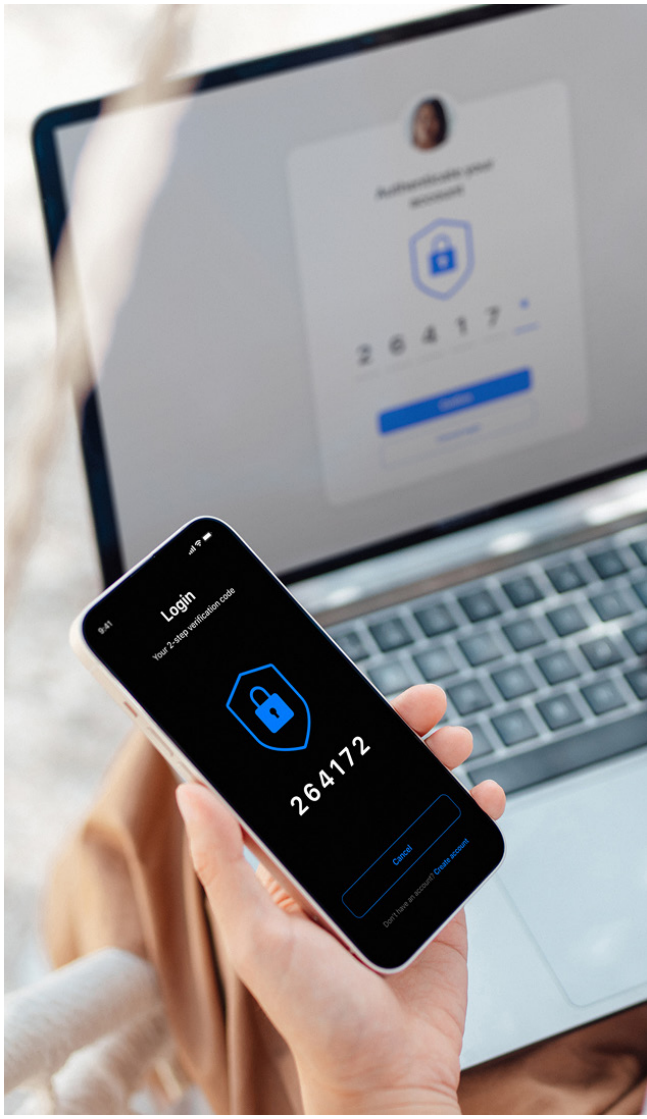
J.P.Morgan
PRIVATE BANK

FRAUD PREVENTION

Fraud scheme: Mobile device takeover

Fraudsters have figured out how to take over your mobile phone without actually stealing it. Instead, they impersonate you to your mobile phone service, which allows them to hijack your phone number by transferring it and your phone data from your existing device to one under the fraudster's control. Once fraudsters gain access, they have the ability to reset your passwords on accounts that use your phone number for auto recovery, and are able to receive one-time verification codes sent to the mobile number by text, phone call or email.



Disruption of your telephone service, such as the inability to receive calls or text messages in a location that normally offers service, can be a sign that you are a victim of mobile device takeover. In the event of a disruption of approximately 15 to 30 minutes, call your service provider immediately to identify the root cause. Also, call your J.P. Morgan team to ensure that we are able to partner with you to help remediate the issue as quickly as we can.

Ways mobile device takeover can occur

Fraudsters have also learned that compromising a mobile phone number, by tricking an individual into clicking on a link within a text message or through the use of a physical SIM card, can be leveraged to commit fraud. Through social engineering, they will attempt to obtain that individual's phone number, name, address and other personally identifying information. Using that information, fraudsters will impersonate the individual when contacting the service provider.

Phone porting:

Phone porting is a service offered by mobile carriers to allow customers to easily switch providers without creating a new phone number. Fraudsters leverage this common practice to redirect an individual's phone number to gain access to it and all associated data.

SIM swap:

The SIM (Subscriber Identity Module) card stores subscriber data and connects an individual's device (and phone number) to the mobile network. Without a SIM card, an individual would not be able to place or receive phone calls or text messages. Fraudsters leverage this process to trick the mobile service provider into activating a new SIM card that the fraudster possesses.

Call forwarding:

Telephone providers offer a feature that allows inbound calls to be forwarded to another number. Fraudsters use this service, by hacking into your online mobile account or calling the provider, to redirect your phone number to another number, which they control.

To help mitigate these risks, consider the following best practices:

1. **Contact your mobile service provider:**
   - If you experience an unexpected interruption in service for a significant period of time
   - To add a verbal password to your account and lock your account to prevent your phone number from being transferred or ported without your authorization (Note: Many mobile service providers now have a service to prevent unauthorized transfers, but not all do. See below for details on how to initiate this security feature.)
2. **Protect your mobile devices and tablets** with your fingerprint or facial recognition technology, if available; if these security features are not available, use strong, complex passwords:
   - Avoid using the same PIN for multiple devices
   - Enable multi-factor authentication for all online accounts, if offered by the mobile service provider
3. **Enable your device to automatically lock itself** after a period of inactivity
4. **Install antivirus software on your mobile device** and activate automatic updates to ensure the device remains protected
5. **Avoid answering calls from unknown individuals;** be wary of impersonators attempting to deceive you into divulging information or taking action on a financial account
   - Verify the caller before providing any information. If you are unsure, call the business on a known number. For example, if you receive a call from JPMorganChase, call the number on the back of your card, or call your J.P. Morgan team before providing any information
   - Never provide your full card number, PIN or one-time authentication passcode to an unknown caller, even if the caller claims to be from J.P. Morgan
6. **Before trading in an old device, erase any personal information** it may contain by resetting it to its factory settings

Contact your mobile service provider to implement additional controls on your account:

In the United States

AT&T Wireless

- **Add extra security to your wireless account**
  - Log in to your online profile > Account setting > Linked Accounts > Manage extra security > Extra security > Re-enter passcode if prompted
- **Download the AT&T ActiveArmor security app** to protect your personal data; go to https://www.att.com/security/security-apps/

Verizon Wireless

- **Set up an account PIN** to verify your identity when you contact Verizon
  - Log in to your "My Verizon" app > Account > Edit profile & setting > Security > Manage Account PIN
- **Download the Verizon Call Filter app** to receive alerts on incoming spam calls, and easily report and block unwanted numbers on your mobile phone; go to https://www.verizon.com/solutions-and-services/call-filter/
- **Protect your mobile number from unauthorized transfers with Number Lock**
  - Log in to your "My Verizon" App > Edit profile & settings > Security > Number Lock (choose phone number if applicable) > Tap the toggle button to select On > click Save Changes. For more information, go to https://www.verizon.com/support/port-out-faqs/#what-transfer-freeze
- **Protect your SIM card by creating your own unique PIN** On your device, go to Settings > Security & Privacy > More Security Settings > SIM card security > Activate Lock SIM card by creating a PIN
- **To protect your account from mobile porting,** log in to your "My Verizon" app > Account > Settings > Security > Number Lock
- For additional tips on how to protect your Verizon account(s), go to www.verizon.com/about/responsibility/account-security

T-Mobile

- **Set up an account PIN for when you contact T-Mobile**
  - Log in to your "My T-Mobile" > Choose a verification method (text message or security question) > Next > Follow the prompts > Enter your desired PIN/Passcode
  - **To protect your account from mobile porting, set up T-Mobile's NOPORT security feature**
  - Call 611 from your T-Mobile number or call 1-800-937-8997 from any phone number to add this feature to your account
- **Set up multi-factor authentication through "account profile" online or by calling T-Mobile**
- **Download T-Mobile Scam Shield app** to identify suspected spam calls and block numbers you don't want to receive calls from
- **Download the Lookout app to protect your device** from viruses, malware and spyware

In Europe and Asia

Coop Mobile

- **Block and reorder SIM** cards if your phone is lost or stolen; call 01608 434 072
- **Block unwanted calls**
  - Log into My Account > Service Settings to activate or deactivate this function

Lebara

- **Lost SIM Card?** Order a replacement at https://www.lebara.co.uk/en/help/smart-help.html
- **To report fraud,** go to https://www.lebara.com.au/support/fraud/
- **Activate Call Filter to block unfair calls;** go to myLebara > Settings > Call filtering

Yallo

- **Lost or stolen: Block your SIM;** go to https://support.yallo.ch/hc/en-gb/sections/360000249358-SIM to learn more
- **Activate the call filter** to block unwanted calls. Log in to your account > Settings > Call Filter
- **Switch to an eSIM**
  - Log in to your account > Settings > eSIM

TalkTalk

- **To report spam,** forward text(s) and the sender phone number(s) to 7726
- **To report phishing,** forward email to phishing@talktalk.co.uk
- **Activate Last Caller Barring** to block the last phone number that called you. Log in to your account > Networks & Connections > My Telephone Settings > Tick the box next to Last Caller Barring > Select Update

Sunrise

- **Report fraud or misconduct** at https://www.sunrise.ch/en/residential/help/kontakt/report-a-fraud-case.html
- **Manage SIM cards** at https://www.sunrise.ch/en/support/mobile/sim-card-esim
- **Register for the Surf Protect** to block malware and unsafe websites by texting SURFPROTECT to 5522
- **Enable the MobileID app** for easy and safe online login at https://www.mobileid.ch/en

Swype

- **To block your SIM if lost or stolen,** log in to the swype app > Number settings (⚙) > SIM settings > Block SIM
- **To order a replacement SIM,** log in to your account > Number settings (⚙) > SIM Settings > Replace SIM Card > confirm shipping address > Confirm Order
- **To block spam calls,** log in to the app > Number Settings (⚙) > Activate Call Filter

EE

- **To block incoming unsolicited calls,** open your phone dialer and go to "Settings" > Call blocking > Manage the list of unwanted callers
- **To block unwanted text messages,** open your phone's messaging app and go to "More/Settings" > "Block" > Select the number
- **If your phone shows the message "This phone has been disabled by EE...,"** the phone has been reported as having been obtained by fraud. That means you won't be able to make calls or access data on the phone. Immediately call EE, as only EE can re-enable the phone
- For additional tips on how to protect your EE account(s), go to https://ee.co.uk/help/help-new/safety-and-security

O_2

- **Set up a PIN** to protect your mobile device under Settings > General or Security > Passcode lock or Screen lock based on your cellular device
- For additional tips on how to protect your O_2 account, go to https://www.o2.co.uk/help/safety-and-security/mobile-security

Swisscom

- **Activate "Callfilter"** on your mobile phone to block incoming unsolicited advertising calls
  - Log in to your "My Swisscom" app > Swisscom Cockpit > "Call Settings" > "Callfilter"
- **If your phone is stolen,** block your SIM in the Customer Center to prevent the thief from using your mobile to make calls, and then report the theft to the police

Vodafone

- **Download the Vodafone Secure Net app to protect your device** from viruses and harmful websites
- **Forward spam texts to 7726** (Android devices can tap the **Report Spam** button in the messaging app)
- For additional tips on how to protect your Vodafone account(s), go to https://www.vodafone.co.uk/privacy/protecting-you

In Asia

Singtel

- **Set up a 4-digit PIN** to verify your identity when you contact Etisalat
- For additional information, go to https://www.etisalat.ae/en/consumer/support/mobile/prepaid/4digit_security_pin_faqs.jsp

1010/CSL

- **Set up a PIN** for your account
  - Log in to "1010.com" with your mobile number > Onetime password > Enter the password and verify
- **Download SafetyNet,** which detects whether content contains malicious software or poses a security risk
- For additional tips on how to protect your 1010 account(s), go to https://www.1010.com.hk/jsp/our_services/network_protect/mobile_protect_eng.htm

Maxis

- **Protect your device by** requesting SIM/Device blocking, and report lost or stolen devices by contacting Maxis customer service or visiting a Maxis store

We can help

If you believe you have been a victim of fraud, speak with your J.P. Morgan team immediately.