

# Fraud Protection Services Go-To Guide

---

## Connect Fraud Protection Services

### Two types of Fraud Protection Services (under Access & security):

Check Protection (formerly Positive Pay) and Check Monitoring (formerly Reverse Positive Pay)

#### Check Protection (formerly Positive Pay)

- Information about every check written is provided, and checks presented for payment are compared to the provided information
- If the information matches, the checks are paid
- If the information does not match, the checks are matched as exceptions, and a decision is made whether to pay or return them
- A decision must be communicated by 4 p.m. local account time whether to pay or return the checks
- If no decision is received by the cutoff time, all exception checks are returned, and a returned check fee may be charged

**Note:** Terms and conditions, including fees and limitations, apply as described in the legal agreement for the online service

**Note:** Fraud Protection Services is available to security administrators. Only Proxy administrators or sub-users entitled to Securities Services (e.g., ACH Debit Block) via Access & Security Manager will see the page

#### Check Monitoring (formerly Reverse Positive Pay)

- A threshold payment amount is set. All checks below the threshold amount are paid automatically, and checks at or above the threshold amount are marked as exceptions
- Flagged checks are reviewed, and a decision is communicated by 4 p.m. local account time regarding whether to pay or return them
- If no decision is received by the cutoff time, the checks are paid

---

# Overview

## Summary

**Fraud Protection Services\*** help safeguard accounts against check fraud. Time should be dedicated to uploading check details (if necessary), reviewing items flagged as exceptions, and making pay or return decisions. These tasks can be performed by the Security Administrator or a user granted access through Access & Security Manager.

## Table of Contents

- I. [Overview](#)
- II. [Enrollment](#)
- III. [Check Protection](#)
- IV. [Upload Checks](#)
- V. [Preparing spreadsheets for upload](#)
- VI. [Customize file format](#)
- VII. [Review Check Exceptions](#)
- VIII. [Reports](#)
- IX. [Alerts](#)
- X. [Fraud Protection Services Tips](#)

\*Prior to enabling Fraud Protection Services, speak with a Sales Representative to ensure it is included in the current bundle

# Enrollment

**Note:** Only the System Administrator (Admin) can enroll in Fraud Protection Services

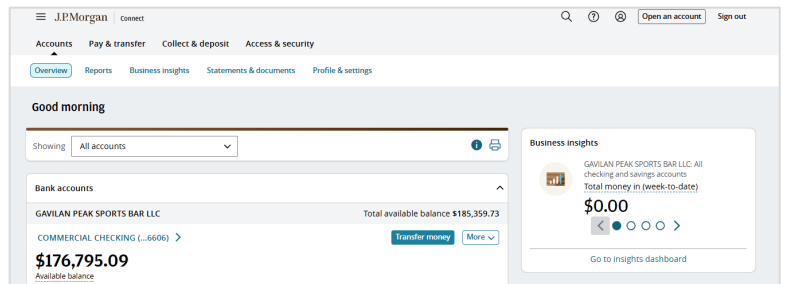
1. Log in to Connect as a System Admin
2. Navigate to the **Access & security** section, then select **Fraud Protection Services**
3. Select **Enroll** in the Check fraud protection tile in the summary tab
4. Select the Fraud Protection Services for each applicable account and select **Next**

**Note:** Each account can be enrolled in one check fraud protection service. Select from the following:

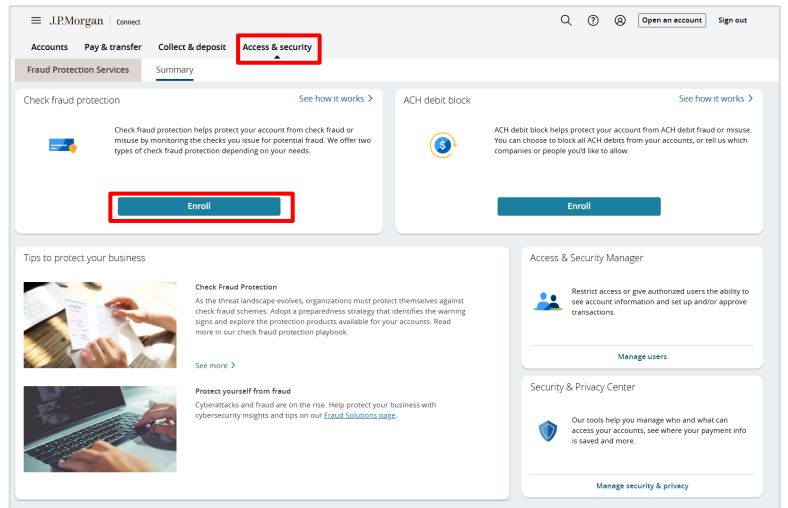
- Check monitoring: Review checks for payments exceeding the specified dollar limit
- Check protection: Verification of checks for payment is based on the provided check information
- No service if the account is enrolled in the offline post-no checks service, or if it simply requires no service

**Note:** If selecting check monitoring, specify the exact amount limit

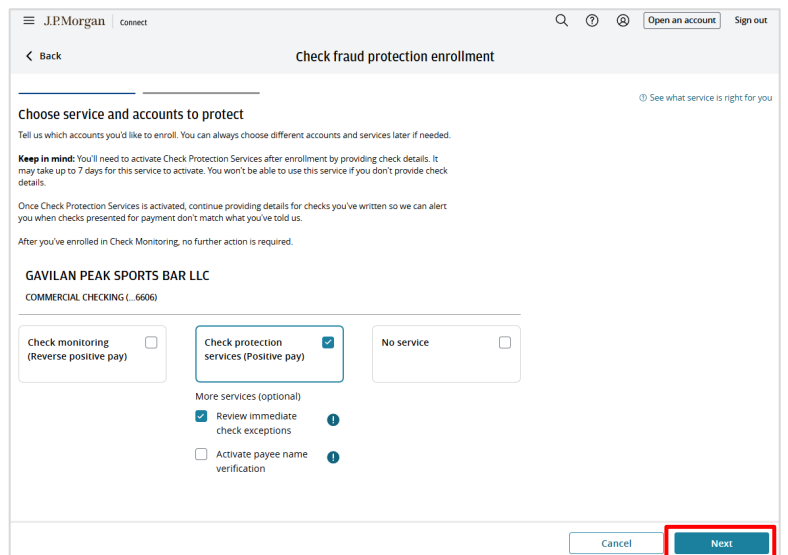
1



2



3



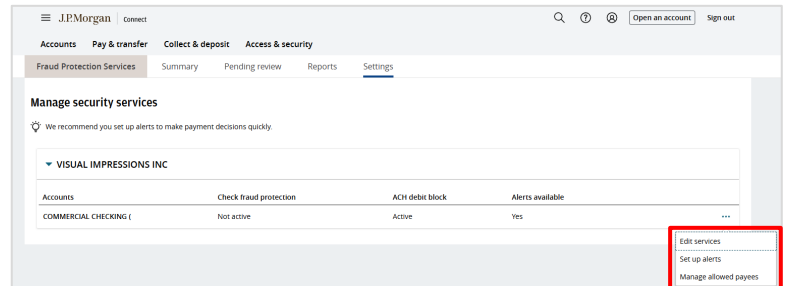
4

## Enrollment (Continued)

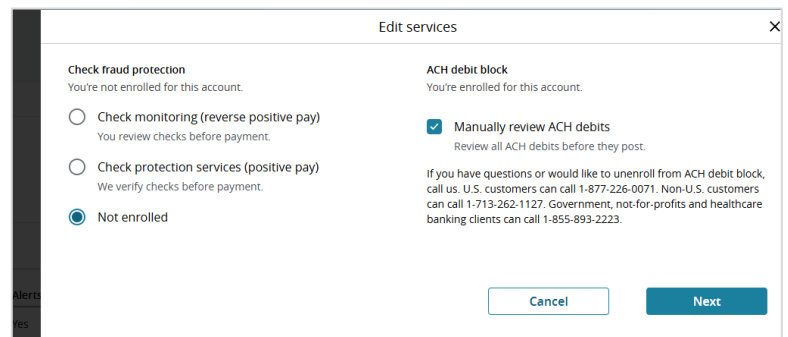
5. Once enrolled, navigate to **Settings**. Select the ellipses menu and then **Edit Services**
6. A side menu will open. Use the menu to check enrolled services or change the current service

**Note:** This tracker is not a comprehensive metric, but rather measures use of eligible digital services

5



6



# Check Protection

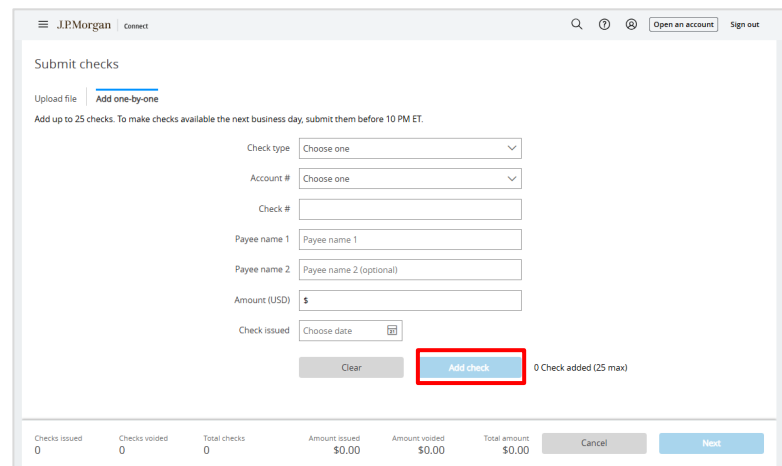
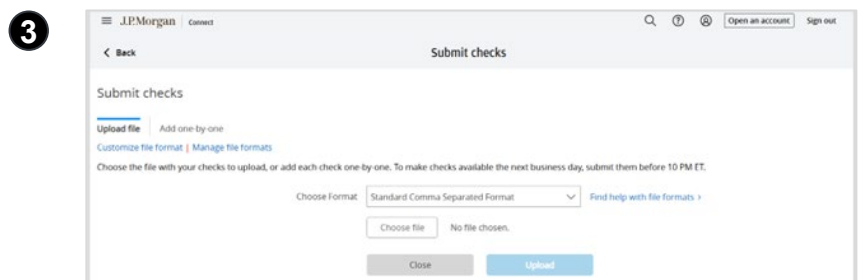
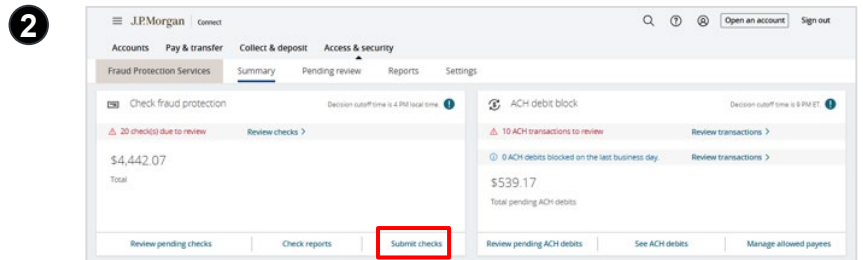
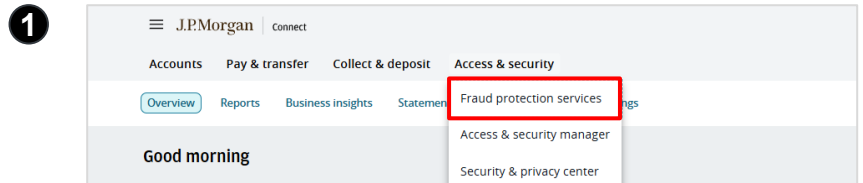
## Upload checks

**Note:** If uploading custom file, instructions on next page. After uploading a file or typing in check information, verification is performed against checks presented for payment. Any checks that do not match or are presented without prior notification are flagged as exceptions for review

1. Select **Access & security**, then **Fraud Protection Services**
2. From the Check fraud protection tile, select **Submit checks**
3. Choose **Upload file** or **Add one-by-one**

a) To upload a file, select **Upload file**, choose the file type, select Choose file, upload the correct file and select **Upload**

b) To add checks individually, select **Add one-by-one**, enter all required information, then select **Add check**



## Check Protection

Preparing spreadsheets for upload

**Note:** Please see the next two screens to format file in advance

**Prepare spreadsheet:** The file cannot have a header – the first row must be the first check written, and each subsequent check follows on its own row. The following information is required in each column. Be sure to follow exact formatting:

- **Column 1 Check type:** I or C. “I” is for issued check, “C” is for canceled check
- **Column 2 Account number for the check you’ve written:** Option to include check issuance information for multiple accounts in one file. Only include numbers in this field
- **Column 3 Check number:** only include numbers in this field
- **Column 4: Check date (Ex: MMDDYY)** some spreadsheets will automatically delete the leading zero; be sure you’ve set the column to accept 6 numbers
- **Column 5 Amount:** Include numbers and a decimal point, but no commas
- **Column 6 Payee line 1:** 40-character max. Characters can include letters, numbers and special characters. Commas can be used only if the entire name is in quotation marks

I	707615678	1001	013007	100	Stephen Morris	Donald Clark
I	707615678	1002	013007	200	John Doe	Simjo
C	707615678	1003	013007	300	John Doe	Simjo
I	707615678	1004	013007	400	John Doe	Simjo
I	707615678	1005	013007	500	John Doe	Simjo
C	707615678	1006	013007	600	John Doe	Simjo
I	707615678	1007	013007	700	John Doe	Simjo
I	707615678	1008	013007	800	Simjo	
C	707615678	1009	013007	900	Simjo	
I	707615678	1010	013007	1000	Simjo	
I	707615678	1011	013007	1100	Simjo	
C	707615678	1012	013007	1200	Simjo	
C	707615678	1013	013007	1300	Simjo	
I	707615678	1014	013007	1400	Simjo	
I	707615678	1015	013007	1500	Simjo	
I	707615678	1016	013007	1600	Simjo	
I	707615678	1017	013007	1700	Simjo	
I	707615678	1018	013007	1800	Simjo	
I	707615678	1019	013007	1900	Simjo	
C	707615678	1020	013007	2000	Simjo	
C	707615678	1021	013007	2100	Simjo	
I	707615678	1022	013007	2200	Simjo	
C	707615678	1023	013007	2300	Simjo	
I	707615678	1024	013007	2400	Simjo	
I	707615678	1025	013007	2500	Stephen Morris	Donald Clark

## Check Protection (Continued)

Preparing spreadsheets for upload

- Column 7 Payee line 2:** Required for clients with Payee Name Verification if more than one line about address on check. Optional for all other checks. 40-character max. Characters can include letters, numbers and special characters. Commas can be used only if the entire name is in quotation marks. Save the file in comma-separated value (CSV) format. Most default to this automatically, but confirm

I	707615678	1001	013007	100	Stephen Morris	Donald Clark
I	707615678	1002	013007	200	John Doe	Simjo
C	707615678	1003	013007	300	John Doe	Simjo
I	707615678	1004	013007	400	John Doe	Simjo
I	707615678	1005	013007	500	John Doe	Simjo
C	707615678	1006	013007	600	John Doe	Simjo
I	707615678	1007	013007	700	John Doe	Simjo
I	707615678	1008	013007	800	Simjo	
C	707615678	1009	013007	900	Simjo	
I	707615678	1010	013007	1000	Simjo	
I	707615678	1011	013007	1100	Simjo	
C	707615678	1012	013007	1200	Simjo	
C	707615678	1013	013007	1300	Simjo	
I	707615678	1014	013007	1400	Simjo	
I	707615678	1015	013007	1500	Simjo	
I	707615678	1016	013007	1600	Simjo	
I	707615678	1017	013007	1700	Simjo	
I	707615678	1018	013007	1800	Simjo	
I	707615678	1019	013007	1900	Simjo	
C	707615678	1020	013007	2000	Simjo	
C	707615678	1021	013007	2100	Simjo	
I	707615678	1022	013007	2200	Simjo	
C	707615678	1023	013007	2300	Simjo	
I	707615678	1024	013007	2400	Simjo	
I	707615678	1025	013007	2500	Stephen Morris	Donald Clark

**Note:** If changing an Excel file to CSV and are using special characters, the file must be modified using Notepad to remove the two additional “” that Excel automatically adds

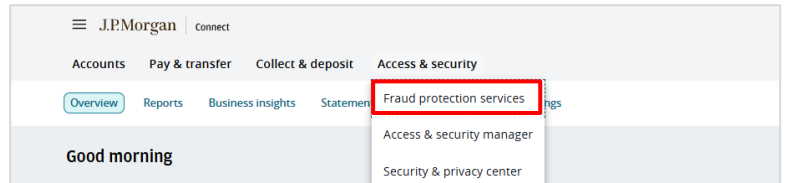
Ex: Change "test payee" to test payee.  
Once the change is made, simply select save and upload

# Check Protection

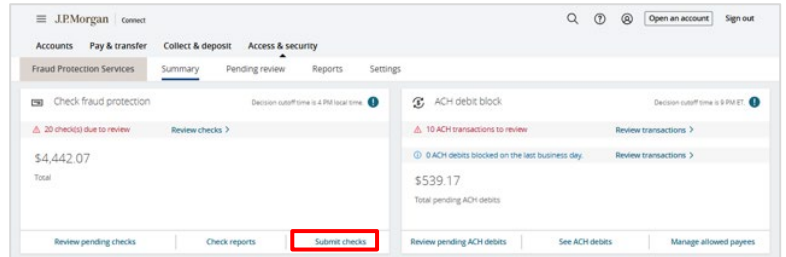
## Customize file format

1. Select **Access & security**, select **Fraud Protection Services**
2. From the Check fraud protection tile, select **Submit checks**
3. Select **Customize file format**
4. Name the file, determine the file format, and select the order for providing the required fields
5. Ensure the file details are exactly as desired then select **Save format**

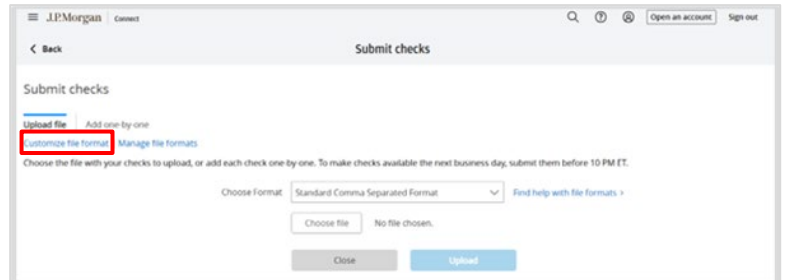
1



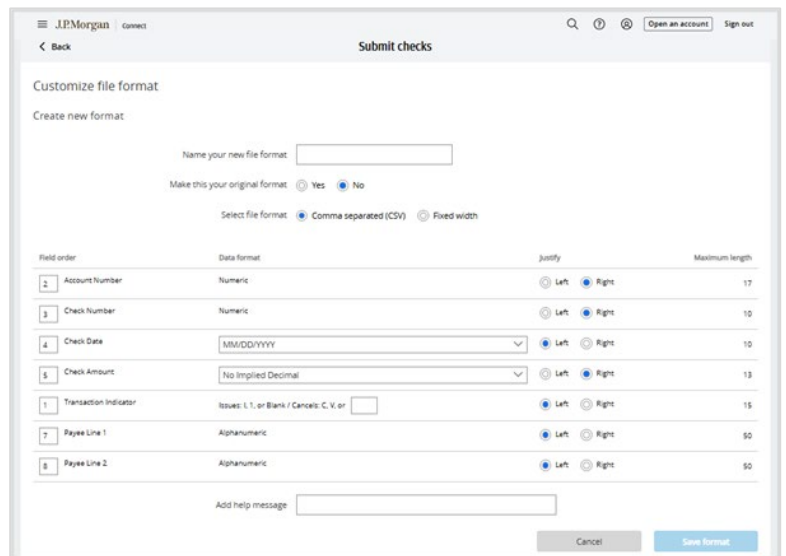
2



3



5



# Check Protection (Continued)

## Customize file format

- Once the file format is saved, it can be managed as needed. Locate the file to review, then select **Test, Edit, or Delete**

6

The screenshot shows the 'Submit checks' interface in the J.P.Morgan Connect environment. A 'Create new format' dialog box is open, displaying a table of field specifications for a new file format. The table has four columns: Field order, Data format, Justify, and Maximum length. The fields are as follows:

Field order	Data format	Justify	Maximum length
2 Account Number	Numeric	Right	17
3 Check Number	Numeric	Right	10
4 Check Date	MM/DD/YYYY	Left	10
5 Check Amount	No implied decimal	Right	13
1 Transaction Indicator	Issues: I, 1, or Blank / Canceled: C, V	Left	15
7 Payee Line 1	Alphanumeric	Left	50
8 Payee Line 2	Alphanumeric	Left	50

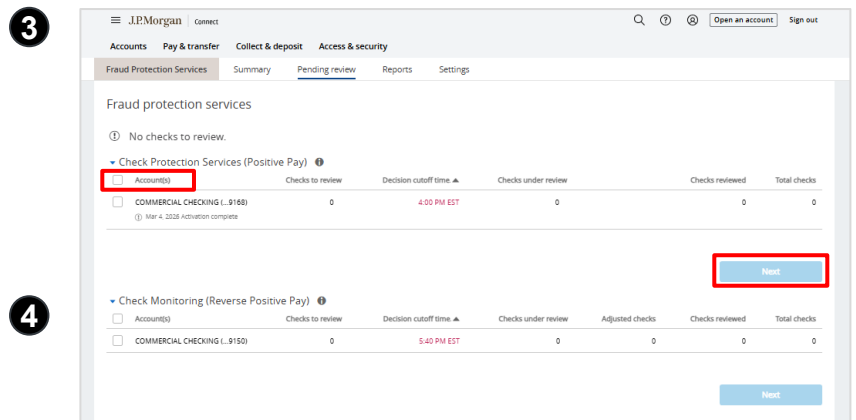
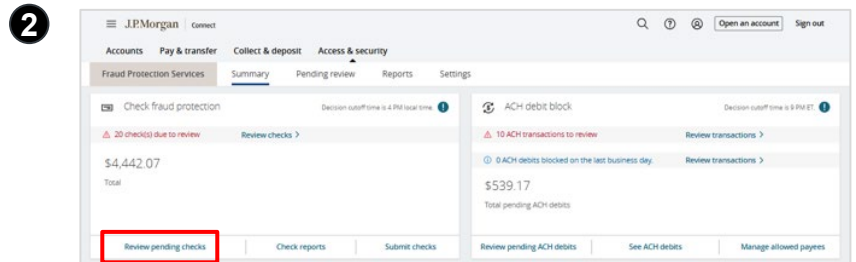
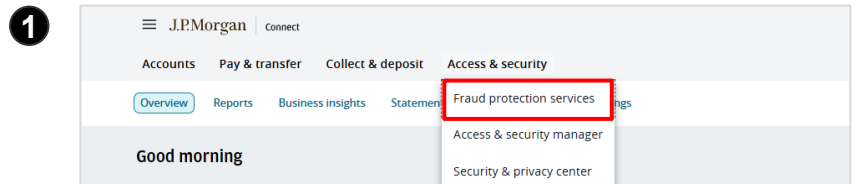
At the bottom of the dialog, there are two buttons: 'Close' and 'Test format'.

# Check Protection

## Review Check Exceptions

Once enrollment is completed, check exceptions can be reviewed from the Access & security tab. The number of exceptions needing review will be indicated. Ensure Check Protection (Positive Pay) and Check Monitoring (Reverse Positive Pay) exceptions are reviewed separately

1. Select Access & security, select **Fraud Protection Services**
2. From the Check fraud protection tile, select **Review Pending Checks**
3. To see every **Check Protection (Positive Pay)** exception from all enrolled accounts, check the box at the top left of the list. To view exceptions from one account at a time, check the box for that individual account
4. Choose Next after selecting at least one account



# Check Protection (Continued)

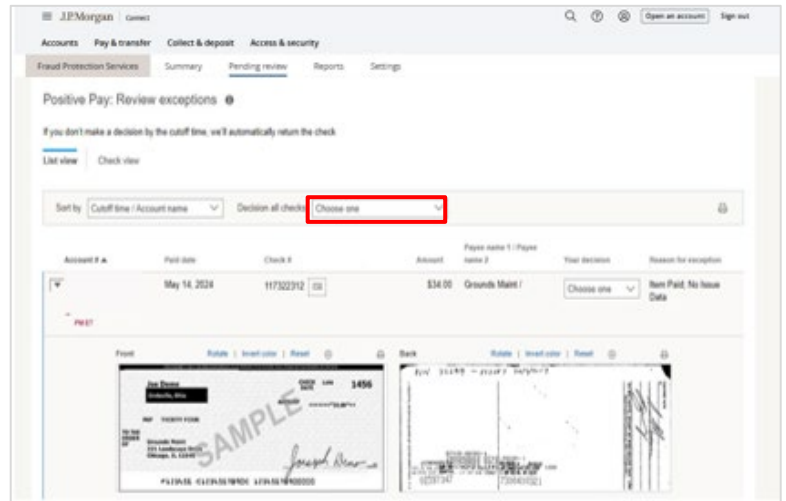
## Review Check Exceptions

- To see a small image of the check, select the Check icon
- To see a larger image, review exceptions using Check view
- Each check and the reason for flagging will be listed. Use the drop-down menu to decide on each check:

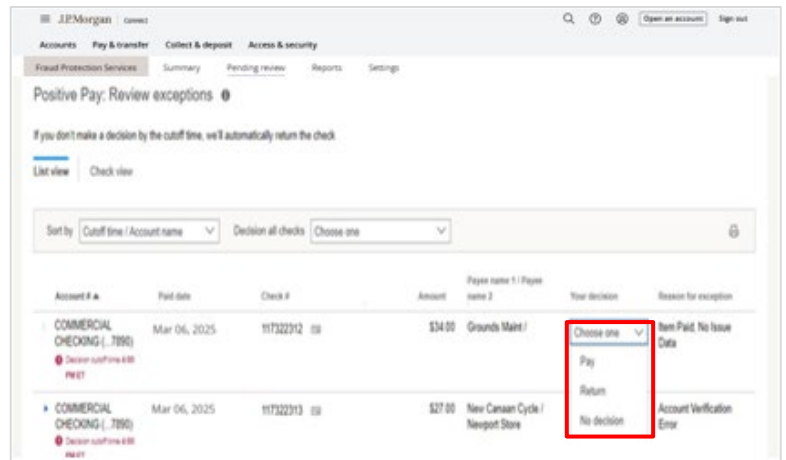
- Pay:** the check will be paid
- Return:** the check will not be paid
- No decision:** The check will be returned if no decision is made by 4 p.m. local account time, and a returned check fee may be charged

**Note:** If **Adjust** is chosen from the dropdown menu, the **Adjusted amount** will be requested. Then choose **Pay** next to the new amount to authorize

6



7



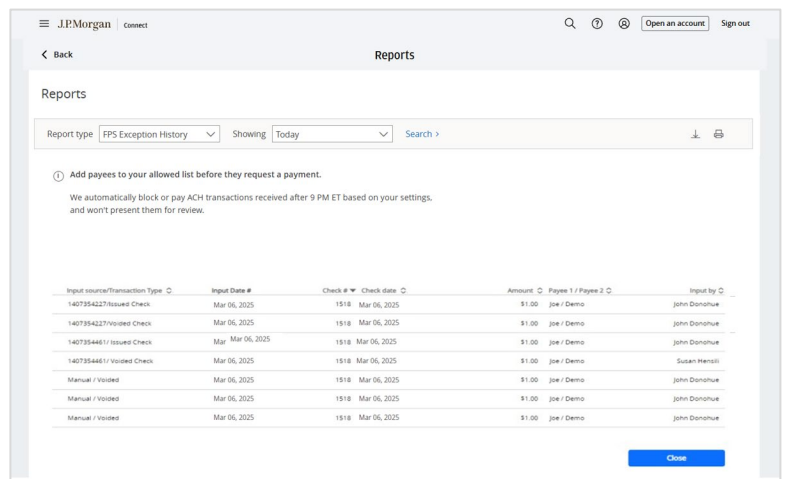
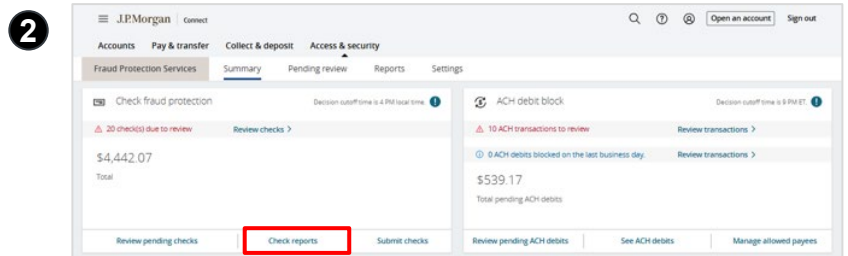
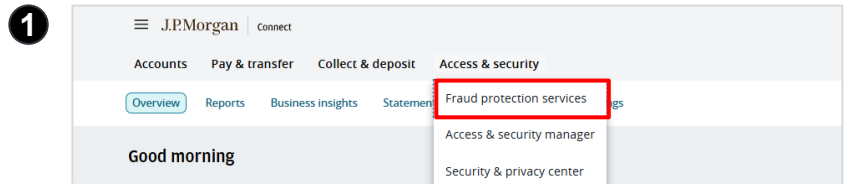
# Reports

1. Select Access & security, select **Fraud Protection Services**
2. From the Check fraud protection tile, select **Check Reports**

Connect offers three reports to help manage fraud protection services:

- **Exceptions history** displays exception information within the selected time (i.e., check details, pay/return decision, status and who reviewed it)
- **Check input history** (Check protection, formerly Positive Pay only) displays information about the check details provided via file upload or manual input
- **Outstanding Checks** (Check protection, formerly Positive Pay only) displays outstanding check liabilities by listing those issued but not yet posted

**Note:** Entitled users can view up to 24 months of check deposit activity online through Connect. Check images are available for 270 days for on-us checks, or 120 days for check drawn on other financial institution

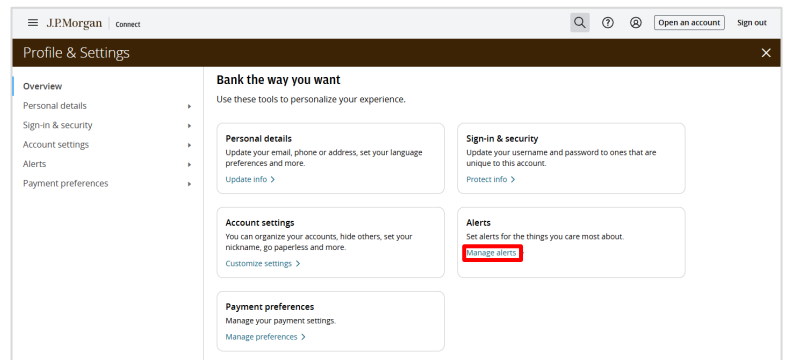
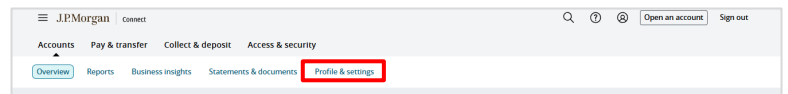
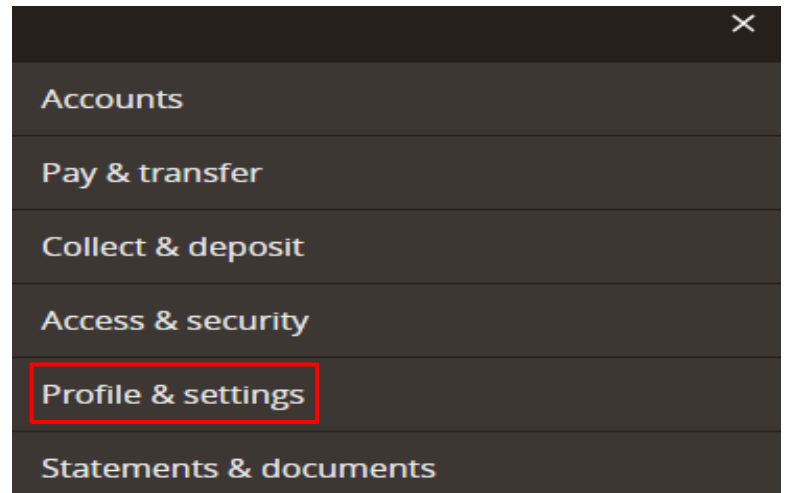
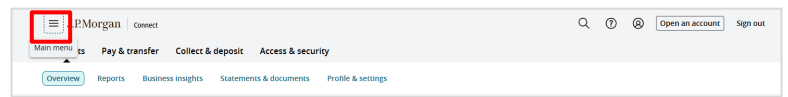


# Alerts

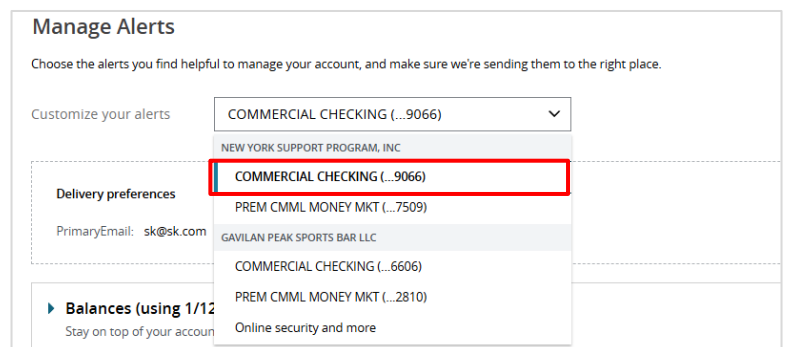
System admins or sub users can subscribe to alerts on Connect to be notified when there are pending Fraud Protection Services

1. There are two ways to get to alerts
  - a. Select the ‘hamburger’ menu, select **Profile & settings** then **Manage Alerts**
  - b. Select **Profile and Settings** from the overview dashboard then **Manage Alerts**
2. Select the account(s) enrolled in Fraud Protection Services to receive alerts from the “Customize your alerts” dropdown

1



2



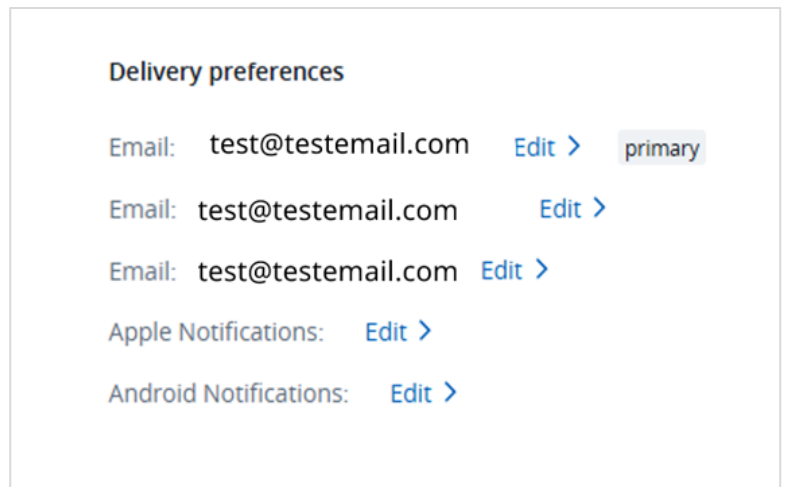
## Alerts (Continued)

3. Select the email where alerts will be delivered

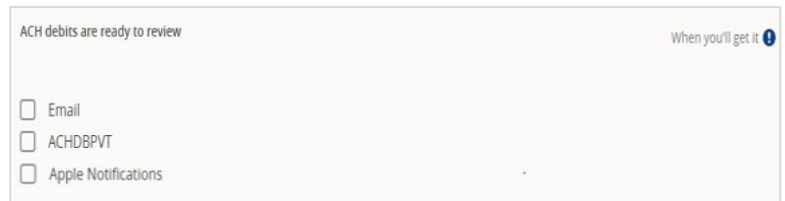
**Note:** Up to 5 email addresses can receive alerts via email

4. Select **Transactions** then select how you want to receive your alerts
5. Select **Settings** from the Fraud Protective Services page to view all alerts for Fraud Protective Services

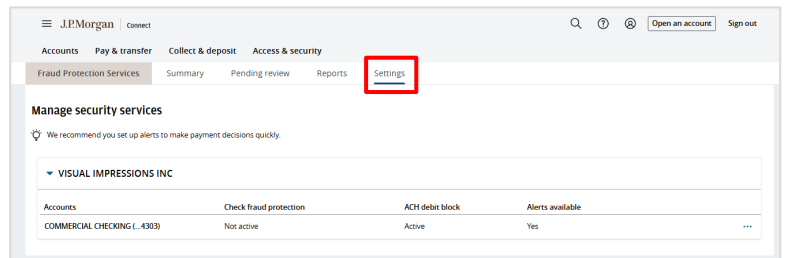
3



4



5



# Security & Privacy Center

## 1. Select **Manage security & privacy** in the Fraud Protection Services page

- This page contains the full suite of options for customizing security and privacy settings for accounts

1

The screenshot shows the J.P.Morgan Connect interface. At the top, there are navigation tabs: Accounts, Pay & transfer, Collect & deposit, and Access & security. The 'Fraud Protection Services' section is active, showing a 'Summary' view. It features two main cards: 'Check fraud protection' (with a total of \$4,442.07) and 'ACH debit block' (with a total of \$539.17). Below these are sections for 'Tips to protect your business' and 'Access & Security Manager'. A red box highlights the 'Manage security & privacy' link in the bottom right corner.

The screenshot shows the J.P.Morgan Connect 'Security & Privacy Center' page. The page is titled 'Security & Privacy Center' and contains several sections: 'Enhance your security', 'Report fraud', 'Manage users and account access', 'Keep track of your data', 'Manage your personal info', and 'Stay informed about security'. The 'Keep track of your data' section shows a table of devices accessed.

Device	Last sign in date
Windows 11 - Chrome (chase.com)	Feb 13, 2026 at 3:46 PM ET
Unknown Device (chase.com)	Feb 13, 2026 at 3:21 PM ET
Windows 11 - Chrome (chase.com)	Feb 13, 2026 at 3:18 PM ET

---

## Fraud Protection Services Tips

### Reduce Exceptions Caused by Readability Errors

Please follow these guidelines to minimize check exceptions due to readability issues. With Check Protection, a charge is applied for each check exception identified

- **Text formatting:** Checks are most readable when the text is printed in 12-point font or larger, in a recommended font style (Courier New, Arial or Times New Roman), black ink, and all uppercase letters. Systems have difficulty reading italicized, underlined or cursive text
- **Printing:** Checks should be printed on ink jet or laser printers with a 600 dpi resolution or higher. Dot matrix or handwritten checks are not recommended. If checks have a design on them, keep in mind that any dark background patterns, images or watermarks in the name and address block area can distort the black and white image and may interfere with readability
- **Payee name:** The name provided must match exactly the name printed on the check in layout, format, letters and punctuation. The name must start on the first line of the payee address block and must not exceed two lines of the payee address block
- **Fraud Protection Alerts:** Managing checks through Fraud Protection

Services allows for receiving Account Alerts to help keep track of account activity

**Note:** Users must subscribe to alerts and can do so from the Things You Can Do menu in Fraud Protection Services, or by selecting the person icon in the upper right corner and choosing Alerts from the dropdown menu

### Fraud Protection On The Go

Access to the Chase Mobile® App or browser allows exception decisions to be made while away from the desk. Details for individual checks can also be entered.

To access, visit the mobile app store or enter [www.chase.com/ChaseConnect](http://www.chase.com/ChaseConnect) into the mobile browser.

System Administrators (primary and proxy administrators) can grant mobile access permission to authorized users through Access & Security Manager.

---

© 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.