TRENDS IN INTERNET FRAUD AND SECURITY BEST PRACTICES

October 11, 2013

J.P.Morgan

Discussion Topics

Define common internet fraud and cybercrime

Review the types and levels of internet fraud:

- In the United States
- Around the World

Understand the payment fraud landscape

Discuss recommended best practices to mitigate payment and internet fraud

Emerging considerations/trends

Language of Internet Fraud and Cybercrime

- **Phishing** – Bogus e-mails that trick users into supplying confidential information
- **Smishing** – Phishing by SMS Messaging. A text message is sent to an individual's mobile phone requesting personal information under false pretenses
- **Vishing** – "War dialers" dial thousands of numbers at a time. When a call is answered, an automated recording claims that a credit card or bank account has been compromised. Dupes account owners into supplying personal information
- **Spear Phishing** – Targeting high profile individuals or employees within an enterprise to obtain confidential information
- Many **attacks** combine vishing and phishing – use an e-mail to lure an individual to call a number manned by fraudsters and unwittingly supply confidential personal information

Language of Internet Fraud and Cybercrime

- **Trojan Attacks** use malicious software that appears to perform a desirable function for the user but instead facilitates unauthorized access of user's computer system

- **MITB (man-in-the-browser)** attack intercepts data using a secure communication between a user and an online application. The Trojan embeds in the browser application and can intercept and manipulate any information that the user submits. Trojans are also being used to attack instant messaging (IM) applications

- **Viruses** spread via ad-related spam e-mail

- **Key Logger Robot or "bot"** programs that record keyboard keystrokes to collect user access IDs and account information

Cybercriminal Supply Chain

- **Organization Leaders** assemble the team and choose targets
- **Coders** write the exploits and malware
- **Distributors** trade and sell stolen data
- **Tech experts** maintain the criminal enterprise's IT infrastructure
- **Hackers** search for an exploit vulnerabilities in applications, systems, and networks
- **Fraudsters** woo potential victims with social engineering schemes like phishing and spam
- **Hosted system providers** offer illicit content servers
- **Cashiers** control drop accounts and provide names and accounts to other criminals
- **Money mules** complete wire transfers between bank accounts
- **Tellers** transfer and launder illicit earnings through digital currency services

Cybercrime Supply Chain

Information Collection

- Phishing
- Spyware
- Crimeware
- Social networking sites
- Social engineering (e.g., rogue phone calls)

Information Exchanges

- Sells information to an information warehouse (wholesale distributor of stolen information). Information could include passwords, credit card numbers and personal information as well as other data elements

Cybercrime Supply Chain

Attack

- Information is purchased from the information warehouse for the purpose of executing an attack
- Compromised information allows stealthy execution of fraud as well as ability to steal more information
- “Botnets” are deployed to launch spam and Denial of Service attacks and distribute crimeware (botnets are available for rent for as little as $8.94 per hour – the same price as a DVD)

In the decade since the term “cybercrime” was first coined, it has quickly emerged as one of the top four economic crimes, just behind asset misappropriation, accounting fraud and bribery and corruption[1]

1; PricewaterhouseCoopers LLP, Global Economic Crime Survey, November 2011

Cybercrime Trends

- Cybercrime knows no borders
  - Aggregately, nearly 38% originated from Asia Pacific/Oceania region, just over 36 % in Europe, 23% in North and South America, and just under 3% from Africa
- Cybercrime is so effective because it is built on emotional triggers:
  - According to RSA[2], the top ploys are: Rewards, Greed, False Accusations, Curiosity, Righting a Wrong, Trust
- "Bring Your Own Devices" (BYOD) can mean bringing along a hacker
  - Expert estimates content that fully 10% of mobile applications leak logins and passwords, 25% expose PII and 40% communicate with third parties[3]
- No business or organizational segment is exempt
  - In 2011, more than half of the targeted attacks measured by Symantec were directed at small and midsized businesses (fewer than 2,500 employees) and 17.8% were directed at companies with fewer than 250 employees[4]
- The frequency and cost of cyber attacks are on the rise
  - No matter the size of the victim organization, the costs of cybercrime cannot be firmly measured in dollars and sense alone. It is nearly impossible to put a price tag on the loss of reputation and of the public trust in general, not to mention loss of user loyalty

2. RSA Blog, Speaking of Security, "Phishing in Season: A Look at Online Fraud in 2012"

3. Zscaler, ThreatLabZ report, http://www.zscaler.com/20121008-press-release-zscaler-threatlabz-free-mobile-app-profiler.html. Accessed October 5, 2012

4. Symantec Corporation. Internet Security Threat Report, 2011 Trends

Internet Crime Statistics – United States & Worldwide

Complainant Statistics by US State

Rank	State	Percent
1	California	13.42
2	Florida	7.98
3	Texas	7.22
4	New York	5.70
5	New Jersey	3.81
6	Pennsylvania	3.70
7	Illinois	3.50
8	Virginia	3.30
9	Ohio	3.05
10	Washington	2.72

Complainant Statistics by Country

Rank	State	Percent
1	United States	91.19
2	Canada	1.43
3	United Kingdom	0.88
4	Australia	0.68
5	India	0.59

Source: Internet Crime Complaint Center – 2012 Internet Crime Report -- National White Collar Crime Center (NW3C)

No One is Exempt

No individual industry category or individual organization size is immune to threat

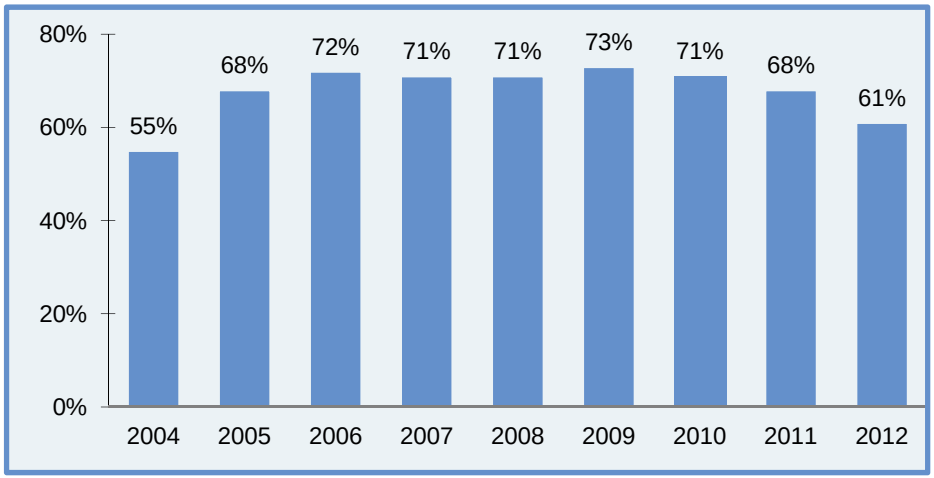
All sectors are vulnerable to malware attacks in pursuit of intellectual and corporate assets and government intelligence

Small and mid-sized commercial, educational and **state and local government entities** in the US are estimated to lose on **tens of thousands of dollars per day to cybercrime** . . . Due in part because they lack appropriate IT services and resources

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

- 61% of organizations experienced attempted or actual payments fraud.
- 87% of affected organizations report that checks were targeted
- 29% of those affected report that corporate/commercial purchasing cards were targeted
- 27% of organizations report that incidents of fraud increased
- 16% of organizations report that the incidents of fraud have decreased
- The typical loss due to payment fraud was $20,300.

Percent of Organizations Subject to Attempted and/or Actual Payments Fraud



Source: 2013 AFP Payments Fraud and Control Survey

No Payment Type is Immune

- ***Checks*** continue to be the most popular target for criminals committing payments fraud, ***87%*** of organizations that experienced attempted or actual payments fraud in 2012 were victims of check fraud (53% of all organizations were check fraud victims)
- Though electronic fraud is a tougher challenge for criminals, ***ACH Debit fraud was cited by 27%*** of financial professionals, up from 24 percent one year ago

Percent of Organizations Subject to Actual or Attempted Payments Fraud in 2012

	All Respondents	Revenues <$1 billion	Revenues > $1 billion
Checks	87%	87%	91%
ACH debits	27%	25%	29%
Corporate/commercial purchasing cards	29%	27%	26%
ACH credits	8%	9%	6%
Wire transfers	11%	%	12%

Source: 2013 AFP Payments Fraud and Control Survey

Sources of Payments Fraud in 2012

- Most payments fraud originates outside the victimized organization. ***80%*** of organizations that experienced attempted or actual payments fraud in 2012 did so as a result of actions taken by an outside individual

- ***18%*** of organizations were subject to payments fraud originating from an organized crime ring while *10%* of organizations were subject to fraud from an internal party.

Percent of Organizations Subject to Actual or Attempted Payments Fraud in 2012

	All Respondents	Revenues <$1 billion	Revenues > $1 billion
Outside Individual	80%	81%	80%
Organized crime ring	18%	18%	19%
Internal Party	10%	4%	15%
Third-party or outsourcer	5%	8%	3%
Account Takeover	5%	4%	4%
Other	5%	5%	5%
Lost or stolen laptop	1%	1%	<1%
Compromised mobile device	<1%	<1%	<1%

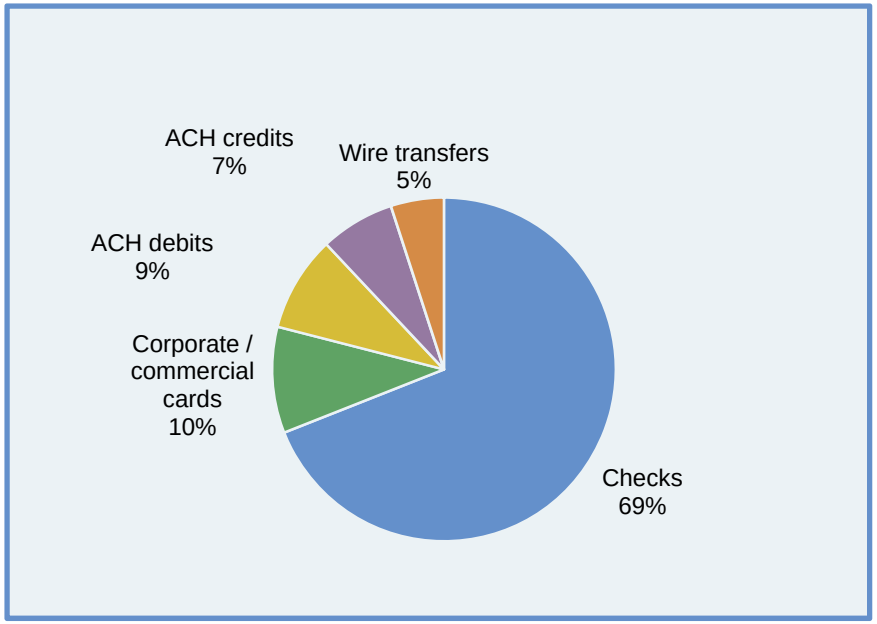
Source: 2013 AFP Payments Fraud and Control Survey

Check Fraud: #1 Payment Type for Fraud

Follow the money

- Checks were the primary method with the greatest financial loss as a result of fraud at 69%
- This rate is up from 60% a year ago
- Fraudulent use of corporate cards accounted for 10% of actual losses while ACH debits, ACH credits, and wire transfers were each responsible for the greatest financial loss as a result of payments fraud at few organizations.
- Smaller organizations with less than $1 billion in annual revenues experienced losses due to fraud from a greater mix of payment methods
- Nearly half of respondents from these organizations report the greatest financial loss as a result of fraud from payment methods other than checks

Payment Method Responsible for the Greatest Financial Loss Resulting from Fraud



Why Checks?

- Easy-to-commit, quick-hit crime, no special skills required
- Technology-assisted crime (scanners, printers, desktop publishing software)

Source: 2013 AFP Payments Fraud and Control Survey

Check Fraud Solutions & Internal Best Practices

Use of Check Fraud Protection Solutions

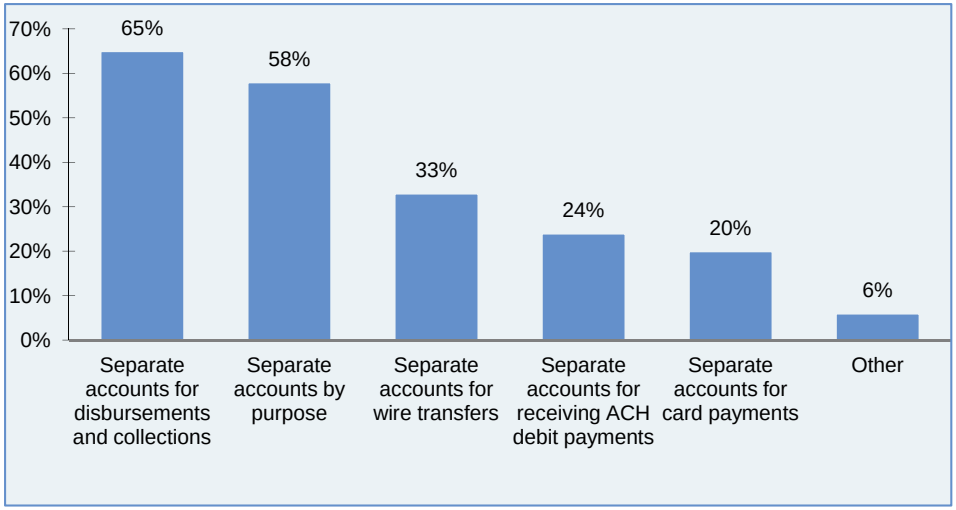
- Positive Pay / Reverse Positive Pay
- Payee Name Positive Pay
- Post No Checks

Best Practices

- Account Segregation (Right)
- Outsourcing check print
- Electronic forms of financial documents
- Document destruction process
- Manage check stock orders & storage
- Segregation of duties and dual approval

"79% of organizations indicate the number of exceptions is relatively small and the items can be easily identified"

Segregating Accounts for Different Payment Method



Source: 2013 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.

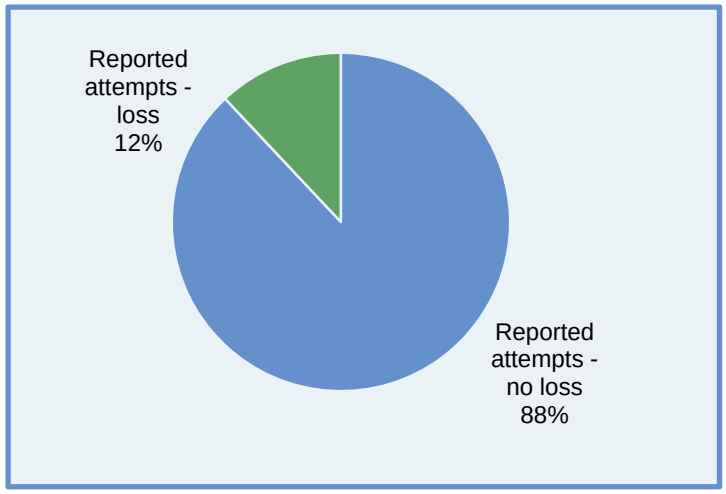
Insider Origination Fraud Insiders at a merchant or bank manipulate an ACH origination file to skim funds from a company.

Counterfeiting ACH debits generated through the electronic conversion of a counterfeit check.

Most likely reasons for sustaining financial loss

- Not reconciling accounts on a timely basis
- Not using ACH debit blocks or ACH debit filters
- ACH return not being timely
- Not using ACH positive pay

ACH Fraud Attempts & Losses



Source: 2013 AFP Payments Fraud and Control Survey

ACH: Fraud Protection Products & Best Practices

Use of ACH Fraud Protection Methods and Solutions

Methods/Solutions Used	All Respondents	Revenues <$1 billion	Revenues >$1 billion
Reconcile accounts daily and return unauthorized ACH debits	77%%	68%	84%
Block all ACH debits except on a single account setup with ACH debit filter/ACH positive pay	41%	50%	38%
Block ACH debits on all accounts	38%	11%	50%
Non-bank fraud control services	12%	4%	16%
"Post no checks" restriction on depository accounts	18%	11%	22%
Daily Reconciliation and other internal processes	7%	7%	8%

Internal Best Practices

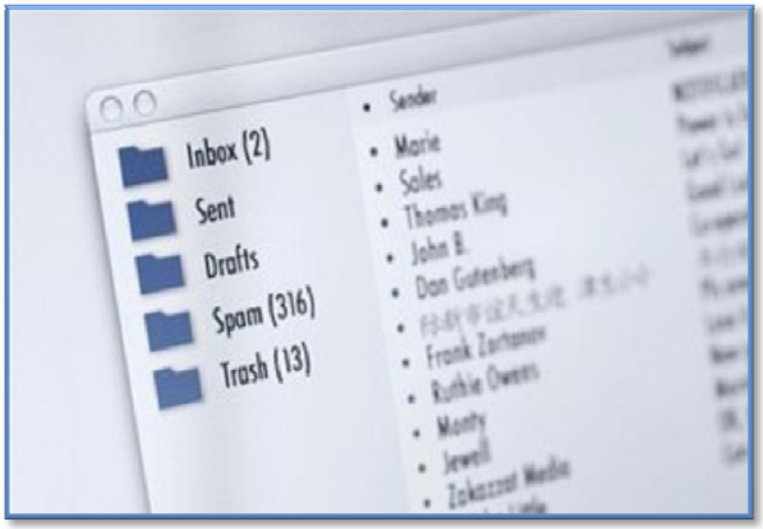
- Know your customers and vendors
- Segregate Accounts and Duties
- ***Protect Sensitive Information: Mask and Encrypt***
- Monitor and reconcile your accounts daily
- Ensure tokens are collected and credentials are changed after employees leave

Source: 2013 AFP Payments Fraud and Control Survey

Phishing Casts a Wider Net

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.

Mitigating the Risk of Payment Fraud

- The best way to protect your business against fraud is to have a plan in place before the problem occurs

- With a combination of strict internal controls and account protection services, you can significantly reduce your exposure to payments fraud

Eliminating checks continues to be the single best way for organizations to combat fraud. Companies have made significant strides in reducing the use of checks, particularly for larger trading partners, but they must continue to push for 100 percent electronic payments and process automation to reduce fraud, transaction expenses, and time requirements to manage exceptions.

— 2012 AFP PAYMENTS FRAUD AND CONTROL SURVEY

Source: 2012 AFP Payments Fraud and Control Survey

Ways to Reduce and/or Mitigate Payment Risk

Segregate Duties

- Checks – Originate payment, approve, release, decision exceptions, reconciliation
- 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

Best Practices in Cybercrime Protection

Cybercrime beings and ends with individual computers and their users

Government entities need to take a risk-based and policy-driven approach to security

Develop and enforce policies and practices to protect your networks and systems from cyberattacks

So helpful tactics…

- Foster enterprise wide awareness of cybercrime threats
- Set strict controls for data access
- Establish a lifecycle management program for organization-controlled devices
- Secure your network with a VPN requirement
- Enforce clear social media guidelines for employees
- Keep basic hardware and software protections current
- Manage and monitor cloud computing
- Log inbound and outbound network traffic
- Use encryption to protect sensitive data
- Enforce an effective password policy
- Empower customers

Best Practices #1 – Issue Electronic Payments

- Use an online banking channel for treasury management needs
- Convert paper payments to electronic delivery whenever possible
  - Wire and ACH fraud are less likely to occur
  - Sensitive account information located on paper statements and cancelled checks is vulnerable to theft
- Establish policies regarding the publishing of executive signatures on any electronic document
- Ensure that secure ID tokens are collected and that passwords are changed after an employee leaves the company

Best Practices #2 – Secure Paper Check Processes

If you continue to issue paper check payments in-house, be sure to implement the following:

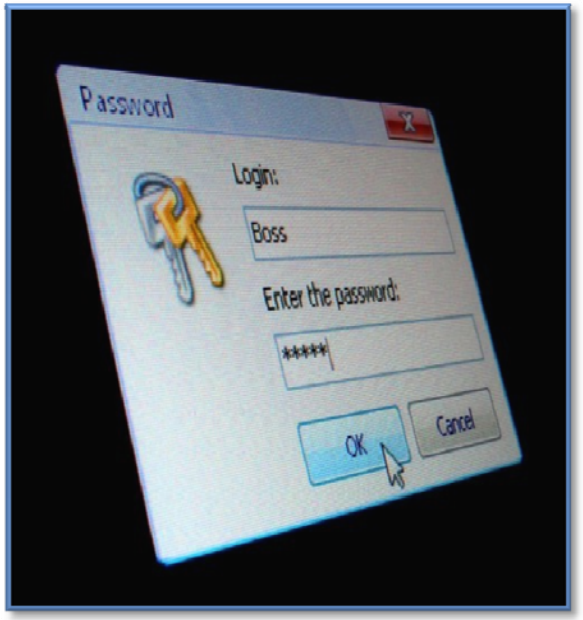
- Use high-quality, blank check stock with built-in security features which may include:
  - *fluorescent fibers, watermark, chemical resistance, bleach-reactive brown stain, photocopy void pantograph, endorsement backer, thermo-chromic ink, micro printing, warning band border, laid lines, non-negotiable mark*
- Securely store check stock, deposit slips, bank statements and cancelled checks
- Implement secure financial document destruction processes
- Establish employee order/re-order policy for stock
- Purchase stock from known vendors
- Segregate access to check stock duties from those associated with check initiation and production

Best Practices #3 – Implement Strong Internal Controls

- Segregate duties
  - Making payments vs. reconciling accounts
  - Require dual approval at critical checkpoints such as creating, approving, releasing wires and approving Positive Pay exception decisions
- Segregate accounts
  - Segregating accounts for different payment vehicles or purposes is a best practice – allows for timely and focused review of payment activity
- Monitor and reconcile accounts daily
  - Use online statements, reporting, and reconcilement services to speed the reconcilement process
- HR policy
  - Enforce vacations and job rotations for sensitive functions

Best Practices #4 – Don’t Forget Online Security Protections

- Mask account numbers and Tax ID numbers in correspondence
- Use encrypted e-mail for confidential, non-public information
- Maintain an awareness of the latest fraud trends such as phishing and malware
  - Email fraud that dupes targets into providing sensitive information or unknowingly downloading malicious software from a phony, look-alike website
- Bank-provided protection:
  - Multi-Factor Authentication – soft or hard tokens
  - Dual Authority or Step Up Authentication for transactions
  - Comprehensive fraud monitoring and detection systems



Questions and Answers

Thank You for Your Time

James F. Lock III, CTP, CSCIP/P

James.f.lock@jpmorgan.com

1-757-440-2725

Primary Sources:

Association of Financial Professionals. 2013. *2013 AFP Payments Fraud and Control Survey*
Internet Crime Complain Center. Ic3.gov. *2012 Internet Crime Report* Accessed on June 13, 2013
Chase Commercial Banking. 2013. *Cybercrime: This is War*