CYBERSECURITY AND FRAUD PROTECTION

Cybersecurity: “An important, continuous and evolving focus” for JPMorgan Chase

A Strategic Priority:

“We cannot do enough as a country when it comes to cybersecurity.”

- I cannot overemphasize the importance of cybersecurity in America. This is a critical issue, not just for financial companies but also for utilities, technology companies, electrical grids and others.
- It is an arms race, and we need to do whatever we can to protect the United States of America. ... In addition, we need to have better international cyber laws (and include them in trade agreements) like we do in maritime and aviation laws.
- We spend an enormous amount of resources to protect all of our clients and customers from fraud, cybersecurity risk and invasion of their privacy.
- The firm engages in regular and ongoing discussions with certain vendors and clients regarding cybersecurity risks and opportunities to improve security. However, where cybersecurity incidents are due to client failure to maintain the security of their own systems and processes, clients will generally be responsible for losses incurred.

Source: JPMorgan Chase & Co. 2017 Annual Report letter to shareholders

Cyber Fraud by the Numbers

$5.3B

Global losses from **Business Email Compromises** (BEC) between October 2013 and December 2016[3]

16K

BEC Complaints reported to the FBI's Internet Crime Complaint Center in 2017[2]

78%

Of surveyed companies were targets of attempted or actual fraud in 2017, up from 60% in 2013[1]

$676M

Losses in the U.S. due to business email compromise in 2017[2]

77%

Of organizations experienced business email compromise in 2017[1]

>$1B

23% of larger organizations experienced losses of more than $1B from business email compromise[1]

[1]The 2018 Association for Financial Professionals Payments Fraud and Controls Report http://dynamic.afponline.org/paymentsfraud/p/1
[2]Federal Bureau of Investigation's 2017 Internet Crime Report https://pdf.ic3.gov/2017_IC3Report.pdf
[3]"Email Account Compromise: The $5 Billion Scam," Federal Bureau of Investigation, May 2017 https://www.ic3.gov/media/2017/170504.aspx

No Industry is Immune to Electronic Payments Fraud

BEC is the most common type of fraud and biggest cause of loss—any industry or company can be a target.

RETAIL

Client received a request to change payment instructions from vendor who had been hacked. The client accepted the change of instructions because the email address matched what they had on file. Bank controls identified the transaction as fraudulent and no money was lost.

Criminal sent a spoof email purporting to be their vendor and the client initiated a fraudulent wire. Bank controls stopped the transaction for validation with the client, however the client approved release of the transaction resulting in more than $100,000 of losses.

GOVERNMENT

Criminal created a domain that looked like a legitimate third-party service provider with whom the organization had a relationship and requested a change to the banking instructions. A portion of the funds were recovered but nearly $60,000 was lost.

Several employees received a phishing email claiming to be Outlook tech support. Employees clicked on the link, provided their IDs and passwords, allowing the criminals the ability to access and change payroll instructions resulting in a significant number of fraudulent payments to accounts controlled by the criminals.

CHEMICAL

Criminal spoofed an email address from an internal employee requesting an update to payment information. On hitting reply, the email changes. Nearly $100,000 was lost.

Payments staff was contacted from a compromised email from a lookalike domain purporting to be their vendor. Nearly $300,000 was lost.

ENGINEERING

A colleague's email was hacked, and the criminal used it to update payment instructions. The payments staff member didn't call the colleague to verify the change was coming from him, resulting in a loss of nearly $500,000.

Criminal masked an email address to appear as an internal employee's and requested an update to the employee's payroll information, resulting in a loss of thousands of dollars.

Other

Criminal spoofed the email address of a client's CEO and sent a request for multiple fraudulent wires to the controller while the controller was on vacation. The controller forwarded the email to a colleague who initiated the wires, resulting in a loss of more than $300,000.

Criminals hacked an attorney's email and changed the wiring instructions to an account controlled by the criminals. Though the client performed a callback to the attorney, the attorney was unaware that they had been compromised and confirmed the criminal account as legitimate, resulting in a significant loss.

EDUCATION

A school official's email was hacked and the criminals used it to provide bank instructions for a bank account they controlled. Resulting in a loss of more than $50,000.

Criminal hacked the email of a client's vendor and used the vendor's email address to request a change to wire instructions. Resulting in a loss of more than $100,000.

Electronic Payments Fraud: Government Examples

Government:

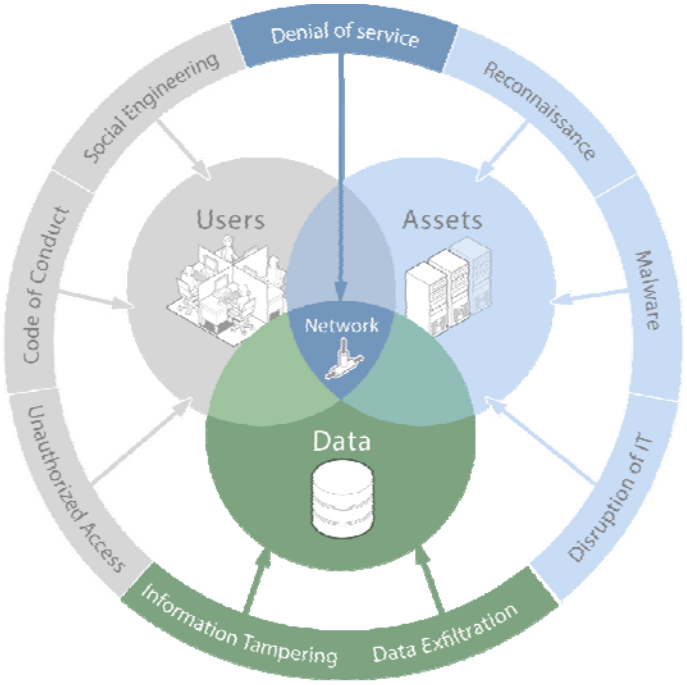
- Criminal created a domain that looked like a legitimate third-party service provider with whom the organization had a relationship and requested a change to the banking instructions. A portion of the funds were recovered, but nearly $60,000 was lost.
- Several employees received a phishing email claiming to be Outlook tech support. Employees clicked on the link, provided their IDs and passwords, allowing criminals the ability to access and change payroll instructions resulting in significant number of fraudulent payments to accounts controlled by the criminals.

Education:

- A school official's email was hacked and the criminals used it to provide bank instructions for a bank account they controlled. Resulting in a loss of more than $50,000.
- Criminal hacked the email of a client's address to request a change in wire instructions. Resulting in a loss of more than $100,000.

Changing Risk Landscape

- Growing Cybersecurity and Payment Fraud Threats
  - Integrity *(Cybercrime & Fraud)* e.g., Manipulation of data with the intention of adjusting payment instructions or prices
  - Confidentiality *(Unauthorized Data Exposure)* e.g., Exposure/theft of client data, unpublished prices, sensitive Information, HR data or cross border/information barrier breaches
  - Availability *(Malicious Disruption of IT)* e.g., 'Distributed Denial of Service' (DDoS) attacks to online services, destructive malware attacks intended to delete critical systems (Wiper) or internal sabotage
- Increasing Regulation
- Heightened Expectations On Internal Controls
- Large Dependencies on Third Parties
- Heavy Reliance on Electronic Communication



Attack Types

Attack Type	Description	Motivation	Actor
▪ **Financial Fraud** ▪ *Risk to data Integrity**	Attacks on the bank and/or its clients/customers with the sole purpose of financial gain	▪ Financial Gain	 Criminal Organizations  Terrorists  Nation States
▪ **Distributed Denial of Service (DDOS)** ▪ *Risk to data Availability**	An attempt to make an online service unavailable through overwhelming it with traffic from multiple sources and flooding the bandwidth	▪ Disruption	 Terrorists  Nation States  Hacktivists
▪ **Ransomware** ▪ *Risk to data Confidentiality and Availability**	A type of malware that encrypts the victims' files, blocking access, and then requests a ransom payment before decrypting	▪ Financial Gain (Extortion)	 Criminal Organizations
▪ **Data Theft** ▪ *Risk to data Confidentiality**	Exposure/theft of data from an unknowing victim with the intent of obtaining confidential information	▪ Espionage Reconnaissance ▪ Financial Gain	 Criminal Organizations  Terrorists  Nation States

Vectors of Attack

EMAIL

- Contain malicious attachments or hyperlinks
- Domain names are spoofed and fake email appear to come from executives

NETWORK

- Distributed Denial of Service (DDoS – large volume of traffic causing an outage)
- Compromised external servers
- Leveraged bot network (botnets – infected computers work together)

WEB

- Spoofed websites (fake, but look real)
- Compromised real websites (watering holes)

SOCIAL ENGINEERING/ CREDENTIALS

- Employee/stolen credentials
- Phone-based social engineering
- Compromised authentication systems
- Compromised social media accounts

MOBILE

- Spoofed company applications
- Malicious applications
- Removing restrictions to gain access to the operating system
- Public Wi-Fi

PHYSICAL

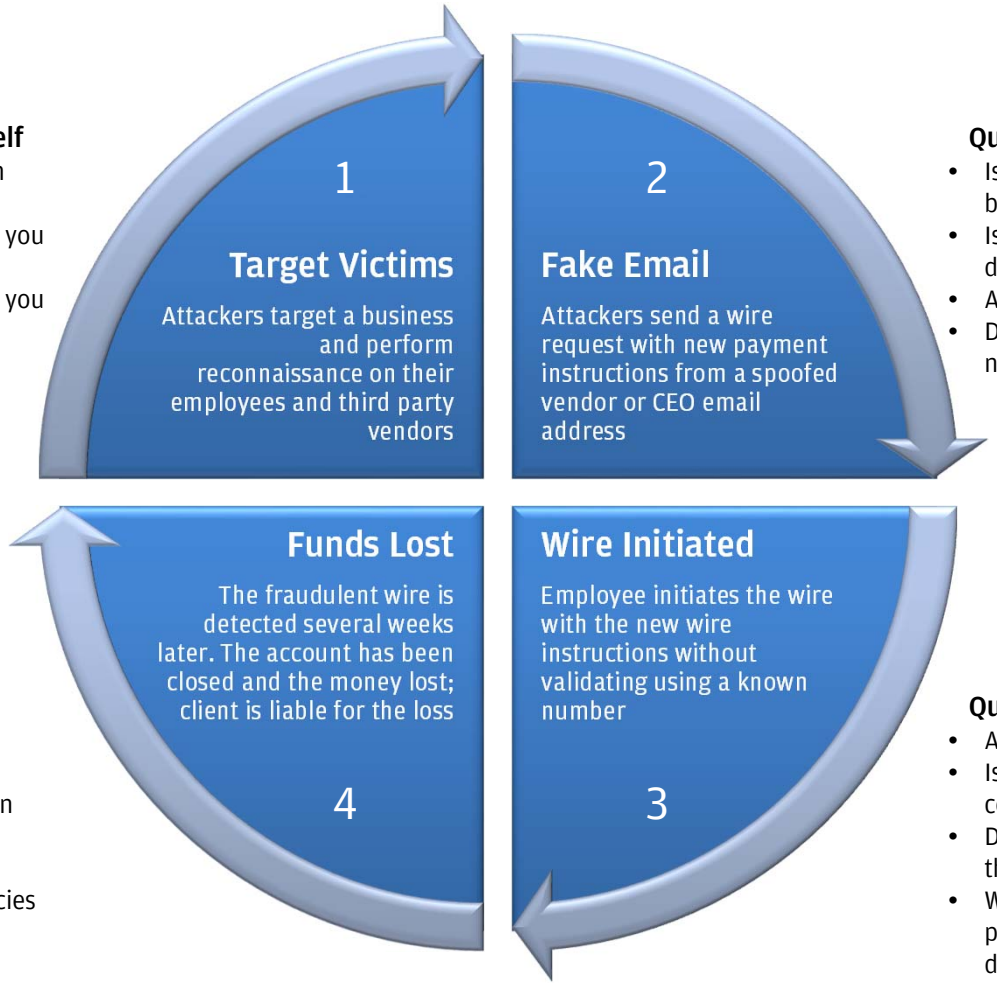
- Device such as USB infected with malicious software and left behind in a public place (then picked up and used by unsuspecting party)
- Connect an infected device to a secure network

Anatomy of a “typical” attack

1

Questions you should ask yourself

- Are you oversharing information on social media?
- Is an external email address asking you for information?
- Is an external email address asking you to click on a misleading link?
- Is a phone call from an unknown number asking you to provide information?



2

Questions you should ask yourself

- Is this an external email pretending to be an internal one?
- Is the email domain a lookalike domain?
- Are they asking for an urgent request?
- Does the email content match the normal trends of the client?

4

Steps you should take

- Perform daily reconciliation of all payment activity
- Report suspected fraud to JPMorgan Chase
- Report suspected fraud to the appropriate law enforcement agencies

3

Questions you should ask yourself

- Are these new wire instructions?
- Is the bank located in a foreign country?
- Does this bank/country make sense for the beneficiary of the money?
- Was a callback performed to a known phone number stored in an internal database?

Phishing/Business Email Compromise

What Is it?

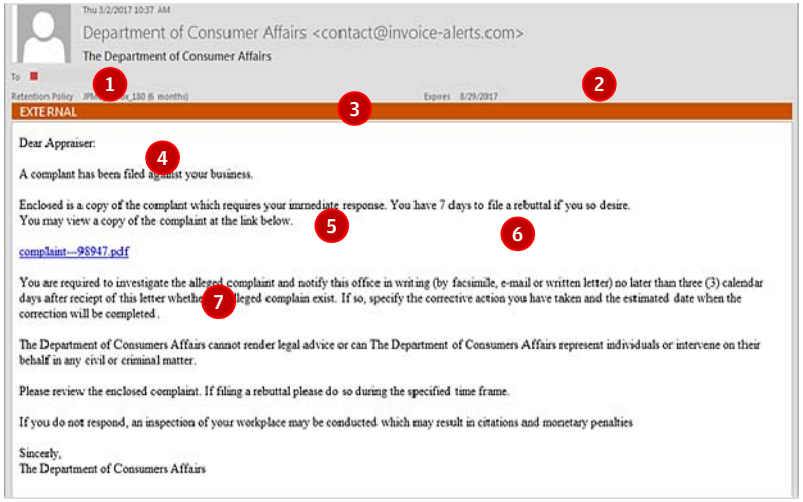
Phishing is the fraudulent practice of sending either blanket emails to large groups or targeted emails to individuals.

Why do attackers use Phishing?

Phishing is the most common method used by cyber criminals to trick victims into either directly **divulging information** or downloading **malware** to be used for financial fraud or as a way infect or gain access to systems.

How To Identify a Phishing Email

1. Sender name is vague and generic
2. Sender address has a suspicious domain (i.e. invoice-alerts.com).
3. Subject does not specify the purpose of the email
4. Email includes the orange External banner indicating it's coming from outside the firm
5. Multiple grammar and spelling mistakes including: *complant, sincerly, punctuation, etc.*
6. Uses authoritative language to entice the user to respond in 7 days but later says to respond in 3 days
7. Link is obfuscated and if you hover over it with your mouse, it will reveal a link of random characters and no mention of a PDF



Additional Checks

- Absence of a logo or improper use of text and graphics
- Unusual web links or attachments

Checking Email on Mobile Devices

If you are unsure, do not click on anything inside the email. Wait until you are back at your regular computer to fully check for the signs of Phishing.

Are you Oversharing?

Social Media websites are not only a popular way for you to share information, but provide a way for criminals to gather information about you and your activities, contacts, friends and family.

PERSONAL IDENTIFICATION
Avoid posting information such as your first car, school name and year of graduation, hometown, date of birth, your mother's maiden name or your pet's name. Be careful to avoid having photos that include your address or license plate on your home page, and never post personal identification information.

LOCATION
Sharing your location could pose a huge security risk for your company because criminals who track you know you are not in the office.

SHARING YOUR PLANS
Avoid announcing that you're on vacation or are planning to be away. It can make your organization vulnerable to an attack when criminals realize someone with less experience may be helping with your job.

TRAVEL PLANS
Publishing pictures of boarding passes or other travel itineraries also tells criminals when it may be the best time to target your company or home. Don't make that information available to the wrong people. Postpone sharing information about a trip until after you've returned home.

Top Tips

- Limit the amount of **personal information** you post online
- Providing too much specific information allows criminals to tailor **social engineering** campaigns against you
- In addition, posting too much information could lead to **identity theft**
- Use **privacy settings** to avoid sharing information widely

How You Can Help Protect Your Agencies

Governance	■ Cross-LOB groups responsible for improved cyberfraud mitigation efforts
Classification	■ Improved tracking and risk-classification systems highlight and block suspicious transactions ■ Irregular payments may include first-time beneficiaries, urgent requests and cross-border payments
Advanced Threat Analytics	■ Development of advanced threat intelligence analytics platform to help prevent abuse by tracking campaigns and identifying victims prior to account connection
Education	■ Cyberfraud awareness program to educate clients, employees and partners on cyberfraud risks, their identification, escalation steps and their mitigation ■ Identify the creation of lookalike domains and notify clients of domains that closely resemble their corporate domains; Send clients information in these cases of tools that can help protect them
Collaboration with Law Enforcement	■ Cooperate with law enforcement in the arrest of criminals carrying out fraud schemes ■ Report all fraud to the appropriate law enforcement agencies as well as notifying your bank.

Clients' Payments Security and Controls

Payments controls

- Make sure you know who has access to your banking relationships and accounts and review entitlements.
- Set payment limits at account and employee level based on payment trends/history (e.g., 12-month history).
- Establish multiple approval levels based on various thresholds (dollar amounts, tenure).
- Require multi-level approvals in areas such as accounts payable.
- Do not allow multiple users to log in from the same computer to initiate or release payments.
- Use approved templates/verified bank lines and restrict use of free form payments.
- Apply strong internal controls regarding changes to vendor bank account information used to complete electronic payments.

Verification

- Always comply with your internal controls and perform testing on a regular basis.
- Never give any information to an unexpected or unknown caller.
- Do not move money or change a vendor's bank account information based solely on an email or telephone instruction(s) even from trusted vendors.
  - Always validate by contacting the entity requesting payment /change in instructions in person or by calling a known telephone number stored on an internal database with controlled access (Never call a number provided via an email or pop-up message.)
  - Validate the sender's email address by hovering over the email address and/or hit reply and carefully examine the characters to ensure they match the exact spelling of the company domain and the individual's name.

Reconciliation

- Perform daily reconciliation of all payment activity – Immediate identification and escalation is critical.
- Consider establishing a program to detect anomalous payments:
  - Identify irregularities (first time beneficiaries, cross-border payments).
  - Verify payment values and velocity.
  - Establish criteria to verify or release payments.
  - Track and trace where a payment is in the environment point to point and if altered at any time.

How Clients Can Help Protect Their Companies

What executives can do:

- Require senior financial officer approval for any request for an immediate payment that is over a standard threshold amount or for any request that a payment be handled in secret.
- Establish and closely follow internal controls for the approvals required to change vendor remittance addresses or bank account information and to pay invoices.
- Promptly review account activity for any suspicious transactions and contact us immediately about any suspicious or erroneous wires.
- Immediately contact your bank if users become suspicious after sending a wire transfer.
- Use the security features available on your bank's online system.

What operations employees can do:

- Stop any online session that makes them uncomfortable, especially at log in, and call your bank.
- Always validate every payment request that has new or changed beneficiary information.
- Never provide sensitive confidential information in an email. This includes account numbers, log-in credentials and passwords, and SecurID® token information.
- Never respond to pop-ups or unsolicited phone calls asking them to resubmit log-in information, or the information of another user, especially on the same computer.
- Look for the personal verification image in reviewing any email that appears to be sent from us through the secure Voltage encryption system.
- Never share user IDs.
- Avoid multiple people using the same computer to process a transaction.

Chase, J.P. Morgan, and JPMorgan Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (collectively, "JPMC").

This document was prepared solely and exclusively for the benefit and internal use of the party to whom it is directly addressed and delivered (the "Company") in order to make a preliminary presentation to the Company regarding certain products or services that might be provided by JPMC. This document and any related presentation materials are for discussion purposes only and are incomplete without reference to, and should be viewed solely in conjunction with, a related oral briefing provided by JPMC. This presentation does not constitute a commitment by any JPMC entity to extend or arrange credit or to provide any other services. The Materials and oral briefing (collectively the "Information") contain information which is confidential and proprietary to JPMC and may only be used by the Company for the purpose of evaluating the products and services described in the Information and may not be copied, published, disclosed or used, in whole or in part, for any other purpose other than as expressly authorized by a JPMC entity. The information is not intended, nor should it be relied upon, to address every aspect of the subject discussed herein. 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.

In preparing the Information, JPMC has relied upon and assumed, without independent verification, the accuracy and completeness of information available from public sources or provided to it by or on behalf of the Company. JPMC does not guarantee the accuracy, completeness or reliability of that information. JPMC's opinions and estimates contained herein reflect prevailing conditions and our views as of this date, which are accordingly subject to change, and should be regarded as indicative, preliminary and for illustrative purposes only. Our analyses are not and do not purport to be appraisals of the assets, stock, or business of the Company or any other entity.

The Information is not intended and shall not be deemed to constitute or contain advice on legal, tax, investment, accounting, regulatory, technology or other matters on which the Company may rely, and the Company should consult with its own financial, legal, tax, accounting, compliance, treasury, technology, information system or similar advisors prior to entering into any agreement for JPMC products or services. The Company is responsible for its own independent assessment as to the cost, benefit, suitability and appropriateness of any products or services it obtains from JPMC. JPMC makes no representations as to the actual value which may be received in connection with any JPMC product or service or the legal, tax, or accounting implications of consummating any transaction contemplated by the Information.

The Information contained herein is intended as general market and/or economic commentary, does not constitute and should not be treated as J.P. Morgan research. The Information may differ from that contained in J.P. Morgan research reports. The Information is not intended as nor shall it be deemed to constitute advice or a recommendation regarding the issuance of municipal securities or the use of any municipal financial products. JPMC is not providing any such advice or acting as the Company's agent, fiduciary or advisor, including, without limitation, as a Municipal Advisor under Section 15B of the Securities and Exchange Act of 1934, as amended.

The Information does not purport to set forth all applicable terms or issues and are not intended as an offer or solicitation for the purchase or sale of any financial product or service or a commitment by JPMC as to the availability of any such product or service at any time. JPMC products and services are subject to applicable laws, regulations, service terms and policies of JPMC. Not all products and services are available in all geographic areas or to all customers. Eligibility for particular products and services is subject to satisfaction of applicable legal, tax, risk, credit and other due diligence, JPMC's "know your customer," anti-money laundering, anti-terrorism and other policies and procedures.

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 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.

All trademarks, trade names and service marks appearing in the Information are the property of their respective registered owners.

JPMorgan Chase Bank, N.A. Member, FDIC