Identifying and Responding to Wire Fraud Attacks
Wire fraud attacks are pervasive and can be costly. They disrupt business operations—including payments systems—and impact corporate reputations. Cybercriminals conduct wire fraud attacks that target payments employees to gain access to sensitive data and steal funds. These attacks use various methods, including business email compromise (BEC), which has cost businesses more than $26 billion in domestic and international exposed dollar losses between June 2016 and July 2019.

As this threat continues to grow, it is important that companies develop resiliency strategies to mitigate their risk and lessen the impact of attacks.

The information provided here is intended to help clients protect themselves from wire fraud. It does not provide a comprehensive list of wire fraud activities or best practices. Your organization is responsible for determining how to best protect yourself against wire fraud and for selecting the best practices that are most appropriate to your organization's needs.
What Is Wire Fraud?

A **wire transfer** is an electronic payment method to move money—domestically or internationally—from one person to another using a bank or a nonbank provider, such as a transfer agency.

**Wire fraud** is any fraudulent activity that occurs over interstate wire communications, which includes the telephone and internet. In many cases, the fraud attempt occurs over email. If such a payment request is not authenticated, it can result in a fraudulent transfer of money.

### Wire Fraud Methods

Cybercriminals use a variety of methods to conduct wire fraud. These include:

- **Malware**, occurs when a user opens an email or clicks on a link that redirects to a website that downloads malware and infects the computer operating system. Criminals can also send malware through removable media, such as a USB flash drive. After the removable media is inserted into a computer drive, criminals can gather user credentials to gain access to payments systems.

- **Phishing**, occurs when criminals send emails that appear to be sent from a known company or vendor, such as a bank. The criminal asks the user to reply to the email or visit a website that looks similar to the company’s domain and submit a username, password, account number or other personal information.

  **Note:** It is not the practice of JPMorgan Chase to ask for your personal information or login credentials in an email.

- **Voice phishing (vishing)** and **SMS phishing (SMShing)**. use live or automated calls (vishing) or text messages (SMShing) to intimidate callers into providing personal information by threatening to close or freeze their bank accounts. The personal information is used to gain access to payment systems or take over accounts.

  **Note:** It is not the practice of JPMorgan Chase to send clients emails threatening to close their account if they do not take immediate action. If you receive a suspicious email, forward it to phishing.org.

- **BEC or email account compromise (EAC)**, occurs when cybercriminals use stolen credentials, look-alike domains, spam or phishing to gain access to an email account. Cybercriminals may impersonate a known vendor or C-suite executive, such as the chief executive officer, and direct another employee to transfer funds to a fraudulent account.
Spotting and Preventing BEC

Senior Executive Spoofing

Cybercriminals rely on social engineering and high-pressure tactics to trick payments employees into wiring funds to fraudulent bank accounts, often by impersonating C-suite executives.

Here are common clues that an email is fraudulent:

- The email domain is incorrect. It should be @yourcompany.com, but the word “company” is misspelled here as “connpany.”
- Familiar greeting
- Mentioning they are away from the office could be a red flag.
- An urgent request to send payment again and modify payment instructions is highly suspicious. Modification of payment instructions, including receiving account, should be in compliance with your company’s internal procedures, which should include confirming request with a known contact using a phone number on file.
Vendor Spoofing

In a different scenario, a payments employee may receive an email from a trusted vendor requesting a change in payment instructions, like the example below.

Without due diligence and validation processes to confirm the request, the employee transfers the funds to the criminal’s bank account. A few days later, the vendor calls informing the company that it has not received the payment. During an investigation, the company discovers that the employee’s email account was compromised.

---

**From:** bill.jones@xyz.contract.company.com  
**Date:** Friday, January 10, 2020 at 4:24 PM  
**To:** George.Williams@company.com  
**Subject:** URGENT - Payment Past Due

Hi George,

We did not receive the regular payment per our supplies contract. Please check that you sent it to our **updated account:**

Amount: $867,123.00  
Routing Number: ABC12345  
Account: 12345678

There will be an additional fee if we do not receive the funds tomorrow. Do not hesitate to call me at 123-456-7890 if you have any questions.

Regards,

Bill Jones  
XYZ Contract Company  
Phone: 123-456-7890

---

Training Employees to Prevent Attacks

Your organization can help prevent these malicious attacks by learning how to spot suspicious emails and using **multifactor authentication (MFA)** with strong passwords on personal and business accounts.

While training employees to validate every request may seem like a daunting task, the repercussions of not doing so can be significant. To prevent wire fraud attacks from reoccurring, companies may consider additional best practices in Cybersecurity: Technology and Tactics.

---

1 Courtesy of the National Institute of Standards and Technology, US Department of Commerce. Not copyrightable in the United States.
Response Planning

An effective incident response plan should define who is responsible for leading the response effort, plus actions to complete before returning to business operations. The plan should also establish incident categories and severity levels and set clear response time periods and escalation procedures.

The incident-response process has four stages: **preparation; detection and analysis; containment, eradication and recovery; and post-incident activity**. Your organization’s response plan should address each stage and include specific actions.

**In addition, an effective incident response plan should:**

- Include a diagram of the incident response process
- Describe each phase of the incident response life cycle, including:
  - Incident detection and reporting procedures
  - Response time requirements and escalation criteria
  - Assessment procedures, including forensic data collection and different severity or priority levels
- List contacts:
  - Law enforcement
  - Legal teams
  - Cyber insurance provider
  - Banks
  - Vendors
  - Members of the fraud or incident response team
- Define procedures, including:
  - Containment, including system quarantine, such as removing access to email accounts
  - Remediation and eradication, including disaster recovery, business continuity, public and media relations, and external support
  - Post-incident activities, including a review of incident de-escalation, system restoration and obtaining response team feedback to strengthen the process

Test the incident response plan at least once a year by using tabletop exercises, operational drills or simulated attacks.
Incident Investigation

Once your organization discovers fraud, it is important to act quickly and gather as much information as possible.

INCIDENT INVESTIGATION CHECKLIST

- **Pinpoint** when the fraud occurred.
- **Determine** who authorized the transaction(s).
- **Establish** how many times the fraud occurred.
- **Calculate** the value of the transaction(s).
- **Find** out who—if anyone—validated the transaction before it was released.
- **Identify** the type of account compromised (i.e., bank, credit card, and email and user names).

This investigation will help identify compromised systems so your organization can isolate, investigate and analyze the attack.

Recovery

After your organization resolves any financial losses, computer systems are still vulnerable. Your company’s IT team should scan your organization’s computer network for signs of malware and reimage any affected systems. If an email account was compromised, identify and delete the affected emails, then update the accounts with stronger, unique passwords.

You may also want to engage with an independent, third-party incident response vendor that specializes in digital forensics and remediation. Your cyberinsurance provider may provide additional assistance.

Finally, organizations should develop an **After Action Report (AAR)** to help lessen the impact of future incidents. The AAR allows businesses to review incident response processes and identify what worked and how to make improvements.

\(^2\) Colorado Department of Transportation
CONTACT

For additional information or questions about how to protect your organization from wire fraud attacks, contact cyber.exercise@jpmchase.com.

© 2020 Chase, JPMorgan and JPMorgan Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (collectively, “JPMC”). The material contained herein is intended for informational purposes only. We prepared these materials for discussion purposes only and for your (“The Company”) benefit. Opinions expressed herein are those of the authors and may differ from those of other I.P. Morgan employees and affiliates. This information in no way constitutes I.P. Morgan research and should not be treated as such. Further, the views expressed herein may differ from that contained in I.P. Morgan research reports. The above summary/quotes/prices/statistics may have been obtained from external sources deemed to be reliable, but we do not guarantee their accuracy or completeness. In no event shall JPMorgan Chase or any of its directors, officers, employees or agents be liable for any use of, for any decision made or action taken in reliance upon, or for any inaccuracy or errors in or omissions from, the information herein. The information is not advice on legal, tax, investment, accounting, regulatory, technology or other matters. You should always consult your own financial, legal, tax, accounting, or similar advisors before entering into any agreement for our products or services. In no event shall JPMC or any of its directors, officers, employees or agents be liable for any use of, for any decision made or action taken in reliance upon or for any inaccuracies or errors in, or omissions from, the information in this material. The Company is responsible for determining how to best protect itself against cyber threats and for selecting the cybersecurity best practices that are most appropriate to its needs. JPMC assumes no responsibility or liability whatsoever to any person in respect of such matters, and nothing within this document shall amend or override the terms and conditions in the agreement(s) between JPMC and the Company, 635684.