









Cybersecurity & Fraud Protection

September 2023

Current and emerging threats

Every company, regardless of size or Industry, is at risk to common threats:

 Business Email Compromise	 Social Engineering
 Fraud	 Ransomware
 Systems Vulnerabilities	 Outdated Software/ Hardware
 Insider Threats	 Human Error Ignorance



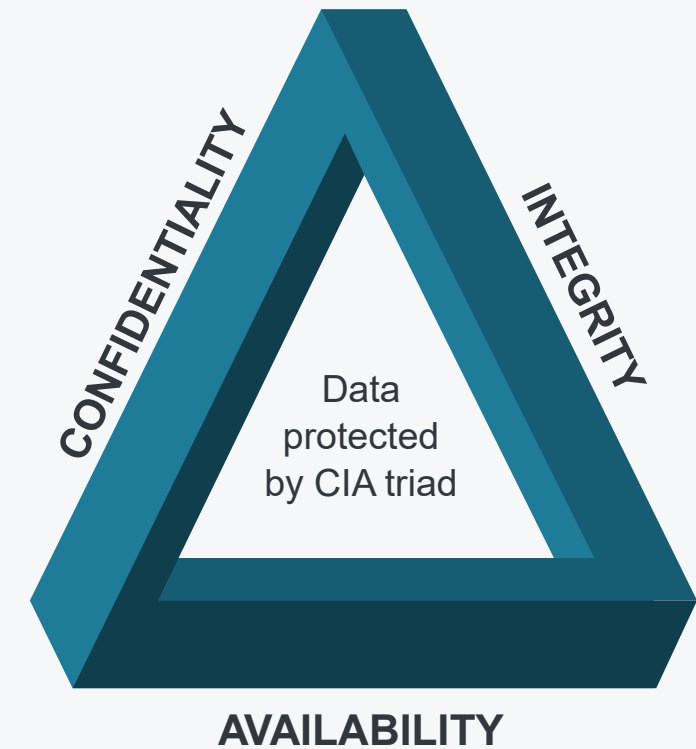
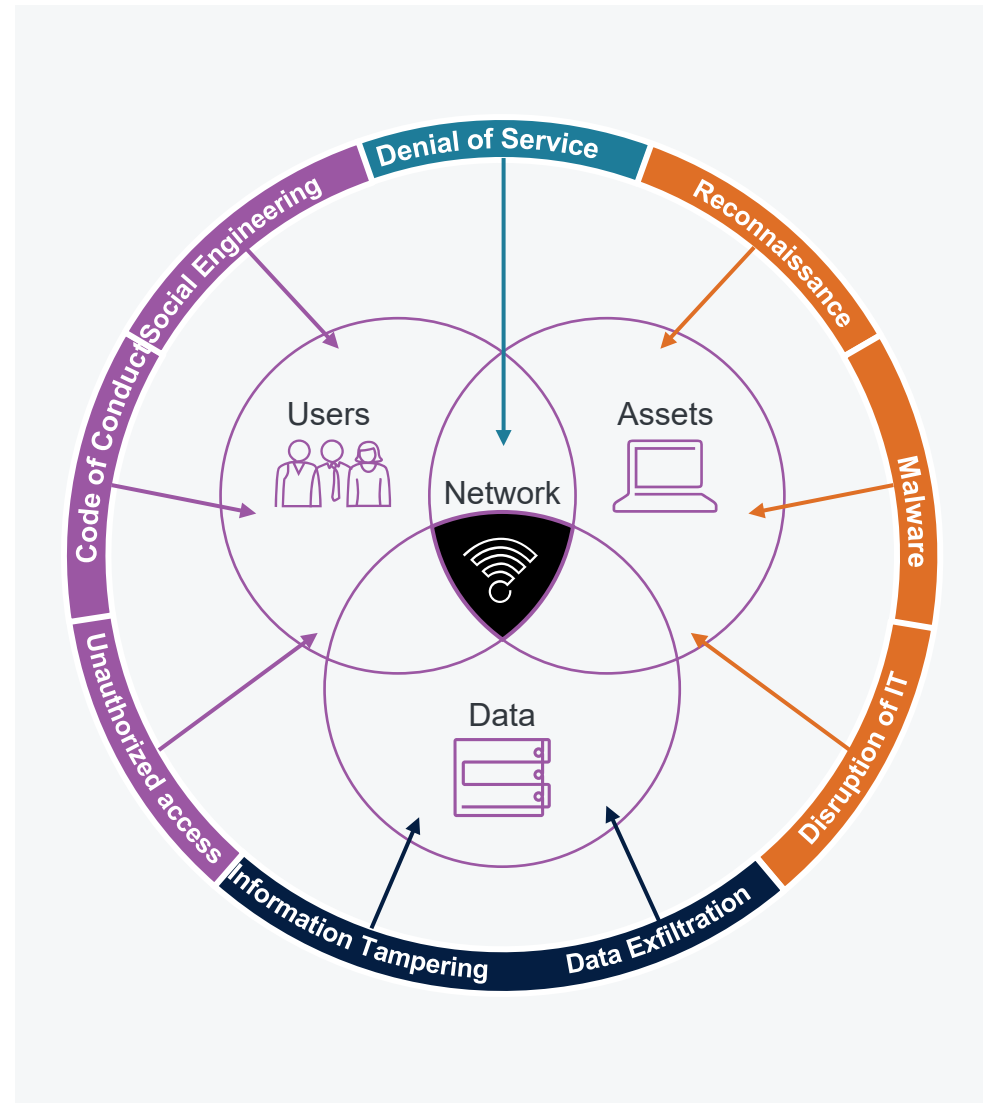
¹ 2022 FBI IC3 Report

Primary targets & vectors of attack

\$10.3B

In Potential
Losses Reported in 2022¹

- Cybercriminals target key components that keep your business running. Consider your:
 - Data
 - Intellectual Property
 - Software and OT Systems
 - Money
 - People



¹ 2022 FBI IC3 Report

Cybercrime in the headlines 2023

Industry Focused Attacks	Tallahassee hospital forced to operate offline, working with FBI to address 'IT security event'
Critical Infrastructure	Radiation Alert system in water treatment facility disabled by two 3 rd party insiders
Preventable Attacks	Misconfigured APIs, ION Group (banking/financial services software)
Money Laundering Crypto	Man pled guilty to laundering crypto from ransomware attacks
Loss of Production	Ransomware attack forced Dole to shut down production plants in North America
Western Financial Sector Threats	Russian-affiliated threat actors announced impending attacks against US and European banks and financial markets



The Power of Artificial Intelligence

AI can empower business to drive growth in an increasingly competitive business landscape.



Automated Processes



Data-Driven Insights



Personalization

Major Financial Impact...

 **\$4.4T**

Added to the global economy annually¹

Opportunities

- Automation and Efficiency
- Data Analysis
- Customization
- Enhanced Security
- Analytics and Forecasting
- Innovation
- Process Optimization

Challenges

- Data Quality
- Talent Gap
- Ethical Considerations
- Integrating Systems
- Trust
- Cybersecurity
- Cost and ROI

Cyber & Fraud Threats

- Data Breaches
- Model Poisoning
- Bias and Discrimination
- Account Takeovers
- Synthetic Identity Fraud
- Insider Threats
- Deepfake Threats

¹ McKinsey & Company, *The economic potential of generative AI*, June 2023

Deepfakes | The Dark Side of Artificial Intelligence

Improper use of AI and synthetic media pose a threat to national security, law enforcement and the financial domain

Deepfakes are realistic, AI-generated videos, images, audio, and text of events designed to deceive targeted groups or individuals

- Inclination to believe what you see makes them effective in spreading mis/disinformation
- Low cost of resources needed to produce them raises the likelihood of successful attacks

In practice, threat actors leverage chatbots and technology developed from large language models to simulate human activity

- Business Email Compromise
- Spear-phishing
- Fake websites and profiles
- Ransomware
- Voice clones for imposter scams, extortion and financial fraud

Example Deepfake Online



Multi-faceted mitigation is critical

- Collaboration between cyber professionals, financial institutions and law enforcement
- Public education, awareness and media literacy
- Regulation
- Detection mechanisms via AI/ML innovation (real-time monitoring, anomaly detection and incident response protocols)

Ransomware

2,385

Ransomware complaints received by the FBI¹

\$34.3M

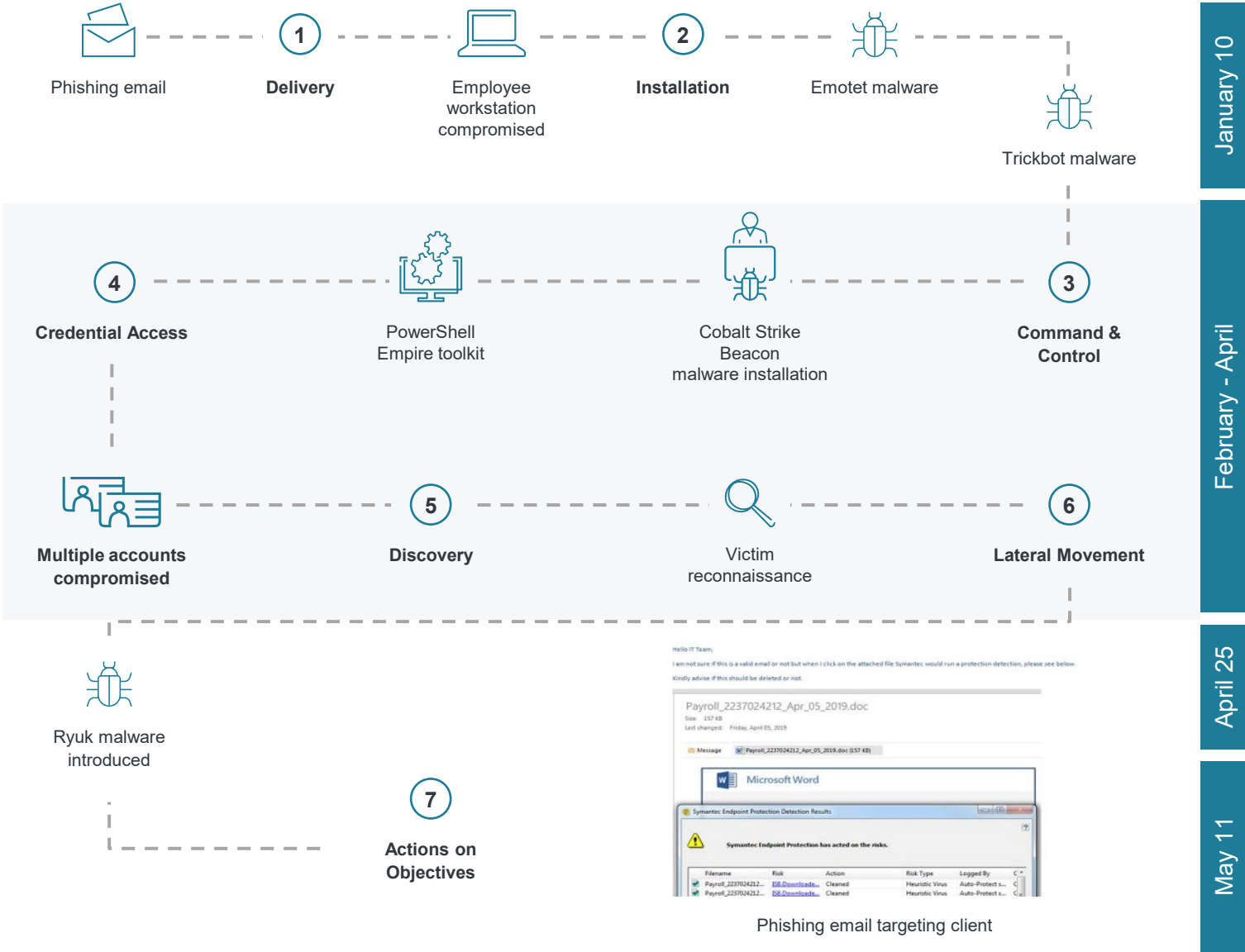
In Adjusted Losses reported to the FBI¹

- Loss of the ability to run your organization and potential permanent loss of data
- Key considerations:
 - How much is the ransom?
 - Should I pay ransom?
 - The FBI does not support paying a ransom to a cybercriminal.
 - Payment does not guarantee an organization will regain access to its data.
 - Paying the ransom may embolden cybercriminals to launch more attacks.
 - How do I ensure my company is resilient?



¹ 2022 FBI IC3 Report

Anatomy of a ransomware attack



Business email compromise (BEC) & impersonation

- Cybercriminals use executive, business partner and vendor email impersonation to trick you into sending them money or data. Common tactics include:
- Phishing attacks
- Use of compromised email accounts
- Claims a bank account can't be used due to an audit
- Multiple account changes sent to victim during attack
- Use of inbox email forwarding rules to send emails to fraudsters

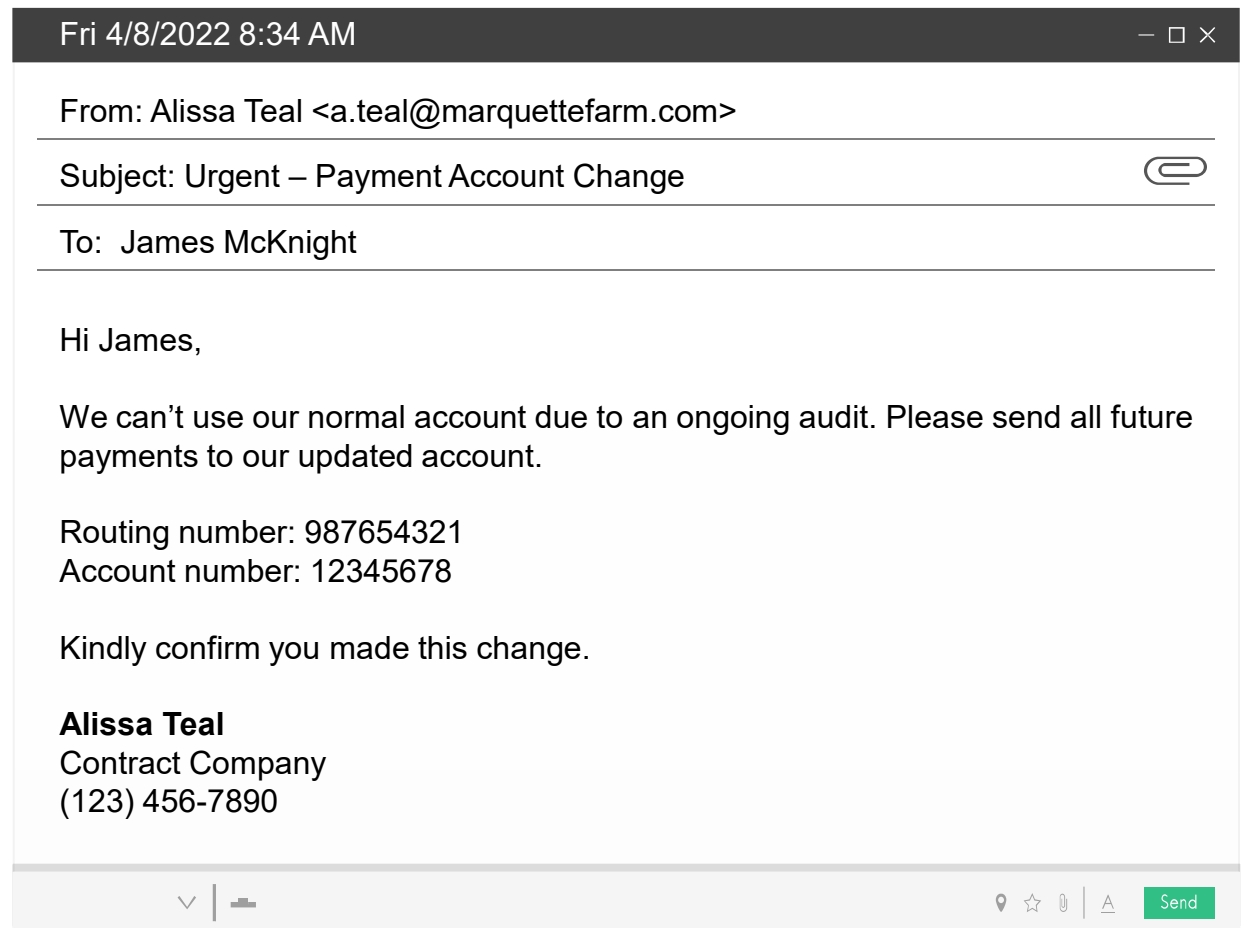
21,832 Victims reported to the FBI¹

\$2.7B Adjusted Losses reported to the FBI¹

Criminals Register Look-alike Domains

Good domain:
marquettefarm.com

Bad domains:
marquettefarm**s**.com,
marquette**fram**.com,
marquettefarm.**co**,
mar**g**uettefarm.com,
marqu**ete**farm.com



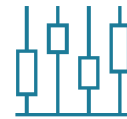
² 2022 FBI IC3 Report

BEC prevention & response



The Critical Control

- ✓ Perform a callback to the person making the request
- ✓ Use a phone number retrieved from a system of record to validate requests for payment, change of payment instructions or contact information
- ✓ Reject out of band payment processes



Additional Controls

- ✓ Establish written policies implementing mandatory callbacks
- ✓ Take calls from your bank regarding unusual transactions seriously
- ✓ Train employees on internal payment verification policies and BEC threats
- ✓ Encourage employee questions and holding a payment if it's suspicious



Response

- ✓ Notify your bank immediately
- ✓ File a report with the FBI's Internet Crime Complaint Center
- ✓ Contact your local FBI field Office
- ✓ Notify other law enforcement agencies as appropriate

These steps are critical to maximize chances for recovery

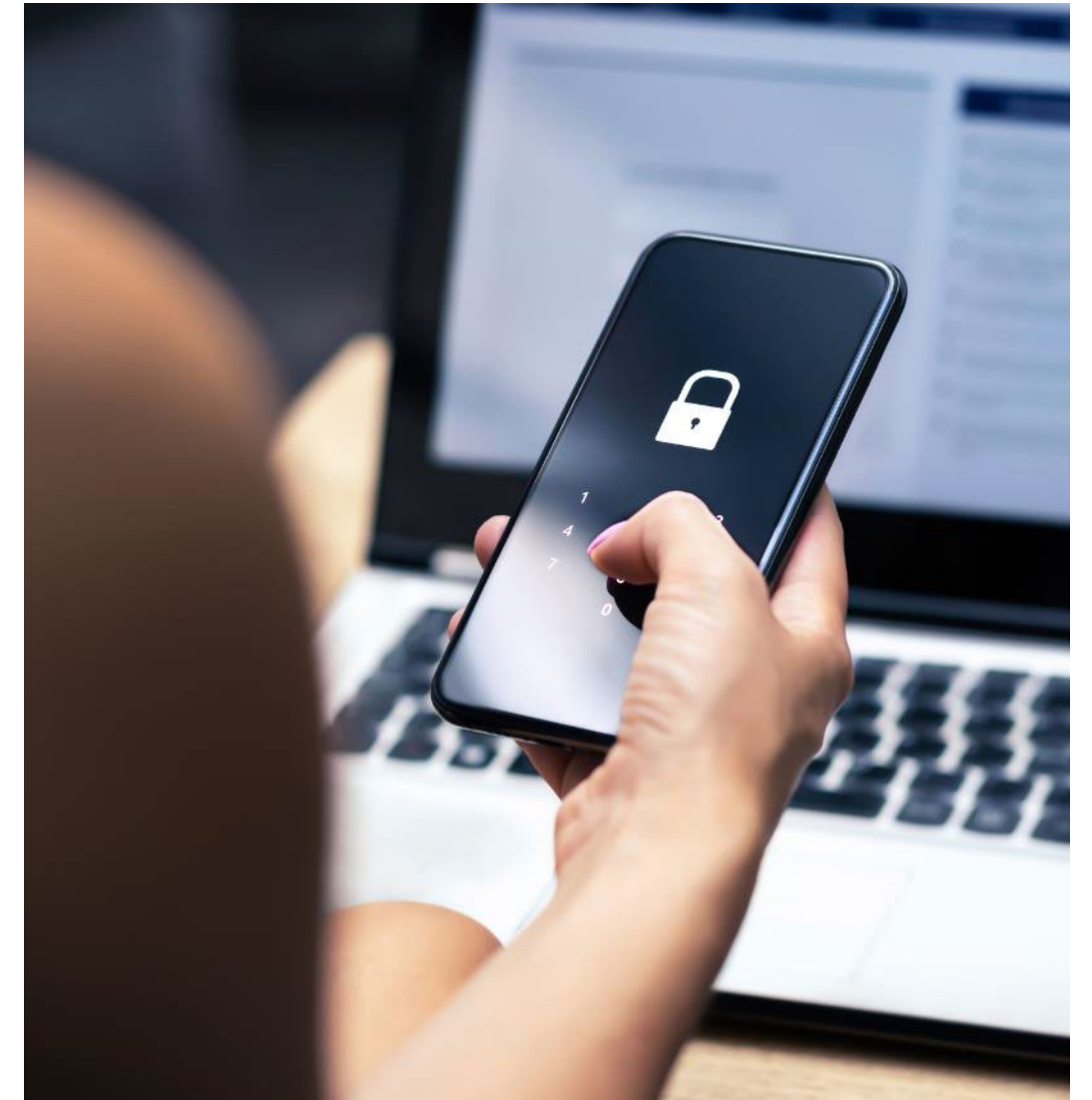
Phishing

300,497

Victims reported to FBI in 2022¹

Practice of sending blanket emails to large groups or targeted emails to individuals as means to commit financial fraud or infect or gain access to systems.

¹ 2022 FBI IC3 Report



Phishing indicators

\$52,089,159

In losses in 2022¹

- Sender name is vague or generic
- Sender address has a suspicious domain
- Email includes an external banner indicating it's coming from outside the company
- Urgent or authoritative language
- Demands for a quick response
- PDF attachment "View File" button in a link, not a PDF

¹ 2022 FBI IC3 Report

File Home Send / Receive Folder View Add-ins Help Banker Utilities Acrobat

New Email New Items ▾ Ignore Clean Up ▾ Delete Junk ▾ Report Email ▾ Blocking Options ▾ Communications Toolkit Reply Reply All Forward IM ▾ Meeting More ▾

New Delete JPMC Email Tools Respond

Thu 4/30/2020 5:30 AM

Accounts Receivable <accounts@accountstatus.com>

Invoice due

To [redacted]

Retention Policy JPMC_Inbox_180 (6months) Expires 10/27/2020

EXTEERNAL SENDER – Review for Phishing. Report if suspicious. For help visit go/Phish

Message Invoice.pdf (377 KB)

Your Invoice is Past Due

Hello,

Attached is your past due invoice, and is ready for your review at Secure Online Invoice Management Portal

Regards.

Check fraud is on the rise

Whether theft, forging or counterfeiting, check fraud continues to be a problem—and your organization needs to plan for it.



63%

of organizations reported being impacted by check fraud¹



680K

check fraud complaints filed in 2022, more than double the previous year³

FIRST HALF OF 2023

305 USPS letter carriers robbed on the job⁴
25K+ incidents of high-volume mail theft reported⁴

“U.S. Postal Service warning users against sending checks through the mail”²

Front-Of-Check Fraud

Altered Checks | Criminals alter the name or payment amount before depositing

Counterfeit Checks | Criminals use printers and desktop publishing software to create counterfeit checks

Back-Of-Check Fraud

Improper Endorsements | Criminal forges endorsement, or chooses not to endorse at all

Mobile Deposit Fraud | Usually perpetrated by the intended recipient, sometimes to double-cash paychecks

¹ 2023 Association for Financial Professionals (AFP) Payments Fraud Survey

² 2023 Delano, Jon. “U.S. Postal Service warning users against sending checks through the mail” CBSNews.com, June 20, 2023, <https://www.cbsnews.com/pittsburgh/news/u-s-postal-service-warning-checks-mail/>

³ FinCEN Alert, FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail, February 27, 2023

⁴ United States Postal Service, USPS, Postal Inspection Service Roll Out Expanded Crime Prevention Measures to Crack Down on Mail Theft, Enhance Employee Safety and Strengthen Consumer Protections, May 12, 2023

What to expect when check fraud happens

Overview of the resolution process

1 | Claim is reported

The client informs the bank and reports a claim

2 | Documentation is provided

The client provides the required documentation to Chase

3 | Investigation

Back-of-check fraud

Chase makes a claim on the bank where the check was deposited

- **If deposited at a Chase bank**, it could take up to 15-20 business days if all the required documents have been provided
- **If the bank was not Chase**, it could take six months or more
- We reach out to the other banks with the claim; however, they control the response time frame

Mobile Deposit Fraud

Chase makes a claim on remote deposit capture bank

- **If deposited at a Chase bank**, it could take up to 15-20 business days if all the required documents have been provided
- **If the bank was not Chase**, it could take up to 30 business days
- We reach out to the other bank with the claim; however, they control the response time frame

4 | Resolution

The claim is paid or denied. If there is a request for more information, then you must go back to Step 3.

Front-of-check fraud or counterfeit

- Internal Chase investigation could take up to 15-20 business days if all the required documents have been provided

Other reasons your claim could be delayed

- The depositing bank could ask for more documentation such as W-9 forms, tax documents, police report, driver's license or a payee-signed affidavit.
- The case could also involve an altered check or dual payees

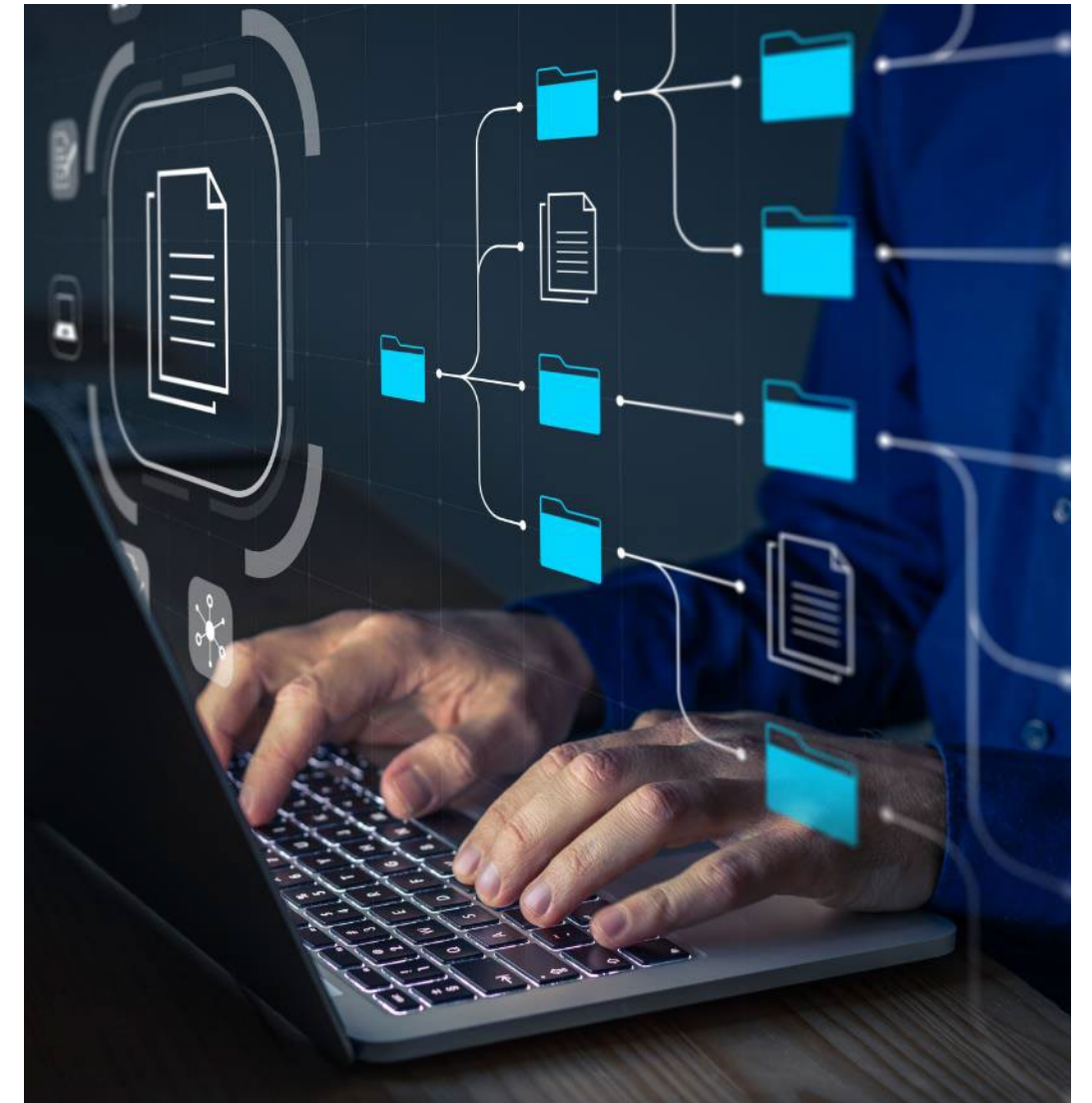
Supply chain risk

742%

YoY Increase in Software Supply Chain Attacks¹

- Third parties are a key entry point to attack businesses.
- Treat vendors like vulnerabilities
- Mitigate their potential impact
- Create and enforce standards for engagement and integration
- Require adherence to industry specific programs

¹ Sonatype 2023 State of the Software Supply Chain Report



Prioritize your risk, assets and threats

- Time is money and cybersecurity is a critical business decision.
- Be proactive and vigilant now, to protect your organization's data, finances and business processes. Fortify your defense strategy, by taking inventory of:
 - Threats are you facing
 - Where you have risk
 - What is most valuable
 - The minimum requirements needed to operate your business



\$4.35M | Average Cost of a Data Breach Globally¹

\$9.44M | Average Cost of a Data Breach in the US¹

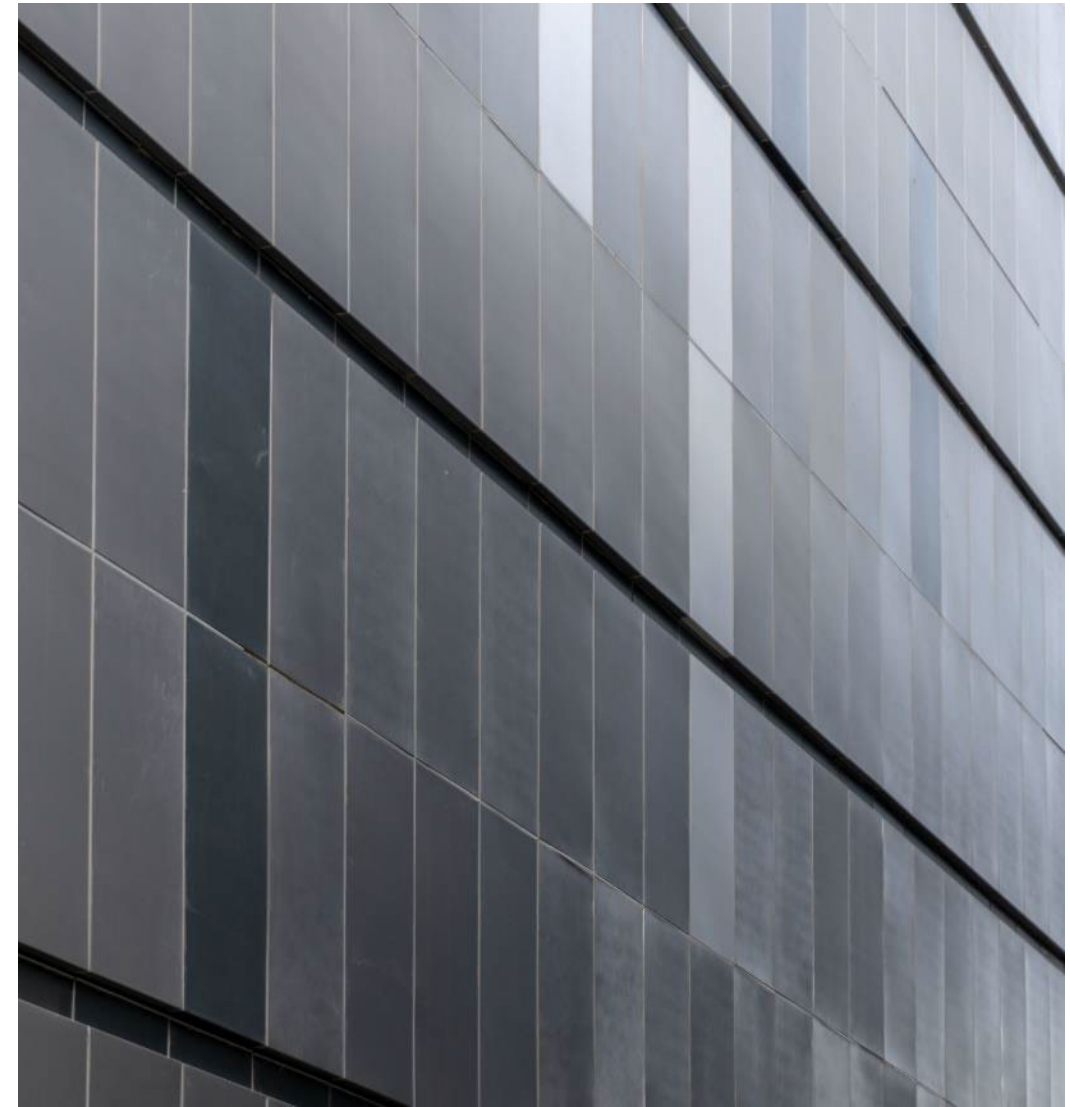
¹IBM Security: Cost of a Data Breach Report 2022



Define and enforce a cybersecurity policy

Key Considerations

- Data loss prevention standards
- Software updates
- Social media requirements
- Encryption & content sharing
- Employee training
- Network access
- Incident reporting process



Protect yourself

- Avoid the dangers of over sharing on social media
- Leverage policies and procedures that restrict employees from divulging personal information that can be used by cybercriminals

Sonya C. Prahbu · 1st

Director of Transactions Services for Commercial Banking

New York, New York

416 connections · [Contact info](#)

Sonya C. Prahbu

Headed to Chicago for your days to attend the commercial Banking Leadership Conference. I'll be leading a discussion on the future of transaction services and technologies

Like · Comment · Share · 1 day ago

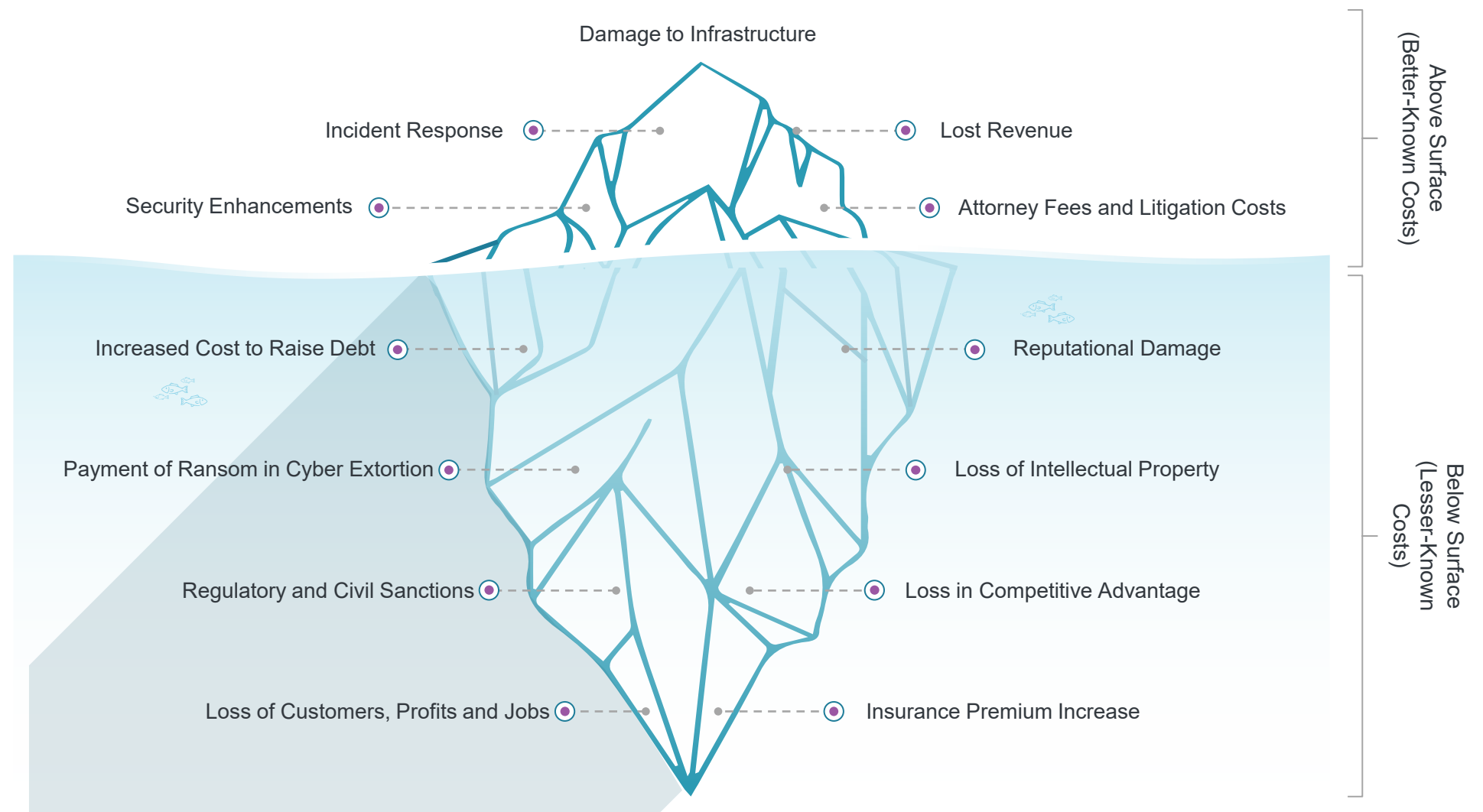
Background

Director of Transaction Services at JP Morgan Chase, Commercial Banking
JPMorgan Chase & Co. is a leading global financial services firm with assets of \$2.4 trillion and operations in more than 60 countries. I lead a great team of 30 Technologists, located around the world. Together we determine and drive the technology solutions for all JP Morgan Chase's Commercial Banking transactions – managing millions and millions of dollars every hour !

Insuring for the worst-case scenario

Cyber insurance is designed to help an organization mitigate risk exposure, through risk transference, by offsetting costs involved with recovery after a cyber-related security breach.

Costs of a Cyber Attack & Which Risks Insurance Can Transfer



Q&A | Discussion



Cybersecurity and fraud protection insights

- Contact your J.P. Morgan Chase relationship team with questions.
 - Visit [Commercial Banking Insights](#) and [Fraud Solutions](#) for resources to mitigate threats.
 - Visit www.ic3.gov for updated PSAs regarding BEC trends and other fraud schemes.
-
- For immediate assistance regarding electronic fraud matters after 5 p.m. EST
 - **J.P. Morgan Access®**: 866-872-3321
 - **Chase Connect®**: 866-619-3053, Option 1

The screenshot shows the J.P. Morgan Chase Commercial Banking website. The header includes the logo and navigation links: Commercial Banking, Solutions, Industries, Insights, Client Stories, Impact, Contact Us, and Login. The main heading is "Cybersecurity and Fraud Protection". Below the heading are six content cards, each with a representative image and a title:

- Card 1:** Image of a man sitting on a ledge by a window. Title: "Report: Most companies will experience fraud >"
- Card 2:** Image of a person working at a computer in an office. Title: "How smaller companies can fight fraud with limited resources >"
- Card 3:** Image of a group of people in a meeting, one in a wheelchair. Title: "Protect your organization against ransomware >"
- Card 4:** Image of hands typing on a laptop keyboard. Title: "Does your disaster recovery plan cover ransomware attacks? >"
- Card 5:** Image of a server room aisle. Title: "12 tips for mitigating cyberattacks >"
- Card 6:** Image of a server rack with lights. Title: "Developing a proactive mindset on ransomware >"

Payment security & 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 trends/history
- ✓ Establish multiple approval levels based on various thresholds
- ✓ Do not permit 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
- ✓ Require multifactor authentication

Verification

- ✓ Don't move money based solely on email, text or phone instructions
- Perform callbacks for request for payments, changing payment instructions or contact information
- ✓ Perform callbacks for request for payments, changing payment instructions or contact information
- ✓ Conduct callbacks with the person making the request via a phone number from a system of record
- ✓ Don't use numbers obtained from sources like email, pop-up messages, texts or voicemail
- ✓ Never give information to an unexpected or unknown caller
- Establish with customers / partners how changes in account information will be communicated and validated
- ✓ Have a process to respond to your financial institution if they call about unusual payments

Reconciliation

- ✓ Perform daily reconciliation
- ✓ Validate that vendors have received payments on payment date.
- ✓ If volume is an issue, perform sampling or set thresholds such as validating payments over a certain amount

Disclosures

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 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. We are not acting as your agent, fiduciary or advisor, including, without limitation, as a Municipal Advisor under the Securities and Exchange Act of 1934.

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.

Changes to Interbank Offered Rates (IBORs) and other benchmark rates: Certain interest rate benchmarks are, or may in the future become, subject to ongoing international, national and other regulatory guidance, reform and proposals for reform. For more information, please consult: https://www.jpmorgan.com/global/disclosures/interbank_offered_rates.

JPMorgan Chase Bank, N.A. Member FDIC.

© 2023 JPMorgan Chase & Co. All rights reserved.