

# Cybersecurity:

## Making Security Personal

### Ransomware Rising

Developing comprehensive and effective resiliency plans is the key to fighting the growing threat of ransomware attacks

### Attracting Skilled Talent

Creating a diverse workforce with the skills needed to combat cyberthreats

### Swift Action Stops Fraud

A quick response from a treasury management officer helps a client stop a potential fraud scheme







# Making Security Personal

**With the spate of recent news headlines focused on cybersecurity issues—from escalating ransomware attacks that target government organizations, to malware schemes that impact small businesses, to cloud-based data breaches that affect millions of individuals—making security personal is a critical, and shared, responsibility.**

As we embark on the 16th annual National Cyber Security Awareness Month (NCSAM) this October, now is a good time to review personal and business security protocols to help stay safe and create a more secure environment for personal data. NCSAM—a collaborative effort between the US Department of Homeland Security and the National Cyber Security Alliance—is a time for all companies and individuals to create personal accountability to help guard against a cyberattack.

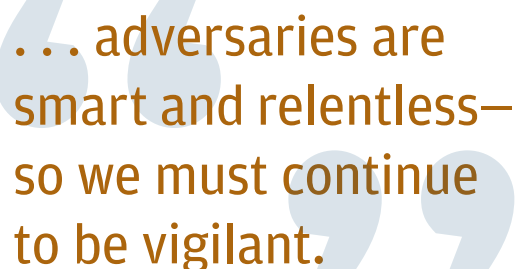
Protecting against cybersecurity threats is a 24/7 operation—it's not a question of *if* an organization will be hit, but *when* it will happen. At least 22 targeted ransomware attacks against state and local municipalities have been reported so far this year, including larger cities such as Baltimore, MD and smaller counties such as Fisher County, TX, according to Recorded Future, a threat intelligence analysis firm.

Experts say the criminals are taking advantage of software vulnerabilities and lapses in employee training and education.

By reviewing and testing your organization's resiliency and recovery plans before an actual cyberattack occurs, your organization can be better prepared to manage responses to internal and external stakeholders, employees and the public.

Ransomware schemes aren't the only attacks making headlines lately. Law enforcement is reporting a new version of an ACH fraud phishing scheme that is hard to detect because the emails follow a different trend using a "high number, low value" approach. Criminals attempt to change employee payroll direct deposit information and transfer the funds to a new bank account. This payroll diversion scheme leverages the company's chief executive officers or payroll director as the point of contact requesting the change.

In this issue, you'll read how Kelly Jean Lomberg, a treasury management officer with the firm, used quick thinking and validation processes to help a client stop a potential fraud attempt payment for almost \$200,000. We also talk with Meagan Ringel



**... adversaries are smart and relentless—so we must continue to be vigilant.**

**JAMIE DIMON**

CHAIRMAN AND CHIEF EXECUTIVE OFFICER  
JPMORGAN CHASE & CO.

from the firm's Corporate Cybersecurity Operations on how companies can attract diverse talent to work in the growing cybersecurity and fraud fields. Globally, women hold a quarter of all cybersecurity-related jobs, and this is shifting the conversation to focus greater awareness around diversity and culture. And because awareness starts with each of us, you'll also read what a few of the talented women working in cybersecurity operations at JPMorgan Chase & Co. say about best practices to help clients and individuals avoid fraud attempts. ■

# Developing Resiliency Strategies to Combat Escalating Ransomware Attacks

**Cybercriminals have escalated ransomware attacks this year targeting companies, local and state governments, and healthcare organizations. A spate of widely publicized attacks targeting cities—such as Baltimore; Atlanta; Albany, NY; and a trio of municipalities in Florida—as well as companies such as Norsk Hydro have captured headlines, heightening public awareness and mounting concerns about ransomware attacks.**

According to the *2019 Verizon Data Breach Investigations Report*, ransomware attacks are an increasing threat to all industries and accounted for nearly 24 percent of attacks when malware was used. In 2019 so far, at least 22 such attacks have been reported, according to Recorded Future, a threat intelligence analysis firm, and ransomware attacks are not unique to US interests. The pattern continues globally, as reported by the Cybersecurity and Infrastructure Security Agency (CISA).

CISA, a part of the Department of Homeland Security, describes ransomware as “a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid” and warns that it usually spreads

through phishing emails and infected websites. Once cybercriminals gain access to a company’s private information, they hold the files hostage until a ransom is paid, usually in a cryptocurrency such as bitcoin. To release the files, the cybercriminals will issue a decryption key to the victim, but sometimes, even if the ransom is paid, they don’t return the data files and instead demand additional payments.

Many organizations and agencies targeted had not applied software patches developed since the last widespread ransomware outbreak and may be operating without backup systems.

“The key to mitigating a ransomware attack is to isolate, isolate, isolate. By creating multiple layers of protection for backups, organizations can help support rapid restoration capabilities, in the event of an attack, by quickly identifying the most recent backup to use,” said Adam Bulava, Global Head of the firm’s Attack Simulation team.

Criminals are brazen in launching ransomware schemes, taking advantage of vulnerabilities in computer systems and lapses in employee training and resources.

“Government agencies or smaller companies may be strapped for resources due to budgeting constraints and are unable to add the software updates that help mitigate potential threats,” said Bulava.

The reality is that no company is immune to cybercrimes, especially ransomware, which is invasive, and the fallout from an attack can be enormous. Some large multinational companies with a tremendous volume of private customer information may choose to pay the ransom when such an attack renders them unable to conduct business, or they may want to avoid potential negative publicity and the resulting fallout with employees, customers and stakeholders.

However, when dealing with criminals, paying a ransom doesn’t guarantee the data will be released. While the decision to pay ransomware or not is an individual organization’s decision based on what is best for their employees and stakeholders, the Federal Bureau of Investigation (FBI) does not advocate paying ransom to criminals. Many times paying ransom perpetuates future crimes and emboldens other cybercriminals to launch similar schemes.

## Prevention is Critical

With the number of attempted or actual payments fraud attempts reaching record levels, the firm is helping clients look at the viability of their resiliency and recovery plans. Ransomware attacks aren't isolated events and can strike a company more than once. Resiliency is the key to helping companies—big and small—deal with a ransomware attack.

“The firm's Threat Intelligence organization evaluates cyberattack information looking for patterns with threat actors to prioritize threats and help protect the firm and clients,” said JF Legault, Global Head of Cybersecurity Operations.

The firm's Attack Simulation team hosts a series of tabletop exercises with clients that simulate a ransomware attack scenario. While the simulations are intended to help test resiliency strategies, Bulava said the sessions demonstrate real-life implications and test an organization's response time and engagement.

“If you don't have a resiliency plan in place, now—before a data breach occurs—is the time to develop a layered approach and make your cyber hygiene protocols more secure. Include as many teams as possible, from communications, technology, operations, legal and executives, to support internal and external resiliency and recovery efforts,” said Brett Wallace, Executive Director, Cybersecurity Intelligence Group with the firm.

Communications teams should be engaged in resiliency planning to help build responses to employees, third-party suppliers, customers and key stakeholders in the event of a data breach.

Possibly adopting cloud-based technology as part of an organization's resiliency and remediation strategy will help avoid a bare metal restoration, which is essentially rebuilding a computer from scratch. It is also important to check and secure any vulnerabilities in configurations with cloud system security to prevent a breach. Practice good cyber hygiene by creating multiple back-up layers to protect network computer systems if they become infected. If a company is considering purchasing cyber insurance, read the fine print to make sure ransomware attacks are covered in the policy.

Bulava added, “It is important to test resiliency plans at least twice a year with simulated drills and implement any necessary changes to ensure all employees are comfortable with processes and procedures.”

While creating an internal security network and best practices is important, relationship building with external partners is also critical. Engaging FBI field offices and the agency's Internet Crime Complaint Center (IC3) in advance of an attack may help improve response time.

“Developing effective resiliency and recovery plans is every client's responsibility and every minute counts during a recovery effort,” said Mike Kelly, Head of Commercial Banking Cybersecurity and Technology Controls. “We want all of our clients to remain vigilant, be prepared and determine the best strategy for mitigating and recovering from a ransomware attack.” ■



# Criminals Target Employee Payroll Direct Deposit Information

**Experts are reporting a new version of an ACH fraud scheme where criminals attempt to change employee payroll direct deposit information and ultimately divert funds to a new offshore bank account. The scheme is different from others because it doesn't contain the typical red flags, such as misspellings or urgent tone, making it more difficult to detect by existing controls.**

According to the Federal Bureau of Investigation, criminals are deploying the scheme across several industries, including education, healthcare and commercial airway transportation, by targeting human resources or payroll employees who have access to online payroll accounts. In 2018, the agency's Internet Crime Complaint Center (IC3) received approximately 100 complaints of payroll diversion, with a combined reported loss of \$100 million—a number experts predict will rise in 2019.

The phishing emails appear to be legitimate and sent from a company employee or the company's chief executive officer, chief financial officer or payroll director requesting a change in the bank account information listed for the direct deposit.

Experts say these emails are well written without the usual misspellings or grammar mistakes seen in typical phishing schemes and project a brief, friendly tone to the sender.

Law enforcement says criminals are using a "high number, low value" approach to these attacks. For example, the criminals will direct payroll records to be updated to allow the deduction of a nominal amount, \$10-\$20, per paycheck, from hundreds if not thousands, of employees. These fraud attempts often escape existing controls because they don't ask for a wire transfer or other payment instruction changes. The smaller amount is less likely to arouse suspicion, and the payoff comes from collecting from the large number of victims.

It's important to remember that company executives or other payroll employees should not email another employee to request a change in bank account information or credentials to access a company's payroll system. And recipients of such requests should always verify the request by calling the requestor using a known telephone number or in person.

The IC3 recommends these best practices to help mitigate the threat of payroll diversion:

- » Reinforce education and awareness about cyberschemes among all employees.
- » Hover over the sender's name in emails to display the real email address or website URL to confirm the actual sender or website.
- » Never share login credentials.
- » Never share personal information in emails.
- » Implement multifactor authentication for access to sensitive systems and information, especially bank account changes initiated by employees who want to update or change direct deposit information.
- » Monitor employee logins that occur outside normal business hours.
- » Submit suspicious emails or criminal activity to your local FBI office and file a complaint with the IC3 at [ic3.gov](https://ic3.gov). Your local FBI office can be determined at [fbi.gov/contact-us/field-offices](https://fbi.gov/contact-us/field-offices). ■





## How We Can Help

We encourage all clients to complete training and use the security measures we offer.

To register for the training:

- » J.P. Morgan Access® users may log on to Access and register for the Cyber Fraud & Secure Online Banking webinar via “Support > Education.”
- » Chase Connect® users may visit [chase.com/cybersecurity](https://chase.com/cybersecurity) and click “Learn More” under “How to Secure Your Online Banking” to access our Cyberfraud and Secure Online Banking webinar.

You also may contact the Chase Connect Service Center at (877) 226-0071; government entities and not-for-profit organizations call (855) 893-2223.







# Client Success: Treasury Management Officer's Immediate Action Saves Almost \$200,000

**It seemed like a regular Monday morning for Kelly Jean Lomberk, a treasury management officer (TMO) for JPMorgan Chase & Co. in Iselin, NJ. Her day had started as usual, she'd had her coffee and she was in the office planning her schedule for the week.**

When she received an email from May Guerrero, one of Commercial Banking's fraud investigators, asking her to call a client to validate a transaction, she didn't think too much of it. She'd performed these validations before, and out-of-pattern transactions can happen. Guerrero had called the client and spoken with the initiator of the transaction, who confirmed she was "confident" it had been properly validated, but Guerrero wasn't comfortable and escalated to Lomberk, the client's TMO.

Lomberk picked up the phone and called Steve\*, the client's corporate treasury director. She described the transaction, a payment for almost \$200,000 to a new vendor, and asked if it was valid.

The client uses robust internal validation processes. These include in-person validations for new relationships and a

callback process for existing relationships that requires calling a contact using a known telephone number. Still, Steve instinctively felt something wasn't right.

"Steve instantly focused on our concerns and took action," said Lomberk when asked about the fraud attempt. "He cancelled the payment immediately and began researching it internally."

The payment recipient was a new vendor for the client and had been validated in person, but the payment instructions were sent via email following the in-person meeting. Unfortunately, the vendor's emails had been hacked and were being surveilled by cybercriminals.

By exploiting a software vulnerability, the hackers were sending and receiving emails undetected through the vendor's legitimate email account and were covering their tracks using rarely opened subfolders. The cybercriminals knew when the meeting would take place and timed a fake email, which looked like a follow-up from the new vendor, with payment instructions that would direct funds to the cybercriminal's bank accounts. Later, the cybercriminals

sent another email to the client, this time with a payment request, which the client had processed and submitted.

"JPMorgan Chase uses sophisticated algorithms to detect and escalate out-of-pattern payments," said Guerrero. "Clients who act quickly—before the payment is released—are more likely to prevent a fraud attempt."

After cancelling the fraudulent payment and saving his organization almost \$200,000, Steve closed the gap in his organization's validation processes. Within minutes of the call from Lomberk, he added a new validation form to be completed during an in-person review for any new vendor relationship. The form includes a field for contact details to use during verbal confirmations of account instructions.

Lomberk insists Steve is the hero for stopping this fraud attempt. "Not every client is receptive to our validation calls, but Steve not only listened to our concerns about the transaction, he also strengthened his organization's processes to prevent it from happening again." ■

*\*Steve's full name is omitted due to privacy considerations.*

# Attracting Skilled Talent to Cybersecurity

*Meagan Ringel is the Head of Operational Excellence for Cybersecurity Operations at JPMorgan Chase & Co., responsible for establishing standards of performance and executing on opportunities to improve efficiency and effectiveness. The Operational Excellence team helps drive goal and priority alignment across Cybersecurity and Technology Controls stakeholder groups, conducts root cause analysis, monitors performance indicators, and implements improvement opportunities. In addition to strategy and risk monitoring functions, the Operational Excellence team maintains two line functions that contribute to the firm's preventative and detective defenses.*

*During her 15 years at JPMorgan Chase, Ringel has performed roles in Compliance and Technology, including managing a financial crimes investigative unit and managing the delivery of strategic technology initiatives to support Commodities Trading and Credit Risk within the Investment Bank.*

**Q. Experts report hundreds of thousands of unfilled cybersecurity jobs and predict that the gap will continue to grow over the next several years. In light of the growing gap between skilled cybersecurity workers and open cybersecurity jobs, how can companies attract qualified talent?**

A. The language we use to describe the cybersecurity field can seem very specialized, but the reality is that the skills needed in cybersecurity translate well from several other disciplines—having a business, operations, or risk perspective are valuable in problem solving.

My own career path has been varied; I started in software engineering and later moved into a compliance role leading a team of financial crimes investigators focused on anti-money laundering (AML) and terrorist financing. I learned about developing risk-based approaches to defining monitoring rules and investigative procedures. Cybersecurity was a natural progression combining my background in

information technology (IT) with financial crimes investigations. To successfully attract talent to cybersecurity, we need to make the industry more relatable and demonstrate that cybersecurity isn't just about hackers.

**Q. In the cybersecurity field, female workers are significantly under-represented. What challenges discourage women from pursuing the field?**

A. Similar to the IT field, cybersecurity lacks diversity in our workforce, and any time there is a lack of diversity in a particular industry, it can become a barrier for anyone who prioritizes working in a field that reflects their own community.

People want to work where they know they are valued and respected. The lack of diversity itself is a barrier to entry, which means the industry loses the benefits of broad experience and problem solving that diversity promotes—benefits that are critically important to stay ahead of cybercriminals.



“... the skills needed in cybersecurity translate well from several other disciplines—having a business, operations, or risk perspective are valuable in problem solving.”



## MEAGAN RINGEL

HEAD OF OPERATIONAL EXCELLENCE FOR CYBERSECURITY OPERATIONS  
JPMORGAN CHASE & CO.

Understanding the root causes underlying the gender gap will help overcome these challenges. Recently, there's been a lot of progress in our education system, as well as the private and public sectors, to raise awareness about the importance of STEM (science, technology, engineering and math) careers for both men and women. Personally, I'm fortunate that JPMorgan Chase & Co. celebrates diversity, and we continue to lead initiatives to improve our representation of diverse talent.

### **Q. How is JPMorgan Chase encouraging diversity in cybersecurity?**

A. The firm practices inclusion, continually fostering a community with a shared purpose. Diversity in our leadership helps reflect and represent a broad range of perspectives. They pay it forward with coaching, mentoring, leading by example and ensuring we recruit traditionally and cognitively diverse talent—and we invest in our communities to build a pipeline of future leaders.

### **Q. What drew you to the field of cybersecurity?**

A. Cybersecurity adds a layer of excitement. The importance of the work and understanding what's at stake makes every day meaningful. The impact of the work of cybersecurity professionals is profoundly valuable and far-reaching. It helps protect the firm, our clients and our national and global infrastructure.

### **Q. The impact of your work in cybersecurity hits close to home too. What are the biggest threats for individuals, and how can they help protect themselves?**

A. Social engineering, specifically phishing, is the most common vector of attack against individuals because it is low-cost and particularly effective for cybercriminals, who continuously evolve their schemes to evade detection. All too often I hear from someone whose identity was stolen through a phishing attack. When asked, my advice always starts with a conversation

about what's at risk. Sometimes people are surprised to learn that their mobile phones and even smart home systems expose them to a cyberattack.

To protect themselves, individuals should follow best practices such as:

- » Use secure credentials with strong passwords and set up multifactor authentication
- » Practice good cybersecurity hygiene while using devices that are connected to the internet, including smart home devices and mobile phones
- » Protect sensitive information
- » Never connect to unsecured Wi-Fi, especially if banking apps are installed on the device
- » Keep devices and systems updated

Individuals should always stay informed about cyberschemes—and know how to recognize a threat *before* it becomes an issue. ■

# Women in Cybersecurity

Statistics show that women work in nearly one-quarter of cybersecurity-related jobs around the globe, and as the awareness for greater diversity and culture shift around technology grows, that number is expected to rise over the next few years. At JPMorgan Chase & Co., the firm encourages increased diversity to ensure employees with a varied skillset work in cybersecurity operations and fraud prevention helping to protect both the firm and our clients. We asked a few of the leading women working cybersecurity operations at the firm about best practices to help clients avoid fraud attempts.



## **JESSICA COLVIN**

GLOBAL HEAD OF VULNERABILITY MANAGEMENT & ASSESSMENTS  
JPMORGAN CHASE & CO.

Colvin is responsible for the discovery, response, remediation, and governance of technology vulnerabilities.

ADVICE: Whenever possible, set your personal computer and devices to auto-update so they always have the latest security.



## **FARRAH PATTERSON**

PRODUCT MANAGER FOR DIGITAL FORENSICS SERVICES  
JPMORGAN CHASE & CO.

Patterson drives firmwide engagement and strategy supporting digital forensics.

ADVICE: Share less and be wary of what you post on social media. Criminals can gather information from your profile that could help them gain access to more sensitive and valuable data.



**RACHAEL SCHULDER**

CUSTOMER SUCCESS LEAD FOR THE CYBER DEFENSE & FRAUD PRODUCT  
JPMORGAN CHASE & CO.

Schulder establishes the end-to-end engagement model for the Cyber Defense & Fraud Product facilitating ongoing client alignment and satisfaction.

ADVICE: Mobile apps can collect personal data or tap into location tracking, cameras, or microphones without users even knowing. When downloading apps, ensure permissions are restricted to only those capabilities required to operate them.

**MICHELLE SHAW**

OPERATIONS LEAD FOR OVERSIGHT AND CONTROLS  
JPMORGAN CHASE & CO.

Shaw manages daily operations including logistics, governance, training and client engagement.

ADVICE: Create separate email accounts for sensitive and non-sensitive websites, e.g. banking, online shopping, etc. Never click on a link or file in an email until you validate the source, and never enter personal information in an email or text message.

**TRICIA REILLY**

PRODUCT MANAGER FOR THREAT AND FRAUD INTELLIGENCE  
JPMORGAN CHASE & CO.

Reilly implements the firm's strategic roadmap for the detection and prevention of fraud.

ADVICE: Always be wary of emails from unknown sources. Take the time to read to ensure that it is from a trusted source, and don't use public Wi-Fi ever!



# Cyberfraud Scenarios

## Scenario:

**Fraud attempts can occur any time and impact any organization. Would you know what to do if you or your employees received a suspicious email or new payment instructions?**

In this cyberfraud scenario, a cybercriminal attempts to extract funds from a payments employee using a fake look-a-like domain. We look at a simulated fraud attempt and show employees suggested protocols for validating a payments request before releasing the funds.

**Important to remember:** Clients who do not use appropriate fraud-prevention tools increase their risk of losses. Clients are liable for all losses incurred for payments originated using any authorized users' security credentials or the credentials of others who have designated transaction authority. ■





# WHAT TO DO?

An email request comes in from a known executive or vendor . . .

Does the email ask for a change in bank and/or account number, or does it have unusual urgency?

**YES**

**Perform validation**

Does the email address look legitimate?

**NO**

**REMEMBER!**

Always validate the sender's email address: hover over the email address or hit *Reply* and carefully examine the characters in the email address to check that they match the **exact** spelling of the company domain and individual's name.

**YES**

Did you call the sender using a known telephone number?

**OR**

Did you validate the request in person?

**NO**

**REMEMBER!**

Always validate a new request in person or by phone using a known telephone number.

**NO**

**YES**

Has the payment been subject to multiple approval levels?

**YES**

**Release funds for payment processing**

**80%**  
of organizations  
experienced business  
email compromise  
in 2018\*

\*According to *The 2019 Association for Financial Professionals Payments Fraud and Controls Survey Report*

The email may be part of a business email compromise scheme.

Ensure policies enforce best practices including dual payment approvals.



## Did you know?

JPM Coin isn't money nor legal tender; it's a digital coin and each JPM Coin equals one US dollar.



# The Firm Plans to Launch JPM Coin

**The prevailing attitude around cryptocurrencies is one of intrigue and suspicion: There's enormous potential, yet concerns about the technology and illegal use remain. That might soon change, as JPMorgan Chase & Co. takes its first steps into the cryptocurrency waters by launching JPM Coin.**

The first digital asset backed by a major US bank, JPM Coin is a digital coin designed to facilitate instantaneous money transfers over a blockchain network. Umar Farooq, Head of Digital Treasury Services and Blockchain, said the firm created JPM Coin to facilitate exchange of value, over a blockchain network.

But JPM Coin isn't money nor legal tender. "It's a digital coin representing US dollars held in accounts at JPMorgan Chase," Farooq clarified, adding that, "A JPM Coin always equals one US dollar."

Farooq said the firm has taken this step because it's in a unique position to do so. On average, the bank processes \$6 trillion in daily payments for clients around the world, and it is constantly looking for ways to increase the efficiency, speed and availability of transfers.

"As a globally regulated bank, we believe the JPM Coin can achieve this in a secure and responsible way with the oversight of regulators," said Farooq. "Ultimately, we believe that JPM Coin can also yield

significant benefits for clients utilizing blockchain applications by reducing counterparty and settlement risk and enabling instant value transfer."

Here's how it works: First, a client converts a set amount of money in their deposit account into an equivalent number of JPM Coins. Next, they transfer those coins via a blockchain network to the designated beneficiary account. The beneficiary account receives the coins and redeems them for the equivalent US dollars. This all happens instantaneously and can be done 24 hours a day, seven days a week, according to Naveen Mallela, Head of Asia Pacific Digital Treasury Services and the designer of JPM Coin.

It might seem surprising that JPMorgan Chase would issue its own digital coin but only to the casual observer. Mallela says the firm has always championed blockchain technology and supports tokens, as long as they're subject to proper controls and regulations.

Farooq asserts the firm is in a strong position to apply blockchain technology for a few different reasons. Chief among them is its \$2.6 trillion fortress balance sheet backing the JPM Coins and its strength in cybersecurity and innovation. "JPMorgan Chase spends hundreds of millions of dollars each year on cybersecurity and has a Blockchain Center

As a globally regulated bank, we believe the JPM Coin can achieve this in a secure and responsible way with the oversight of regulators.

**UMAR FAROOQ**

HEAD OF DIGITAL TREASURY SERVICES  
AND BLOCKCHAIN  
JPMORGAN CHASE & CO.

of Excellence that is leading innovation in financial circles," said Farooq.

JPM Coin is currently in the prototype stage and has successfully transferred money between accounts in early testing. It will be rolled out in a pilot with multiple institutional clients later this year. As of now, there aren't plans to make this available to retail.

While only used for the US dollar, Mallela says JPM Coin will eventually be extended to other major currencies based on client demand. "The product and technology capabilities are currency agnostic," he added. ■

# Logon Awareness

## Did you know?

According to the Federal Bureau of Investigation's 2018 Internet Crime Report\*, in 2018, total losses from cybercrimes reached

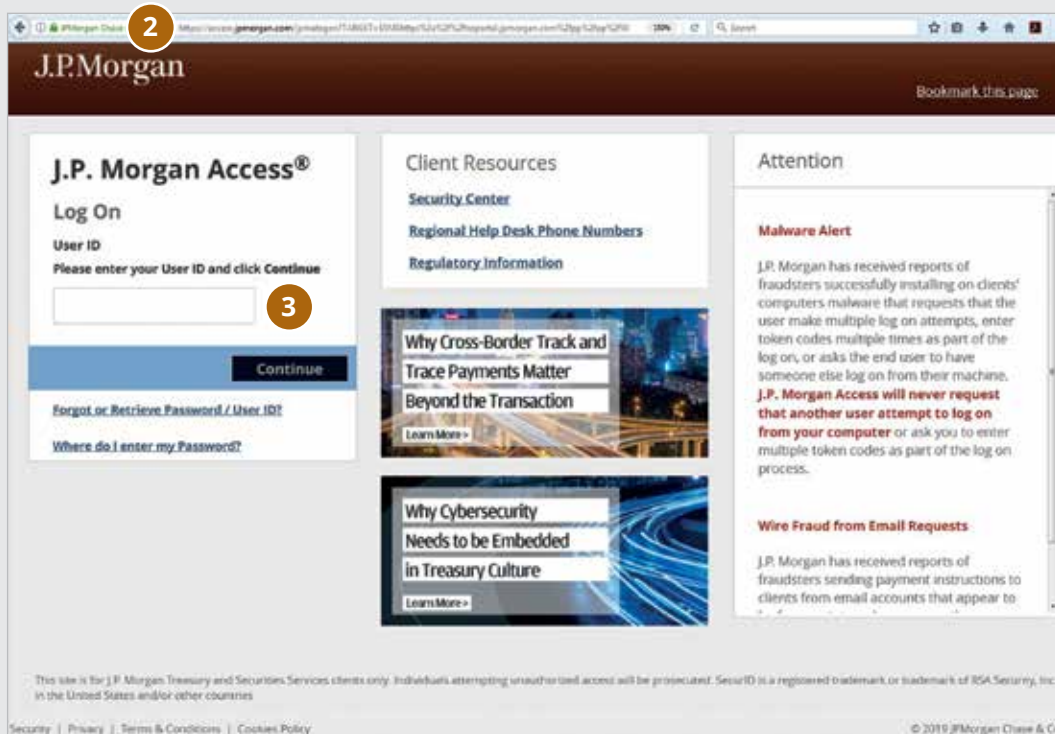
# \$7.45B

up from \$800.5 million in 2014.

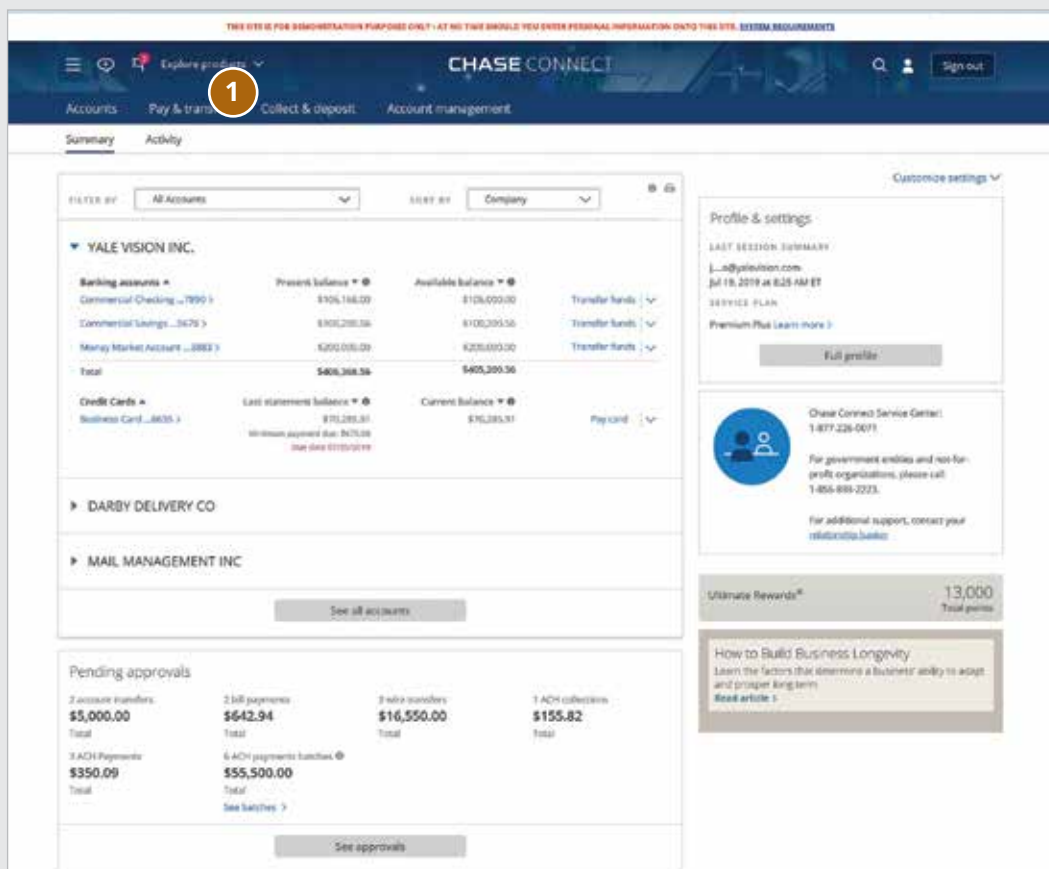
\*ic3.gov

**Criminals will try to replicate the look and feel of a portal page or use a demonstration site, if available, to obtain users' credentials. Here are some tips to help guide developers, sales representatives and service teams, when building—or using—websites.**

- » Always clearly identify demonstration sites with a banner on the page to caution users to exercise care, e.g., “Demo site; Do NOT enter personal information.” This will help stop criminals from using the site to trick clients into providing usernames, passwords or financial information. **1**
- » Check that a page's web address begins with “https://” because the “s” indicates the site is secure. URLs beginning with only “http” indicate that the site is *not* secure. **2**
- » Legitimate login screens will not ask for more than your user name and password before granting access to the platform. A fake login page may ask users for their secure ID token information to provide secondary authorization. Do not provide more than your user name and password. **3**
- » Users should be aware of unusual delays loading pages or “Please Wait” messages that appear; these could indicate that criminals are trying to collect information.
- » Spelling errors or missing characters, particularly in small fonts at the bottom of a page, are another indication that a site may be fake.
- » Always report concerns about a login page immediately using only known contact information, and never use telephone numbers, email addresses or links in suspicious pages.



J.P. Morgan Access® Logon Page



Chase Connect® Demo Site Logon Page

(All client information presented is fictitious and any similarity to real entities is purely coincidental.)







# Protect Your Phone (and Your Number) from Cybercriminals!

**Your debit card isn't the only thing requiring a secure PIN. Your mobile carrier account should have one too.**

Cybercriminals are using a fraud scheme that interrupts mobile phone service by “porting” a victim’s cell phone number to a new carrier without their knowledge. When the victim notices a service interruption in cell phone service, they call their mobile carrier for support only to find out that their phone number no longer exists in the system. This year, approximately 40,000 mobile owners will fall victim to this criminal porting tactic.

Cybercriminals are able to trick telephone companies into thinking that they are the cell phone owner by providing the carrier a phone number, home address and the last four digits of a Social Security number. They then use the cell phone number to manipulate multifactor authentication verification and gain access to other accounts—including bank accounts saved on the mobile device. All the credentials and sensitive information contained on mobile

devices—from banking to travel plans to personal medical records—make mobile devices a rich target for criminals.

Once cybercriminals have accessed your personal data, they can launch additional cyberschemes, such as:

- » Using your mobile device to create Distributed Denial of Service (DDoS) attacks on a computer system
- » Using your mobile device to open other accounts by leveraging your credit history and other personal information
- » Installing malware to steal your personal information or take control of your device

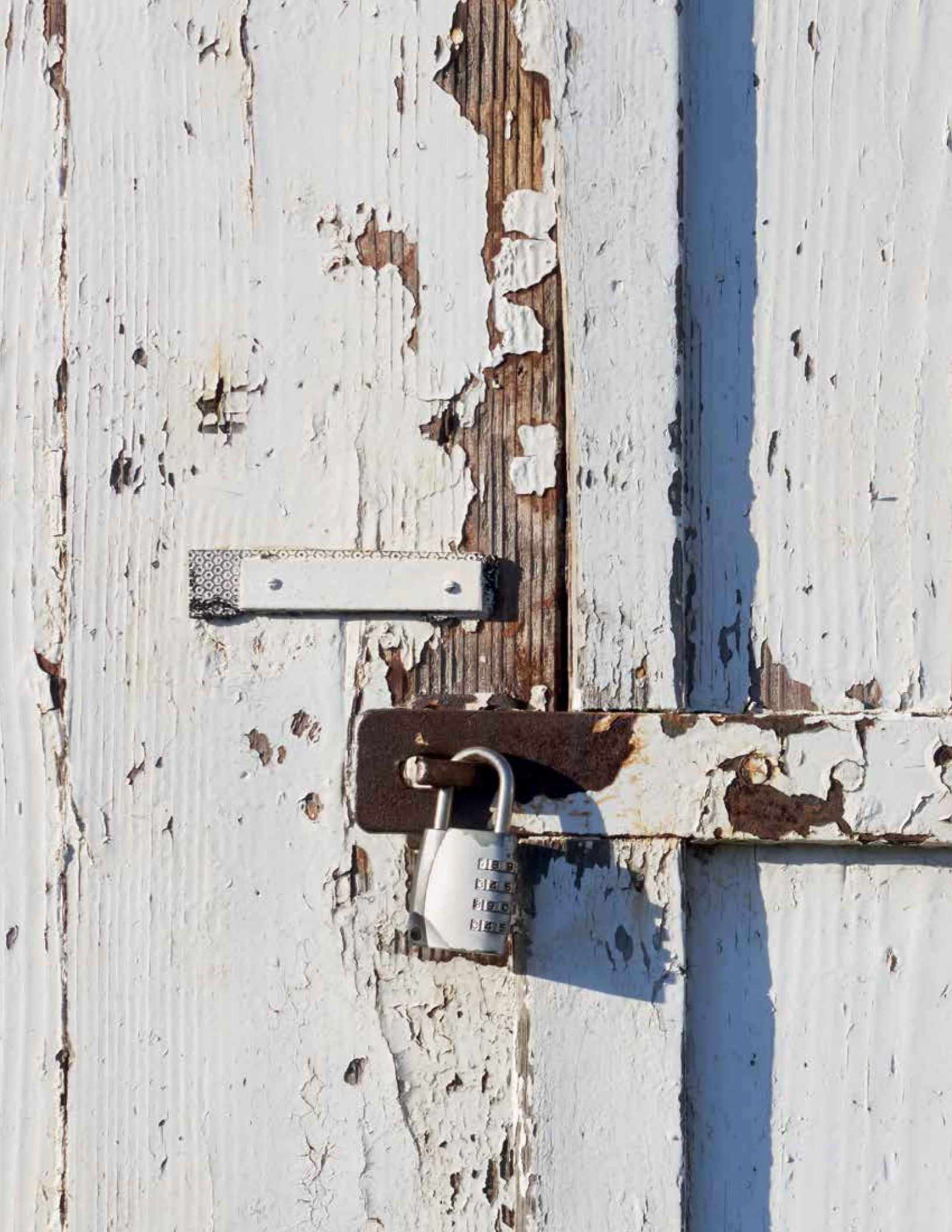
## What to Do

Contact your mobile phone company to learn more about security options. In many instances, you can set up a unique PIN to better secure your account and help prevent criminals from impersonating you. You also can notify your service provider that they must request the PIN before

making any changes to your account. Criminals have to know that unique code to access your account, which could make all the difference.

Here are some additional best practices to follow:

- » Implement multifactor authentication on your accounts and mobile devices (e.g., thumbprint, facial recognition, passcodes, etc.)
- » Use security questions with tricky answers
- » Always use unique, strong and different passwords on all accounts
- » Install an anti-virus application on your mobile device
- » Securely destroy old cell phones
- » Always contact your service provider if you notice a service disruption
- » Do not answer “phishy” phone calls or messages and report them to authorities ■





# Cybersecurity Awareness: Passwords and Password Managers

Creating strong passwords is critical to protecting your personal information including your business and personal accounts. Experts say the longer and more complex the password—for example using a series of upper- and lowercase letters, numbers and symbols—the better it can help protect your personal information.

## Best Practices

- » Create unique passwords with at least eight characters. Try something more complex: use a book, song title, or a line from a poem as a password—something unique to you:
  - 2BorNot2B\_ThatIsThe?
  - DONTstop.B3li3v1n
- » Do not use the same password for more than one account
- » Include upper- and lowercase letters and numbers and special characters, such as: ! & \$ # @ ?

## Benefits of a Password Manager


- » One single password: You only need to remember the master password to the password manager.
- » Secure password suggestions: A built-in password generator will suggest secure and unique passwords whenever you create or update an account.
- » Auto-entry: Once you enter the login credentials for a site, the password manager will autofill this information whenever you return to the site.
- » Password syncing: Login data syncs in the cloud, so passwords are available on all of your devices and across users.

## Using a Password Manager

Consider using a password manager with state-of-the-art encryption to help you better secure multiple passwords for all accounts.

A good password manager should offer these key features:

- » Secure sharing across users, such as other family members or colleagues.
- » Digital legacy contact; this allows you to designate an emergency contact who can access your online accounts in case of emergency.
- » Digital vault; this provides a repository where you may enter information such as a passport number, answers to security questions, or Wi-Fi passwords.
- » Multifactor authentication. ■



J.P. Morgan and Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (JPMC). Any example of cyber or other fraud or loss in this material is for illustrative purposes only; any similarity to any actual event or person is unintended and unfounded. This document was prepared exclusively for the benefit and internal use of the party to whom it is delivered (each, a "Recipient"). The content is not intended as, nor shall be deemed to constitute or contain, advice on which the Recipient may rely; does not constitute in any way JPMC research, and should not be treated as such; and is confidential and proprietary to JPMC. The content may not be copied, published, disclosed or used, in whole or in part, for any purpose other than as expressly authorized by JPMC. This document is not intended, nor should it be relied upon, to address every aspect of the subject discussed herein. The Recipient 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 Recipient.