



## Cybersecurity and Fraud Protection

## Strategic Priority

---

The threat of cybersecurity may very well be the biggest threat to the US financial system.

Jamie Dimon, Chairman and CEO,  
JPMorgan Chase & Co.



*“We remain devoted and diligent to protect privacy and stay cyber safe—we will do what it takes.”*

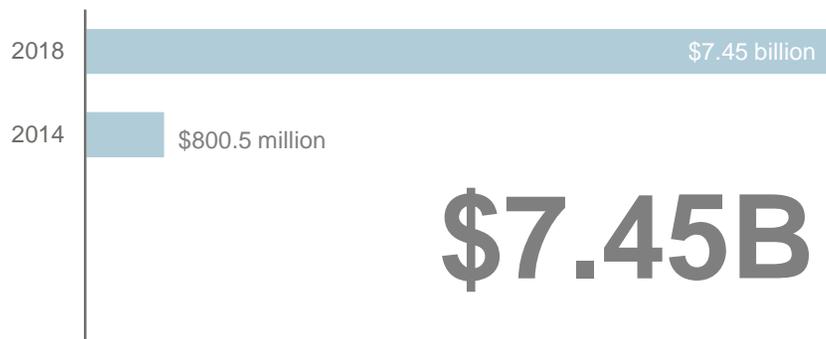
*We spend nearly \$600 million a year on these efforts and have more than 3,000 employees deployed to this mission in some way.*

*We also spend a lot of time and effort trying to protect our company in different ways as part of the ordinary course of running the business. But the financial system is interconnected, and adversaries are smart and relentless—so we must continue to be vigilant.*

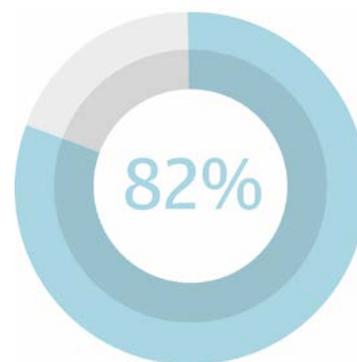
Source: JPMorgan Chase & Co. 2018 Annual Report letter to shareholders

# Cyber Fraud by the Numbers

## Total losses from cybercrimes in 2018, up from \$800.5M in 2014<sup>1</sup>

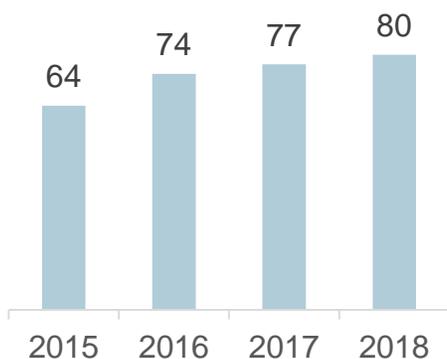


## Percent of companies targeted for fraud attacks in 2018



**82** percent of surveyed companies were targets of attempted or actual fraud in 2018, up from 62% in 2014<sup>1</sup>

## Business Email Compromise (BEC) Attacks Continue to Rise



**80** percent of organizations experienced BEC in 2018, up from 64% in 2014<sup>1</sup>

## BEC Complaints to the FBI

**20k**

**20** thousand BEC complaints were reported to the FBI's Internet Crime Complaint Center in 2018<sup>2</sup>

Source:

1 The 2019 Association for Financial Professionals Payments Fraud and Controls Survey Report (<https://www.jpmorgan.com/commercial-banking/insights/2019-afp-payments-fraud-control-survey-report>)

2 Federal Bureau of Investigation's 2018 Internet Crime Report ([https://pdf.ic3.gov/2018\\_IC3Report.pdf](https://pdf.ic3.gov/2018_IC3Report.pdf))

# How We Defend Ourselves

## Architect and engineering security from the ground up

- Build a fortress foundation and provide firmwide resiliency
- Technology operations governed by “Rules of the Road”
- Enhance security hygiene of applications and infrastructure environment

## Strong security operations provide constant vigilance against attack

- Utilize advanced technology and best people
- Proactively anticipate the next threats
- Testing ourselves through constant drills, exercises and “red teaming”

## Protect business and customer data throughout the organization

- Understand our critical data flows to focus our efforts
- Leverage technology, process and people to enhance our efforts

## Engage the business and clients on cybersecurity awareness

- Strong security culture, reinforced by training and communications programs
- Educate our business leaders to help protect our clients

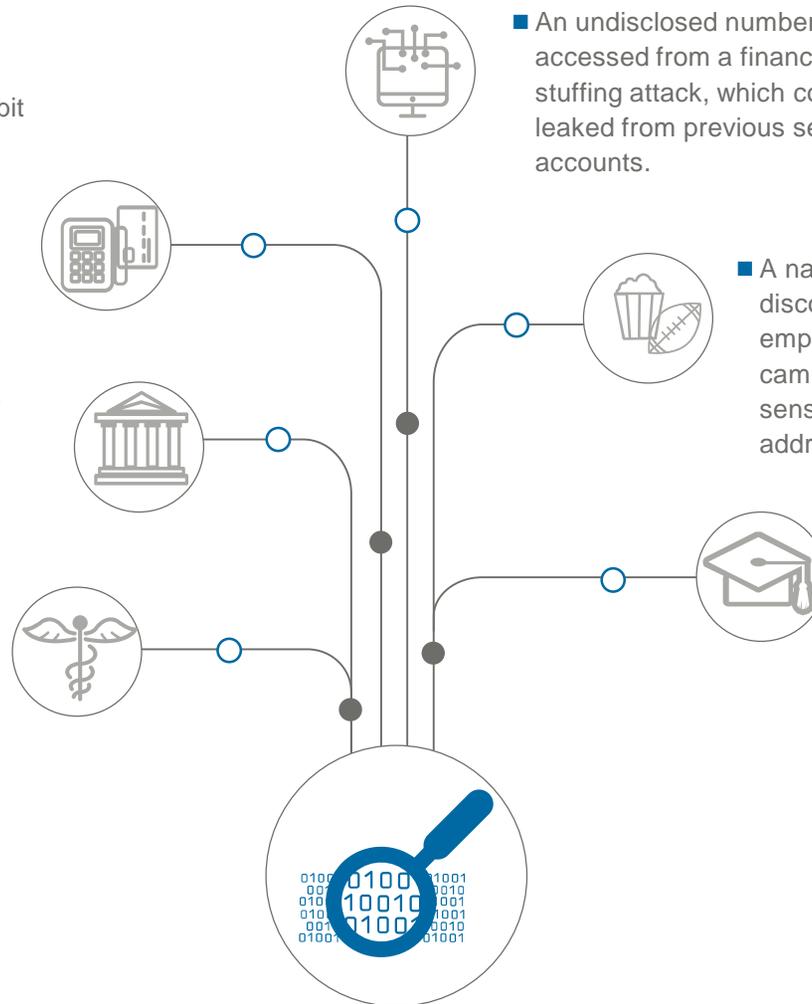
## Integrate into national and global cybersecurity systems

- Work with government to improve our awareness and ability to respond
- Drive a healthier ecosystem for our customers

# 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.

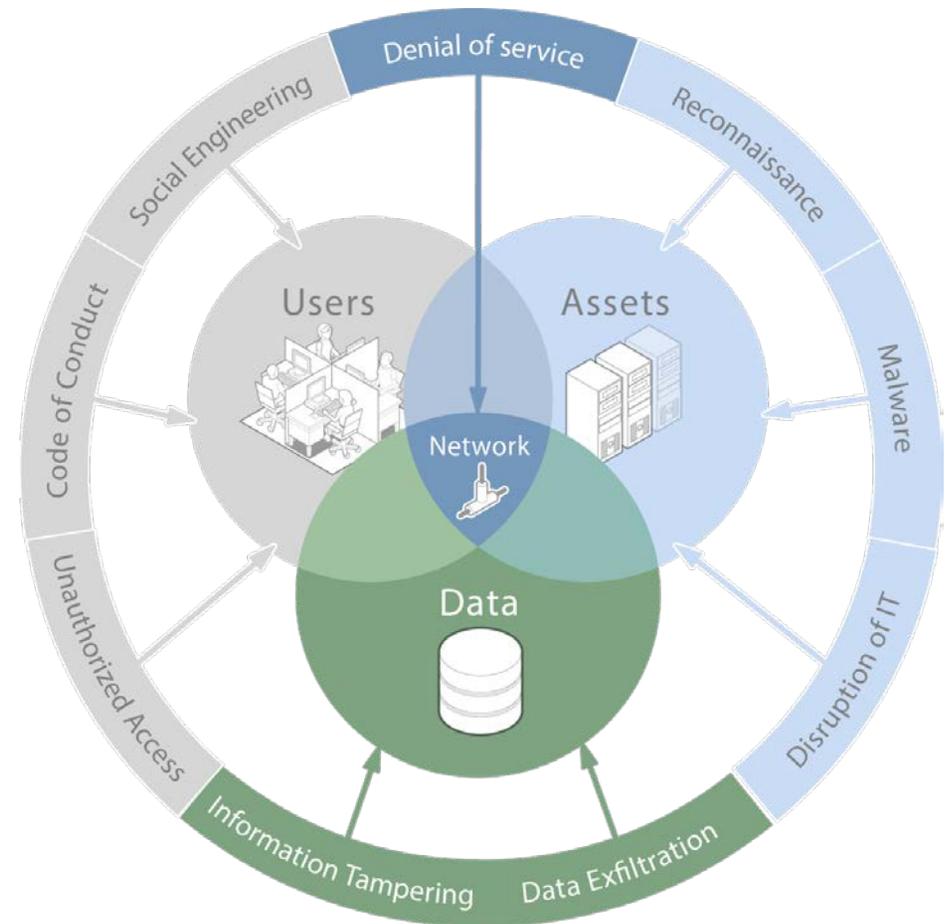
- More than two million credit and debit card numbers and expiration dates were stolen over several months using malware on a point-of-sale payment system.
- Multiple municipal governments were victims of ransomware attacks impacting computer systems and services; cybercriminals encrypted data and locked employees out of computer systems.
- December 2018: A hospital discovered a data breach that compromised nearly one million patients after criminals were able to penetrate a vulnerability on a website server.



- An undisclosed number of tax return information was accessed from a financial software company in a credential stuffing attack, which compiles usernames and passwords leaked from previous security breaches to access other accounts.
- A national sports and entertainment company discovered criminals successfully gained access to employee email accounts. Using a phishing campaign, the criminals were able to access sensitive user information including names, addresses and credit card numbers.
- A data breach at a collegiate campus exposed personal information including names, addresses, Social Security numbers and birthdates for more than one million current and former faculty and students.

# Changing Risk Landscape

- Growing cybersecurity and payment fraud threats
  - Integrity: Cybercrime and 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, 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		
<ul style="list-style-type: none"> <li>Financial Fraud</li> <li>Risk to data Integrity*</li> </ul>	Attacks on the bank and/or its clients/customers with the sole purpose of financial gain	<ul style="list-style-type: none"> <li>Financial Gain</li> </ul>	 Criminal Organizations	 Terrorists	 Nation States
<ul style="list-style-type: none"> <li>Distributed Denial of Service (DDOS)</li> <li>Risk to data Availability*</li> </ul>	An attempt to make an online service unavailable through overwhelming it with traffic from multiple sources and flooding the bandwidth	<ul style="list-style-type: none"> <li>Disruption</li> </ul>	 Terrorists	 Nation States	 Hacktivists
<ul style="list-style-type: none"> <li>Ransomware</li> <li>Risk to data Confidentiality and Availability*</li> </ul>	A type of malware that encrypts the victims' files, blocking access, and then requests a ransom payment before decrypting	<ul style="list-style-type: none"> <li>Financial Gain (Extortion)</li> </ul>	 Criminal Organizations		
<ul style="list-style-type: none"> <li>Data Theft</li> <li>Risk to data Confidentiality*</li> </ul>	Exposure/theft of data from an unknowing victim with the intent of obtaining confidential information	<ul style="list-style-type: none"> <li>Espionage Reconnaissance</li> <li>Financial Gain</li> </ul>	 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 (botnet–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

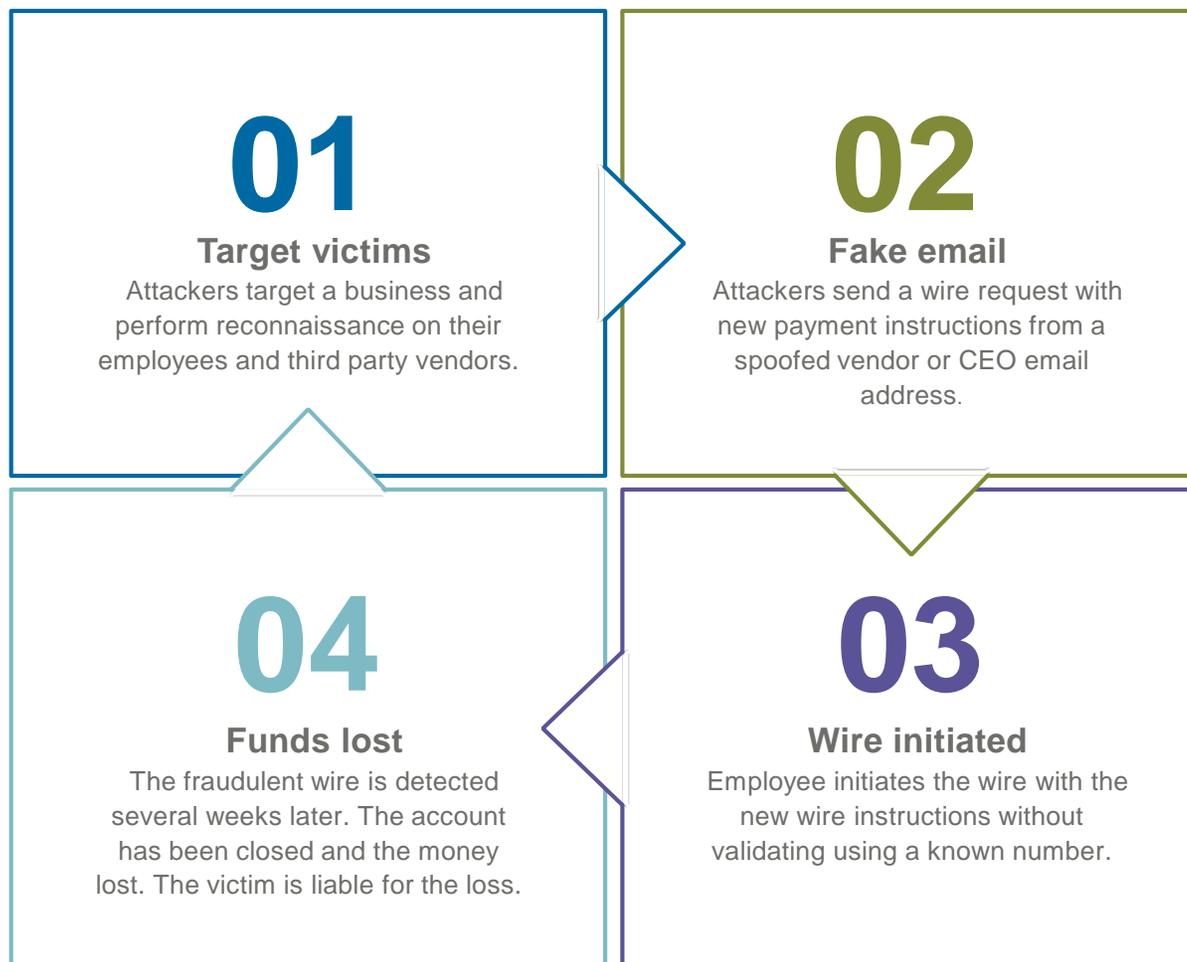
# Anatomy of a Typical Attack

## Ask:

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

## Do:

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



## Ask:

- 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?

## Ask:

- 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?

# Business Email Compromise (BEC)

**BEC is an electronic scam to obtain confidential, personal or financial information from clients through email.**

From: bill.jones@xyz.contract.company

To: george.williams@company.abc

Sent: January 11, 2019

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

## Email Spoofing/Masking

A spoofed or masked email contains a forged email header that hides the true origination of a message. Fraudsters trick employees of victim companies into divulging company sensitive information and/or initiating payments based on fraudulent instructions.

## Client Email Compromise

Fraudsters compromise an employee's email account at a victim company; often referred to as account takeover or hacking. Fraudsters leverage access to an email account or corporate network to gain an understanding of the communication style of the firm or executive, and ultimately send an email to an employee with fraudulent payment instructions.

## Vendor Email Compromise/Supply Chain

Fraudsters impersonate a company's vendor rather than a company's employee. A vendor's clients receive requests with updated accounts, then send funds to what is believed to be a valid account from their trusted vendor.

## Lookalike Domain

Fraudsters purchase/register a domain closely resembling that of a legitimate company, then setup a related email account to target the victim company. Victim companies' employees often do not notice the difference between their legitimate corporate domain and the lookalike, which is very similar visually.

## Best practices

- Consider available email security solutions to defend against lookalike domains
- Enable controls so all emails from outside your company are marked as external
- Train employees who process payments to properly verify all payment account changes rather than rely solely on email instructions
- Train all employees on suspicious email trends and test them regularly

# Phishing | What does it look like?

## Warning signs

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 an external banner indicating it's coming from outside the company
5. Multiple grammar and spelling mistakes including: complant, sincerely, punctuation, etc.
6. Uses urgent or authoritative language demanding a quick response
7. Link hides its origin; if you hover over it with your mouse, it will reveal a link of random characters but no PDF

## Phishing example

The screenshot shows an email interface with the following elements and callouts:

- 1**: Sender name icon (vague/generic)
- 2**: Sender address: Department of Consumer Affairs <contact@invoice-alerts.com>
- 3**: Sender name: The Department of Consumer Affairs
- 4**: External banner: EXTERNAL
- 5**: Urgent language: "You are required to investigate the alleged complaint and notify this office in writing (facsimile, email or written letter) no later than three (3) calendar days after receipt of this letter whether the alleged complain exist. If so specify the corrective action you have taken and the estimated date when the correction will be completed."
- 6**: Suspicious link: [Complaint—98947.pdf](#)
- 7**: Link hides its origin (no PDF)

Dear Appraiser,

A complaint has been filed against your business.

Enclosed is a copy of the complaint, which requires your immediate response. You have 7 days to file a rebuttal if you so desire. You may view a copy of the complaint at the link below.

[Complaint—98947.pdf](#)

You are required to investigate the alleged complaint and notify this office in writing (facsimile, email or written letter) no later than three (3) calendar days after receipt of this letter whether the alleged complain exist. If so specify the corrective action you have taken and the estimated date when the correction will be completed.

The Department of Consumer Affairs cannot render legal advice or can The Department of Consumer Affairs represent individuals or intervene on their behalf in any civil or criminal matter.

Please review the enclosed complaint. If filing a rebuttal please do so during the specified time frame.

If you do not respond, an inspection of your workplace may be conducted which may result in citations and monetary penalties.

Sincerely,  
The Department of Consumer Affairs

# Social Engineering | What does it look like?

## Best practices

- 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

## Are you oversharing?



### 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.

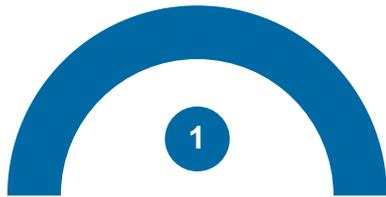
### Sharing your plans

Avoid announcing that you're on vacation or 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 an ideal 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.

# Best Practices | Payment Security and Controls



## User access

- Know who has access to your banking relationships and accounts; review entitlements regularly
- 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)
- Ensure robust and multi-level approvals required in areas such as accounts payable
- Don't have multiple users log in from the same computer to initiate or release payments
- Use approved templates/verified bank lines and restrict use of free form payments

## Verification

- Don't move money based solely on an email or telephone instruction(s), even from trusted vendors
- Validate by calling the entity requesting payment/change in instructions at their known telephone number
- Never call a number provided via an email or pop-up message
- Always validate the sender's email address and hover over the email address and/or hit reply and carefully examine the characters in the email address to ensure they match the exact spelling of the company domain and the spelling of the individual's name
- Never give any information to an unexpected or unknown caller



## Reconciliation

- Perform daily reconciliation of all payment activity
- Immediate identification and escalation is critical

## 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



## Best Practices | Technology

---

### System controls

- Ensure your company is running anti-virus software regularly and keeping it up to date
- Use the latest internet browsers to maintain security to detect unauthorized downloads
- Create intrusion detection system rules that flag emails with extensions that are similar to company email; for example, legitimate email of *abc\_company.com* would flag fraudulent email of *abc-company.com*
- Enable the strongest encryption available for Wi-Fi, hotspots, or internet
- Never install unauthorized applications or external media on your work computer
- Don't allow external devices to connect to work computers (e.g. mobile devices)

### User controls

- Require your employees to lock their screen every time they step away from their workstation
- Require employees to not leave confidential information or credentials on their desks unattended and in plain view
- Restrict the use of public computers for business purposes and avoid public Wi-Fi networks for business
- Work vs Personal: Do not allow your employees to use their office email address to register with a non-business related website
- Restrict the use of free web-based email accounts for business. Establish a company domain name and use it to establish company email accounts in lieu of free web-based accounts. If possible, register all company domains that are slightly different than your actual company domain.
- Educate employees to not disclose specific details of your job on company or social media sites

### Secure passwords

- Never provide user IDs or passwords to others
- Change passwords frequently
- Make sure passwords are complex, unique, unpredictable and inaccessible
- Passwords should be alpha/numeric, upper and lower case and at least 8 characters long

---

Chase, J.P. Morgan, and JPMorgan Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its affiliates and subsidiaries worldwide (collectively, “JPMC”, “We”, “Our” or “Us”, as the context may require).

We prepared these materials for discussion purposes only and for your (“The Company”) sole and exclusive benefit. This information is confidential and proprietary to our firm and may only be used by you to evaluate the products and services described here. You may not copy, publish, disclose or use this information for any other purpose unless you receive our express authorization.

These materials do not represent an offer or commitment to provide any product or service. [In preparing the information, we have relied upon, without independently verifying, the accuracy and completeness of publicly available information or information that you have provided to us. Our opinions, analyses and estimates included here reflect prevailing conditions and our views as of this date. These factors could change, and you should consider this information to be indicative, preliminary and for illustrative purposes only. This Information is provided as general market and/or economic commentary. It in no way constitutes research and should not be treated as such.

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.

The information does not include all applicable terms or issues and is not intended as an offer or solicitation for the purchase or sale of any product or service. Our products and services are subject to applicable laws and regulations, as well as our service terms and policies. Not all products and services are available in all geographic areas or to all customers. In addition, 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 Banking affiliates, securities affiliates or other JPMC affiliates or entities. In particular, securities brokerage services other than those that can be provided by Commercial Banking affiliates will be provided by appropriate registered broker/dealer affiliates, including J.P. Morgan Securities LLC and J.P. Morgan Institutional Investments Inc. Any securities provided or otherwise administered by such brokerage services are not deposits or other obligations of, and are not guaranteed by, any Commercial Banking affiliate and are not insured by the Federal Deposit Insurance Corporation.

JPMorgan Chase Bank, N.A. Member FDIC.

© 2019 JPMorgan Chase & Co. All rights reserved.

