

J.P.Morgan

Access & Security Manager Go-To Guide

Overview

Summary

Access & Security Manager allows users to easily manage company entitlements. The feature can be accessed through the “Access & Security” tab and is available to all System administrators. Within Access & Security Manager, Primary admins can:

- Add additional users
- Manage user info, company-level and account-level rights as well as daily transaction limits for users
- Add up to three proxy admin(s) to assist with account management tasks
- View recent user and transaction activity
- Initiate and edit IP Security
- Activate Dual Control for administrative actions and transactions for added security

Proxy admins have access to Access & Security Manager but do not have the full rights of a Primary admin. Please refer to the [Proxy Administrator Go-To Guide](#) for more information.

New Connect users will need to review and activate applicable Pay & Transfer, Collect & Deposit and Security features before building user profiles.

Table of Contents

- I. [Adding Authorized Users](#)
- II. [Choosing a Secure Authenticator](#)
- III. [Managing Entitlements for Authorized Users](#)
- IV. [View Account Activity](#)
- V. [IP Security](#)
- VI. [Activating Dual Control-Administration](#)
- VII. [Activating Dual Control-Transaction](#)

Adding Authorized Users

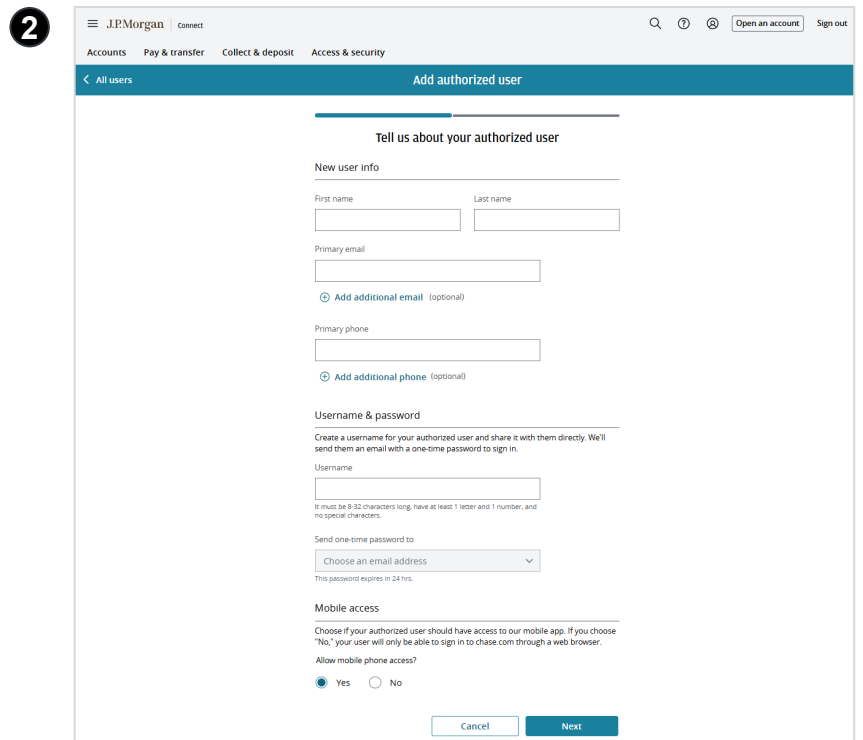
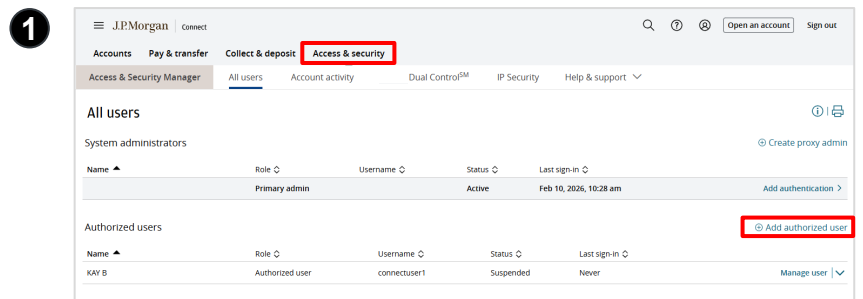
Note: Before adding additional users, ensure there are email addresses and phone numbers for individuals

1. Select **Access & Security Manager** from the **Access & Security** menu
 - a. On the **All users** page, select **Add authorized user**
2. Enter details about authorized user
 - a. Enter First Name, Last Name, Primary email, and Primary phone
 - b. Set a Username
 - a. Determine if Mobile access is needed

Note: Usernames must be at least eight characters and contain at least one letter, one number and no special characters

Note: The system defaults to allow Mobile Access

3. The new user will receive an email detailing how to sign in for the first time, including authenticator instructions and a temporary password



Choosing a Secure Authenticator

1. Enhance online account security by choosing one of the following authenticator options:
 - a. **RSA Authenticator App (recommended):** Download the app, available on iOS or Android. Enjoy the convenience of accessing authenticator directly from smartphone
 - b. **RSA Authenticator Device:** Receive a physical device, which will be mailed to the address provided
2. Review the user details and authenticator request, then confirm by selecting **Set up now**

1

Set up multifactor authentication


Choose an authentication method

After adding an RSA Authenticator App or Device, you'll need to enter a unique token code generated by that authenticator every time you sign in.

a

RSA Authenticator App


Download a third-party mobile app and start using multifactor authentication immediately.

 Download the RSA Authenticator App on iOS® or Android™.

b

RSA Authenticator Device

Get a token code from a physical device. We'll mail it to the address we have on file within 2 business days.

 To change this address, contact your client-service professional.
Primary business mailing address

Next

2

Set up multifactor authentication

Does everything look OK?

User info

First name User

Last name —

Multifactor authentication

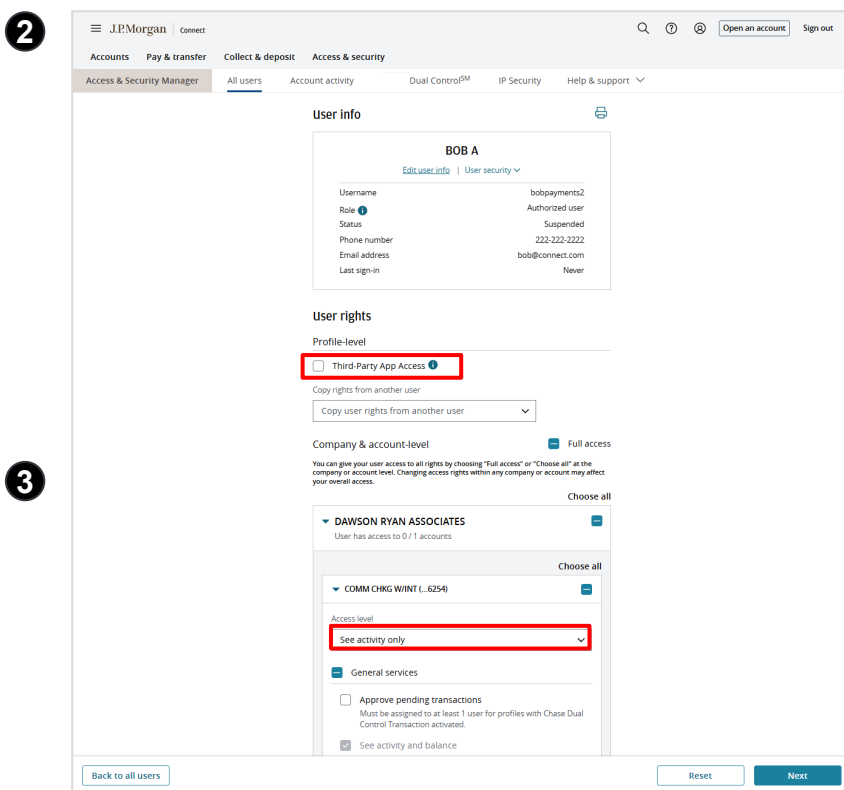
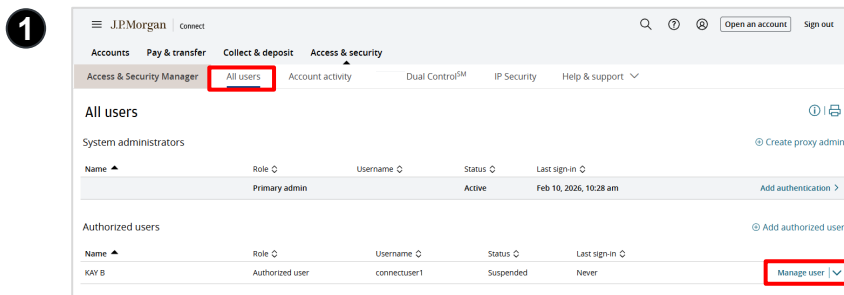
Authentication method RSA Authenticator App

Set up now

Managing Entitlements for Authorized Users

System administrators can assign user rights at the account level for enabled services. Every company and account in the profile will be listed, and access can be assigned for each one. If there are existing users, their settings can be copied by selecting **Copy access level from another user**. Time can also be saved by granting the user **Full access** or by selecting **Choose all** for an entire company or account

1. Select **Manage user** on the **All users** page
2. Select the **Third-party app access** checkbox for user access to connect and upload Connect account information into authorized third-party applications
3. For each account, select the **Access level**:
 - **See activity only:** User can see balances and account history, but can't initiate or approve transactions
 - **Transact only:** User can submit transactions for approval, but can't see balances or account history
 - **See activity and transact:** User can both see balances and account history as well as submit transactions for approval



Managing Entitlements for Authorized Users (Continued)

4. Next, assign user rights, including daily limits and whether their transactions need approval. Options will vary based on services activated, account types and Access level

- **General services:** Includes transaction approval, see activity and balances, see check images, see statements and documents
- **Incoming services:** Includes entitlements for ACH Collections and QuickDepositSM
- **Outgoing services:** Includes entitlements for ACH Payments (Employee & Vendor), Wires, Account Transfers, etc.
- **Security services:** Includes issuing a stop payment on checks, ACH Debit Block and Fraud Protection Services

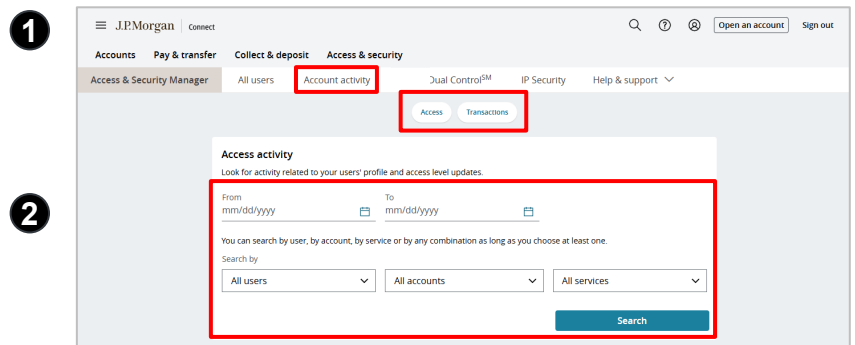
4

The screenshot shows a configuration page for a user profile named 'COMM CHKG'. At the top, it states 'User has access to 0 / 1 accounts'. Below this, there is a 'Choose all' button. The 'Access level' is set to 'See activity and transact'. The 'General services' section is checked and includes options for 'Approve pending transactions', 'See activity and balance' (checked), 'See check images', and 'See statements and documents'. The 'Incoming services' section includes 'QuickDepositSM'. The 'Outgoing services' section includes 'ACH Payment Services—Employees' (with a sub-option for 'Real-time employee payments') and 'ACH Payment Services—Vendors' (with a sub-option for 'Real-time vendor payments'). Both outgoing services have a 'Daily limit' set to 'Profile max'. The 'Cashflow360SM' service also has a 'Daily limit' set to 'Profile max'. The 'Transfers and payments' section has a 'Daily limit' set to 'Profile max' and an 'Approval required' option set to '\$0.00'. The 'Wires' service has a 'Daily limit' set to 'Profile max'. The 'Security services' section is checked and includes 'Stop payment on checks'.

View Account Activity

Primary admins can view up to one year of user activity and 90 days of transaction reports from within Access & Security Manager

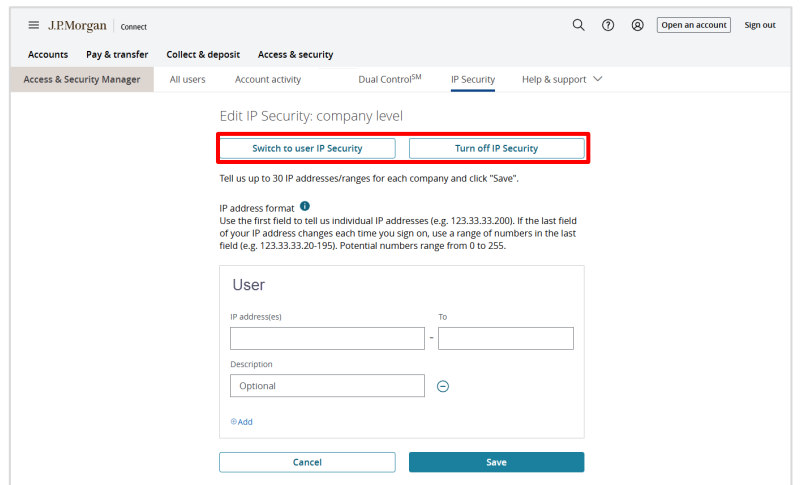
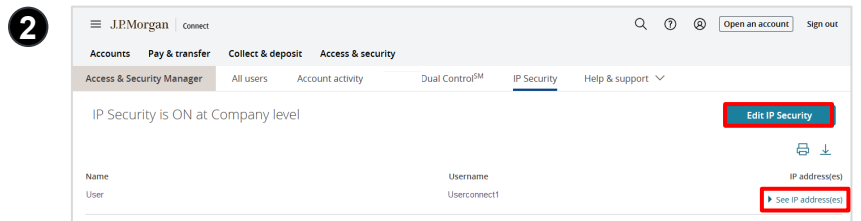
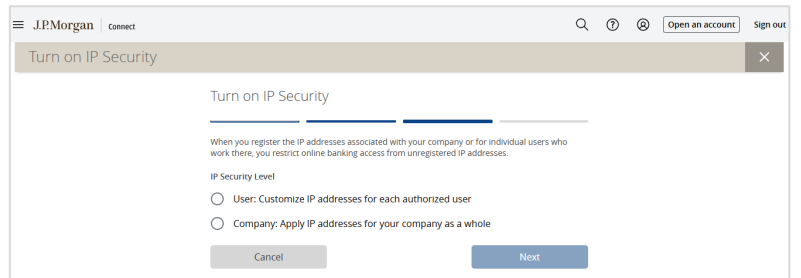
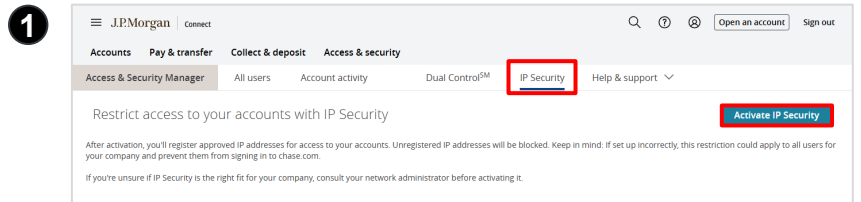
1. Select **Account Activity** then select **Activity type**
 - a. **Transactions:** Results will include who made what transactions against the accounts
 - b. **Access:** Results will include history of changes to user rights and access to accounts
2. Select the date range and **Search by** parameters
 - a. Select **Search**



IP Security

Ensure Primary Admin activates IP Security, utilizing the RSA Authenticator and choosing either a company or user level. Non-authenticator clients need to call in for an activation code from service

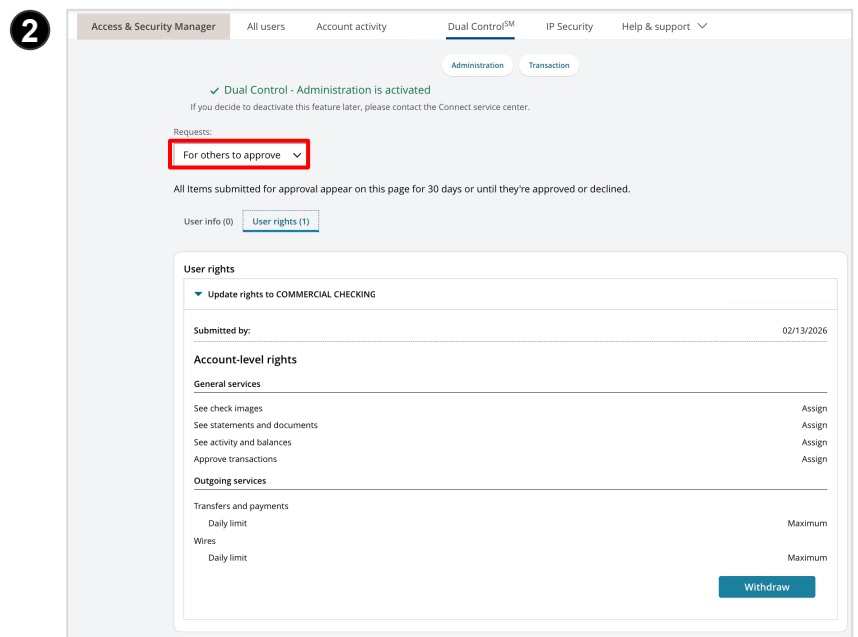
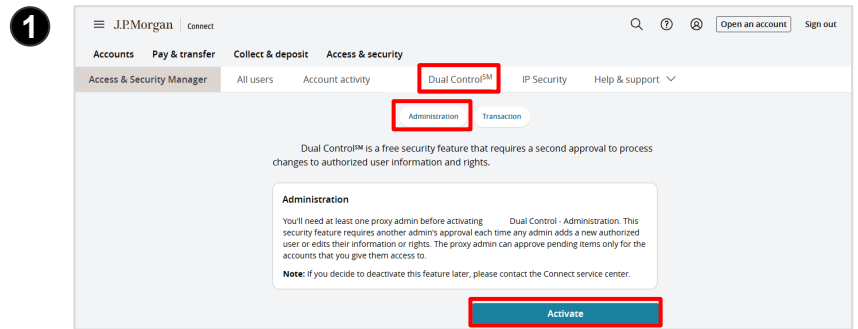
1. Select **IP Security** in the Access & Security Manager tab
 - a. To Turn on IP Security, select **Activate IP Security** and the security level
2. Select **See IP address(es)** to see all addresses. For edits, select **Edit IP Security**
 - a. Can switch between user and company level IP Security
 - b. Option to turn off service
 - c. Change/add addresses



Activating Dual Control – Administration – Activation

When Dual Control–Administration is activated, all administrative actions (e.g., updating user info, account-level rights, company-level rights) require approval by another System Administrator. Only primary admins can activate this feature, but proxy admins can review administrative tasks pending approval if they have account rights. Before activating, ensure there is at least one proxy admin created

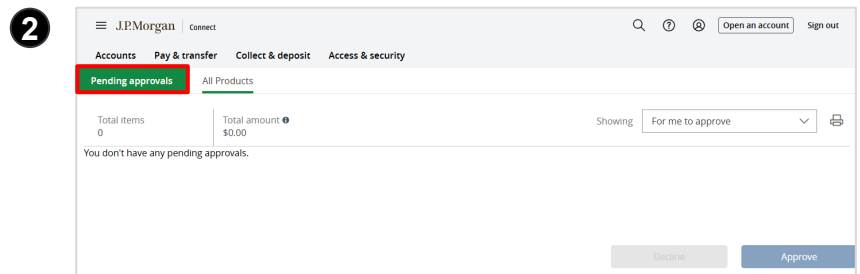
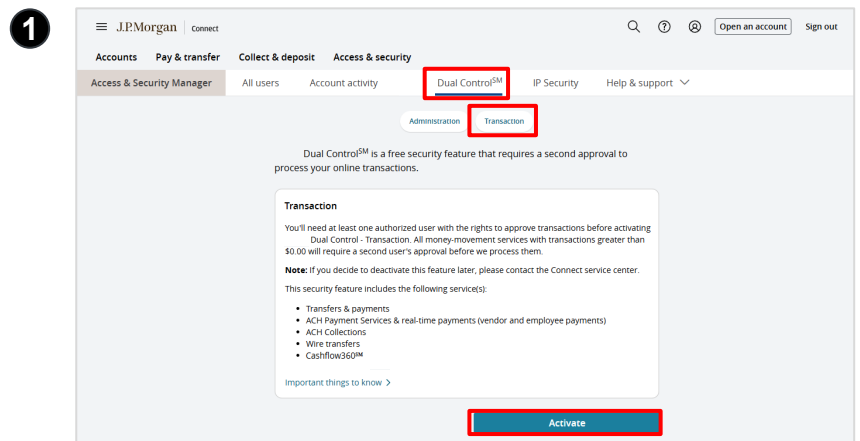
1. Select **Dual Control** from Access & Security Manager
 - a. Select **Administration** and read the information presented on the screen
 - b. Select **Activate**
2. Once activated, actions that require approval can be found within Access & Security Manager on the **Dual Control–Administration** page. View actions that require approval or those that are assigned to others using the **Requests** dropdown. Transactions must be approved within three days



Activating Dual Control - Transaction

When Dual Control-Transaction is activated, all transactions will automatically require approval by another user except for transfers between J.P. Morgan accounts, loan advances and loan payments. Only Primary admins can activate this feature. Before activating, ensure that at least one authorized user has rights to approve transactions by choosing **Approve pending transactions** within an account for that user

1. Select **Dual Control** from Access & Security Manager
 - a. Select **Transaction** and read the information presented on the screen
 - b. Select **Activate**
2. Once activated, pending transactions will appear in **Pending approvals** through **Pay & transfer** until another user approves them



© 2026 JPMorgan Chase & Co. All rights reserved. JPMorgan Chase Bank, N.A. Member FDIC. Deposits held in non-U.S. branches are not FDIC insured. Non-deposit products are not FDIC insured. Visit [jpmorgan.com/cb-disclaimer](https://www.jpmorgan.com/cb-disclaimer) for full disclosures and disclaimers related to this content. Chase, J.P. Morgan, JPMorgan, JPMorgan Chase, and Story by J.P. Morgan are marketing names for certain businesses of JPMorgan Chase & Co. and its affiliates and subsidiaries worldwide (collectively, "JPMC", "We", "Our" or "Us", as the context may require).

The information in this content (website, article, event invitation or other form) does not represent an offer or commitment to provide any product or service. The views, opinions, analyses, estimates and strategies, as the case may be ("views"), expressed in this content are those of the respective authors and speakers named in those pieces, and/or the JPMC departments that publish the content, and may differ from those of JPMorgan Chase Commercial Banking and/or other JPMC employees and affiliates. These views are as of a certain date and often based on current market conditions, and are subject to change without notice. Any examples used are generic, hypothetical and for illustration purposes only. Any prices/quotes/statistics included have been obtained from sources deemed to be reliable, but we do not guarantee their accuracy or completeness. To the extent indices have been used in this content, please note that it is not possible to invest directly in an index. This information in no way constitutes research and should not be treated as such. Any information related to cybersecurity provided is intended to help clients protect themselves from cyber fraud, not to provide a comprehensive list of all types of cyber fraud activities nor to identify all types of cybersecurity best practices.

Copying, re-publishing, or using this material or any of its contents for any other purpose is strictly prohibited without prior written consent from JPMorgan. In preparing this material, we have relied upon and assumed, without independent verification, the accuracy and completeness of all information that was acquired from public sources. Any mentions of third-party trademarks, brand names, products and services are for referential purposes only and any mention thereof is not meant to imply any sponsorship, endorsement, or affiliation unless otherwise noted. Notwithstanding anything to the contrary, the statements in this material are not intended to be legally binding. Any products, services, terms or other matters described herein (other than in respect of confidentiality) are subject to, and superseded by, the terms of separate legally binding documentation and/or are subject to change without notice.

The information in this content is not advice on legal, tax, investment, accounting, regulatory, technology or other matters. You should always consult your own financial, legal, tax, accounting or similar advisors before making any financial or investment decisions, or entering into any agreement for JPMC products or services. In no event shall JPMC or any of its directors, officers, employees or agents be liable for any use of, for any decision made or action taken in reliance upon, or for any inaccuracies or errors in or omissions from, the information in this content. We are not acting as your or any client's agent, fiduciary or advisor, including, without limitation, as a Municipal Advisor under the Securities and Exchange Act of 1934. JPMC assumes no responsibility or liability whatsoever to you or any client with respect to such matters, and nothing herein shall amend or override the terms and conditions in the agreement(s) between JPMC and any client or other person.

The information in this content does not include all applicable terms or issues, and is not intended as an offer or solicitation for the purchase or sale of any product or service. Our products and services are subject to applicable laws and regulations, as well as our service terms and policies. Not all products and services are available in all geographic areas or to all customers. In addition, eligibility for particular products and services will be determined by JPMC, including satisfaction of applicable legal, tax, risk, credit and other due diligence, and JPMC's "know your customer", anti-money laundering, anti-terrorism and other policies and procedures. Credit is subject to approval. Rates and programs are subject to change. Certain restrictions apply.

Products and services may be provided by banking affiliates, securities affiliates or other JPMC affiliates or entities. In particular, securities brokerage services other than those that can be provided by banking affiliates will be provided by appropriate registered broker/dealer affiliates, including J.P. Morgan Securities LLC and J.P. Morgan Institutional Investments Inc. Any securities provided or otherwise administered by such brokerage services are not deposits or other obligations of, and are not guaranteed by, any banking affiliate and are not insured by the Federal Deposit Insurance Corporation. Certain financial products and services are required by law to be provided only by licensed representatives and affiliates. Inquiries regarding such products and services will be referred to a licensed representative or a licensed affiliate. The information in this content is not an offer to sell, or solicit an offer to purchase, any securities by anyone in any jurisdiction in which such offer or solicitation is not authorized, or in which JPMC or the person making such an offer is not qualified to do so, or to anyone to whom it is unlawful to make such an offer or solicitation, or to anyone in any jurisdiction outside of the United States. Nothing in this content constitutes any commitment by JPMC to underwrite, subscribe for or place any securities, or to extend or arrange credit, or to provide any other product or service. JPMC contact persons may be employees or officers of any JPMC subsidiary or affiliate.