VOLUME 11 | FALL 2021

Fraud+Cybersecurity

Cyber smart is
just the start

CHASE J.P.Morgan

Cyber smart is just the start

Cybersecurity Awareness Month is an opportunity to recognize that every individual is accountable for keeping their organization safe and secure online. This year's headlines reminded everyone that any company can be a target for a zero-day or ransomware attack, and the effects can cause a chain reaction that is felt across supply chains and industries.

Cyber smart organizations incorporate cybersecurity into every aspect of their business and operational decisions. Effective leaders understand how to prevent attacks, detect threats and respond to incidents. They're engaged with their employees, vendors and the public sector to understand new cyber trends and to reinforce best practices, strategies and solutions that mitigate the threats.

In this issue, we share tips to help your business become and remain cyber smart and avoid losses from check or payment fraud schemes.

JPMorgan Chase is here to help inform you of new threats, empower you with tools that can spot and disrupt fraud attempts and assist you if an attack occurs. Our Commercial Banking fraud protection solutions can help you assess risk, implement controls and build a culture of awareness. We encourage you to take our cybersecurity and fraud training, available through J.P. Morgan Access® and Chase Connect®, and schedule a session with our cyber or fraud experts who can guide you toward the right security measures for your organization.

OUR FRAUD + CYBERSECURITY LEADERS

Alec Grant

Head of Client
Fraud Prevention,
Commercial Banking

Anne Davis

Head of Cybersecurity
& Technology Controls,
Commercial Banking

Steve Turk

Chief Data & Analytics
Officer, Commercial Banking

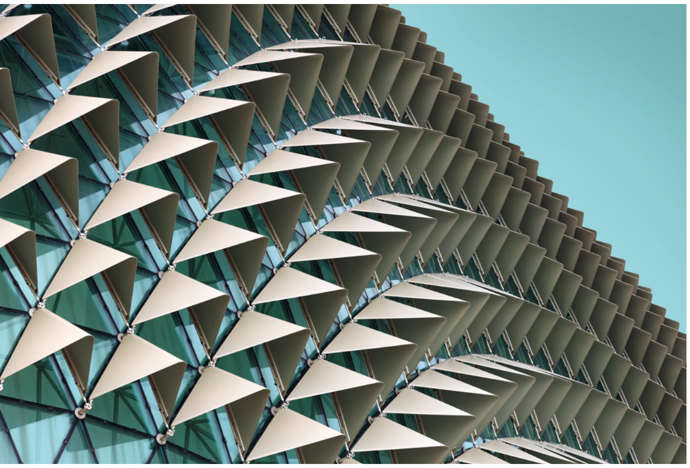
Nick Donohue

Head of Business Continuity,
Commercial Banking

VOLUME 11 | FALL 2021

Fraud + Cybersecurity

VISIT OUR FRAUD HUB



In this issue

Nearly two out of three businesses that use checks reported actual or attempted check fraud attempts in 2020.[1]

Even in a digital world, many organizations still pay by check. But criminals can use current technology and key information on checks to commit fraud. Cat Moore, Head of Payment Product Delivery, Commercial Banking, explains the opportunities fraudsters use to exploit checks and the proactive steps your organization can take to prevent check theft or misuse from internal and external actors.

[1] 2021 Association for Financial Professionals Payments Fraud and Controls Survey Report

VISIT OUR FRAUD HUB

8 ways to stay cyber smart

Use these tips to help you protect your data and financial information.

Cybersecurity is a critical business function. It should be just as important as sales, human resources and business operations.

By being proactive and vigilant, you can help protect your organization's data, finances and business processes. Use these eight tips to build an incident response plan or review and fortify your cybersecurity defense strategy.

1

Have a plan

Outline the steps you'll need to take to prevent an attack—and what you'll do if you are targeted. Your plan should cover protection, identification, detection, response and recovery. Planning shouldn't fall only on your chief information security officer or technology teams. Create holistic teams across your organization that can plan for various risks and act quickly if a cyber event occurs. A sound plan can help your business function for up to two weeks without access to certain systems.

2

Test, test, test

You'll never know how good your plan is if you don't test it. Does your plan consider all possible attack vectors? Does everyone know what to do when something goes wrong? What if communications are offline or compromised? Who is responsible for activating your incident response plan? Test your plan regularly and fix any gaps that emerge.

continued on next page >

Educate everyone

Your entire company should complete regular cybersecurity training—from interns and contractors to employees, including executive leadership. Training can include educational videos, webinars and other interactive tools. Refresh the training with evolving attack scenarios, such as social engineering, credential stuffing tactics and mobile device compromise. Physical security is also important. The person walking through the office with an official-looking polo shirt might not be an approved vendor or invited guest.

Phish for answers

Business email compromise (BEC) is one of the leading ways that cybercriminals can infiltrate a company and trick employees into divulging confidential information or sending fraudulent payments. Create a phishing awareness and testing program to check your employees' email security protocols. Conducting regular phishing and social engineering tests can help reduce the chances of an attack.

Don't sit still

Cybercriminals are always changing their methods and evolving with technology. You should too. Stay up to date on ransomware information so you can implement effective countermeasures. Consult resources like the U.S. Cybersecurity & Infrastructure Security Agency (CISA) and sector-specific Information Sharing and Analysis Centers (ISACs) that spread critical security information across industries.

Divide to conquer

Use network segmentation to isolate parts of your network so that if attacked, only a small portion of your network is affected. You can implement the same concept with data storage, access management and physical access controls. Consider adding an application "allow list" that only permits certain apps on your network. Create multiple networks to lock sensitive systems and data. No users should be trusted by default, and everyone should be verified and authenticated before accessing your network.

Layer on the protection

Think about security in terms of rings, with the most precious assets in the center. At the outermost layer, you should start with domain security to prevent spoofing and domain takeover. Consider deploying a web application firewall to inspect internet traffic as it comes into your company. The protections continue as you progress to the system's core and your data—which should be encrypted. This layered protection applies to hardware too. You should also require multifactor authentication—such as a one-time password or token—in case a username-password combination is compromised.

Create a virtual cyber council

Establish relationships with experts in multiple cybersecurity agencies to be your go-to resources for advice and strategic guidance. For instance, you could add law enforcement and the FBI to your council. If you have cloud operations, find someone who can guide your decisions around tools, policies and operational risk. Industry regulators are also great resources. Recognizing you don't have to know it all is an asset, not a liability. Using experts where needed can bolster your cybersecurity program.

Key takeaway

- Visit our Cybersecurity and Fraud Protection Insights page to learn more about how JPMorgan Chase experts can help keep your organization safe.

VISIT OUR FRAUD HUB

Developing a proactive mindset on ransomware

As cyberattack threats loom large over businesses, our expert says companies should focus on prevention, detection, response and recovery.

Anne Davis
Head of Cybersecurity & Technology
Controls, Commercial Banking

Anne Davis oversees firmwide global technology control management. In more than two decades with the firm, Davis has held roles in information security, technology and business controls and technology execution. We sat down with Anne for her advice on how clients can develop a proactive mindset to prevent ransomware attacks.

continued on next page >

VISIT OUR FRAUD HUB

Q: In June 2021, the White House called on business leaders to take action and launched stopransomware.gov to help inform the public and remain vigilant. Why is ransomware a national security issue?

A: Ransomware is a leading national security topic right now because of the growing frequency and sophistication of attacks. Ransomware impacts the livelihood of all Americans and requires business and government to work together to strengthen national resilience. It's also because of an increase in attacks on businesses that provide critical infrastructure—think oil pipelines, food processing plants and hospitals. These attacks have created costly ripple effects through government and beyond to other businesses, ultimately impacting their customers too. The best way to mitigate risk is to implement baseline cyber hygiene practices and develop standards and controls that apply broadly to consumers, businesses and the government.

Q: When it comes to ransomware, what does it mean to be prepared? How can companies know whether they're targets for attacks?

A: Ransomware attacks are now so widespread that all organizations should assume they will be targeted. There is no way to completely ensure you will not be a victim of ransomware, so heightened diligence and ongoing review of your controls with your internal and external partners is of paramount importance. You should focus on four areas to prepare for threats: prevention, detection, response and recovery.

Q: Let's start with prevention. What does that entail?

A: Good cyber hygiene is key to preventing ransomware. That involves keeping systems patched and keeping them up-to-date using a risk-based approach. You also need to implement a layered defense strategy and use multifactor authentication and backup systems for your data. And you have to maintain extensive oversight and security controls over any third-party vendors that may have access to your computer network or handle sensitive data. Employee awareness is at the core of prevention. Helping them understand how attacks happen and how they can help is critical.

Q: Can you explain risk-based approaches to software patches?

A: Software providers regularly provide updates to fix newly discovered security gaps, and those gaps remain as potential vulnerabilities that criminals can discover unless those patches are added. Organizations need to consider several factors before deciding if, when and how to install patches and updates: Is the system internal or external? How critical is the system to your business? If you delay patch updates, are there regulatory or compliance considerations, such as fines?

Q: What does an effective detection strategy look like?

A: It means being able to detect anomalous activity as quickly as possible. The sooner you detect an intrusion, the sooner you can contain it and reduce the overall impact. Perform a regular review of log files and monitor outbound data. Consider using a tool that looks for encryption activity stops it immediately and sends alerts.

continued on next page >

Q: Even with sound prevention and detection strategies, some ransomware attacks will occur. What are the steps businesses should take so they can respond quickly?

A: Being prepared means having a concrete plan and proper training to respond to an attack before it occurs. In the chaotic situation following a ransomware attack, time to act is limited, stress will be sky-high and normal organizational, financial and communications tools may be offline. So create a plan. The plan contains details on identification, detection, containment and recovery. Regular testing will help your team and response time improve.

Q: How often should a business review its response plan?

A: Reviewing a plan should be a regular practice so that the details are up-to-date at the moment an attacker strikes. Perhaps employees' roles have changed, or new hardware or cloud systems have been added. Test your plan regularly to make sure everyone is familiar with it and you can identify any gaps in security protocols.

Q: What other pieces need to be part of any organization's response plan?

A: The plan should document all systems and in what order they should be restored. It should also address who needs to be contacted to begin recovery and which people or teams will handle different aspects of managing the crisis, from legal and compliance to information technology, billing and public relations.

The plan should also account for backups so that data and operations can be restored. An effective response plan will detail how to access backups and test them prior to restoration.

A response plan is about keeping the business running and mitigating your recovery time. It's up to the technology and cybersecurity teams to remain diligent and expedient.

Q: What should an organization do when it's hit by a ransomware attack?

A: JPMorgan Chase has a process in place to help clients when they're impacted by a ransomware attack. Affected clients should contact their Commercial Banking relationship team as soon as they suspect a malware or ransomware incident. The firm will work with your business to implement protective controls on payment platforms and will assist with other resiliency needs. If faced with a ransomware payment demand, each business must understand the regulatory and legal implications.

You should also contact the local FBI field office and submit a complaint to the FBI's Internet Crime Complaint Center, or IC3.

Key takeaways

- Prevent attacks by patching systems and keeping them updated.
- Detect intrusions quickly so you can contain them as soon as possible.
- Develop a response plan for ransomware attacks, and keep it up-to-date.
- Understand legal and regulatory implications before considering payment of any ransom-related demand.

VISIT OUR
FRAUD HUB

Protect your fortress:

Keeping bad actors at bay

Businesses must make industry-specific considerations to prevent cyberattacks and fraud. We look at healthcare and commercial real estate companies to see this in action.

continued on next page >

VISIT OUR FRAUD HUB

> *"It's life or death. Nursing homes, for example, wouldn't be able to know what medication to give their residents."*
>
> Kerry Jessani, National Head of Healthcare, Higher Education & Nonprofit Industries, Commercial Banking

The cybersecurity stakes have never been higher: According to our 2021 Business Leaders Outlook Pulse Survey from June, one-third of company executives said they had been directly impacted by some type of cyberattack or fraud attempt during the pandemic.

For many, the fortress is under constant attack. Ransomware, business email compromise (BEC) and other fraud threats continue to proliferate and evolve. To protect their organizations, business leaders must take action and build a comprehensive defense.

While investment, training and controls are broad cyber preparedness priorities, each business has unique considerations depending on its industry. The cyber threats are often the same, but the playing field has changed.

Cyber preparedness can be life or death in healthcare

For companies in healthcare, Kerry Jessani, National Head of Healthcare, Higher Education & Nonprofit Industries, JPMorgan Chase Commercial Banking, says fortress defenses hinge on two critical points: protecting data and identifying indirect vulnerabilities.

Healthcare providers are more awash in data than ever before, thanks to the adoption of electronic health records and other technologies. However, this makes hospitals and other organizations a top target for cybercriminals.

One challenge is that this data is frequently in transit, moving in and out of organizations to other places like insurance companies and doctor's offices. Each access point is an opportunity for sensitive patient data to be intercepted or abused.

"Data is sacred," Jessani says. "But what hospitals need to understand is they must create a framework for understanding who has your data. The fewer touchpoints, the better."

The constant exchange of data with outside parties further elevates the risks of BEC or ransomware. Without rigorous controls, there may be an increased chance that a healthcare provider's data could be held hostage, breached or otherwise manipulated for criminal gain. One slip and the worst could come to pass.

"It's life or death," Jessani says. "Nursing homes, for example, wouldn't be able to know what medication to give their residents."

Given the stakes, it's critical to have an effective data security program in place that utilizes a stacked approach to protection, including:

1. **Shutting down systems when not needed.** Why continue to run a patient database over the weekend when the office is closed and no one is using it?
2. **Activating unused security controls.** Work your way through all your systems and activate security features such as multifactor authentication, encryption tools and firewalls. Don't forget your router: Many elevated security settings are not activated by default.
3. **Segmenting your network.** Creating and utilizing separate networks for patients and the practice can help you keep random, unauthorized users away from your company network traffic.

continued on next page >

VISIT OUR FRAUD HUB

Vulnerabilities

Organizations can prevent intrusions or attacks before they happen by proactively identifying vulnerabilities. At healthcare organizations, the weak point may not exist internally and could be several steps down the supply chain.

"For hospital systems, the refrain you should consistently hear is 'You're only as strong as your supplier's weakest supplier,'" Jessani says. "For instance, the situation during the pandemic was, 'Yes you might use this supplier to provide masks, and they're just an intermediary supplier,' but they have 15 suppliers. So, you need to go through all of those to find the weak points."

The degrees of separation along a supply chain might not be front of mind for a healthcare business, but the consequences could cost them. That's why these organizations need a culture of vigilance.

"It has to be in the DNA in everything," Jessani says. "Get all the senior people in the room together from various departments. This impacts everyone; but often not everyone understands the importance of developing a preparedness culture until it's too late."

You can help to foster such a proactive culture by establishing a vulnerability management cadence. This includes:

1. Scanning and identifying vulnerabilities
2. Prioritizing vulnerabilities
3. Remediating
4. Rescanning to ensure you have closed the gap

When conducting an internal scan of your network(s), look specifically for unknown users and devices. To strengthen your vulnerability program, review current threat intelligence data and read about current vulnerabilities, how they are being exploited and what remediation options are available.

Wire volume multiplies the risks for commercial real estate

Protecting a commercial real estate fortress entails more than just maintaining physical properties. Winston Fant, Managing Director and Head of Commercial Real Estate Treasury Services, JPMorgan Chase, says it requires strict attention to detail given the vast volume of wire transfers these companies initiate.

Running fast and going hard

Commercial real estate businesses conduct massive amounts of wire transfers each day. With payments moving in and out, the rush of wire activity can create openings for fraud.

"Even for big companies, treasury staff is not usually large," Fant says. "They're running fast and going hard."

Without serious controls in place and in use, companies may risk multimillion dollar fraud losses. "It's not a matter of if, but when," he says.

Businesses should place a major focus on process hygiene and training employees to be vigilant in their diligence. For instance, a known email account can still be taken over by a fraudster, and it won't show a telltale spelling error in the

> *"There's no one single defense that can prevent everything."*
>
> Winston Fant, Managing Director and Head of Commercial Real Estate Treasury Services, Commercial Banking

continued on next page >

domain name. Following procedures like calling a trusted number can prevent a loss.

Even though added controls may slow down business, it's a necessary side effect.

"Businesses need to feel comfortable with having layered checks on dollars flowing out," Fant says. "There's no one single defense that can prevent everything."

Employee training is a best practice to help ensure that controls are followed. In the 2021 Business Leaders Outlook Pulse Survey, 79% of business executives said **employee education was the most helpful** measure undertaken by companies that experienced a cyberattack or fraud.

While training treasury staff is crucial for commercial real estate organizations, Fant doesn't think companies should stop there.

"It's advantageous for companies to train a broad swath of employees, not just those in treasury," he says. "Fraud happens because people make mistakes, and real estate is a people business, whether they're moving money, transacting or doing deals. The more people that are trained, the better."

Lastly, commercial real estate companies must look externally as vendors can be targets, too. Businesses should consider talking with suppliers about their security policies and how they are protecting their own organizations. Many companies require vendors to undergo an oversight process and submit documented security protocols.

Don't delay: Protect your fortress

Your cyber preparedness can never be considered complete if you don't account for industry-specific factors. Just as healthcare providers must focus on patient data and commercial real estate businesses must focus on wires, your business has its own set of special considerations that should govern how you address cyber and fraud risks.

Regardless of your industry, however, you should have a sense of urgency about your cybersecurity posture. A great place to start is by doing one thing each day to protect your company, such as:

- Reading an intelligence article (you can find some on the JPMorgan Chase Commercial Banking **Insights** page)
- Reminding colleagues about trending scams and attacks
- Asking your information technology or security team to review settings on patched systems (sometimes the updates make changes without proper notifications)

Key takeaways

- Evaluate your business to determine which industry-specific factors present an increased risk for fraud or cybercrime.
- Create a framework that minimizes touchpoints to sensitive data.
- Enforce process hygiene with payments, even at the expense of speed.
- Build security into your corporate culture.

VISIT OUR FRAUD HUB

Forecasting the future of fraud

Our fraud prevention experts are studying recent trends to understand what cyberattacks may look like down the line—and help businesses prepare now.

continued on next page >

Fraud is snowballing

The total payment value of business email compromise (BEC) attacks is growing aggressively this year, up more than 100% in 2021 compared with the same period of 2020, according to Commercial Banking estimates.

Ransomware also poses a serious threat. Commercial Banking clients reported more than four times as many ransomware attacks in the first half of 2021 compared with the first half of 2020.

> *“Fraud is pervasive, and it’s only going to keep growing. Bad actors are finding and exploiting weaknesses in companies’ payment control environment, and every successful fraud improves the criminals’ incentives for newer, bigger attacks.”*
>
> John Geronimo, Executive Director and Fraud Strategy Director, Commercial Banking

THE FORECAST

Fraudsters, emboldened by the high value of a successful fraud scheme, will continue to escalate their attempts. With the disturbing rise of the ransomware-as-a-service business model, criminals can buy ransomware tools on the dark web as easily as your business leases software from legitimate developers. That means it’s no longer necessary for criminals to have a sophisticated skill set to launch ransomware attacks. They don’t need every attack to succeed to make off with a fortune—instead, they’ll prey on as many targets as possible, as often as possible.

BEC is the main driver of fraud

Fraudsters continue to attempt BEC attacks—deceptive emails aimed at tricking victims into redirecting invoice payments to accounts that criminals control. The average amount stolen in a BEC attempt is up by 129% year over year, according to Commercial Banking estimates, meaning when businesses do fall victim, they are losing more money.

> *“By making sure you dial out to verify details using the trusted contact information you have on file, you’re less likely to be manipulated by a call placed to you by a fraudster. Answering the phone isn’t a proper callback.”*
>
> Eric Huber, Fraud Strategy Manager, Commercial Banking

THE FORECAST

Criminals will get more sophisticated in their efforts to avoid detection when attempting BEC—sometimes by compromising more than an email address. They’ve already started to utilize deepfake technology to impersonate executives’ voices on phone calls and even their likenesses over video to add an air of legitimacy to their attacks. As deepfakes become more lifelike, phone calls, video chats and other forms of communication will be more vulnerable to abuse.

continued on next page >

VISIT OUR FRAUD HUB

Nobody is immune

Businesses in every region of the country and across every industry have reported attacks. Cybercriminals don't care about your physical address. If you've got an IP address, you're a target.

> *"Fraud is not a region-specific issue. Cybercriminals follow people, money and vulnerable technology—not geography."*
>
> John Geronimo, Executive Director and Fraud Strategy Director, Commercial Banking

THE FORECAST

We expect industry groups and the public sector to ramp up efforts to coordinate their fraud and cybercrime prevention strategies, especially ones focused on protecting critical infrastructure and supply chains. While we don't know where the next hotspot will appear, we do know criminals are constantly improving their methods to launch attacks. To amplify their efforts, criminals use malware or internet bots to do their dirty work. Bots roam the internet looking for unguarded data and system vulnerabilities to launch malicious attacks that allow an attacker to remotely take control of computer systems.

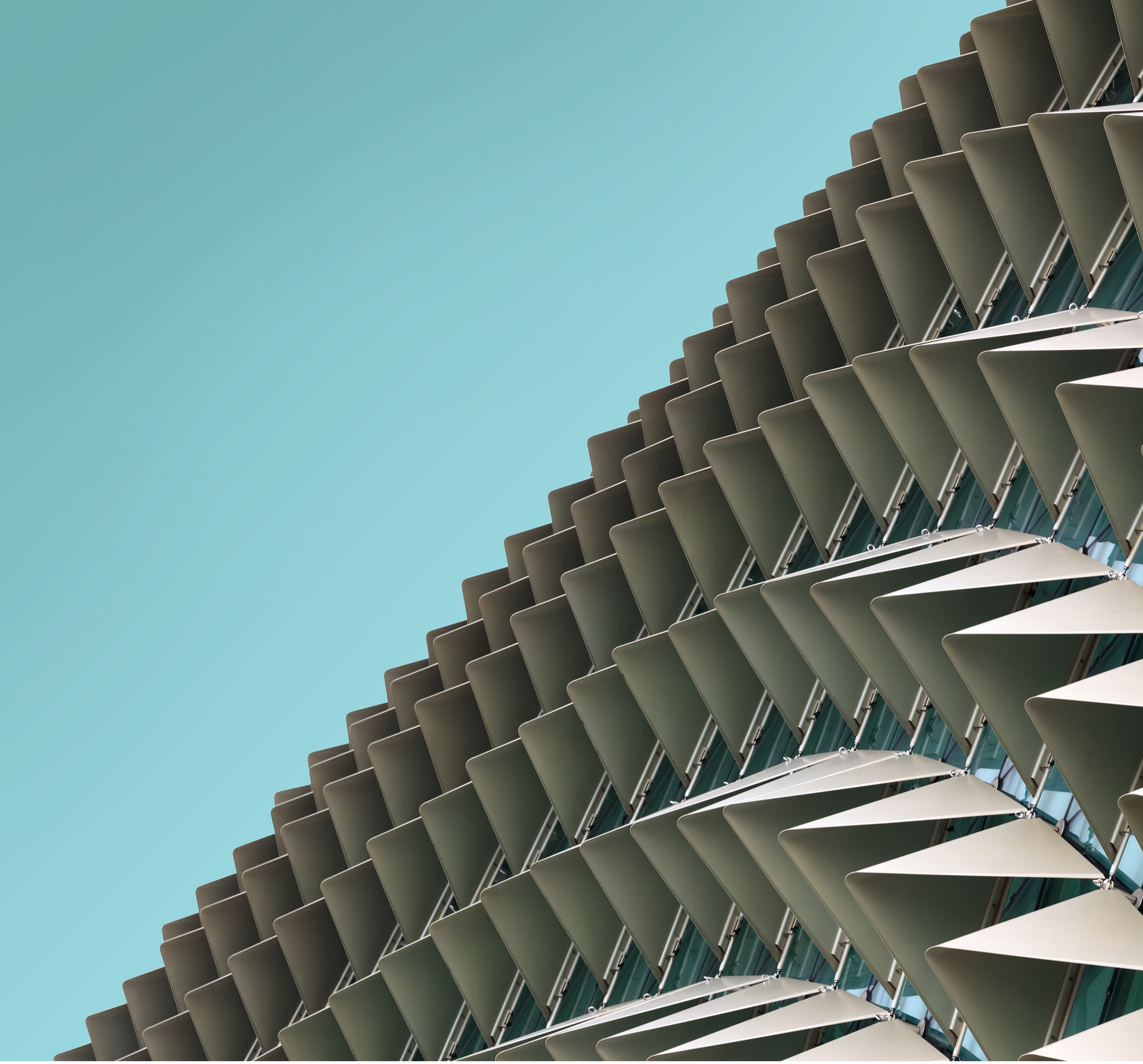
You've got resources to fight back

The fight against fraud is constantly evolving. As financial institutions and clients–as well as law enforcement–improve controls and counter-fraud measures, criminals will adapt and escalate in new ways. But the fundamentals of cybersecurity remain the same: Study the threats, follow your controls and ensure your entire team is vigilant. The majority of money lost to BEC schemes by Commercial Banking clients in the first half of 2021 were flagged as irregular by bank control and released by clients.

> *"The common denominator for these attacks is the same: human nature and an overreliance on email. In those cases, a proper callback could have stopped the fraud attempts cold."*
>
> Krysta Gnidziejko, Fraud Strategy Associate, Commercial Banking

Key takeaway

- JPMorgan Chase will continue to research and present the latest advice on how to protect your business. Ready to take action? **Download our BEC Guide.**



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 is provided for educational and informational purposes only and is not intended, nor should it be relied upon, to address every aspect of the subject discussed herein. The information provided is intended to help clients protect themselves from malicious cyber activity. It does not provide a comprehensive list of all types of malicious cyber activities and it does not identify all types of cybersecurity best practices. You, your company or organization are responsible for determining how to best protect against malicious cyber activities and for selecting the cybersecurity best practices that are most appropriate to your 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.