jack henry™

PAYCENTER PORTAL

USER GUIDE

STONE BANK

Member FDIC EQUAL HOUSING LENDER

Logging in to and out of the PayCenter Portal

Use this information to log in to and out of the PayCenter Portal.

The number of log-in attempts that users have do not appear on the screen. However, users are locked out after three failed attempts.

1. Navigate to the PayCenter Portal: https://portal.jhapaycenter.com/portal.
2. Fill in the **Email** and **Password** fields, and then select **Sign in**.

   > **NOTE**
   > Users can paste their password into the **Password** field.

3. When finished with your session, select the **Arrow** button to the right of the **Username** field, and then select **Logout**.

Password Management

The following information relates to password management for PayCenter Portal users.

Users must reset their password after 90 days. This action is done from the *PayCenter Portal* login screen. Users must also reset their password for lockouts.

> **NOTE**
> Users cannot reset their password to any of their three previously used passwords.

Password Reset After 90 Days

Users are required to reset their passwords if they are 90 days or older. This is a security precaution that applies to all PayCenter Portal users.

Password Reset After Lockout

Users are locked out of the PayCenter Portal when three failed login attempts occur. Before resetting their password, a financial institution administrator must reset their account. Once the account is reset, users can reset their password.

Resetting Your Password

Use this information to reset your PayCenter Portal password.

1. Navigate to the PayCenter Portal.
2. Select **Forgot Password?**.
3. Enter your email address, and select **Submit**.
   The screen refreshes to display the message: `Password reset requested`.
4. Check your email for a new PayCenter Portal invitation.

Multifactor Authentication

As of January 21, 2024, Multifactor Authentication (MFA) is required for each login to the PayCenter Portal.

A one-time Multifactor Authentication (MFA) code is sent to the email address on file during login for additional security. The security code expires in six minutes.

Users can select **Resend Code** if they did not receive a code or it expired. The original code becomes invalid and a new code is sent to the user's email. After selecting **Resend Code**, the following message appears: `A new code has been sent. Please allow up to 45 seconds to receive the code.`

If the MFA code is entered incorrectly three or more times, the user is locked out. Financial institution administrators must follow standard account unlock procedures to unlock a user from an MFA lockout.

Session Timeout Warning

After a period of inactivity, a session timeout warning appears.

The portal timeout period is 30 minutes. A warning appears five minutes before the automatic logout occurs. The warning provides options to **Continue** or **Log Out**. If you do not select an option, the system automatically logs you off the portal.

When users are automatically logged out of the PayCenter Portal, the following message appears: `You are now logged out of the PayCenter Portal`. **Click here to log back into the PayCenter Portal** appears as a hyperlink. When this link is selected, the user is navigated back to the PayCenter Portal login page.

User Management

Administrators can manage PayCenter Portal users.

The **Users** button provides options to add, edit, and delete users.

Financial Institution Administrators (FI Admins) can search for users on the *Users* screen. Administrators can search for a user using their first name, last name, or email address.

Inviting a User

Use this information to add a PayCenter Portal user.

1. Select **Users**, and then select **Invite User**.
2. Fill in the **Email**, **First Name**, and **Last Name** fields.
3. Select the appropriate **Products** for the new user, and then select **Add User**.

   > **NOTE**
   > If the email address is already defined, an error message momentarily appears.

   The screen updates and user roles appear.
4. Under *Roles for this User*, select the roles to activate for the user.

   > **NOTE**
   > Selecting a role populates permission information under **Role Permissions**. Selecting the caret on the right side of the screen allows the permissions associated with the role to appear. Permissions associated with a role cannot be modified.

5. Select **Invite User**.

Editing a User

Use this information to edit a PayCenter Portal user's name and roles.

1. Select **Users**.
2. Find the user that you want to edit, and then select **Edit**.
3. Update the **First Name** and **Last Name** fields, if necessary.
4. Under *Roles for this User*, select the roles you want to enable or disable for the user.

> **NOTE**
> Selecting a role populates permission information under **Role Permissions**. Selecting the caret on the right side of the screen allows the permissions associated with the role to appear. Permissions associated with a role cannot be modified.

5. When your updates are complete, select **Update User**.

Deleting a User

Use this information to delete a PayCenter Portal user.

This option is only available to FI Admins.

1. Select **Users**.
2. Find the user that you want to delete, and then select **Delete**.
   A dialog box appears to confirm you want to delete the user.
3. Select **Confirm**.

Resending an Invitation

Use this information to resend an invitation to a PayCenter Portal user.

> **NOTE**
> This option is only available when the **Status** for the user is `Inviting` or `Expired`.

1. Select **Users**.
2. Find the user that you want to edit, and then select **Edit**.
3. Select **Resend Invitation**.

View and Reposition Windows

Users can reposition windows that appear on their screen to view multiple windows.

Organizations

Administrators can view PayCenter Portal organization information.

The 🏛 **Organizations** button allows users to view their financial institution's **Name**, **Description**, **PeopleSoft Id**, **Zelle® Org Id**, **RTP® Participant Id**, and **FedNow® Routing Number**.

Standard Role Permission Sets

PayCenter Portal includes several standard permission sets. This section provides the permissions available to users with each standard permission set.

> **NOTE**
> Only roles consistent with your institution's Network offerings appear.

You can also view this information when editing users.

User Management

This role allows the user to add, edit, and delete PayCenter Portal users.

Zelle® Token Management

This role allows the user to look up, view, delete, restrict, and unrestrict Zelle® tokens.

Zelle® Token Lookup

This role allows the user to look up and view Zelle® tokens.

Zelle® Limits Management

This role allows the user to view and edit customer-specific limits.

Zelle® Limits Lookup

This role allows the user to view customer-specific limits.

Zelle® Transactions Management

This role allows the user to look up and view Zelle® transactions. Users can also report fraudulent transactions.

Zelle® Transactions Lookup

This role allows the user to look up and view Zelle® transactions.

RTP Transactions Management

This role allows the user to look up and view RTP transactions. Users can also reprocess RTP transactions.

RTP Transactions Lookup

This role allows the user to look up and view RTP transactions.

FedNow Transactions Management

This role allows the user to look up and view FedNow transactions.

> **NOTE**
> Additional permissions will be added to this role in a future release.

FedNow Transactions Lookup

This role allows the user to look up and view FedNow transactions.

Reporting Access

This role allows the user to access the FI reports.

Auditing Access

This role allows the user access to the auditing data that is available in the PayCenter Portal.

Zelle® Token Management

PayCenter Portal administrators can manage token limits.

Token Management allows administrators to search, view, modify, and delete tokens.

Previously, all account numbers in the PayCenter Portal were masked. Account numbers that belong to the user's financial institution now appear. This change applies to the Zelle®, FedNow, and RTP Networks.

> **NOTE**
> **Account Numbers** from other institutions remain masked.

Searching a Token

Use this information to search a token.

1. Select **Token Management**.
2. In the **Token** field, enter the email address or 10-digit phone number.
3. Select **Search**.

The screen displays the following token information:

- **Token**
- **Customer First Name**
- **Customer Last Name**
- **Account Number** (masked to last four digits)
- **Zelle® Org Id**
- **Status**
- **Reason**
- **EventDateTime (UTC)**

> **NOTE**
> Users with the following role permissions see additional options:
>
> - Users with **Zelle® Token Management** role permission have **Restrict** and **Delete** buttons to restrict and delete tokens.
> - Users with **Zelle® Limits Lookup** role permission have a **User-Specific Limits** button to view Zelle® limits.

- Users with **Zelle® Limits Management** role permission have a **User-Specific Limits** button to view and edit Zelle® limits.
- Users with **Zelle® Transaction Lookup** role permission have a **Find Payments** button to view Zelle® transactions.
- Users with **Zelle® Transaction Management** role permission have a **Find Payments** button to view and manage Zelle® transactions.

Restricting a Token

Use this information to restrict a token.

To restrict a token, a user must have the Zelle® Token Management role.

1. Select **Token Management**.
2. In the **Token** field, enter the email address or 10-digit phone number.
3. Select **Search**.
4. Select the **Restricted** toggle.
   The *Select Restrict Reason* dialog box appears.
5. In the **Select Reason** drop-down list, select one of the following restriction reasons:
   - `Invalid Mobile Phone Number`
   - `OFAC`
   - `AML`
   - `Brand Damaging Activity`
   - `Fraud-Scam`
   - `Fraud-Friendly Fraud`
   - `Fraud-First Party`
   - `Fraud-Account Takeover`
6. Select **Confirm**.
   A *SELECT ONE* dialog box appears.
7. Select one of the following restriction types:
   - `Only restrict the token, and allow the customer to continue using Zelle®.`
   - `Restrict the customer from using Zelle®.`
8. Select **Restrict**.
   The *CONFIRM* dialog box appears.
9. Select **Restrict** again.
   The *Success* dialog box appears.
10. Select **OK** to return to the *Search Token* screen.

Removing a Token Restriction

Use this information to remove a restriction from a token.

1. Select **Token Management**.
2. In the **Token** field, enter the email address or 10-digit phone number.
3. Select **Search**.
4. Select the **Restricted** toggle.
   The *Are you sure?* dialog box appears.
5. Enter the reason in the **Please Enter a Reason** field.
6. Select **Remove Restriction**.
   The *Success* dialog box appears.
7. Select **OK** to return to the *Search Token* screen.

Deleting a Token

Use this information to delete a token.

Only active tokens can be deleted. If a token has a status of deactivated, restricted, or unrestricted, there is no delete option.

1. Select **Token Management**.
2. In the **Token** field, enter the email address or 10-digit phone number.
3. Select **Search**.
4. Select **Delete**.
   A *Confirm Delete Token* dialog box appears.
5. Select **Confirm**.

Searching a Transaction

Use this information to search for transactions.

1. Select **Token Management**.
2. In the **Token** field, enter the email address or 10-digit phone number.
3. Select **Search**.
4. Select **Find Payments**.
5. Complete the **Start Date** and **End Date** fields and select **Search** to filter by date.
   Search is available in 15-day increments.

> **NOTE**
> To redirect to the *Zelle® transaction detail* page, select the **Payment ID**.

Zelle® Payments by Token Details

The following data is available in the Zelle® *Payments for Token* page.

- **Payment ID** - This option directs users to the *Zelle Transaction Detail* page.
- **Sender Org**
- **Receiving Org**
- **Direction**
- **Amount**
- **Transaction Date**
- **LogTimeStamp** (UTC)
- **Status**
- **RT** (Real Time) with values:
  - `true`
  - `false`
- **Sender Name**
- **Sender Token** - This option directs users to the *Search Token* results page for the sender.
- **Sender Account** - This option is masked so that the last four digits appear.
- **Recipient Name**
- **Recipient Token** - This option directs users to the *Search Token* results page for the recipient.
- **Recipient Account** - This option is masked so that the last four digits appear.

Reviewing User-Specific Limits

Use this information to review user-specific limits.

1. Select **Token Management**.
2. In the **Token** field, enter the email address or 10-digit phone number.
3. Select **Search**.
4. Select **User-Specific Limits**.
   The screen refreshes, and the following information populates in a table for each limit:
   - **Type**
   - **Range**
   - **Value**

- **FI Default**
- **Created Date Time (UTC)**
- **Modified Date Time (UTC)**

Updating User-Specific Limits

Use this information to update the user-specific limits for a token.

1. Select **Token Management**.
2. In the **Token** field, enter the email address or 10-digit phone number.
3. Select **Search**.
4. Select **User-Specific Limits**, and then select **Edit User-Specific Limits**.
5. Update any of the following limit fields:
   - **User Override Limits (Payment)**
     - **Per Transaction**
     - **Daily**
     - **Weekly**
     - **Monthly**
   - **User Override Limits (Velocity)**
     - **Daily**
     - **Weekly**
     - **Monthly**
6. Select **Update User-Specific Limits**.

   > **NOTE**
   > If you select **Back** before selecting **Update User-Specific Limits**, field updates are not saved.

   A confirmation dialog box appears.
7. Select **Update Limits**.

Deleting User-Specific Limits

Use this information to delete user-specific payment or velocity limits for a token.

1. Select **Token Management**.
2. In the **Token** field, enter the email address or 10-digit phone number.
3. Select **Search**.
4. Select **User-Specific Limits**.
5. Select the type of user-specific limit that you want to delete:

- **Delete Payment Limits**
- **Delete Velocity Limits**

A *Confirm* dialog box appears.

6. Select **Delete Limits**.

Zelle® Token Search History

The PayCenter Portal now provides search history for tokens that were last modified by Early Warning® Services (EWS).

EWS can **Delete**, **Restrict**, and **Unrestrict** tokens.

When searching for tokens that were last modified by EWS, one of the following statuses appear:

- `Restricted`
- `Inactive`

> **NOTE**
> This status appears when a token is **Restricted** or **Deleted**.

Zelle® Transactions

PayCenter Portal users can look up Zelle® transactions.

The **Zelle Transactions** button allows users to search for transaction details and settlement information.

The **Zelle Transactions** button appears above **Audit Logs**.

Looking Up Transaction Details

Use this information to look up payment and settlement details.

1. Select **Zelle® Transactions**.
2. Enter the **Transaction Id**, and select the type of details you want to view.
   - **Get Payment Details**
   - **Get Settlement Details**

> **NOTE**
> Users are able to select, copy, and paste data from the **Settlement Detail** field.

Zelle® Transaction Payment Details

The following information is available on the *Zelle® Transaction Detail* screen when users select the **Get Payment Details** button.

Payment Details

- **Payment ID**
- **Amount**
- **Initiation Time** (UTC)
- **Memo**
- **RT** - Real Time
  - `True`
  - `False`
- **Sender Org**
- **Sender Name**
- **In/Out of Network**
  - `INN`

    - `OON`
- **Known Recipient?**
    - `True`
    - `False`

Status

- **Status** with values
    - `Delivered` - This value is the final status for expedited payments.
    - `Sent` - When searching for a standard payment using **Additional Info**, the final status of the payment appears as `Sent`.
    - `Failed`

      > **NOTE**
      > If the **Status** is `Failed`, **Reason** and **Description** fields appear to provide more information.

    - `Fraud Review-Recipient Rejected` - This status appears when a payment is denied by the recipient financial institution because of potential fraud risk. This status is provided for informational purposes and users are encouraged to review the activity.
- **Delivery Time** (UTC)

Debit Network Details

- **Registration Date**
- **Last 4 Digits**
- **Card Issuing Bank Name**
- **Card Issuing Bank OrgId**

Recipient Info

- **Recipient Org Id**
- **Recipient Payment Profile ID**

Zelle® Transaction Settlement Details

The following data is available under *Zelle® Transaction Details* when users select the **Settlement Details** button.

Settlement Details

- **Settlement Date**
- **Payment Date**
- **Last Report Date**
- **Recon Status**
- **Amount**
- **Sender Org**
- **Receiving Org**
- **Sender Account** - This option is masked so that the last four digits appear.
- **Recipient Account** - This option is masked so that the last four digits appear.
- **TrnRcptId**
- **Direction**
- **SRACH Debit Trace Number**
- **SRACH Credit Trace Number**
- **Identifier Visa®**
- **Identifier MC**

Record Count

On the *Zelle Transaction Detail* screen, a record count of the **Additional Info** and the **Error Info** buttons appear.

Additional Info Record Count

This count provides the number of records users can expect to see when they select **Additional Info**.

Error Info Record Count

This count provides the number of records users can expect to see when they select **Error Info**.

> **NOTE**
> **Error Info** only appears when error information is available.

Zelle Payment Errors

Information regarding Zelle® payment errors is included in this topic.

If a payment has an error, the **Additional Info** and **Error Info** buttons appear. If there is no error, the **Additional Info** and **Error Info** buttons do not appear.

Select **Error Info** to view the following:

- Service Name
- LogTimeStamp (UTC)
- Error Message
- Error Code

Select **Additional Info** to view the following:

- Payment ID
- Sender Org
- Receiving Org
- Direction
- Amount
- Transaction Date
- LogTimeStamp (UTC)
- Status
- RT
- Sender Name
- Sender Token
- Sender Account
- Recipient Name
- Recipient Token
- Recipient Account

> **NOTE**
> Any account numbers sent or received from other financial institutions are masked. The last four digits of the account number appear.

A list of errors can be found by navigating to **For Clients** > **Product & Services** > **JHA Payment Solutions** > **JHA PayCenter** > **Documentation** > **Zelle Error and Response Codes**.

Failed Reason Verbiage

The following verbiage now appears in the PayCenter Portal.

The same failed verbiage that appears on the *PayCenter Daily Zelle® Failed Transaction* report appears in the PayCenter Portal.

Outbound Payments

Verbiage	Status	Reason
Expired	Failed	Payment Expired
Canceled	Failed	Canceled by Sender
Denied	Failed	Issue on Recipient Side
Denied	Failed	Fraud Review - Recipient Rejected
Failed	Failed	Issue on Recipient Side
All other Zelle® statuses for failed payments	Failed	Not Available

Inbound Payments

Verbiage	Status	Reason
All Zelle® statuses for failed payments	Failed	Not Available

Mark as Fraud

This feature allows PayCenter Portal users to report fraudulent transactions to Early Warning® Services (EWS), as required by Zelle® Network rules.

Previously, Zelle® fraud reporting was done using a *Fraud Reporting Form* that was emailed to the PayCenter Fraud Mailbox.

Users with **Zelle Transaction Management** permissions can **Mark As Fraud** and **Unmark Fraud**. Users can also mark inbound payments as fraudulent.

> **NOTE**
> Review the PayCenter Portal Release Notes_02.18.24 on *For Clients* for more information.

Users with **Zelle Transaction Lookup** permissions can view **Fraud Details**, but not modify them.

Marking a Payment as Fraudulent

The following steps walk you through the **Mark as Fraud** function.

Only users with **Zelle Transaction Management** permissions can **Mark As Fraud** and **Unmark Fraud**.

1. Go to **Zelle Transactions**.
2. Enter your **Payment ID**.
3. Select **Get Payment Details**.
   The *Fraud Details* section appears.
4. Select the **Mark Fraud** toggle.
   A *Fraud Details* screen appears with drop-down menus related to the details required by the Zelle® Network.

   The following drop-down menus appear:
   - **Fraud Reason**
     - **Account Takeover**
     - **Elder Abuse**
     - **Friendly Fraud**
     - **Social Engineering**
     - **Third Party Fraud**
     - **Identity Takeover (ITO)**
     - **First Party Fraud**
     - **Bad Customer**
     - **OON Chargeback**
     - **Scam - Charity**
       - **For an Individual Person**
       - **For an Organization/Cause**
       - **Other**
     - **Scam - Not Classified**
       - **Jail/Bail Bond/Deportation**
       - **Termination of Existing Service**
       - **Me 2 me/Pay Yourself**
       - **Pay Your Taxes**

        - Other
    - Scam - Investment
        - Stock/Foreign Exchange
        - Gold/Precious Metals
        - Crypto
        - Lottery/Gambling
        - Other
    - Scam - Goods/Services
        - Goods - Animals
        - Goods - Tickets
        - Goods - Other
        - Services - Moving and Shipping
        - Services - Household
        - Services - Other
        - Send Payment Back/Upgrade
    - Scam - Jobs
        - Employment
    - Scam - Property/Real Estate
        - Purchase
        - Rental
        - Other
    - Scam - Romance
        - Fake Romance
    - Scam - Well-Known Family/Friend
        - Loan/Borrow Money
        - Other
- Disaster Related
    - Y
    - N
- Who the Scammer Was Impersonating
    - Person/Individual
    - Business/Company/School/Non-Profit
    - Utility Company
    - Financial Institution
    - Government/Law Enforcement
    - Not a Scam (e.g., 1st Party, 3rd Party Fraud)
- Contact Method
    - Independent Website
    - Email

- **Phone Call**
- **Text (SMS) Message**
- **Social Media**
- **In Person**
- **Friend/Family Referral**
- **Craigslist**
- **Facebook Marketplace**
- **Other Digital Marketplace**
- **Unknown**

5. When all required details are provided, select **Mark As Fraud**.
   The *Fraud Details* screen closes and the transaction is reported to the Zelle® Network. PayCenter sends Early Warning® Services (EWS) a file containing all reported fraud transactions at 4:00 p.m. ET each day. If your transaction is reported after 4:00 p.m. ET, it is sent to EWS the following day.

Viewing and Editing a Fraudulent Payment

The following steps walk you through viewing and editing payments that are marked as fraudulent.

Only users with **Zelle Transaction Management** permissions can view or edit the transaction. Users with **Zelle Transaction Lookup** permissions can view the transaction and fraud details, but not modify them.

1. Go to **Zelle Transactions**.
2. Enter your **Payment ID**.
3. Select **Get Payment Details**.
   The *Fraud Details* section appears.
4. Select **View/Edit Fraud** in the *Fraud Details* section of the *Zelle Transactions* screen.
5. Select the appropriate process from the following table.

Situation	Steps
Change the Fraud or Scam Classification	a. Choose from the **Please Select a Fraud Reason** drop-down menu. b. Choose from the **Disaster Related** drop-down menu. c. Choose from the **Who the Scammer Was Impersonating** drop-down menu.

Situation	Steps
	d. Select **Mark As Fraud**.
Unmark the Payment as Fraudulent	a. Select **Unmark Fraud**.

RTP Batch Warning

RTP Batch Warning is used by RTP credit unions only.

Users must have **RTP Transactions Management** permissions to reprocess the transactions

When Credit Unions have **RTP** configured, users that have **RTP Lookup** or **RTP Transaction Management** permissions can see the **RTP Batch Warning** icon. **RTP Batch Warning** and **RTP Transactions** appear on the left, side menu.

When a transaction fails because of a batch warning, a notification is sent to the financial institution's (FI) contact on file. The institution has 2 options:

- Remove the batch warning from the account and reprocess the transaction
- Manually post the transaction

  This option does not require your institution to remove the batch warning.

> **NOTE**
> The FI contact is added to the file during RTP on-boarding.

Reprocessing a Transaction

RTP Batch Warning is used by RTP credit unions only.

Users must have **RTP Transactions Management** permissions to reprocess the transactions.

1. Remove the batch warning from the account.
2. Go to **RTP Batch Warning** in the PayCenter Portal.
3. Select **Details**.
4. Select **Reprocess**.

The financial institution (FI) users receive an email when an **RTP Transaction** has successfully reprocessed.

Manually Posting a Transaction

RTP Batch Warning is used by RTP credit unions only.

Users must have **RTP Transactions Management** permissions to mark a transaction as **Manually Processed**.

1. Go to **RTP Batch Warning** in the PayCenter Portal.
2. Select **Details**.
3. Select **Manually Posted**.
4. Enter the **Receipt ID**.
   A confirmation window appears.
5. Go to *RTP Transactions* and confirm that the payment has a **Reprocess Status** of `Manually Processed`.

RTP Transactions

The following information is related to the **RTP Transactions** field in the PayCenter Portal.

RTP Transaction Lookup

Users in the PayCenter Portal can look up an RTP transaction if the following applies:

- The Financial Institution has RTP configured.
- The **RTP Lookup** and **RTP Transaction Management** permissions are configured.

When a user searches for and selects a transaction, the following appear:

- PayCenter Reference ID
- Network Transaction ID
- Transaction Receipt ID
- Amount
- Status Code
- Status Description
- Reason Code
- Reason Description
- Direction
  - Inbound
  - Outbound
- Transaction Notes
- Transaction Date (ET)
- GL Posting Date (ET)
- Sender Participant ID
- Sender RTN
- Sender Account Number
- Sender Account Type
- Sender Name
- Ultimate Debtor Name
- Receiver Participant ID
- Receiver RTN
- Receiver Account Number
- Receiver Account Type
- Receiver Name

- Ultimate Creditor Name

> **NOTE**
> Timestamps included in RTP transactions are in Eastern Standard time. Any account numbers included in these transactions appear with only the last four digits visible.

FedNow Transactions

Administrators can provide **FedNow Transactions Lookup** and **FedNow Transactions Management** permissions.

FedNow Transaction Lookup

This functionality is available for financial institutions that have **FedNow** configured.

FedNow Transactions is available on the left, side menu, for users with **FedNow Transaction Lookup** and **FedNow Transaction Management** permissions configured.

Users can search for **FedNow Transactions** using a **Message ID** or a **Transaction Receipt ID**.

FedNow Transactions includes transactions from October 2023 to the present day. When a transaction is found, the following appears:

- PayCenter Reference ID
- Network Transaction ID
- End to End ID
- Sender RTN
- Sender Account Number
- Sender Name
- Receiver Participant ID
- Receiver RTN
- Receiver Account Number
- Receiver Name
- Ultimate Creditor Name
- Ultimate Debtor Name
- Transaction Receipt ID
- Amount
- Status Code
- Reason Code
- Direction
- Transaction Notes
- Transaction Date

NOTE

Any account numbers sent or received from other financial institutions are masked. The last four digits of the account number appear.

Audit Logs

Token activity is available to view in **Audit Logs**.

> **NOTE**
> The **Audit Logs** icon does not appear if the FI does not have any audit records.

In **Audit Logs**, administrators can access the token audit changes. These changes include **Limits Added**, **Limits Edited**, **Limits Deleted**, **Token Restricted**, **Token UnRestricted**, **Token Deleted**, and **Customer Restricted**.

The **Date** and **Event Name** filters are used to search for token activity. The following filter options appear in the **Event Name** drop-down menu.

- **Limits Added**
- **Limits Edited**
- **Limits Deleted**
- **Token Restricted**
- **Token UnRestricted**
- **Token Deleted**
- **Customer Restricted**

When the filters are applied, users can view the **Date**, **Event Name**, **Description**, and who made the change for each event.

Reports

Administrators can view all available reports in the **Reports** field of the PayCenter Portal.

User Permissions Reports

Administrators have access to the *Reports* tab where users can view a **Users Permissions Report** link.

When the **Users Permissions Report** link is selected, all registered users for the institution and their roles appear. This report can be viewed in the PayCenter Portal or downloaded in .csv format.

The following columns appear on the report:

- Email Address
- First Name
- Last Name
- Organization Name
- PeopleSoft ID
- Zelle® Org ID
- RTP Participant ID
- FedNow RTN
- Invitation Status
- User Management
- Zelle® Token Management
- Zelle® Token Lookup
- Zelle® Limits Management
- Zelle® Limits Lookup
- RTP Reprocess Transactions Management
- RTP Reprocess Transactions Lookup
- Zelle® Transactions Management
- Zelle® Reprocess Transactions Lookup

Zelle Fraud Marked Payments Report

Users with **Reporting Access** permissions can generate the *Zelle® Fraud Marked Payments* report. This report includes all payments that are marked as fraud.

Generating the Report

To view the *Zelle® Fraud Marked Payments* report, do the following:

1. Go to **Reports** > **Zelle Frauds Marked Payments Report**.
2. Enter the **Report Start Date** and **Report End Date**.

> **NOTE**
> A default date range of the last seven days appears when users view the **Zelle Frauds Marked Payments Report**.

3. Select **Generate Report**.

The following appears on the report.

- **Payment ID** - This field is a hyperlink to the *Zelle Payment Details* screen.
- **Payment Amount**
- **Payment Date**
- **Reported Date**
- **Fraud Reason**
- **Notes** - This field is not required and may appear blank.
- **Disaster Related** - (Y/N)
- **Contact Method**
- **Impersonation By Scammer**
- **Portal User Who Updated The Payment**
- **Update Type** - **Mark Fraud**, **Edit**, and **Unmark** appear in this field.
- **Update Date**

Downloading the Report

Users can download the generated *Zelle® Fraud Marked Payments* report by selecting **Download**.