Protecting against and recovering from **fraud** and **identity theft**

WHAT TO DO

JPMorgan Chase & Co.

Our commitment

At J.P. Morgan, protecting your information and assets is our top priority. As a client, you benefit from the controls and processes we have in place to maintain the privacy and confidentiality of your financial information. While we deploy sophisticated fraud prevention strategies, you are an integral component to preventing fraudulent activity, and are ultimately responsible for ensuring your own cybersecurity.

If you have any questions, please call your J.P. Morgan representative about additional steps you may be able to take to protect yourself.

Responding to **a growing threat**

Fraud and identity theft are growing and serious threats, making it essential that fraud prevention is incorporated into your daily activities.

The following pages identify fraud trends and areas of serious vulnerability—and provide detailed steps you can take to help protect yourself, your assets and your personal information.

How **fraud** and **identity theft** happen

Fraud can be perpetrated in many ways. Fraudsters no longer only steal your information through physical means, but also leverage technology to compromise your confidential and financial information for financial gain.

HOW FRAUD HAPPENS

Social engineering

Fraudsters go to great lengths to deceive individuals into providing confidential or sensitive information via email (**phishing**), phone (**vishing**), or text message (**SMiShing**) by claiming to be a trusted associate or organization.

J.P. Morgan Chase will never ask you to disclose confidential information or credentials in an email or text message.

Email compromise

Fraudsters target individuals and businesses that regularly perform wire payments by using language specific to you or your company, and attempt to impersonate you or your trusted associates in order to redirect funds to accounts under their control, via email in a number of ways.

Email Compromise can occur through **hacking**, when a fraudster gains unauthorized access to a legitimate email account, and/or **spoofing**, when a fraudster creates an email address that looks similar to a legitimate email address in order to trick individuals into believing it is genuine.

Third Party Email Compromise: Both individuals and organizations can fall victim to third party email compromise fraud. Fraud occurs when fraudsters exploit trusted relationships between you, your business, and vendors or third party service providers. Fraudsters often target third parties you work with in an attempt to redirect payments to their accounts. They may hack the third party's email system or spoof their email address and send genuine-looking invoices to deceive you or your business.

HOW FRAUD HAPPENS

Remote access attack	Fraudsters can gain remote access to your computer through **malware** or **social engineering** attempts claiming to be reputable service protection providers. With this access, fraudsters can take over your computer and complete transactions without your knowledge.
Mobile device takeover	**Mobile device takeover** occurs when fraudsters hijack a phone number without having possession of the physical device. Fraudsters trick cell phone service providers into transferring (or porting) the victim's phone number from an existing device to a new device, giving fraudsters the ability to reset the victim's passwords on every account that uses the phone number for auto recovery and access to information sent to the mobile number by text, phone call or email.
Physical theft	Fraudsters may: **Access** your personal information, including medical records or other sensitive documents, by targeting institutions/entities to whom you've previously provided personal data in the normal course of doing business. **Steal** or **divert** your mail to another location through the postal service. **Steal** your laptop or mobile phone.

Your personal or your firm's information can be used to:

- Open a bank account or apply for credit using your name, date of birth and other personal identification numbers
- Initiate money movement transfers from accounts
- Hold your information or other sensitive data for ransom
- Enroll in wireless service or other utilities in your name
- Forge existing or print counterfeit checks or debit cards
- File a fake tax return and steal your refund

TYPES OF FRAUD

Wire fraud

Wire fraud occurs when a fraudster transfers funds to an account unbeknownst to the account holder, or when the account holder unintentionally sends a wire transfer to a fraudulent account. Fraud often occurs when fraudulent payment instructions are received via email.

Online banking fraud

Online banking fraud occurs via **social engineering**, or when **malware** is installed on your device. Through these tactics, fraudsters gather login credentials.

Once your online account is compromised, a fraudster is able to view account information, initiate payments and update contact information.

Check fraud

Traditional paper checks contain sensitive and personal information such as your name, address, account number, routing number and signature, which fraudsters can use to illegally access your accounts. **Check fraud** occurs when fraudsters steal and/or forge physical checks, create counterfeit checks using genuine account and routing details, chemically remove and replace details on a check (check washing) or trick individuals into withdrawing funds against a check that has not cleared (check kiting).

ACH fraud

Automated Clearing House (ACH) is an electronic payment network that enables businesses and individuals to securely transfer funds via their banks. **ACH fraud** occurs when fraudsters trick you into sharing your bank routing number and account number, or by obtaining the information from a check. Fraudsters can sometimes initiate payments from your bank account through a third party service provider by knowing these two pieces of information.

Payroll fraud

Payroll fraud occurs when fraudsters hack into businesses' networks, deploy sophisticated malware or impersonate employees, ultimately to change details in the payroll system.

Targeted financial exploitation of individuals

Targeted financial exploitation of individuals occurs when fraudsters misuse, misappropriate or steal funds from elder or vulnerable persons. Fraudsters can be unknown individuals or trusted individuals like family members, care givers or professionals, like an attorney or financial advisor.

TYPES OF COMMON FRAUD SCAMS

Tech support	A fraudster impersonates a software technician and requests to access your computer remotely to remediate an issue. Sometimes an alert appears on your device that instructs you to call a technical support staff. Do not allow anyone to access your device remotely.
Extortion	A fraudster claims that a loved one has been arrested or hospitalized and requests payment for their release or medical expenses. Often, the fraudster creates a sense of urgency and states the transaction must be "confidential" to bypass controls.
Tax	A fraudster claims you owe a debt to a government agency and requests for credit card, gift card or account information over the phone or email.
Lottery and inheritance	A fraudster promises cash prizes or an inheritance reward if fees or taxes are paid in advance.
Investment	**Investment fraud** occurs when fraudsters use deceptive methods to persuade potential investors into making purchases or sale decisions. They may take advantage of common interests or associations to build trust among potential investors, and use false or misleading information or fictitious opportunities. A fraudster requests payment, such as bitcoin, for an investment or business opportunity, typically offered without credible background, history or documentation.
Romance	A fraudster expresses a pretense of romantic interest to build an emotional connection, typically via social media or online dating sites.

Protect yourself from fraud and identity theft

At J.P. Morgan, we believe that one of the best ways to fight fraud and identity theft is to prevent it from happening in the first place. A few simple precautionary measures can go a long way to help prevent someone from stealing important personal and financial information.

Top actions you can take to protect yourself from fraud

GENERAL FRAUD PREVENTION GUIDELINES

1. **Be mindful of the information you share with others, even in the normal course of doing business**
2. **Do not use personally identifying information as your username or password**
3. **Create strong and complex passwords on all devices and online accounts,** never share them, change them frequently and consider using a password management tool
4. **Be mindful when using public Wi-Fi.** Confirm the network name before connecting. Avoid using your card to make online purchases or logging into your banking accounts
5. **Remain vigilant for suspicious activity** online and in your physical surroundings
6. **Keep financial documents and records in a secure place,** and destroy sensitive documents you no longer need
7. **Carry only what you need.** The less personal information you have with you, including personal checks, the better off you will be if your purse or wallet is stolen

MONEY MOVEMENT AND ONLINE BANKING GUIDELINES

1. **Never share banking credentials and passwords,** and each user should have a unique user ID. Additionally, consider leveraging an RSA token to help secure your online accounts. A token is a real-time code that refreshes every minute and is needed to login to your account, in addition to your username and password
2. **Adopt multi-factor authentication** for all online banking and email accounts, and always log off your online accounts when not in use
3. **Always validate payment instructions** by calling the originator, or source of the instructions, on a known number when instructions are received via email, even if the email is from a senior member of the company or a trusted vendor
4. **Consider using online bill pay,** and print your statements at home or in the office through a secure connection rather than receiving them through the mail
5. **Check your online banking accounts for unauthorized activity** periodically, and **set up online alerts** to notify you of account changes and transactions
6. **Do not preprint or include personal information** on checks, and store them in a safe place

COMPUTER, EMAIL AND TELEPHONE GUIDELINES

1. **Be wary of the following red flags in emails:**
   - Spoofed email address
   - Poor grammar or spelling
   - Urgency around payment transmission
   - Last-minute changes of payment instructions
   - Suspicious attachments or links
   - Blurred company logo on an invoice

2. **Do not allow anyone to access your computer remotely**
3. **Do not assume a phone call is genuine** because the person on the other end has your information; call the business back on a known number as listed on its website
4. **Do not call or text an unknown phone number;** call a known number (such as contact information on the back of your credit card or your J.P. Morgan representative) to help prevent a possible fraud incident
5. **Protect your mobile devices.** Contact your service provider to implement additional controls, like an account PIN or password, to protect you from authorized transactions
6. **Ensure operating systems and data protection software** on your computer and mobile devices, including anti-malware and anti-virus software, are up-to-date

In the United States, additional steps you may take are:

1. Monitor credit

Monitoring your credit report is the single best way to spot signs of identity theft, such as errors, suspicious activity and accounts or addresses you don't recognize. The three U.S. credit bureaus are required to provide one free credit report per year upon request. However, you may find different information on each bureau's report; consider reviewing all three reports. Any suspicious or fraudulent credit listing should be reported to the credit bureau that is showing the activity.

2. Place a fraud alert

Placing a fraud alert requires creditors to contact you first before opening a new account in your name or making any changes to existing accounts.

Fraud alerts may be effective at stopping someone from opening new credit accounts in your name; however, they do not freeze your credit. Your credit score may continue to change, as alerts do not prevent the misuse of existing accounts. Please note: You only need to contact one credit bureau to have a fraud alert put in place, as that bureau is required to share the alert with the other two bureaus.

Three types of fraud alerts are available:

- **Initial Fraud Alert:** Primarily used by individuals who feel their identity has been compromised. Initial Fraud Alerts last 90 days from the date issued, are free of charge, and can be continuously renewed
- **Extended Fraud Alert:** Reserved exclusively for victims of identity theft and designed to protect your credit for seven years
- **Active Duty Military Alert:** Reserved for military personnel who want to protect their credit during deployment. Alerts last for one year and can be renewed

3. Implement a credit freeze

Also known as a security freeze, a credit freeze restricts access to your credit report, making it more difficult for identity thieves to open accounts in your name and/or abuse your credit. A credit freeze prevents a person, merchant or institution from making an inquiry about your credit report unless you temporarily lift or remove the freeze. Your credit report will continue to be accessible to your existing creditors or to debt collectors acting on their behalf. Your credit score will not be impacted by the credit freeze; it will continue to increase or decrease based on activity in your existing accounts.

Implement a credit freeze (cont.)

Putting a credit freeze in place must be done separately with each of the three U.S. credit bureaus. The cost of identity theft far outweighs any nominal fee incurred.

4. Lift a credit freeze

A credit freeze remains in place until you direct the credit bureau to either temporarily lift it or remove it entirely. For example, you can temporarily lift the credit freeze when you are applying for credit or employment. If possible, find out which credit bureau a merchant or prospective employer plans to use for its inquiry, and lift the freeze at that particular bureau. Please note: It can take up to three days for a bureau to lift a credit freeze.

The three major U.S. credit bureaus have set up a central website and telephone number where you can secure, or freeze, your credit and order your free annual reports:

877-322-8228 www.annualcreditreport.com

Contact each of the three credit bureaus if you wish to order your credit report:

Equifax	Experian	TransUnion
800-685-1111	888-397-3742	800-888-4213

Contact one of the three credit bureaus if you wish to place a fraud alert:

Equifax	Experian	TransUnion
888-766-0008 www.equifax.com/ CreditReportAssistance	888-397-3742 www.experian.com/ fraudalert	800-680-7289 www.transunion.com/ fraud

Contact each of the three credit bureaus if you wish to put a freeze in place or lift a freeze:

Equifax	Experian	TransUnion
800-349-9960 www.freeze.equifax.com	888-397-3742 www.experian.com/ freeze	888-909-8872 www.transunion.com/ freeze

Recovering from fraud and identity theft

Regardless of where you're located, as soon as you become aware of fraudulent activity on your account, or that your information may have been used, stolen or compromised, notify your J.P. Morgan representative. The sooner you notify your representative, the faster we can help you.

WHEN APPLICABLE, WE WILL:

- **Close any compromised J.P. Morgan account(s) and open new account(s)**
- **Block online access to your account(s), debit and credit cards, and checks** to protect your account while we determine if your online profile has been compromised
- **Place a fraud alert on your accounts** to prevent potential loss
- **Provide guidance on reclaiming your identity**

Your J.P. Morgan representative can also walk you through the basic steps that apply to most identity theft cases.

ADDITIONAL STEPS YOU CAN TAKE TO RECOVER FROM IDENTITY THEFT

Contact your local police department

Many creditors and institutions will require a record of the theft in order to mitigate the damage created by fraudsters, including removing any fraudulent debt that might have accrued.

- File a police report, request a copy and retain all documents related to the compromised accounts

Contact various fraud departments

Contact the fraud department of each of your creditors and financial institutions

It's important to remember that when an account is compromised, other accounts may also be at risk.

- Report the incident to any creditor with whom you have a relationship, provide a copy of the police report and follow their guidance, even if your account at that financial institution has not been compromised
- Confirm all conversations with creditors in writing; consider following up phone calls with a letter and any necessary documentation to support your claim

Be alert to malware

Identify if your computer or mobile device has been infected with malware, and use an uncompromised device to begin the process of recovering your identity

- Consult an IT professional for guidance if you suspect your device has been compromised, and repair as needed
- Disconnect your device from the Internet, install reputable anti-virus software and run a scan to identify malicious software
- Ensure your device and system are updated and secure before using them again

Secure your online accounts

Ensure your online accounts are secure

- Use an uncompromised device to change login credentials, including passwords and PINs
- Alert your contacts to be aware of fraudulent emails

The following pages will provide additional steps you can take to recover from identity theft and fraud in each major region.

Recovering from identity theft and fraud in the United States

1. Report the incident to all three of the major credit bureaus

Your identity and credit history can be used to secure loans, gain employment and open credit cards, so it is essential to report the incident to all three major U.S. credit bureaus, and either place a "credit freeze" or a "fraud alert" on your account.

- A "credit freeze" restricts access to your credit report unless you direct the credit bureau to temporarily or permanently lift the restriction
- A "fraud alert" and a "victim's statement" will direct creditors to contact you before opening any new accounts in your name or making any changes to those already listed in your credit report

Regularly monitor your personal information and online accounts for unauthorized charges to existing accounts. Request copies of your credit reports and review them for fraudulent accounts.

Equifax	Experian	TransUnion
To order your report: 800-685-1111	To order your report: 888-397-3742	To order your report: 800-888-4213
To report fraud: 888-766-0008 www.equifax.com/ CreditReportAssistance	To report fraud: 888-397-3742 www.experian.com/ fraudalert	To report fraud: 800-680-7289 www.transunion.com/ fraud
To place a credit freeze: 800-349-9960 www.freeze.equifax.com	To place a credit freeze: 888-397-3742 www.experian.com/ freeze	To place a credit freeze: 888-909-8872 www.freeze.transunion.com

2. Complete an Identity Theft Affidavit provided by the Federal Trade Commission (FTC)

An Identity Theft Affidavit will provide creditors and financial institutions with the information and contacts needed to protect your identity and investigate any fraud event.

File the affidavit, retain a copy, and provide it to all creditors, investigators and financial institutions.

3. Report fraud to the Internet Crime Complaint Center (IC3)

IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center, and allows you to easily report cyber incidents and identity theft to agencies at the federal, state, local and international levels.

www.ic3.gov

Additional resources in the United States

There are additional steps you can take to further protect yourself and help minimize future losses.

- Report mail theft to the **U.S. Postal Inspection Service**

  www.postalinspectors.uspis.gov

- Report passport loss and/or fraud to the **U.S. Department of State**

  www.travel.state.gov/passports

- Report Social Security fraud to the **Social Security Fraud Hotline**

  800-269-0271
  www.oig.ssa.gov/report

- If you suspect your name is being used by a fraudster to obtain a driver's license or state ID card, or if your driver's license has been lost or stolen, contact your local **Department of Motor Vehicles**

- If you suspect your checks have been compromised, contact the major check verification companies and request that they notify retailers that use their databases to not accept your checks

  Certergy, Inc.
  800-437-5120

  International Check Services
  800-631-9656

  TeleCheck
  800-710-9898 or 800-927-0188

  You may also contact **Scan,** a check verification service, to learn if any fraudulent checks have been passed in your name. Scan also provides retailers with access to a database of returned checks.

  800-262-7771

Recovering from identity theft and fraud in the United Kingdom

1. Check your credit information

Regularly monitor your personal information and online profiles. Request copies of your credit reports and review them for fraudulent accounts and unauthorized charges to existing accounts.

Credit Agency	Website
Equifax	www.equifax.co.uk
Experian	www.experian.co.uk
Call Credit	www.callcredit.co.uk
Noddle	www.noddle.co.uk

2. Report the incident to Action Fraud

Action Fraud is the United Kingdom's national fraud and cybercrime reporting center.

- Contact Action Fraud to report the theft; they can also help advise on next steps to take and additional organizations to contact

  www.actionfraud.police.uk
  0300-123-2040

3. Report the incident to Cifas

Cifas works with organizations and individuals in the United Kingdom to detect and prevent financial crime.

- Contact Cifas to place a "Protective Registration" warning on your credit file, which alerts lenders to conduct extra checks to ensure the person applying for credit is you and not a fraudster

  www.cifas.org.uk/pr

Additional resources in the United Kingdom

To further protect yourself and help minimize future losses:

- Report mail theft to the **Royal Mail Customer Enquiry** or your local post office to prevent any false mail redirection instructions

  0845-774-0740

Recovering from identity theft and fraud in Latin America

1. Check your credit information

Regularly monitor your personal information and online profiles. Request copies of your credit reports, and review them for fraudulent accounts and unauthorized charges to existing accounts.

Country	Credit Agency	Website
Argentina	Experian Equifax	www.experian.com.ar www.soluciones.equifax.com.ar
Brazil	Serasa Experian Equifax	www.serasaexperian.com.br www.equifax.com.br
Chile	Experian Equifax	www.experian.cl www.soluciones.equifax.cl
Colombia	Datacrédito Experian	www.datacredito.com.co
Costa Rica	Equifax	www.equifax.co.cr
Ecuador	Equifax	www.equifax.com/home/es_ec
El Salvador	Equifax	www.equifax.sv
Honduras	Equifax	www.equifax.hn
Mexico	Experian Equifax	www.experian.com.mx www.equifax.com.mx
Paraguay	Equifax	www.equifax.com/home/es_py
Peru	Equifax	www.equifax.com/home/es_pe
Uruguay	Equifax	www.equifax.com/home/es_ur

Additional resources in Latin America

To further protect yourself and help minimize future losses:

- Report mail theft to your local post office to prevent any false mail redirection instructions

Recovering from identity theft and fraud in Asia

Hong Kong residents: Receive consultation services about your fraud incident by contacting the Anti-Deception Coordination Centre (ADCC)

- If calling from Hong Kong, dial 999
- If calling from the United States, dial 011-852-999 or +852-999

Singapore residents: Contact Credit Bureau Singapore (CBS) for assistance.

- CBS Hotline: +65 6565 6363
- Email: consumer_services@creditbureau.com.sg

Japan residents: Report identity theft incidents to:

- Japan Credit Information Reference Corp. (JICC)

Prevent future identity theft

- Do not share account information with any unauthorized user, including family, friends or any unknown individuals
- Ensure each authorized user has a unique login ID and complex password for online banking accounts
- Do not allow anyone to remotely access your device
- Do not share private information in response to an email, text message, letter or phone call
- Always verify a website's authenticity before making online transactions
- Always conduct a verbal call back to confirm wire instructions if instructions were provided through email
- Always keep your credit card in sight while making in-person transactions
- Shred any receipts or documents that may contain your identification number

J.P. Morgan will never:

– Ask you to log in to the same computer with more than one user's credentials

– Ask you to repeatedly submit login credentials

– Contact you about online problems, such as logging in, if you haven't contacted us first

If you believe you have been targeted by a fraud scheme or your login credentials have been compromised, please contact your J.P. Morgan representative.

Remember, if you receive a request to provide personal or financial information, take a step back from the situation to evaluate it. Even if the requestor claims to be your bank or other trusted organization, don't rush to action!

We can help

Speak with your J.P. Morgan representative to learn more about our cybersecurity and fraud awareness programs, for additional educational information, and to schedule a session with our experts.

AMCYBER_ID_THEFT_BKLT_V13_032020