CHASE J.P.Morgan

Remaining Resilient

Learn how to handle disruption and prepare for the unknown

COVID-19 has caused major disruptions to day-to-day business operations, forcing companies to make many adjustments to stay up and running. By late November, 84% of executives said at least some of their employees were still working from home, according to the **2021 Business Leaders Outlook Survey**.

As the pandemic continues and the future remains uncertain, countless issues are likely weighing on your mind as you try to best manage your business. In this e-book, you'll find insights from experts on important topics to consider moving forward.

Visit **jpmorgan.com/cb** for more insights from our experts. To further discuss how we can help, contact your banker. If you're not a current JPMorgan Chase client, visit **jpmorgan.com/cb/contact**.

TOPICS COVERED

Spotting and Preventing COVID-19 Social Engineering Attacks

During times of widespread fear and uncertainty—like the COVID-19 pandemic—cybercriminals use social engineering to trick people into taking part in their own fraud. By posing as a legitimate business, nonprofit, government or other trustworthy source, fraudsters can manipulate victims into installing malware on personal and business devices or divulging sensitive data, such as usernames and passwords, personally identifying information and financial account information.

Social engineering attacks can spawn from practically any means of communication, but most are conducted via email, social media, phone call or text message. Cybercriminals often cast a wide net, targeting both individuals and businesses.

Learn ways to identify and avoid COVID-19 social engineering attacks.

What an Attack Can Look Like

Cybercriminals have escalated social engineering attacks during the COVID-19 pandemic. Recent threats include:

- Impersonating global health organizations in emails that contain malicious links or attachments or ask for fraudulent donations to combat COVID-19.
- Creating fake COVID-19 websites that distribute malware or pandemic tracking apps that contain ransomware or spyware.
- Sending emails with malicious links or attachments that claim to offer products that are in short supply, such as face masks and other personal protective equipment, or faster access to COVID-19 vaccines.
- Posing as a health insurance company that offers COVID-19 insurance plans and sending a malicious link that claims to provide access to an account invoice.
- Conducting smishing (SMS phishing) attacks, in which cybercriminals use text messages to target victims. Hackers may send texts with malicious links claiming to offer vaccines ahead of distribution lines in addition to information about the virus, free masks or stimulus payments.

How to Avoid Falling Victim

Cybercriminals also use social engineering to target employees for business email compromise (BEC) scams. Businesses can take steps to remain on high alert during these times:

1. Be extra vigilant about payment controls and wary of emails that contain an attachment or link. When in doubt, contact your information security or information technology department about a dubious message.

2. Reconcile your accounts frequently and confirm that business partners have received payments by calling a verified number. Be cautious with payment and account change requests and pay close attention to whom you are paying.

3. With many employees now working from home, keep contact information up to date so your bank can contact you quickly if they detect a suspicious payment.

4. Don't trust any requests for payments or account changes that come in through email alone. Always perform callbacks to the person making the request using a known phone number from a system of record.

5. Always perform call backs when changing the contact information for business partners as well. Don't simply trust an email asking to change a trusted callback number.

Finally, if you do become a victim of a social engineering attack, immediately notify your bank, file a report with IC3.gov and contact your local FBI field office to notify them of the fraud. Performing these three steps as quickly as possible may increase your chances of recovering funds.

Treasury Readiness: How Prepared Are You?

Whether it's a natural disaster, an employee illness or a cyberattack, unexpected events can wreak havoc on your business. That's why you need to develop contingency plans now—before unpredictable, yet inevitable, disruptions occur.

Readiness requires that leaders take a hard look at current operations and ask the tough questions. This is business critical. Solidify your crisis-response strategy and make sure everyone in your organization can meet any emergency with clarity, confidence and relative calm.

The questions below will help you assess your treasury readiness and develop the emergency plans your company and your people really need.

Management and Communications

- Do you have a designated emergency management team? You need people who are accountable for the immediate response after an emergency and for ensuring your employees stay safe.
- Do you have a predetermined chain of command in an emergency? You should know who will take on key responsibilities and leadership roles if those typically in charge are unable to do so.
- Have you documented the chain of command and distributed the information throughout the organization? Internal awareness is a crucial component of an effective emergency response.
- Have you developed internal and external communications plans for each type of crisis? This includes a list of key vendors, outside partners and even public agencies that you may need to inform.

- Do your employees, clients, suppliers and other key business contacts have your emergency contact information?
- Have you shared your disaster preparedness procedures with local services and government agencies so that they're primed to respond?
- Have you considered employees' emotional needs in a crisis? You should be ready to offer access to support resources.

Procedures

- Have you prepared supplies you might need in a disaster, such as potable water, emergency food and flashlights?
- Do you have alternate power sources for your main server? Do you have a backup plan if your internet provider goes down?
- Do you have a plan for securing data and facilities, as well as processing payments? This requires close contact and communication with existing vendors, financial institutions and external partners.
- Do you have locations where you can rapidly shift accounting operations during a crisis? Being able to quickly pivot will allow your business to continue running smoothly.
- Do your banks also have dispersed payment centers so that you can avoid accounting disruptions? Internal preparation will only get you so far if your financial partners are not also prepared.
- Have you allocated emergency funds across different accounts? If a partner is also affected, this can help you maintain access to your money.
- Have you tested your contingency site to be sure it has all the functionality of your primary site? Will there be proper equipment and sufficient space for your employees?
- If your contingency site is being leased, have you communicated with the tenants about space allocation during an emergency?

Tests and Reviews

- Do you conduct tests by logging in to your backup system and generating at least one live transaction per month? Running regular tests can help you avoid unexpected hiccups during a real emergency.
- Do you have a set schedule for conducting full end-to-end tests that validate your ability to recover quickly?
- Have you audited your tests? An additional layer of confirmation can help safeguard your business and give you peace of mind.
- Have you reviewed your account information to ensure accuracy and added authorized signers, security administrators, user IDs and entitlements with each of your banks?

- Have you scheduled periodic connectivity reviews between your backup systems and your internal departments, customers, suppliers and other key business contacts to ensure they are compliant and operational?
- Have you completed a comprehensive review of your insurance coverage as it relates to recovery and restoration?

Remember that communication, preparation and testing will help your business conquer any crisis that comes along with minimal disruption to your operations. But readiness also means doing the right thing for any employee or customer who experiences the stress of an emergency. By focusing on preparedness and bringing everyone along, in the process, you're sending an important message: We don't only care about the business—we also care deeply about you.

PAYABLES AND RECEIVABLES OPERATIONS

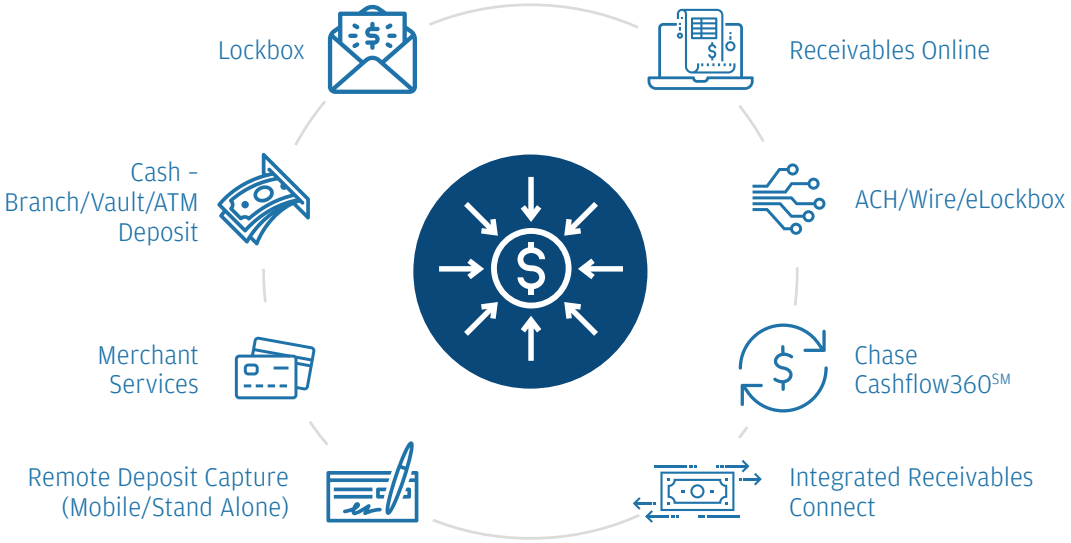
Prepare for the Inevitable

Whether COVID-19, a natural disaster or another event is the cause, business disruption is inevitable. This makes your disaster recovery and business resiliency plans critical. **Watch this webinar** in which product specialists answer questions about how companies can most effectively manage their payables and receivables processes.

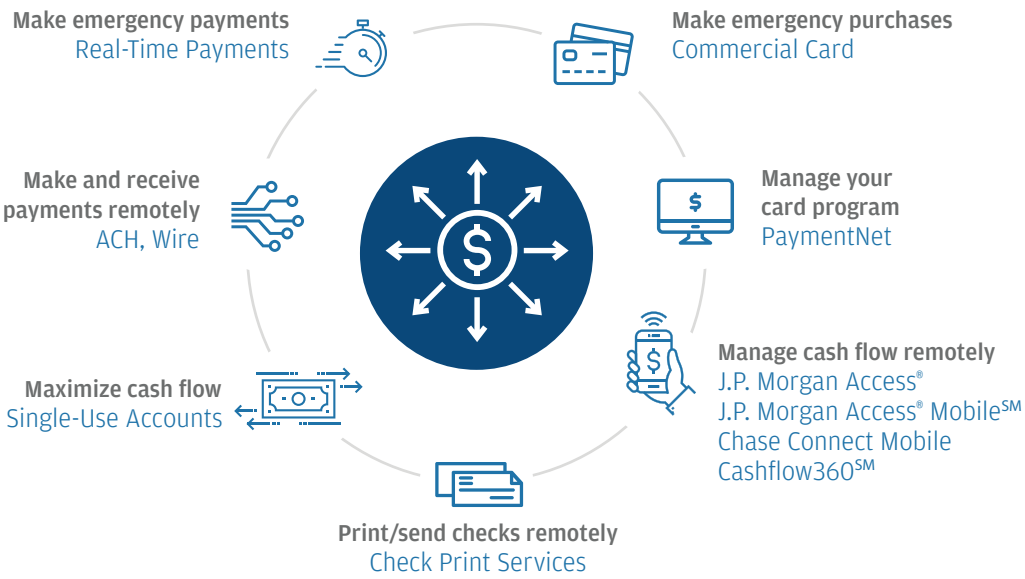
Develop Short- and Long-Term Solutions to Manage Payables and Receivables Remotely

When it comes to making and accepting payments, it's critical that you can implement changes within weeks or days. At the same time, you should also consider long-term solutions. For example, you may initially encourage customers to pay via ACH or enroll in auto debit. Later, you may shift to online payment channels and enroll in an e-lockbox service. At first you may expand your current card program to pay suppliers with your purchasing card. As time passes you can craft a more integrated payables approach that includes check print outsourcing and supplier enrollment for Single-Use Accounts or ACH.

Manage Receivables Remotely



Make Payments Remotely



Best Practices for Treasury Management in a Crisis

Check your info

- Review bank account information for accuracy. This includes verifying authorized signers, security administrators, active user IDs and proper entitlements across all banking systems.
- Confirm your bank relationship team's contact information: email addresses, office phone numbers and cellphone numbers.
- Review and update processing instructions for each bank service and transaction limits.

Check your access

- Confirm remote access is active and test RSA SecurID tokens.
- Confirm you have enough system administrators to manage entitlements.
- Review IP security settings from home or other locations.

Contact customers

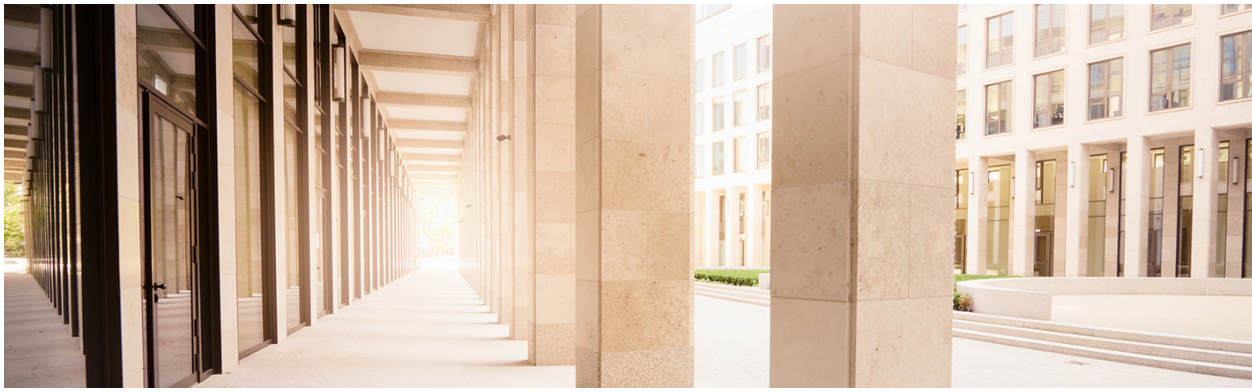
- Request customers pay via electronic methods.

Think ahead

- Plan for credit and cash needs by: consolidating liquidity across accounts, countries and currencies; leveraging intercompany funding; and evaluating cash management sources.
- Prioritize transactions and send your bank a list of urgent, scheduled transactions, such as loan closings.
- Prepare and submit payroll, ACH and wire payment files, and Positive Pay check issue files as early as possible. Establish alternatives for distributing payroll checks.
- Cross-train personnel so staff can assume multiple roles if necessary.
- Record what you learn during the crisis so that afterward you can upgrade operations and contingency plans.

Increase attention

- Be aware of the higher risk for cyber threats. Criminals exploit these situations.
- Do not change payment instructions for vendors, suppliers or any payees without validating with a callback to a known contact. Follow internal control procedures to change accounts payable remittance information.



5 Pillars to Protect Your Business Amid Economic Uncertainty

Leverage data to develop a comprehensive strategy that can help you minimize risks to your business and respond quickly during market shifts.

By: Ezra Maddox, Executive Director, Corporate Treasury Consulting, Commercial Banking

How will your business react when—not if—unexpected events occur? Business resiliency plans are rapidly changing from hypothetical situations to practical actions, as leaders respond in real time to the COVID-19 pandemic and its impact.

While it's impossible to completely eliminate risks to your organization, you can minimize them. If you don't have an appropriate risk framework in place, now is the time to create one. And if you do it's time to build upon your risk strategy so your organization can remain strong during challenging times.

Draw on these five pillars to establish and improve your risk strategy.

1. Create a Scorecard for Counterparties

Your business works with many counterparties. Banks may be the first that come to mind, but customers and vendors are counterparties too. While reputation and past experience may inform these relationships, it's important to develop a risk profile using research and data, which are more effective evaluation metrics. Start by creating scorecards to assess each counterparty's risk to your business. Be sure to use quantitative and qualitative metrics when developing your scoring system, and consider the following questions, as part of a broader set of considerations.

Banks

- What is the market confidence in the bank's ability to meet future obligations?
- Does the bank have an adequate capital structure to withstand an adverse stress scenario?
- Is the bank profitable and investing in its technology infrastructure to improve its services and capabilities?
- Does the bank offer a full suite of electronic payment and collection services that can operate even if mail or physical facilities are disrupted?

Customers

- What is the level of risk tolerance toward customers' ability to provide full or partial payment of the invoiced amount due?
- How profitable is the relationship? For example, is it a sticky business with multiyear contracts?
- Are the products and services tied to any single buyer?

Vendors

- What is the level of security protecting confidential data from cybersecurity threats and fraud breaches?
- Does the company accept check payments exclusively?
- What percentage of production is affected by interruptions to the flow of raw materials or parts within your supply chain?

2. Analyze Data to Anticipate Your Future Risk

The next step is to examine objective risk indicators and financial ratios for similar counterparties so you can see how your banks, customers and vendors stack up to their peers. This benchmarking analysis can also help you anticipate future risks illustrating patterns, trends and blind spots, as well as the target company's emerging gaps relative to its peers. When building your peer assessment, consider the following key components:

- Cash conversion cycle, calculating the number of days to obtain liquidity through the operating cycle
- Liquidity risk, examining available cash balances versus used bank lines

- Financial risk, measuring capital structure costs and any FX exposure
- Operational risk, calculating the company's employee turnover rate
- Compliance risk, looking at reported breaches and events with negative press

3. Reduce Liquidity Risk With Visibility and Access

For many organizations, the strategy to manage liquidity exposure is determined with limited visibility into their global cash. Rather than make intuition-based decisions, implement end-to-end technology, optimize global liquidity sources and rationalize account structures to enable real-time visibility into your liquidity at the domestic, regional and global level.

Forecasting global cash flows continues to be an important tool to evaluate access to primary and secondary liquidity sources. Incorporating stress scenarios will also help provide data-driven insights to assess future liquidity needs. For example, what are the potential effects of foreign exchange and interest rate shifts; a 30-, 60- or 90-day delay in accounts receivable; or significant outflows? Determining those effects will help establish a diverse, well-developed contingency funding plan.

4. Reduce Operational Risk

From people, processes and technology to volatility in the markets, a wide range of factors can drive operational risk. That's why it's critical to establish:

- A robust control framework with standard business-wide policies and processes. Be sure to include a dedicated cross-functional response team that can provide real-time internal and external communications.
- A strong internal accountability structure that clarifies roles within the organization, team and individual ownership of tasks, and expectations during and after disruptive events.
- A business resiliency plan that covers management, communications and procedures, plus tests and reviews to ensure your organization is operational as soon as possible during a crisis. Concentrate on initiatives that provide high value not only to customers and vendors, but also to your organization.
- Prioritize efforts that increase efficiency and savings. Focus on freeing up working capital and streamlining your processes and systems. This way, your organization can be agile and resilient enough to adapt to rapid market shifts.
- Commit to long-term strategies: From employee training and professional development to upgrading company systems, these strategies are valuable to your business. Your knee-jerk reaction may be to tighten discretionary expenses amid uncertainty, but continue to evaluate long-term investments even while focused on short-term performance. Whether your current plan is to grow your business or to maintain profitability at your current size, industry best practices and changes in technology don't halt because of economic concerns—so neither should your business strategy.

5. Leverage Big Data to Monitor Risk

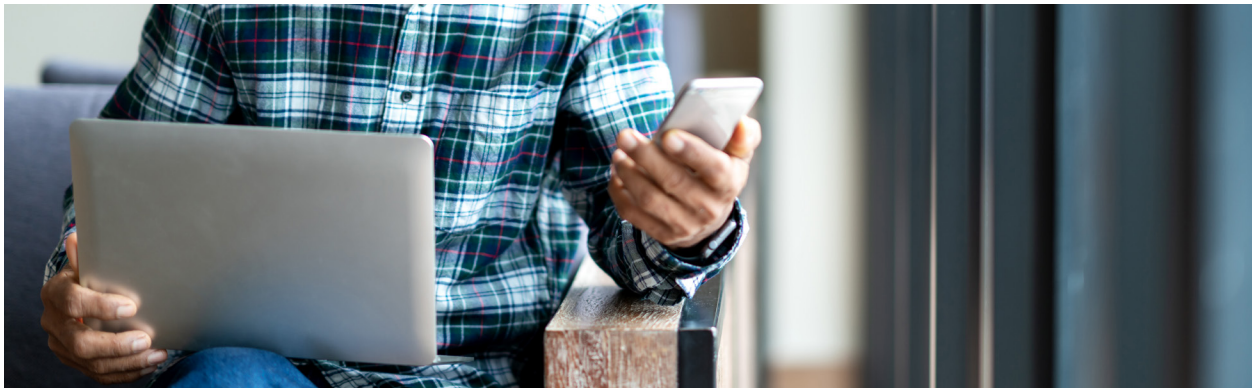
Big Data analysis can help your business predict and plan for disruptive events that traditional means cannot identify. For example, some Big Data tools can replicate specific scenarios to analyze the potential impact of disruptive events that range from natural disasters to military conflicts. Likewise, these platforms can help you develop a better business continuity plan by identifying operational inefficiencies, issues with internal systems, and cybersecurity and fraud threats. As a result, your organization can make thoughtful, data-driven decisions rather than rely on intuition.

Look Ahead

A comprehensive risk strategy is always critical in minimizing exposure to your business and increasing its stability. That strategy is even more important now, especially with the anticipated uptick in mergers and acquisition activity as we come out from the COVID-19 pandemic.

Organizations that successfully navigate this challenging time period can emerge stronger by taking proactive measures. Follow suit with corporations that have grown during difficult times and perform due diligence as your business recovers. That means identifying the right targets and integrating operational and strategic aspects into your plans going forward. These efforts will be core to your mergers and acquisition strategy and position you to grow into a market leader.

TECHNOLOGY AND COMMUNICATIONS



Digital Payment Solutions to Help You Navigate Any Situation

In this ever-changing environment, stay connected to your buyers and suppliers with best-in-class digital payment and treasury solutions.

Digital Cash Management Solutions to Help You Optimize Your Business

As industries evolve and current events like the COVID-19 pandemic impact the way we do business, your operations and resiliency plans are more critical than ever. With our integrated digital solutions, you can manage payables and receivables easily from one secure portal and exchange documentation online quickly and securely—all while improving cost efficiency and streamlining operations.

Chase Connect

Get access to flexible payments, seamless receivables and secure account management in real time. Remote and mobile deposit: Deposit checks from anywhere in the U.S. with Chase QuickDeposit℠.

ACH payment services: Quickly send one-time or repeating payments to employees and vendors.

Wire transfers: With nearly 70 currency options available, you can easily pay international and domestic vendors virtually anywhere your business takes you.

Bill pay: One-time, future-dated or repeating payments, delivered electronically or by check to U.S. mailing addresses.

Chase Cashflow360℠

No matter where you're working, Cashflow360 helps you digitally connect with clients and suppliers to make and receive payments.

Payment controls: You and designated employees can approve payments and invoices from anywhere, anytime with automated workflows.

Electronic payment options: Pay bills via ACH using a vendor network of millions, and outsource your check printing to pay your vendors seamlessly.

Check print outsourcing: Improve efficiency and alleviate a signification portion of check fraud liability by outsourcing your check print services.

Security and fraud protection: Leverage permissions and approval workflows to help prevent and detect fraud.

Quick setup: Your business can be up and running within days. Our implementation experts are on standby to help you get started—all it takes is a one-to-two-hour setup and training appointment. **Dependent upon Bill.com implementation specialists' availability*

Virtual cards: Send one-time card numbers you control to vendors, check the status of payments in real time, and earn cash back on every processed virtual card transaction.

Fraud Protection

Help protect your organization from the increasing threat of cyberfraud with our comprehensive offerings—from security to resiliency planning to crisis management.

Check protection and monitoring services: Minimize your exposure to fraud with check protection services or check monitoring—using check identifiers, payee name verification or threshold payment accounts to monitor checks.

ACH debit block: Protect your company from paying unauthorized ACH debit transactions by specifying which companies are authorized to post debits and setting dollar-limits.

Access & security manager: Delegate cash management tasks while maintaining the control you need by setting entitlements and limits for individual users.

Chase Dual Control—transactions: Requiring a second layer of approval for all transactions, this feature allows you to set internal controls to help identify fraudulent activity and errors before they occur.

Chase Dual Control—administration: Add another layer of protection by requiring primary and proxy admins to provide approval when another admin adds or edits authorized user information or entitlements.

Fraud training: In this training module, learn how to protect your business and empower your employees to fight back against cyberfraud.

We're Here for You No Matter What

As your business continues to evolve, we're here to provide support today and help you prepare for the future.

Team preparedness: Teams in multiple geographic locations help manage operations to minimize the impact of disruptive events on you and your business.

Responsiveness: Our safety and resiliency plans will activate as necessary to address your needs.

Readiness tested: Our plans have been rigorously tested, with key personnel and business activities able to move to other sites as necessary.

Support in place: Depending on the location of disruption, staff at unaffected locations are well-prepared to support this model and have the capabilities to meet your needs.

ADDITIONAL INSIGHTS

Visit jpmorgan.com/cb for more on these and other topics.

How Will You Bring Employees Back to the Workplace?

5 Steps to Identify and Assess Vendor and Customer Risk

Adapting to an Expanding Cyber and Fraud Threat Landscape

Now vs. Later: Which Technologies to Implement When