TOOLS AND TECHNIQUES-FRAUD PREVENTION AND DETECTION

February 2014

J.P.Morgan

This presentation was prepared exclusively for the benefit and internal use of the J.P. Morgan client or potential client to whom it is directly delivered and/or addressed (including subsidiaries and affiliates, the "Company") in order to assist the Company in evaluating, on a preliminary basis, the feasibility of a possible transaction or transactions or other business relationship and does not carry any right of publication or disclosure, in whole or in part, to any other party. This presentation is for discussion purposes only and is incomplete without reference to, and should be viewed solely in conjunction with, the oral briefing provided by J.P. Morgan. Neither this presentation nor any of its contents may be disclosed or used for any other purpose without the prior written consent of J.P. Morgan.

To the extent that the information in this presentation is based upon any management forecasts or other information supplied to us by or on behalf of the Company, it reflects such information as well as prevailing conditions and our views as of this date, all of which are accordingly subject to change. J.P. Morgan's opinions and estimates constitute J.P. Morgan's judgment and should be regarded as indicative, preliminary and for illustrative purposes only. In preparing this presentation, we have relied upon and assumed, without independent verification, the accuracy and completeness of all information available from public sources or which was provided to us by or on behalf of the Company or which was otherwise reviewed by us. J.P. Morgan makes no representations as to the actual value which may be received in connection with a transaction nor the legal, tax or accounting effects of consummating a transaction. Unless expressly contemplated hereby, the information in this presentation does not take into account the effects of a possible transaction or transactions involving an actual or potential change of control, which may have significant valuation and other effects.

Notwithstanding anything herein to the contrary, the Company and each of its employees, representatives or other agents may disclose to any and all persons, without limitation of any kind, the U.S. federal and state income tax treatment and the U.S. federal and state income tax structure (if applicable) of the transactions contemplated hereby and all materials of any kind (including opinions or other tax analyses) that are provided to the Company insofar as such treatment and/or structure relates to a U.S. federal or state income tax strategy provided to the Company by J.P. Morgan. J.P. Morgan's policies on data privacy can be found at http://www.jpmorgan.com/pages/privacy.

IRS Circular 230 Disclosure: JPMorgan Chase & Co. and its affiliates do not provide tax advice. Accordingly, any discussion of U.S. tax matters included herein (including any attachments) is not intended or written to be used, and cannot be used, in connection with the promotion, marketing or recommendation by anyone not affiliated with JPMorgan Chase & Co. of any of the matters addressed herein or for the purpose of avoiding U.S. tax-related penalties.

Chase, JPMorgan and JPMorgan Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (collectively, "JPMC") and if and as used herein may include as applicable employees or officers of any or all of such entities irrespective of the marketing name used. Products and services may be provided by commercial bank affiliates, securities affiliates or other JPMC affiliates or entities. In particular, securities brokerage services other than those which can be provided by commercial bank affiliates under applicable law will be provided by registered broker/dealer affiliates such as J.P. Morgan Securities LLC, J.P. Morgan Institutional Investments Inc. or Chase Investment Services Corporation or by such other affiliates as may be appropriate to provide such services under applicable law. Such securities are not deposits or other obligations of any such commercial bank, are not guaranteed by any such commercial bank and are not insured by the Federal Deposit Insurance Corporation.

This presentation does not constitute a commitment by any JPMC entity to extend or arrange credit or to provide any other services.

Outline

Check Fraud Methods

- Statistics
- Types of Check Fraud
- ACH Fraud

Prevention Strategies

- What is J.P. Morgan doing to combat fraud?
- Our client's role in preventing fraud
- Fraud schemes targeting our clients and their companies

Poll Question

By a show of hands, has your organization experienced a payments fraud attempt?

Statistics

Fraud continues to increase:

- According to the FBI, fraud costs consumers, banks and businesses $18 to $20 billion per year.
- The AFP Payments Risk Survey for 2013 reported 61% of organizations were targets of attempted or actual payment fraud.
- Seven out of ten organizations that were victims of actual and/or attempted fraud suffered no loss, however among the organizations that did suffer losses the average amount was $20,300.

Why are fraud losses on the rise?

- Organized and professional fraud rings are becoming more prevalent and sophisticated.
  - Fraud rings are now global enterprises with key organizers residing in uncooperative countries.
- Cyber-crime advances make it possible to compromise large quantities of data.
- Desktop publishing makes counterfeiting checks relatively cheap and easy.
  - Some utilities are delivered through non-criminal websites.
- The potential victims of fraudulent checks include millions of consumers.
  - Lottery scams, internet job postings, work-at-home opportunities.
- Regulation CC availability requirements have decreased the window of opportunity for banks to identify and return suspicious checks.

Types of check fraud

- Alteration
- Forged/Missing endorsement
- Counterfeit
- Forged maker
- Deposit fraud
- Kiting

ACH fraud

Automated Clearing House (ACH) debit fraud risk is the risk that a transaction will be initiated or altered in an attempt to misdirect or misappropriate funds. Although ACH fraud risk does occur, the frequency is relatively low when compared to other payment systems fraud.

- Any ACH may debit post to your account. No authorization is required by the client.
- Critical elements of ACH fraud — account and routing numbers that can be obtained from any given check.
- Organizations that were victims of attempted ACH fraud were more likely to suffer a loss because the did not use defenses available from institutions.
- The number of days after which a client may recover a fraudulent ACH transaction is limited as compared to checks:
  - 60 days for Web and telephone-initiated transactions
  - Two days for business-to-business transactions

PREVENTION STRATEGIES

What is J.P. Morgan doing to combat fraud?

Prevention tools

J.P. Morgan proactively develops prevention tools to reduce the risk of loss due to fraudulent activity. We work closely with our clients to provide up-to-date security features in a controlled environment.

- ASI-16 fraud detection software
  - A fraud detection filter that examines daily check transactions and compares them to the individual's check writing history through a predefined set of bank parameters.
- Large-dollar item review
  - Items above a specified dollar threshold are out sorted for additional fraud review.
- Teller system alerts
  - The bank may mark an account with a caution/surveillance restraint as an interim step to protect against additional losses while account closing is pending.

Prevention tools

- Multiple Identification
  - Tellers require non-J.P. Morgan clients to present two forms of identification and a thumbprint when cashing checks.
- Loss avoidance warehouse (LAW)
  - Tracks and reports deposit-account-related losses. The system is designed to help
    - improve understanding of how the losses occur
    - improve decision making for loss reduction initiatives
    - improve audit controls
- Proprietary transaction monitoring systems
  - AMEX – Partner in traveler check verification system
  - FPS - Internal fraud prevention system used for vetting
- Participation in industry wide exchanges

Positive Pay services

- Positive Pay
  - Positive pay provides the ability to make pay or return decisions on checks presented against an account that do not match an issue record (exception item). Fraud risk is reduced through tighter controls and the ability to choose either to authorize payment or return the check prior to the return deadline.
- Payee verification
  - An enhancement to Positive Pay that also matches the payee line of the check presented for payment to the payee name provided on the issue file from the client. Provides fraud protection against payee name alterations.
- Teller protection
  - Checks presented at a J.P. Morgan banking center are matched against a Positive Pay file. If the check appears on the file, it will be honored. If the check is not on the file, the teller will not pay the item and the presenter will be directed to contact the originator of the check.

ACH debit blocking

ACH debit blocking service guards corporate accounts against unauthorized ACH debit transactions. It is an optional service that provides a means of returning unauthorized ACH debits in a timely manner.

- Benefits
  - Security — no unauthorized ACH transactions will be posted.
  - Fraud protection — eliminates outside access to your account.
  - Reduced effort — your staff spends less time reconciling and investigating debit transactions.
- Filtering criteria selected by clients
  - Block all debits
  - Block all debits over a certain dollar threshold
  - Block all debits except from specific originators
  - Allow all debits except from specific originators
- ACH debit blocking automatically rejects unauthorized transactions.

PREVENTION STRATEGIES

Client's role

Implementing Tools & Controls

Implementation of payment fraud protection tools and internal controls is essential for a successful payment fraud protection program – don't wait to become a statistic.

According to the 2013 AFP Payment Fraud and Control Survey:

- Checks remain the payment method most frequently preferred by criminals .
- Organizations that suffered ACH fraud did so because they did not follow best practices or neglected to execute their own business rules expeditiously.
- Heightened awareness of the threats continue to lead respondents to improve internal controls.

Liability for check fraud

The laws governing checks are primarily the Uniform Commercial Code. For most states, the UCC provides for several defenses that can be raised to a claim of loss due to fraud on the entity's account.

- **UCC 3-103 “Ordinary Care”**
  - The observance of reasonable commercial standards that prevail in the area in which the person is located and with respect to the business in which the person is engaged.

- **UCC 3-405 “Comparative Negligence”**
  - In situations where there is risk loss due to fraud, a court would compare the entity's negligence against the bank's negligence to determine who should be liable.

Liability for check fraud (cont'd)

UCC 3-406 "Contributory Negligence"

- The entity could be found to have contributed to the loss if, for example, if it fails to safeguard checks from forgery or alteration by a "reasonable commercial standard", and that failure to safeguard contributes to the forgery or alteration

UCC 4-406 "Reasonable Promptness"

- Clients must exercise reasonable promptness in examining statements or items to determine if any payment was not authorized and to notify the bank.

**This presentation is given to for your general information and is not legal advice. Not all state's versions of the UCC contain such provisions. Please consult your own attorney for any legal advice with regard to liability for fraud on the entity's account.*

Liability for check fraud (cont'd)

- Corporate clients may be found to be negligent if they fail to:
  - maintain sufficient controls for check storage, issuance and reconciliation
  - notify the bank in a timely manner when fraud occurs
  - review the bank statement
  - reconcile accounts in a timely manner
  - use standard fraud protection offerings (i.e., positive pay)
- Clients should engage their relationship advisors to reduce fraud:
  - understand the fraud mitigation technology used by the bank
  - understand the fraud protection tools the bank offers

The risk of loss from check fraud is substantial, therefore the bank and its client must work together in preventing check fraud.

What can you do to prevent payment fraud?

- Convert as many payments as possible to electronic delivery such as ACH, EDI, wire and card
- Implement positive pay and payee verification
- Implement secure financial document destruction processes
- Reconcile accounts frequently and regularly
  - Use online statements, reporting and reconcilement services for faster reconcilement
- Physical controls on check stock
  - Secure storage and access to check stock and signature plates
  - Usage
  - Dual Controls
  - Policies on how check stock is ordered, received
- Use image survivable and other high-security check stock features

What can you do to prevent payment fraud? (cont'd)

- Separate accounts
  - Collection and disbursement activity
  - Check and electronic payments
  - Payroll and accounts payable disbursements
  - High-volume accounts and low-volume petty cash/emergency accounts
  - ACH credit accounts and ACH debit accounts
- Implement ACH Debit Block
- Implement "Post No Checks" restriction on electronic payment accounts
- Segregate duties — making payments and reconciling accounts
- Limit number of official signers on checks and update bank records
- Mask account numbers and Tax ID numbers in your correspondence

What can you do to prevent payment fraud? (cont'd)

- Form an internal "anti-fraud" committee
  - Use prior fraud occurrences to level set
  - Match industry "best practices"
  - Establish and maintain general controls:
  - Document and enforce procedures
- Awareness and training
- Screen new employees and temporary help
- Know who you do business with
  - Vendors
  - Clients
  - Maintenance staff

Final Thoughts

J.P. Morgan is focused on reducing fraud and fraud expense to our client's and ourselves:

- We proactively develop tools and processes to reduce the risk of loss due to fraudulent activity. We work closely with our clients to provide state-of-the-art fraud protection services and security features.
- We want our clients to know the we are there to assist throughout the fraud investigation and resolution process.
- Combating check fraud is a collective effort among the bank, the client and law enforcement working together to prevent payment fraud.

CHECK FRAUD: RECOGNIZE AND MANAGE RISK — ARE YOU PROTECTED?

Fraud schemes targeting you & your entity

Phishing

- Phishing is an email fraud that dupes targets into providing sensitive information or unknowingly downloading malicious software from a phony, look-alike web site
- The victim receives an e-mail purporting to be from a legitimate source – PayPal, eBay, or a financial institution
- Victim compromises their bank account or credit card numbers, passwords, or other personal or financial information
- Identify theft or financial loss often result
- Instead of decreasing effectiveness, increased awareness has forced innovation and increased effectiveness.

New Methods of Cyber Fraud

Vishing — uses the telephone system to gain fraudulent access to personal and financial information

- Typical attack uses a “war dialer” to call thousands of phone numbers at a time
- Automated recordings warn target about suspicious activity on card or bank account and urge them to contact the bank immediately
- Unsuspecting individuals comply, only to find later that they have given personal information to fraudsters using a false phone number

Smishing — or SMS (Short Message Service) phishing

- Smishers send a text message to an individual’s mobile phone asking them to call a phony phone number or to visit a look-alike website to confirm personal information
- The opportunities for fraudsters are nearly limitless: more than 300 million Americans pay for wireless connections; nearly one-half billion text messages sent each day in the U.S. alone

New Methods of Cyber Fraud

Spear Phishing — targets employees or high-profile individuals within an organization

- Attempts to obtain sensitive information or download malicious software
- Once malware is installed, anything the user types on the computer can be accessed by the criminals, including corporate credentials or bank account information

Typical phishing e-mail

From: Chase Bank
Subject: **Possible Account Problems**
Priority: **URGENT**

An Important Notice Concerning Your Personal Information

Dear Chase Bank Customer:
We have recently noticed several attempts to log into your Chase Bank account from a foreign IP address. We have reasons to believe that your account my be compromised by a third party.

However if you are the rightful Account holder, click on the link below and login as we try to verify your identity:
https://chaseonline.chase.com/

Typical phishing e-mail

(Continued)

We ask that you allow at least 48-72 hrs for the case to be investigated and we strongly recommend not making any changes to your account in that time.

The information contained in this notice contains some terms we are required to disclose to ensure that we comply with privacy laws. If you have any questions about the information contained in this notice, please call us at (212) 334-0555 or write to: Chase Bank, 231 Grand St, New York, NY 10013.

Typical phishing e-mail

Dear Name of Recipient

A complaint has been filled against you and the entity you are affiliated to by Mr. George Hanson and sent to Federal Trade Commission by fax in witch he's claiming that he has been cheated by you and your entity in paying a greater amount of money than the one appearing on the invoice you gave him for using your services.

The complaint states he contacted your entity on MON,22 OCT 2007, trying to solve this situation without interference from any Governmental Institution , but your entity refused to take action.

On WED,24 OCT 2007, the complaint was sent by fax to Federal Trade Commission and we forwarded it to Internal Revenue and Better Business Bureau.

Typical phishing e-mail

(continued)

Complaint was filled against :

Name : Name of recipient

Entity : - Entity Name

If you feel that this message has been sent to you in error or if you have any questions regarding the next steps of
this process, please download the original comp! laint by clicking the link below :
http://ftc.gov/fraud/complaints/24_oct_2007_george_hanson.doc

Please take knowledge of the complaint's content and complete the form at the bottom of forward it to
fraudcomplaint@ftc.gov.

Bruce Jameson
Complaint Officer

Variations on phishing e-mail

- Including a valid phone number for the bank or credit card entity hoping you will consider them valid e-mails and log into their site without call
- Offering a $25 account credit for the inconvenience caused by having to reactivate or confirm your account
- Offering a free “Fraud Busters” enrollment

Tips to avoid phishing scams

- Be suspicious of any e-mail that:
- Requires you to enter personal information directly into the e-mail or submit that information some other way.
- Threatens to close or suspend your account if you do not take immediate action by providing personal information.
- States that your account has been compromised or that there has been third-party activity on your account and requests you to enter or confirm your account information.
- States that there are unauthorized charges on your account and requests your account information.
- Asks you to confirm, verify, or refresh your account, credit card, or billing information.

Tips to avoid phishing scams

- Don’t use the links in an e-mail to get to any web page, if you suspect the message might not be authentic
- Avoid filling out forms in e-mails that ask for personal financial information
- Always ensure that you are using a secure website when submitting credit card or other sensitive information via your Web browser
  - Web addresses beginning with “https://”
- Regularly check your online accounts, as well as bank and credit card statements
- Ensure that your browser is up to date and all security patches are applied

Report phishing scams

If you do anything other than ignoring and deleting “phishing” or “spoofed” e-mails, you may consider reporting them to the following groups

- Federal Trade Commission at spam@uce.gove
- Internet Fraud Complaint Center of the FBI at www.ifccfbi.gov/
- Chase Bank at abuse@jpmchase.com

Lottery Schemes

We are pleased to inform you of the official announcement today that you have emerged as one of the winners of the international lotto program. You have therefore been awarded a lump sum pay out of US $45,000 cash. You need only to pay the insurance and stamp duty. The winnings are yours to use as you see fit.

You may provide your account number and bank routing number, or you may accept the enclosed check as a loan if you cannot afford to pay the required charges.

Please call your claims coordinator as soon as you receive this confirmation to assist you in finalizing the payment process.

Employment Schemes

- Victim finds a job on an electronic board/site (Monster.com or Jobseekers.com).
- The “employer” hooks the victim on the promise of a nice salary, bonus or advanced commissions.
- “Employee” soon receives his first paycheck and receivables with instructions to deposit the check and wire the funds back to the “employer” minus the commission.
- Checks are deposited and appear good however subsequently are returned.
- Financial hardship occurs as well as identity theft potential as personal information may have been provided to the bogus “employer”

Why these schemes work

- Organized networks of professional fraudsters are behind it
- The pitch is very convincing
- Presumed legitimacy – “They couldn’t print it if it wasn’t true.”
- The lure of “easy money” is so tempting
- Prosecution is difficult because the scammers are often outside the U.S. or never positively identified

Variations on these schemes

- Romance
- Inheritance
- Unclaimed Property
- Traditional 4-1-9 Letter
- Guaranteed Loans

Questions?