraud has decreased slightly over the past few years, the **majority** of companies surveyed are still targeted
  - Fraud is from **external *and* internal** sources
- The larger the number of payment accounts an organization has, the more likely they have been exposed to payments fraud



•Source: 2013 AFP Payments Fraud and Control Survey

Who's Liable for Fraud Losses?

It's crucial to understand that businesses can be held liable for payment fraud. Currently banks and their business clients share responsibility for taking appropriate steps to mitigate fraud risk. If a company fails to take these steps, it may bear liability for fraud losses

In cases of check fraud losses, the Uniform Commercial Code (UCC) is the legal basis for determining liability. Revisions to the UCC in 1990 increased corporate responsibility in check fraud loss situations and softened the burden for banks. Today the UCC requires corporate account holders to follow "reasonable commercial standards" to guard against check fraud. It suggests that banks and corporate account holders should divide responsibility for a loss based on the extent to which each party contributed to the loss by failing to meet reasonable commercial standards

Capital One

Fraud Risks

Primary Reasons Companies Experience Losses

- Failure to enforce internal controls
- Failure to reconcile or return checks on a **timely** basis
- Internal fraud by employees
- Loss, theft or counterfeit payroll checks
- Mismanagement of online users
  - Suspend or delete as appropriate
- Changes of vendor addresses to employee's address
  - Match your AP vendor address file to your employee file
- Failure to use Fraud Prevention Services and Products

Capital One

Popular Check Fraud Methods

- **Forgery** – Can take the form of an employee issuing a check without proper authorization or criminals stealing a check, endorsing it and presenting it for payment, typically in conjunction with false identification
- **Counterfeiting** – Wholly fabricating a check using desktop publishing software and printing on check stock
- **Alteration** – Using chemicals and solvents such as acetone, brake fluid and bleach to remove/alter details and signature(s) on the check
- **Paperhanging** – Writing checks on closed accounts
- **Check Kiting** – Opening accounts at two or more FI's and using the float time of available funds fraudulently

Capital One

•Source: http://www.ckfraud.org/ckfraud.html

Types of ACH Fraud

- One form of ACH fraud can occur when someone steals your check and rather than forging the physical check, uses the check's routing and bank account numbers to order goods by phone or online

- Another form of ACH fraud can occur when a dishonest employee uses the MICR-line information on a paycheck to initiate a fraudulent ACH debit

- "Money mules" scams exist when cyber criminals hack into corporate payroll files and direct them to co-conspirators. The fraudsters replace the payroll file with one that has the same aggregate payroll dollar amount and the same number of employees, but a subset of the employees is replaced with the names and routing/account numbers of the criminals' money mules

The biggest issue in combatting these types of low-tech ACH fraud is that NACHA, the electronic payments association, stipulates that a company has only 24 hours to contact its bank to dispute a fraudulent ACH debit. Failure to initiate a dispute within the 24-hour window shifts all liability for fraud losses to the corporate account holder.

Capital One

Cyber Fraud Scams

- In a **“phishing”** attack, someone receives an email from what appears to be a trusted business partner. The email may ask the reader to open an attachment or click a link. The website the reader lands on may appear to be legitimate, but in actuality, it’s a counterfeit site. Once on a counterfeit site, a treasury professional may be asked to divulge bank account numbers and online banking credentials, such as usernames and passwords

- In a **“reverse phishing”** attack, a corporate staff member receives an email that appears to be from a known vendor. Rather than asking for online banking credentials, the message’s sender asks the recipient to take an action, such as redirecting an electronic trade payment to a different bank account. The victimized company may not even realize it has been scammed until weeks later, when the actual vendor calls to ask why its invoice is unpaid

- In a credential-stealing “**malware”** incident, a finance manager receives an email falsely purporting to be from a credible source, such as the BBB. The email asks the recipient to view a document, and when he opens the message’s attachment or clicks the provided link, malware installs on his computer. The next time the victim visits an online banking site, the malware alerts the criminal, who uses keystroke logging technology to capture the victim’s login and security credentials

Most banks’ online services agreements outline liability – but in general, a company is liable for payment fraud losses that occur because the company failed to protect its systems.

Capital One

Commercial Card Opportunities for Fraud

- Of the 29 percent of the respondents to the AFP's 2013 survey who were affected by Commercial Card fraud, 48% of those affected reported that the fraud resulted from the *improper use of their own commercial cards*

- 26 percent of AFP survey respondents said they were subject to *fraud perpetrated by their own employees*, such as use of a Commercial Card to pay for an unauthorized purchase

- **"Vishing"** occurs when a cardholder receives a call from someone who has their purchasing card number. Pretending to be reporting a fraudulent transaction, the caller asks for the cardholder's CVV2 code over the phone. With the card number and code, the criminal can then successfully make unauthorized purchases

Capital One

Products and Services to Help Mitigate Fraud Risk

Dual Control Authorization

- Payments fraud from **internal sources** is a real, constant threat
  - Dual Control Authorization offers an excellent prevention measure, usually at no charge
- Establishes "**maker-checker**" functionality to reduce this internal risk exposure
- Available for **ACH** and **Wire Transfer** payments, as well as **User Administration**
- One employee is responsible for **initiating** the payment or action and a different employee is responsible for verifying the authenticity and **approving** the payment or action
- The authorized administrator with approval rights can **reject** the payment or action and produce a report as a paper trail
- **Increases the level of difficulty** for fraudsters as one set of log on credentials is no longer enough

Capital One

ACH Debit Protection/ACH Positive Pay

- ACH debits are second only to checks when it comes to payment methods targeted by fraudsters
- **64%** of all respondents of the 2013 AFP survey were subject to at least one attempt of ACH fraud in 2012
- ACH Debit Protection is used to **reduce risk exposure** from ACH debits from your bank accounts
- With ACH Debit Protection, you can choose to block **All** ACH debits or those that do not match an **authorized list;** set up one-time authorizations; and setting **dollar thresholds** for **selected** ACH debit filters
- A further layer of protection is available through ACH Positive Pay which will allow companies to decision their incoming ACH transactions daily

Capital One

•Source: 2013 AFP Payments Fraud and Control Survey

Positive Pay/Reverse Positive Pay

- You send your check issue information electronically
- As your checks clear your account, the bank makes sure the **serial number** and **dollar amount** match the information you sent to us **exactly**
- For an even **greater level of protection**, the system can also match against payee name
- A **daily report** is provided to notify you of any checks presented for payment that don't match the information submitted
- You review an online image of the check in question to determine whether or not it is fraudulent and advise the bank to either **pay** or **return**
- Reverse Positive Pay is an alternative to Positive Pay that allows companies to receive items that are expected to clear their bank each morning and decision those items accordingly

Capital One

Account Reconciliation

- **76%** of organizations perform **daily** reconciliations to defend against attacks on security credentials
- Maximize efficiency with the ability to **automate reconciliation** and import paid check data directly into your accounting systems
- Eliminate administrative tasks associated with manual processes
- Provides clients with easy, efficient methods to assist with balancing their organization's checking account(s)
- You can send and retrieve account reconciliation files **online**, as well as via **secure file transfer** or **mainframe transmission**
- Receive notifications by e-mail when reconciliation files are available for downloading and importing into your company's accounting systems

Capital One

•Source: 2013 AFP Payments Fraud and Control Survey

Commercial Card Program Controls

- Have employees sign a Commercial Card agreement and keep on file detailing appropriate and inappropriate card use
- Individual card limit and purchase restrictions
- Utilizing “ghost” cards
- Use of card program’s online reporting tools to monitor employee spending and look for fraud

•Source: 2013 AFP Payments Fraud and Control Survey

Best Practices

Access to Accounts and Financial Information

- Restrict access to bank accounts, financial details and other confidential materials, including credit cards and petty cash, to a few high-level and trustworthy employees
- Avoid giving one person too much financial responsibility and access by:
  - Separating financial duties out among a number of employees
  - Having financial staff take turns with various tasks
- Business owners should review bank account statements regularly
- Flag selected accounts as Debit/Credit Only or “Post No Checks” with Account Restrictions

Capital One

Initiating Transactions

- Institute rules about how transactions can be made, including who has authorization to initiate and approve specific transaction types
- For transactions that involve the movement of funds out of accounts, such as ACH payments or wire transfers, implement a “maker-checker” process whereby one employee initiates a transaction and another approves it
- Review all transfers, payroll and outgoing payments on a regular basis, or use an automated monitoring program
- Make use of Alerts: Alerts through email or SMS can be set to flag your attention to large and unusual transactions and activities

Keeping Up with Technology

- In networked environments, follow the appropriate security protocols to protect the information on individual computers
- Regularly update firewalls, spyware and anti-virus software on servers and individual computers
- Install each new patch and version update to computer operating systems
- Implement multiple layers of security
- Implement solutions that form a barrier to malicious code, that spot and remove malware when it breaches those defenses, and that prevent critical data from being pried from company computers and altered
- When accessing accounts and information via online portals – the responsible employees should have their own unique login credentials. Admin user ID should only be used by authorized Administrator at the company

Capital One

Computer Use

- Generally, company-owned computers should be used for business purposes only
- Establish guidelines for keeping computers secure and limiting access to those that are used primarily for financial data and functions
- In addition, employees **should never**:
  - Download or install software directly from the Web and/or from unknown third parties
  - Open email or email attachments from unknown individuals, businesses or email addresses
  - Open personal email attachments, **even from known sources**
  - Open or respond to suspicious e-mails or click on **any hyperlinks** embedded in a suspicious e-mail

Capital One

Computer Use (continued)

- Use strong passwords including letters, numbers and special characters
  - Change these passwords frequently
  - Do not write your passwords down
- Protect confidential information -- Passwords/PINs
- Trust your eyes: Most online systems provide visual clues that something may be amiss, e.g. displaying the last time you logged on, a distinct look and/or process
- Logout: When you have completed your use of the site do not simply close the browser, make sure you actually use the log-out feature
- Train and review online users

Head Fraud Off from the Start

- You can safeguard your business against the risk of internal fraud by hiring the right people, as well as providing a positive work environment that allows employees to thrive.
- Conduct thorough background checks on each employee, including credit and criminal records, regardless of their role in the company
- Contact references and verify resume details such as education and former employment history
- Publish a code of ethics that clearly states what is considered fraud and what the penalty is for each fraudulent act
- Check accounting records closely for several months

Capital One

Detect Fraud

- Reconcile regularly; Review accounts daily, and reconcile accounts weekly or at least monthly, so that anomalies are spotted
- Have an outside accounting firm conduct regular audits of business finances to uncover potential vulnerability
- Conduct your own unannounced audits internally to check day-to-day processes
- Monitor business bank accounts constantly for unusual activity
- Give employees, customers and business partners the ability to report suspected fraud anonymously

Capital One

Internal Controls

- Structure your accounts: Separate your operating accounts, rather than sharing accounts and access-and only allow access based on defined function
- Review daily activity online
- Implement physical controls over pre-printed check stock/facsimile signatures
- Close accounts which have had fraudulent activity
- Keep authorizations up –to-date
- Know your vendors
- Protect your access credentials

Capital One

Internal Controls (continued)

- Limit the number and dollar amount of transactions
- Limit the number of times payment templates can be used
- Take advantage of check security features, such as watermarks and micro-chemical sensitivity
- Create a protocol for reporting suspected fraud
- Use Multi-Factor Authentication (MFA) devices such as hard or soft tokens
- Report lost or stolen tokens/ID cards immediately
- If you suspect Fraud, contact your Relationship Manager or Treasury Management Advisor immediately

Conclusion

In Conclusion…

- Fraud prevention is only successful if both banks and their business clients do their part
- Business clients need to continue to employ best practices in fraud prevention, including employee education, and use of bank fraud-prevention products where appropriate
- Organizations need to be proactive, rather than reactive when focusing on fraud
- As criminals and fraudsters continue to evolve, so should companies and their risk mitigation strategy
- “Inspect what you expect”

Capital One

Fighting Fraud
Risks, Solutions and Best Practices

Tammy Ledet, Treasury Management Sales Advisor
Government Banking – Louisiana/Texas

Debbie K. Nolan, CTP, VP
Louisiana Sales Manager – Treasury Management

Capital One