AFP®
Annual Conference

Association for Financial Professionals®

November 7-10, 2010 | San Antonio

ORIGINAL
ESSENTIAL
UNBIASED
INFORMATION

Mitigating the Risk of Payment Fraud

Stephen W. Markwell
Disbursements Product Executive
J.P. Morgan

Pamela R. Malmos
Director, Treasury Operations
ConAgra Foods, Inc.

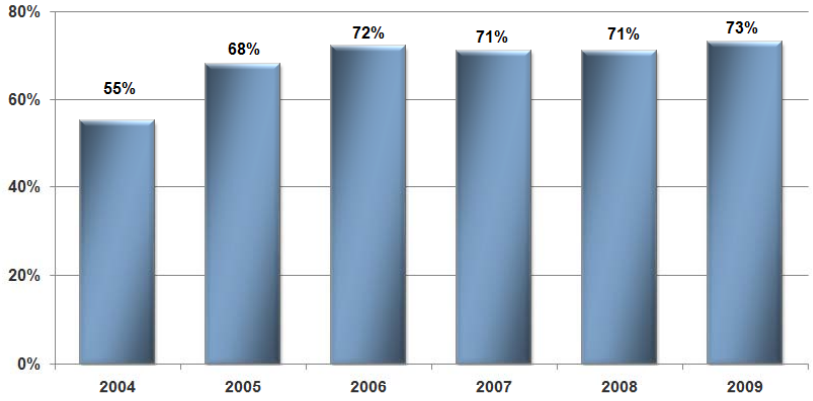
Laura Howley, CTP
Senior Manager, Global Treasury Operations
The Boeing Company

Who's at Risk and What's at Stake?

In 2009:

- Almost three-quarters of organizations were victims of payments fraud
- 81% of organizations with annual revenues over $1 billion were victims of payments fraud
- 63% of organizations with annual revenues under $1 billion were victims of payments fraud
- 30% of organizations report that incidents of fraud increased
- The median loss of organizations that sustained any financial losses resulting from payments fraud was $17,100.

Percent of Organizations Subject to Attempted or Actual Payments Fraud



Source: 2010 AFP Payments Fraud and Control Survey

No Payment Type Is Immune

- Nine out of 10 organizations that experienced attempted or actual payments fraud in 2009 were victims of check fraud
- Though electronic fraud is a tougher challenge for criminals, ACH Debit fraud ranks second as a target
- Consumer credit/debit card fraud is up from 18% in 2008 to 20% in 2009; commercial card fraud is up from 14% to 17% in the same period

Prevalence of Payments Fraud in 2009
(Percentage of Respondents)

	All Respondents	Revenues > $1 billion	Revenues < $1 billion
Checks	90%	93%	89%
ACH debits	25	23	25
Consumer credit/debit cards	20	18	22
Corporate/commercial purchasing cards	17	18	13
ACH credits	7	5	4
Wire transfers	3	3	3

Source: 2010 AFP Payments Fraud and Control Survey

Internal Best Practices

- Segregate Duties
  - Checks – Originate payment, Submit Issuance, Decision Exceptions
  - Wires - Creating, Approving, Releasing Wires
- Dual Approval
  - Require dual approval at critical checkpoints such as approving wires or approving Positive Pay exception decisions
- Segregate Accounts
  - Account Type: Deposits or Disbursements
  - Payment Method: Check, ACH, Wire
  - Payment Type: Payroll, Claims
  - Payment Amount/Volume: High or low
- Monitor and reconcile accounts daily
- Centralized Fraud Protection Governance
- HR Policy – Forced vacations and job rotations

Segregating accounts for different payment vehicles is a best practice highlighted by 90% of respondents.

Separation of accounts allows for timely and focused review of payment activity.

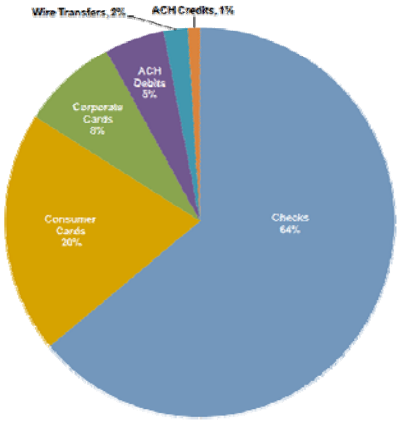
2010 AFP Payments Fraud and Control Survey, sponsored by J.P. Morgan

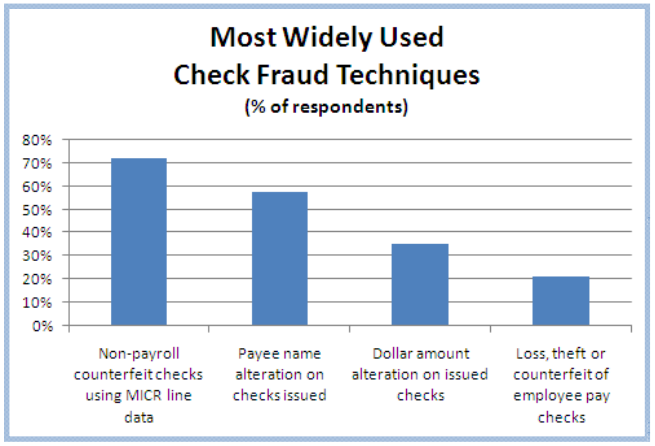
Source: 2010 AFP Payments Fraud and Control Survey

Check Fraud: #1 and Growing

- Follow the money
  - Checks as a percent of total payments is decreasing at a rate of approximately 7%
  - However, the value of checks is increasing
- A Growing Trend?
  - 64% of organizations suffering financial losses report that checks resulted in the greatest loss.
  - Fully 89% of the victims of check fraud attempts report that check fraud attacks have increased
- Why Checks?
  - Easy-to-commit, quick-hit crime
  - Requires no special skills
  - Technology-assisted crime (scanners, printers, desktop publishing software)

Payment Method Responsible for the Greatest Financial Loss Resulting from Fraud in 2009





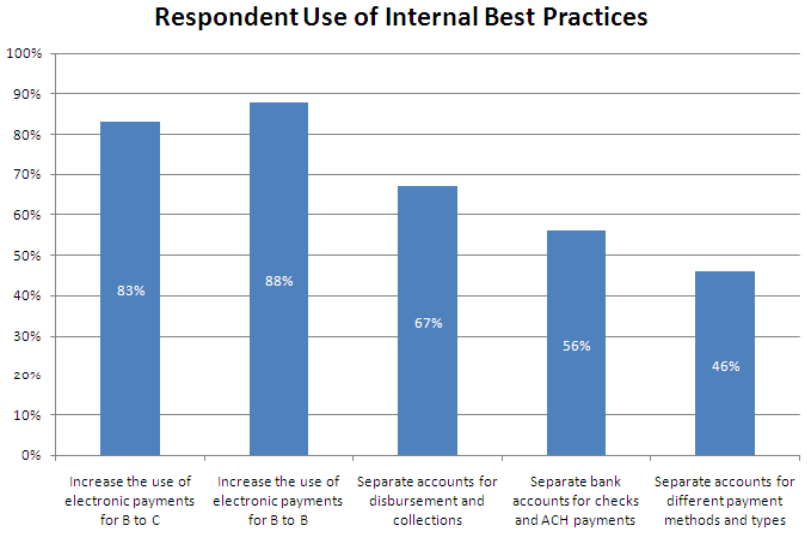
Source: 2010 AFP Payments Fraud and Control Survey

Check Fraud: Fraud Protection Solutions & Internal Best Practices

- Use of Check Fraud Protection Solutions

Services/Methods Used	All Respondents	Revenues >$1 billion	Revenues <$1 billion
Positive Pay & Reverse Positive Pay	83%	85%	81%
Payee Name Positive Pay	52	60	45
Post No Checks	37	46	26

- Use of best practices to mitigate check fraud (Right)
- Other best practices include:
  - Outsourcing check print
  - Electronic forms of financial documents
  - Document destruction process
  - Manage check stock orders & storage
  - Segregation of duties and dual approval

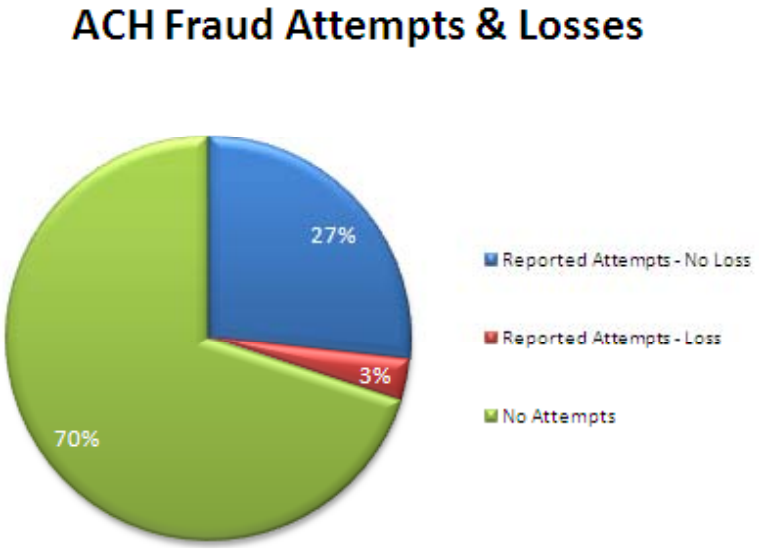


Source: 2010 AFP Payments Fraud and Control Survey

ACH Fraud: As Use Broadens, ACH Fraud Schemes Grow

Popular ACH Fraud Schemes

- **Account Hijacking** Fraudsters use compromised customer credentials to hijack the origination system and use it in the legitimate account holder's name.
- **Identity Fraud** Criminals create false identities, social engineer their way into obtaining ACH origination capabilities and then initiate fraudulent debits.
- **ACH Kiting** A version of check kiting with a cyber twist, ACH kiting involves a pair of accounts used for fraudulent purposes where an ACH debit is originated from one account and drawn on the other; the available balance is taken out before settlement.
- **Reverse Phishing** Instead of e-mails attempting to fraudulently obtain corporate banking information, perpetrators send e-mails to corporates that provide fraudulent banking information, redirecting ACH payments to an account they control.
- **Insider Origination Fraud** Insiders at a merchant or bank manipulate an ACH origination file to skim funds from a company.
- **Counterfeiting** ACH debits generated through the electronic conversion of a counterfeit check.



ACH: Fraud Protection Products & Best Practices

- Use of ACH Fraud Protection Products

Services/Methods Used	All Respondents	Revenues >$1 billion	Revenues <$1 billion
ACH debit blocks	77%	83%	69%
ACH debit filters	58	66	49
ACH positive pay	21	18	20
UPIC for ACH credits	5	5	5

- Internal Best Practices
  - Know your customers and vendors
  - Segregate Accounts and Duties
  - Protect Sensitive Information: Mask and Encrypt
  - Monitor and reconcile your accounts daily
  - Ensure tokens are collected and credentials are changed after employees leave

Source: 2010 AFP Payments Fraud and Control Survey

Phishing Casts a Wider Net

- Phishing = email fraud that dupes targets into providing sensitive information or unknowingly downloading malicious software from a phony, look-alike web site

- More than three quarters (76 percent) of consumers said they were aware of “phishing,” double the 38 percent that responded similarly in 2007

- Instead of decreasing effectiveness, increased awareness has simply forced innovation — and increased effectiveness

Sources: RSA Security Inc. (December 2009). 2010 Global Online Consumer Security Survey;
RSA Security Inc. (2010). Special Online Fraud Report: What to Expect in 2010;
CTIA, The Wireless Association. (Accessed April 9, 2010). http://ctia.org/media/industry_info/index.cfm/AID/10323.

Phishing: Attack Methods and Protection from your Bank

- Popular Phishing Schemes
  - "Vishing" - uses the telephone system to solicit sensitive information
  - "Smishing" - SMS (Short Message Service) phishing
  - "Spear Phishing" - targets employees or high-profile individuals within an organization

- Protection from your Bank
  - Encryption
  - Multi-Factor Authentication: Soft or Hard tokens
  - Dual authority or Step Up Authentication for Transactions
  - Comprehensive fraud monitoring and detection systems
  - Customer education programs

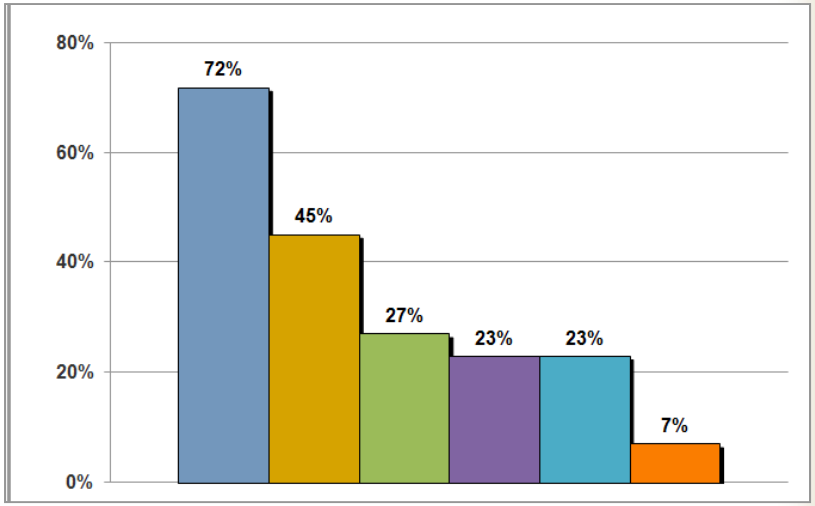
Sources: RSA Security Inc. (2010). Special Online Fraud Report: What to Expect in 2010.

Commercial Cards: Coming of Age

- In 2009, more than three quarters (77 percent) of businesses used some sort of corporate or commercial cards
  - 72 %, purchasing cards
  - 45%, travel and entertainment cards
  - 27%, multiple-use cards
  - 23%, ghost or virtual cards
  - 23%, fleet cards
  - 7%, other types

Types of Cards Used in Making B2B Payments

(Percent of Organizations that Suffered B2B Card Fraud)



Source: 2010 AFP Payments Fraud and Control Survey

Corporate Card: Common Threats & Best Practices

Typically, B2B payments fraud involving such cards is committed by an outside party; however, employees were responsible for over a quarter of 2009 fraud cases (27 percent)

Primary Party Responsible for Fraud from Making B2B Card Payments

External	Unknown external party	73%
	Third-party or outsourcer (e.g., vendor, professional services provider, business trading partner)	16%
Internal	Employee	27%

A J.P. Morgan Treasury Services survey of purchasing card clients identified best practices in managing a solid, secure card program, responders shared these key internal measures as most important in detecting and preventing card fraud:

- Senior management sponsorship
- Segregate duties and accounts
- Promote consistency within Policies and Procedures
- Effectively train managers and employees
- Define controls upfront
- Conduct peer reviews to validate business rules
- Partner with issuer that provides web based payment tools with rich spend analysis

Source: J.P. Morgan Treasury Services. Auditing and Compliance Strategies for a Solid Purchasing Card Program

Case Study: Needs Assessment

Property & Casualty Insurance Provider – Midwest Division

- P&C provider with large check claim payment volume
- Performs all transactions through single operate account
- 12 Fraud Attempts in the last 30 days

Account	Account Type	Monthly Activity	Recommended Solutions
XXXXXX7214	Check: --Claims Payments --Misc Payables ACH: --Payroll through ADP --Vendor Payments --Refunds Deposit --Client Receipts	87,263 Checks 69 ACH Debits 7 ACH Credits 370,440 Deposits	Close Compromised Account Segregate activity into multiple accounts Apply Fraud Protection Solutions

Case Study: Segregate Accounts

Segregate Accounts By:

- Purpose
- Payment Vehicle
- Volume
- Amount

Account	Account Type	Monthly Activity	Recommended Solutions
XXXXXX8765	Check: Client Claims	87,526 Checks	
XXXXXX8768	ACH: AP, Payroll through ADP	4 ACH Debits	
XXXXXX8770	Deposit: AR, Client Receipts	370,440 Deposits	
XXXXXX8772	ACH: Vendor Payments & Refunds	65 ACH Debits 7 ACH Credits	
XXXXXX8774	Check: Misc Payables	263 Checks	

*Fictitious client created for purposes of this case study

Case Study: Fraud Protection Solutions

- Protect accounts with Fraud Protection Solutions that match your payment behavior

Account	Account Type	Monthly Activity	Recommended Solutions
XXXXXX8765	Check: Client Claims	87,526 Checks	Positive Pay with Payee Name verification ACH Debit Block-All
XXXXXX8768	ACH: AP, Payroll through ADP	4 ACH Debits	ACH Debit Block- Exclude all but ADP Post No Checks
XXXXXX8770	Deposit: AR, Client Receipts	370,440 Deposits	ACH Debit Block-All Post No Checks
XXXXXX8772	ACH: Vendor Payments & Refunds	65 ACH Debits 7 ACH Credits	ACH Transaction Review Post No Checks
XXXXXX8774	Check: Misc Payables	263 Checks	Positive Pay with Payee Name verification No Check Cashing. ACH Debit Block-All

*Fictitious client created for purposes of this case study

Payments Fraud Panel Discussion

- Today's Panel will discuss their Payments Fraud Experience
  - Making payment fraud protection a priority
  - Institutionalizing fraud protection measures across businesses
  - Monitoring and mitigating the latest in fraud trends
  - Calibrating internal best practices
  - Leveraging appropriate fraud protection solutions

Stephen W. Markwell
Disbursements Product Executive
J.P. Morgan

Pamela R. Malmos
Director, Treasury Operations
ConAgra Foods, Inc.

Laura Howley, CTP
Senior Manager, Global Treasury Operations
The Boeing Company