J.P.Morgan

J.P. Morgan International Private Bank Client Website System Requirements and Security Precaution

SYSTEM REQUIREMENTS

- The J.P. Morgan Private Bank Client Website is optimized for the latest version of the following browsers/operating systems:
  Desktop: Microsoft Edge, Google Chrome, Mozilla Firefox and Apple Safari
  Mobile App: iOS and Android

ASSISTANCE

- If you have any queries or feedback about logging on, accessibility, or security, please do not hesitate to contact your Client Service Specialist
- Any complaint that you may have relating to this service may be addressed to us in accordance with the Private Client Terms General Terms
- We shall immediately investigate any complaint/dispute brought to our attention and provide you an update of our investigations and the status of your case. Security incidents will be escalated to our technical support staff as a matter of priority

PRIVACY & SECURITY

Our clients' privacy and security is of primary importance to us. At J.P. Morgan Private Bank, we are committed to ensure we achieve these objectives. In this respect, we have taken the appropriate steps to secure your information using the latest available software and techniques for data protection over the Internet, as explained hereafter. Furthermore, we will only permit authorised employees, who are trained in the proper handling of customer information, to have access to that information.

J.P. Morgan's Private Bank Client Website takes advantage of the latest security software for authentication, encryption and audit trail. It uses Siteminder authentication software and incorporates TLS 1.2 to transmit data. You will be given both a user name and a temporary password, your account is also protected through additional authentication process (One-time passcode via SMS or Voice call). You should however be aware that since the Internet is a public network, your identity and J.P. Morgan's identity as Internet users cannot be kept secret. Consequently, there is a risk that one may infer from the flow of encrypted data between your computer and J.P. Morgan's Private Bank's computers that a banking relationship exists with you.

In order to prevent others from gaining access to your information, it is advisable that you log off using the Log Off button once you have finished using the site, especially if the computer you use can be accessed by another person. Please note that as a safety precaution, the Client Website will log off automatically after 15 minutes of inactivity. You should in addition be aware that despite the security measures taken by us, connecting to the Internet involves the risk of unwillingly downloading computer viruses or monitoring devices (cookies). We advise you to take appropriate measures to prevent unauthorised persons from accessing your computer by protecting it with a secret password and using virus detection software.

SECURITY PRECAUTIONS

Examples of security practices that can help you to protect yourself:

a) Security in relation to your Password:

- Password must be kept confidential at all times and not be divulged to anyone.
- The same Password should not be used for different websites, applications or services, particularly when they relate to different entities.
- Use strong passwords, such as a mixture of letters, numbers and symbols. Do not use easily accessible personal information such as telephone numbers or date of birth to create your password.
- Do not write down or record the Password without disguising it.
- Do not write down the Password on any device for accessing e-banking services or on anything usually kept with or near it.
- Never disclose your Password to anyone including our staff or regulators. Please be aware of masquerading techniques used by unauthorised parties to encourage you to surrender your Password.
- You should immediately contact your Client Service Specialist for a new Password if you think that the existing Password has been compromised.

b) If you request access to your account for a third party it is your responsibility to inform us if and when you require that access to be removed.

c) At login the website provides your last login date and time. Please check this information as it is an important means of identifying if someone else has accessed your account. If your login data and time do not reconcile with your last usage, please immediately change your password and contact your Client Service Specialist to report the situation.

d) Your access will be locked if you have not accessed the site for 12 months.

e) You should not leave your computer unattended if you are in the middle of a session. Lock the screen or logout if you will be away from the computer.

f) Once you have finished using the website, you should promptly log out using the log off button, and then close your web browser.

g) Do not use a computer or a device that cannot be trusted. Avoid using public or internet café computers to access the site.

h) You should regularly check your account balances and statements to identify unusual transactions.

i) It is your responsibility to use suitable firewall software and anti-virus technology to screen any software or other material that you may download from this site and to ensure compatibility of such software or material with your equipment and software. Do not install software or run programs of unknown origin. Update the anti-virus and firewall products with security patches or newer versions on a regular basis.

j) Browsers and application software should be upgraded to support the highest encryption standard.

k) Do not select the option on browsers for storing or retaining user name and password.

l) Remove file and printer sharing in your computers, especially when you have internet access via cable modems, broadband connections or similar set-ups.

m) You should check the authenticity of the bank's website by comparing the URL and the bank's name in its digital certificate.

n) You should check that the bank's website address changes from http://to https://and a security icon that looks like a lock or key appears when authentication and encryption is expected.

o) Due to the site's enhanced security structure, it is advisable to avoid using the Back button on your browser when you want to return to a previous page. Instead, use the links shown throughout the site.

p) Make regular backups of critical data.

q) Consider the use of encryption technology to protect highly sensitive data.

r) Delete junk or chain email. Do not open email attachments from strangers.

s) Do not disclose personal, financial or credit card information to little-known or suspect websites.

t) We recommend you verify the authenticity of an email before accessing embedded hyperlinks. You will not be asked for sensitive information by email.

u) Please be mindful of Phishing and Pharming techniques specifically designed to gather your personal and financial information to perform identity theft.

- Phishing is email fraud where the perpetrator sends out legitimate-looking email that appear to come from well-known and trustworthy Web sites in an attempt to gather personal and financial information from the recipient.
- Pharming is a scamming practice in which connections to web sites are misdirected to fraudulent sites without the user's knowledge or consent. In pharming, larger numbers of computer users can be victimised because it is not necessary to target individuals one by one and no conscious action is required on the part of the victim.

v) Please do not subscribe to SMS forwarding service for a mobile number which you may use to receive One-time passcode via SMS or subscribe to voice forwarding for a phone number which you may use to receive One-time passcode via Voice.

w) Please download the J.P. Morgan Private Bank mobile app from secure, recognized platforms only i.e. App Store or Google Play.

x) Provide accurate contact information for your bank to send transaction notifications.

y) Take steps to protect your username, personal identification number ("PIN"), password and/or relevant security devices or security key ("Token") and access to your protected accounts.

z) In the event you keep a record of your username and password, you should make reasonable effort to secure the record including:

i. Keeping the record in a secure electronic or physical location accessible or known only to you; and

ii. Keeping the record in a place where it is unlikely to be found by a third party.

aa) Enable and monitor transaction notifications and report unauthorized transactions as soon as possible.

bb) Provide information on unauthorized transactions as requested by your bank to support investigations.

cc) Make a police report if your bank requests such a report to be made to facilitate claims investigation.

dd) Comply with device's security features and do not take any action that might disable any security feature on your device. For example, do not use a "rooted" or a "jailbroken" mobile device.

Risks Associated with Online Pay & Transfer

The terms and conditions which govern this service can be found in the Private Client Terms. We would use this opportunity to highlight the risks specific to using this service on the Site:

a) Payments initiated online will be processed according to the details you enter. It is your responsibility to verify the payee information when initiating an online payment request to ensure funds are sent to the intended recipient. J.P. Morgan bears no responsibility to recover funds sent to an incorrect payee;

b) Payments that are initiated online will be subject to the standard verification processes that all payment requests follow. Submitting a payment request does not guarantee that it will be completed, J.P. Morgan is not obligated to reimburse expenses incurred due to a delayed or rejected payment;

c) Payments or transfers that involve a currency conversion will execute the FX conversion immediately at the current market rate that is provided by J.P. Morgan. Successful FX conversions are final, any conversion initiated to reverse the conversion will be executed at the current market rate and may result in financial loss that J.P. Morgan is not obligated to reimburse;

d) Payments or transfers that involve a currency conversion will display a rate of conversion in real-time based on the amount that you are intending to convert. Normal market activity and unforeseen technical issues between the time of entering a payment and submitting the payment may result in your payment request being rejected. If this occurs, you will be required to re-enter your payment details and obtain a new rate of conversion at the current market rate which may be less favorable than the previous rate. J.P. Morgan is under no obligation to honor previous FX rates in this scenario.