

Getting Started

Hardware/Software Requirements

The following requirements and recommendations will ensure that you are able to fully utilize the system:

Operating Systems / Browsers

Microsoft Windows

Operating System	Version	Processor Architecture	Browser
Windows XP	Professional	32-Bit	Internet Explorer 8, 32-bit Firefox 5.x, 32-bit
Windows Vista	Business	32-Bit	Internet Explorer 8, 32-bit Internet Explorer 9, 32-bit Firefox 5.x, 32-bit
		64-Bit	Internet Explorer 8, 32-bit Internet Explorer 9, 32-bit Firefox 5.x, 32-bit Firefox 6.x, 32-bit
Windows 7	Professional	32-Bit	Internet Explorer 8, 32-bit Internet Explorer 9, 32-bit Firefox 5.x, 32-bit Firefox 6.x, 32-bit
		64-Bit	Internet Explorer 8, 32-bit Internet Explorer 9, 32-bit Firefox 5.x, 32-bit Firefox 6.x, 32-bit

Notes:

- The Remote Deposit module is not supported on Firefox.
- 64-bit operating systems are supported for Remote Deposit Capture only if customer has been upgraded to the updated IQA and CAR/LAR component.

Apple Macintosh OS X

Operating System	Version	Processor Architecture	Browser
v10.6 ("Snow Leopard")	n/a	n/a	Safari v4.04 or 5.01 Firefox 5.x, 32-bit Firefox 6.x, 32-bit

Note: The Remote Deposit module is not supported on Macintosh.

Other Requirements and Recommendations

Item	Required	Recommended
Browser Feature	Pop-up windows, session cookies, and JavaScript must be enabled. Additionally, if you are using Internet Explorer, the site should be added to your browser's Trusted Sites list, and your security settings should be set to require prompting when downloading files. See the Help for Internet Explorer for additional information.	
Additional Installations	It may be helpful to have the latest Java Runtime Environment ("Java") installed on your machine. Download and install it from www.java.com .	
Adobe Reader	7.0, with all Adobe-required updates installed	The most recent version of the Reader plug-in, up to v9 For Safari users, the most recent version of the Reader plug-in is required. (v9.3.4 or more recent)
Browser Encryption	128-bit encryption	
Graphics Capability	VGA	
Color Palette	16-bit	
Screen Resolution	800x600 pixels	1024x768 pixels For Remote Deposit, resolution must be 1024x768 pixels.
ISP Connection	56.6 Kbkps	DSL or higher

For Remote Deposit check-scanning computers, the following also apply:

Item	Required	Recommended
Operating System	Microsoft Windows, any supported version	
Web Browser	Internet Explorer, any supported 32-bit* version	
ISP Connection	Broadband	
Memory	Meets operating system requirements and is at least ... 512 MB	1 GB+
Processor	Intel Pentium IV - 1 GHz minimum	

* 64-bit operating systems are supported for Remote Deposit if the customer has been upgraded to the updated IQA and CAR/LAR component.

Getting Started (Cont'd)

User Name Rules

All user names must:

- Be unique.
- Be between six and 40 alphanumeric characters in length.

Notes:

- User names must consist only of alphanumeric characters (A-Z, 0-9).
- A user name will be suspended if it has not been used within any 90 day period.

A user name may be logged on to the system only once at any time.

In other words:

- If you are logged on to the system, you may not initiate another session using the same user name.
- If you close the browser window without logging off, you may be temporarily unable to log on again until your session "times out" (approximately 20 minutes).

Note: Three consecutive unsuccessful login attempts will lock the user name to prevent unauthorized usage. A password reset will be required.

Password Rules

Passwords must:

- Be between 8 and 15 characters in length.
- Contain at least one letter and one number.
- Contain at least three unique characters.
- Not be identical to the User Name.
- Contain only letters and numbers.
- Be changed at the interval specified by your System Manager.
- Be used only once within any 24-month timeframe.

Accessing the System for the First Time

To log on to the site for the first time, you will need a temporary User ID, a temporary password and the system Web address. Please see your System Administrator if you do not have this information.

To access the system for the first time:

1. Open a supported Web browser.
2. In the browser's **Address** field, enter the system address provided to you by the System Administrator.
3. Press the **Enter** key on your keyboard to access the system web-site.
4. In the **User Name** field, enter your temporary User ID.
5. Click the **Next** button. The Password field is displayed.
6. In the **Password** field, enter your temporary password.
7. Click the **Login** button. The Welcome screen is displayed.

8. Read the presented information, then click the **Next** button. The User Information screen is displayed.
9. Provide information about yourself. All fields are mandatory, except **Middle Initial**.
 - *[Optional]* In the **First Name**, **Middle Initial**, and/or **Last Name** fields, modify your name.
 - In the **E-Mail Address** field, enter your email address.
Note: Since this address is used to help reset forgotten application passwords, it is **critical** that you provide a correct, permanent email address. If multi-factor authentication has been implemented for your company or location, and if you might use an unregistered machine to access the system, use an email address you'll be able to access from the unregistered machine; this will allow you to retrieve the temporary URL necessary to access the system.
 - In the **User Name** field, enter your permanent user name. This is the user name you will use to log on to the system in the future.
 - In the **Password** field, enter a new password. This password must conform to the rules set forth in the "Password Rules" section of this document.
 - In the **Confirm** fields, re-enter the information entered in the previous steps.
10. Click the **Next** button. The Security Questions screen is displayed.
11. Choose and answer any three security questions.
 1. From each **Question** drop-down list, select a different question to be answered.
 2. In each **Answer** field, answer the selected question.
 3. In the appropriate **Confirm** field, re-enter the answer.
12. Click the **Submit** button.
 - If no multi-factor authentication has been enabled for your company or location, the Home tab is displayed.
 - If RSA Authentication multi-factor authentication has been implemented for your company or location, before you may access the system you must select a RSA Authentication image and phrase. See the "Registering for RSA Authentication" section of the Multi-Factor Authentication reference for additional instructions.
 - If token-based multi-factor authentication has been implemented for your company or location, before you may access the system you must register your token. See the "Registering an MFA Token" section of the Multi-Factor Authentication reference for additional instructions.

Getting Started (Cont'd)

Logging On After the First Time

Once you have logged on to the system for the first time and selected a permanent user name, use one of the following procedures to log on, depending on your company and site's multi-factor authentication option, if any.

No Multi-Factor Authentication

1. Navigate to the system website.
2. In the **User Name** field, enter your permanent user name.
3. Click the **Next** button. The Password field is displayed.
4. In the **Password** field, enter your password.
5. Click the **Login** button to log on to the system.

RSA Authentication Multi-Factor Authentication

1. Navigate to the system website.
2. In the **User Name** field, enter your permanent user name.
3. Click the **Next** button.
 - If you have not yet registered for RSA Authentication
 1. The **Password** field is displayed. Enter your password.
 2. Click the **Next** button. The RSA Authentication registration screen is displayed.

You must register a RSA Authentication image and phrase before continuing to access the system. See the "Registering for RSA Authentication" section of the Multi-Factor Authentication reference for additional instructions.

- If you have registered for RSA Authentication but did not register your computer
 1. Do one of the following:
 - If your company site is configured to require that you receive an email at your registered email address

When you click the **Next** button in step 3 from the original procedure, a time-sensitive email is sent to the address you have registered with the system. Open the email and either click the included link or copy-and-paste it to the browser's **Address** field and press the **Enter** key on your keyboard.
 - If your company site is configured to allow you direct access to your security questions

Do nothing.

The RSA Authentication Alert: Unknown Computer screen is displayed.

2. Enter the answers to the security questions you provided during your initial setup. These questions will help verify your identity to the system.
3. Click the **Next** button.
4. Proceed as if you had newly registered your computer. Once you have provided your password, you will be given another opportunity to register your computer to simplify the log-on procedure.

- If you have registered for RSA Authentication and registered your computer

The **Password** field is displayed; your RSA Authentication image and phrase should be displayed to the right.

- If the image and phrase you selected during your initial setup are displayed

In the **Password** field, enter your password. For security purposes, an asterisk (*) is displayed for each entered character, instead of the character itself.

Before clicking the **Login** button to continue, you can click the **Change RSA Authentication** button to update your RSA Authentication image, phrase, or registration preferences.

- If either the image or the phrase is incorrect or missing

The security of your access to the system may be compromised. Do **NOT** proceed. Print the screen and contact Customer Service immediately. [End Procedure]

5. Click the **Login** button to log on to the system.

If you have not previously registered your computer with the system (if registration is applicable), you will be given an opportunity to do so.

Continued

Getting Started (Cont'd)

Logging On After the First Time (Cont'd)

Token-Based Multi-Factor Authentication

1. Navigate to the system website.
2. In the **User Name** field, enter your permanent user name.
3. Click the **Next** button. The **Password** field is displayed.
 - If you have not yet registered your token
 1. In the **Password** field, enter your password.
 2. Click the **Next** button. The Welcome to Token Registration screen is displayed.

See the "Registering an MFA Token" section of the Multi-Factor Authentication reference for instructions on registering your token.
 - If you have already registered your token
 1. In the **Password** field, enter your password, leaving your cursor in the field when you finish typing.
 2. Generate a token passcode by pressing the button on the token, or by using whatever method the token documentation instructs you to use. This token passcode will be displayed on the token for approximately 30 seconds, although it may still be used for a few minutes after the displayed password changes.
 3. Enter the token passcode immediately after your password. Do not separate the two passwords with spaces or any other character.

Example: If your password is "password" and the generated token passcode is "123456", then enter password123456.
 4. Click the **Next** button. The Home tab is displayed.

Timing Out

As a security precaution you will automatically be logged off from the system after a period of inactivity (usually approximately 20 minutes). If your session times out while you are logged on, the Login screen is displayed. A message is displayed to inform you that your session was terminated due to timeout. Any unsaved work will be lost.

Logging Off

For security purposes, you should always log out after each work session. To log off, click the **Sign Out** hyperlink in the upper right-hand corner of the application screen.

Forget Your Password?

1. On the initial log-on screen, in the **User Name** field, enter your user name.
2. Click the **Next** button. The second log-on screen is displayed.
3. Click the **Forgot Password?** button. An email is sent to the address you registered when you first set up your account.

Note: This email will include a customized Web address that will be valid for 15 minutes from the time you clicked the **Forgot Password?** button.
4. When the email arrives, follow its instructions to choose a new password.

If your company and site use token-based multi-factor authentication, you will have additional options to help you handle temporarily-unavailable and permanently-lost tokens.

1. The following options will be available when you access the **Forgot Password** page via the link provided in the email. Choose the appropriate option:
 - **Reset Static Password:** This option allows you to reset the password used to log on to the system.
 - **Lost Token and Have a Spare One:** Use this option if this radio button if your token is not available and you will not be using it again in the future.

Note: This feature is unavailable if multiple tokens have been registered to you. Contact your System Manager to de-activate the lost token.
2. Click the **SUBMIT** button. If you chose:
 - **Reset Static Password:** Change your password as if your company and site do not use token-based MFA.
 - **Misplaced Token:** A time-sensitive one-time password is displayed.
 1. Make a note of the temporary password.
 2. Click the **CONTINUE** button. You are returned to the password-entry screen.
 3. Enter your password, appending the temporary password as if it were a token passcode.
 4. Click the **Login** button. You are logged on to the system.
 - **Lost Token and Have a Spare One:** Click this radio button if your token is not available and you will not be using it again in the future. The token will be de-linked, and you can register a new token when you get one. You will not be able to use the system without a new token.

Getting Started (Cont'd)

Entering Dates


The Calendar utility provides you with an alternate method for entering dates throughout the system.

Notes:

- You can also enter all dates manually, using mm/dd/yyyy format.
- If a date is displayed in red, with the box surrounding it appearing slightly "grayed-out," that date is a bank holiday or closed-day, and may not be selected. If you manually enter a date unavailable for selection, you will be notified of the date's unavailability.

Because the list of available dates is linked to individual accounts, where this feature is available, it will be active only if an account has already been selected.

To enter a date:

1. Click the rectangular **Calendar** button  located below or beside the date field.
A pop-up Calendar window is displayed, set to the current month.
2. From the **Month** drop-down list, select a month.
3. From the **Year** drop-down list, select a year.
4. Select the date by clicking it on the calendar. The pop-up window closes, and the selected date is entered for you into the date field.

Approving Items, Batches, and Templates

Depending on the settings for your company and the requirements of a module, approvals may be required before an item, batch, or template can be submitted for processing.

Regardless of system validations, users can approve only those items, batches, or templates that other users have created. Users may not approve their own items, batches, and templates.

Note: Depending on the module, a special validation may be required to approve items. See the Quick Reference for each module for approval requirements.

To approve pending items, batches, and templates:

From the Home tab:

1. In the Pending Items pane, click the **Approve** tab.
2. Click the pane header associated with the module containing the item to be approved. The pane expands to display all items within that module that are pending approval.
3. Select the checkboxes associated with the items to be approved.
4. Click the **Approve** button. A confirmation message is displayed, and the selected items are approved.

From elsewhere in the system:

1. Move your mouse cursor over or click a navigation tab. The associated submenu is displayed.
2. From the submenu, click a hyperlink to access the module in which the item, batch, or template is located.
3. On the Pending Items tab:
 - Click the **approve** hyperlink associated with a single item, batch, or template to be approved.
 - Select the checkboxes associated with multiple items, batches, or templates to be approved, then click the **Approve** button.

If the user is validated for batch submission and the required number of approvals have been given, the **approve** hyperlinks are replaced by **submit** hyperlinks. The items, batches, or templates are now ready to be submitted.

Submitting Items, Batches, and Templates

Any item, batch, or template present on a module's Pending Items tab must be submitted before it can be used.

To submit pending items, batches, and templates:

From the Home tab:

1. In the Pending Items pane, click the **Submit** tab.
2. Click the pane header associated with the module containing the items to be submitted. The pane expands to display all items within that module that are pending submission.
3. Select the checkboxes associated with the items to be submitted.
4. Click the **Submit** button. A confirmation message is displayed, and the selected items are submitted.

From elsewhere in the system:

1. Move your mouse cursor over or click a navigation tab. The associated submenu is displayed.
2. From the submenu, click a hyperlink to access the module in which the item, batch, or template is located.
3. On the Pending Items tab:
 - Click the **submit** hyperlink associated with a single item, batch, or template to be submitted.
 - Select the checkboxes associated with multiple items, batches, or templates to be submitted, then click the **Submit** button.

The Submit Confirmation screen is displayed.

4. *[Optional]* To print the confirmation, click the **Print** button. Make the necessary selections in the Print dialog box, then click the **OK** button.
5. Click the **OK** button to close the confirmation screen and return to the Pending Items tab.

Getting Started (Cont'd)

Modifying Pending Items, Batches, and Templates

Unless otherwise specified in a particular module's description, pending items, batches, and templates can be modified from a module's Pending Items tab.

You can modify items with the status "Awaiting Submission," "Rejected," "Awaiting Approval," or "Stale Date."

To modify an item:

1. Move your mouse cursor over or click a navigation tab. The associated submenu is displayed.
2. From the submenu, click a hyperlink to access the module in which the item, batch, or template is located.
3. On the Pending Items tab, click the **modify** hyperlink associated with the item, batch, or template to be modified. The Modify [item] screen is displayed.
4. Make the necessary changes.
5. Click the **Save** button.

Note: If a modified item requires approval, it must be approved again—even if it was approved prior to modification.

Deleting Pending Items, Batches, and Templates

To delete a pending item, batch, or template:

From the Home tab:

1. In the Pending Items pane, click the **Approve** or **Submit** tab, as appropriate.
2. Click the pane header associated with the module containing the items to be deleted. The pane expands to display all items within that module that are pending approval or submission.
3. Select the checkboxes associated with the items to be deleted.
4. Click the **Delete** button. A confirmation dialog box is displayed.
5. Click the **OK** button. A confirmation message is displayed, and the selected items are deleted.

From elsewhere in the system:

1. Move your mouse cursor over or click a navigation tab. The associated submenu is displayed.
2. From the submenu, click a hyperlink to access the module in which the item, batch, or template is located.
3. On the Pending Items tab:
 - Click the **delete** hyperlink associated with a single item, batch, or template to be deleted.
 - Select the checkboxes associated with multiple items, batches, or templates to be deleted, then click the **Delete** button.

A confirmation dialog box is displayed in a pop-up window.

4. Click the **OK** button to delete the item, batch, or template.

Activating Pending Transaction Schedules

Once a transfer schedule has been created, it must be activated before it can be used.

Transfer schedules can be activated from the Pending Items pane on the Home tab, or from the Pending Items tab in the Book Transfers module.

From the Home tab:

1. In the Pending Items pane, click the **Activate** tab.
2. Click the pane header associated with the module containing the schedule to be activated. The pane expands to display all schedules within that module that are pending activation.
3. Select a checkbox associated with a schedule to be activated. Only one checkbox may be selected at a time.
4. Click the **Activate** button. A confirmation message is displayed, and the selected schedule is activated and removed from the Pending Items pane.

From elsewhere in the system:

1. Move your mouse cursor over or click a navigation tab. The associated submenu is displayed.
2. From the submenu, click a hyperlink to access the module in which the schedule is located.
3. On the Pending Items tab, click the **activate** hyperlink associated with the schedule to be activated. The schedule is activated, and will begin generating transactions as specified.

Multi-Factor Authentication

About Multi-Factor Authentication

In security terms, "authentication factors" are methods by which users prove their identity to a system. Single-factor authentication requires one method; multi-factor authentication requires two or more.

The "traditional" single-factor authentication method is the well-known user ID/password combination. This method is relatively secure, as long as the username and password are not compromised or easily guessed.

Other examples of authentication methods might include a temporary unique code from a random-number generating token that you and only you have in your possession, biometric information such as fingerprints or retinal scans, or unique characteristics that identify the personal computer you use to access a system.

Multi-factor authentication increases transaction security by making it more difficult for unauthorized individuals to gain access to the system through a stolen set of user credentials.

About RSA Authentication

The RSA Authentication multi-factor authentication system provides for three types of security:

- User authentication via passwords
- User-to-system authentication via system characteristics
- System-to-user authentication via image and text

When all three security types are used:

- You can be comfortable that you are accessing the genuine system.
- The system will have been provided two independent sets of information that will help ensure that you are a legitimate user.

User Authentication Via Passwords

Since you choose your user name and password, only you should know this combination—and since the system requires certain password characteristics designed to make your password harder to guess or computationally determine, it is reasonably secure.

User-to-System Authentication Via System Characteristics

When you log on for the first time, you are invited to allow the system to gather certain metrics that combine to uniquely identify your machine ("registration"). These metrics are checked each time you log on to the system; registration creates a "trusted relationship" between your machine and the system and helps to ensure that an authorized user is logging on.

No files or data that could be used to identify you as an individual are retrieved or checked during registration; instead, this process might collect such data as your computer's processor speed, time zone setting, and its country code settings. Please be assured that this information is used only to identify your computer to the system; it will always remain private and it will never be used in any other way.

Important: Since the system considers a registered computer to be "safe," you should not register a computer if it is shared by multiple users in any setting outside of the home or office, is a public computer (such as one located in a library), or if its physical security is likely to be compromised.

If you opt not to register your computer, or if you access the system from an unregistered computer, once you provide your user name and password one of two things will happen, depending on the setting established for your company:

- If your company site is configured to send emails

You will be sent an email containing a one-time link to a pair of the security questions that you answered during user-profile creation. This email will be sent to the address you have registered with the system. For additional security, this link expires 15 minutes after it is sent.

Because the link to access the security questions is sent via email instead of presented as part of the normal screen flow, it adds additional security; an unauthorized user must have access to your email account as well as to your user name, password, and security question answers. (See the "Security Questions" section for additional information.)

- If your company site is configured to allow direct access to your security questions

You will be presented with the security questions you chose and answered when you set up your user profile. After correctly answering the questions, you will be given the opportunity to register your computer, then the Home tab will be displayed.

System-to-User Authentication Via Image and Text

The system-to-user authentication feature consists of two elements:

- An image that you choose from our extensive database of images.
- A code phrase that you provide when you choose your image.

Each time you access the system, your code phrase and image will be presented to you. Since the image and text should be known only to you and the system, when you see your combination during the log-on process, you can be sure that you are accessing the certified system.

Multi-Factor Authentication (Cont'd)

Registering for RSA Authentication

Once RSA Authentication multi-factor authentication has been implemented for your company or location, you will be required to select a RSA Authentication image and phrase and to decide whether or not to register your computer with the system.

If you are accessing the system for the first time, the RSA Authentication registration screen is displayed at the end of the log-on process; if you have already created a user profile, the screen is displayed upon your first log-on attempt after your company signs up for the feature.

When you first access the RSA Authentication registration screen, a random image is selected from the image database and displayed in the **Your RSA Authentication Image** area.

1. Do one of the following:
 - Accept the selected image
Enter a phrase in the **Your RSA Authentication** phrase field. This phrase should be 1 to 30 characters long, and may be any text you will recognize on future visits.
 - Choose a new image
 1. Click the **change image** link in the paragraph above the image. A catalog of images is displayed.
 2. Click one of the images to select it, or click more images to load additional images. You can also select a category from the To view other images by category drop-down list. When you have found an image that meets your needs, click the image. You are returned to the previous screen.
 3. Enter a phrase in the **Your RSA Authentication** phrase field. This phrase should be 1 to 30 characters long, and may be any text you will recognize on future visits. The phrase should not describe the image itself.
2. From the radio buttons at the bottom of the screen:
 - Register the computer
Select the **Yes, register this personal computer** radio button.
 - Do not register the computer
Select the **No, do not register it...** radio button.
3. Click the **Next** button. A confirmation screen is displayed.
4. Confirm your selections, then click the **Next** button. A confirmation message is displayed.
5. Click **OK**. The Home tab is displayed.

About Token-Based Multi-Factor Authentication

You may have been provided with a security token to use in conjunction with your password. Tokens add a great deal of security to online interactions, by providing a physical second factor necessary to log on to the system and to submit transactions.

The system supports multiple types of tokens, but in general all tokens function in a similar fashion. Through some mechanism—usually a button pressed on the token, though some tokens will work automatically—a passcode is displayed on the token's display screen. This token passcode will be displayed on the token for approximately 30 seconds, although it may still be used for a few minutes after the displayed password changes. Simply append your token passcode to your self-chosen password to verify your identity.

Since the token passcode is always changing, tokens provide a highly secure secondary authentication method; someone attempting to attack the system using your log-on credentials must also have your token in his possession.

See the documentation that accompanied your token for details about the token you have been provided.

Registering an MFA Token

Once token-based multi-factor authentication has been implemented for your company or location, you will be required to register the MFA token you have been given for use with the system. The token registration screen is displayed upon your first logon or first template/transaction submission after your company signs up for the feature.

To register your token:

1. In the **Enter Token Serial Number** field, enter the token serial number. This serial number is usually found on the back of the token, though it may be on the box or in another location.
Enter the serial number without dashes or other separators; if the token serial number is 1-234-56 enter 123456.
2. Generate a token passcode by pressing the button on the token, or by using whatever method the token documentation instructs you to use. This token passcode will be displayed on the token for approximately 30 seconds, although it may still be used for a few minutes after the displayed password changes.
3. In the **Enter Token Password** field, enter the generated password.
4. Click the **Register** button. A confirmation screen is displayed.
You can also click the **Cancel** button to abandon the registration attempt. You will not be able to access the system until the token is registered. If you are registering for the first time, however, your initial registration information is retained.
5. Click **OK**. The Home tab is displayed.

Help and User Info

Help

Three types of on-line help are typically available to you as you navigate through the system:

- *How Do I...* help is accessible from the bottom of each screen for which this type of help is available; if no *How Do I...* help is available for a screen, the drop-down list will not be displayed. *How Do I...* help provides you with step-by-step procedures to perform tasks related to the screen you are currently viewing. To access *How Do I...* help, make a selection from the drop-down list at the bottom of the system window. Help is displayed in a pop-up window.
- “Narrative” help is accessible via a link next to the *How Do I...* drop-down list at the bottom of the screen. Narrative help provides you with more general information about the screen or module from which you accessed it. To access narrative help for a screen, click the **help** hyperlink. Help is displayed in a pop-up window.
- “Item” help is displayed, when available, in the bottom right-hand corner of the screen when you click a field or use the **Tab** key to access a field.

Contact Information

Click the **Contact Us** link, located at the top of the application window, to find contact information for technical support and account information.

User Information

Caller ID and User ID

The Customer Service Center may require your “Caller ID” (also known as “internal ID” or “site ID”) and “User ID” in the event that you contact them for assistance.

Use the mouse to position the cursor over your user name, located in the bottom right-hand corner of the system’s browser window.


Your Caller ID and User ID are displayed to the left of your user name, above the release information.

Viewing System Information

To view system information, click your Caller ID/User ID or User Name, located in the bottom right-hand corner of the system’s browser window. A pop-up window is displayed.

Information is available on the following tabs:

- **User Map:** Provides information about user profiles set up on the system.
- **User Privileges:** Provides information about system functionality available for your use.
Note: The System Manager can view all users and their privileges.
- **Account Display:** Provides information about accounts, including available system functionality.

Click  to close the pop-up window.

Accessing Preferences

To access system preferences settings:

1. Click the **Preferences** hyperlink, in the upper right-hand corner of the system window. The Preferences tabs are displayed.
2. Click the appropriate tab. Sub-tabs, if available, are displayed.

Changing Passwords

For security reasons, you will periodically be prompted to change your password. 7 days before your password expires, upon logon to the system you will be prompted to choose a new password. You may also change your password at any time.

Changing Your Password During Logon

If applicable, you will be prompted to change your password immediately after you enter your password for logon and click the Submit button. On the resulting screen, the following options are available:

- Postpone the password change, if the password has not already expired, but be prompted for a new password at next logon
Click the **Skip** button.
- Postpone the password change, if the password has not already expired, and receive no further prompts until password expiration
 1. Select the **Do not remind me again** checkbox.
 2. Click the **Skip** button.
- Change your password immediately
 1. Click the **Change Password** button. The Password Change pane is displayed.
 2. In the **Current Password** field, enter your current password.
 3. In the **New Password** field, enter a new password.
 4. In the **Confirm Password** field, re-enter your new password.
 5. Click the **Change** button.

The Home tab is displayed.

Changing Your Password On Demand

To change a password if not required by password expiration:

1. From the Preferences tabs, click the **Change Password** tab. The Change Password pane is displayed.
2. In the **Current Password** field, enter your current password.
3. In the **New Password** field, enter a new password.
4. In the **Confirm Password** field, re-enter your new password.
5. Click the **Change** button. Your change is saved.

Quicklinks

Quicklinks give you quick access to frequently-used system functionality, allowing you to jump right to a particular module's Create or Reporting tabs, etc. Quicklinks are available from any screen via the **Go To** drop-down list in the top right-hand corner of the screen.

To set Quicklink preferences:

1. From the **Go To** drop-down list, select **Manage Quicklinks**.
From the Preferences tabs, you can also click the **Quicklinks** tab.
2. From the **Quicklink #1** drop-down list, select the activity or module to be listed first in the **Go To** drop-down list.
[Optional] Add up to eleven additional links to the list by making selections from the **Quicklink #2** through **Quicklink #12** drop-down lists.
3. Click the **Submit** button. The contents of the **Go To** drop-down list are updated, and a confirmation message is displayed.

To use a Quicklink:

From the **Go To** drop-down list, select the feature to be accessed. The corresponding screen is displayed.

Preferences (Cont'd)

Favorite Accounts

If available, Favorite Accounts are displayed in the Account Balances pane on the Home tab, giving you balance information and one-click access to the Account Detail report for up to twelve accounts.

Note: For your convenience, Information Reporting and Loan Reporting accounts are automatically added to the Favorite Accounts list as they are associated with your user profile by a System Manager.

1. Do one of the following:
 - From the Home tab
Click the **Manage Accounts** hyperlink, located near the top of the Account Balances pane. The Favorite Accounts tab is displayed.
 - From anywhere else in the system
From the Preferences tabs, click the Favorite Accounts tab.
If you have access to both loan and asset accounts, two columns of drop-down lists are displayed. If you have access only to one or the other, only one column of drop-down lists is displayed.
2. From the **Balance type** (for asset accounts) and **Loan Balance type** (for loan accounts) drop-down lists, choose the types of balances to be reflected in the Account Balances pane (Available Balance, Collected Balance, or Ledger Balance for asset accounts; Outstanding Balance and Available Balance for loan accounts).
Either one or two balance types may be selected for each account type. Hold down the **Ctrl** key when clicking listbox entries to select multiple balance types.
3. From the **Account #[#]** drop-down lists, select accounts to be included in the Account Balances pane. You may select up to twelve accounts distributed between the two columns, e.g., 12 asset account balances, 12 loan account balances, 3 of one and 9 of the other, etc.
4. Click the **Submit** button. A confirmation message is displayed.

When you return to the Home tab, the selected accounts are displayed the Account Balances pane.

Selecting a Scanner for Use with Remote Deposit

To scan checks using the Remote Deposit module, you will need to select a scanner supported by the system.

To select a scanner for use with Remote Deposit:

1. From the Preferences tabs, click the **Remote Deposit** tab.
2. From the **Scanner Type** drop-down list, select the check scanner you will be using to upload checks into the system.
3. Click the **Submit** button. Your changes are saved.

The Customer Alerts module helps you use the system more efficiently by enabling you to request that email messages be sent to one or more recipients when certain events occur.

Both the list of alerts and the Address Book are shared by all users at your location; if one user at your location creates an alert, that alert will be available to all users with the appropriate access; if one user enters an address, that address will be available to all users.

Accessing the Customer Alerts Feature

To access the Customer Alerts feature:

1. Click the **Preferences** hyperlink, in the upper right-hand corner of the system window. The Preferences tabs are displayed.
2. Click the **Alerts** tab. A pair of tabs (*Create* and *Address Book*) is displayed in the area beneath the Alerts tab.

Creating Customer Alerts

Alerts can be created by any user validated to compose alerts. Users can create alerts only for events that occur in relation to modules for which they are validated.

Notes:

- Alert creation requires that at least one recipient exist in the Address Book.
- The Address Book cannot be modified during the process of creating an alert, so be sure that your alert's intended recipients have been added to the Address Book before creating an alert.
- Alert additions are processed at midnight EST. Your changes will become effective at that time.

To create an alert:

1. On the **Create** tab, click the **Create Alert** button. The Customer Alerts - Create pane is displayed.
2. From the **Category** drop-down list, select the module in which the event is expected to occur. The contents of the **Title** drop-down list change to reflect the alerts available for that module.
3. From the **Title** drop-down list, select the alert to be created.
4. In the **Alert Name** field, enter a name for the alert. You can skip this step and come back to it later, if you're not sure what you'll be naming it at this point.

Important: A particular name may be used only once for a particular combination of Category and Title.

5. Click the **Continue** button. The Customer Alerts-Create pane expands to reveal the criteria on which the alert will be based.

6. In the **Criteria** section, specify the criteria to be used to generate the alert. See the table below these instructions for additional details. The parenthetical phrases following the step descriptions correspond to the **Feature** column in the **Alert Criteria Field Reference** section.

- ACH Origination

The following alerts are available for ACH Origination:

- Transaction Batch Awaiting Approval
- Transaction Batch Awaiting Submission
- Transaction Batch Rejected
- Transaction Batch Modified
- Transaction Batch Deleted
- Transaction Batch Submitted
- Schedule Activated
- Schedule Awaiting Approval
- Schedule Deactivated
- Schedule Deleted
- Schedule Ended
- Schedule Failed
- Schedule Modified
- Schedule Suspended
- ACH Template Created
- ACH Template Modified
- ACH Template Deleted
- ACH Template Copied
- ACH Template Awaiting Approval
- ACH Template Approved

In each case, the following criteria apply:

1. Specify the accounts to be monitored. ("Accounts Included")
2. Specify upper and lower boundaries for the batch. ("Amount Threshold")
3. Indicate whether the total value of the batch is to be included in the alert text. ("Include Amount in Message")

Continued

Alerts (Cont'd)

Creating Alerts (Cont'd)

- Information Reporting

The following alerts are available for Information Reporting:

- **Previous Day Incoming Wire / Current Day Incoming Wire**
Triggered when a wire transfer is credited to one or more specified accounts, when the transaction is added to the previous-day or current-day databases, respectively.

1. Specify the accounts to be monitored for incoming wire transfers. ("Accounts Included")
2. Specify upper and lower boundaries for incoming wire transfer values. ("Amount Threshold")

- **Account Targets**

Triggered when an account balance reaches the notification level set in the Account Targets feature.

Enter the message to be sent when the target level is reached. ("Message")

- **Balance Alerts**

Triggered when account balances fall below or rise above specified thresholds.

1. Specify the accounts to be monitored for balances. ("Accounts Included")
2. Specify upper and lower boundaries for balance alert values. ("Amount Threshold")
3. Indicate whether the balance amount is to be included in the alert text. ("Include Amount in Message")
4. Select the balance types to be monitored. ("Balance Type")

- Wire Transfers

The following alerts are available for Wire Transfers:

- Wire Submitted, Awaiting Bank Confirmation
- Wire Template Awaiting Approval
- Wire Template Created
- Wire Template Deleted
- Wire Template Modified
- Wire Template Rejected
- Wire Transaction Awaiting Approval
- Wire Transaction Awaiting Submission
- Wire Transaction Created
- Wire Transaction Deleted
- Wire Transaction Modified
- Wire Transaction Rejected

For each of these alerts, do the following:

1. Specify the accounts to be monitored for incoming wire transfers. ("Accounts Included")
2. Specify value date criteria for the alert. ("Type & Date")
Note: This entry is used only for the Wire Transaction Awaiting Approval alert.
3. Specify upper and lower boundaries for outgoing wire transfer values. ("Amount Threshold")
4. Indicate whether the wire amount is to be included in the alert text. ("Include Amount in Message")

- Other: Reminder Alerts

This alert provides users with the ability to send recipients a "free-form" reminder message on a specified date.

1. Enter the message text to be sent. ("Message")
2. Specify the date on which the message is to be sent.

- Positive Payment: Positive Payment Exception Awaiting Decision

Triggered when one or more Positive Pay exception items become available for decisioning.

1. Specify the accounts to be monitored for exception items. ("Accounts Included")
2. Indicate whether check number and amount are to be included in the alert message. ("Include Check # and Amount in Message")

- Security

The following security-related alerts provide users with the ability to specify "free-form" messages to be sent when the triggering condition occurs.

- Application Password Modified
- Email Address Modified
- Existing User Deleted
- Existing User Modified
- New User Added
- Transaction Password Modified
- User Challenged
- User Limits Modified

For each alert, enter the message text to be sent. ("Message")

7. In the **Recipients** section, add one or more recipients from the Address Book:
 1. From the **Recipients** drop-down list, select a recipient.
 2. Click the **Add** button to add the account to the Included list.
To remove recipients, select them from the Included list, then click the **Remove** button.
8. Click the **Save** button to save the alert.

Alerts (Cont'd)

Customer Alert Criteria Field Reference

Feature	Instructions	Feature	Instructions
Accounts Included	<ol style="list-style-type: none"> From the drop-down list, select an account to be monitored. Click the Add button to add the account to the Accounts Included list. <p>To remove accounts from the Accounts Included list, select them and click the Remove button.</p>	Amount Threshold	<ul style="list-style-type: none"> <u>All transactions involving the selected accounts</u> Select the All radio button. <u>Amounts falling within a selected range</u> <ol style="list-style-type: none"> Select the Amount Range radio button. From the first Amount Range drop-down list, select one of the following: <ul style="list-style-type: none"> From: If the alert is to be generated for amounts that include the value. Above: If the alert is to be generated for amounts over the value. Equal: If the alert is to be generated for amounts exactly equal to the value. In the first Amount Range field, enter a "floor" value for the alert. *From the second Amount Range drop-down list, select one of the following: <ul style="list-style-type: none"> To: If the alert is to be generated for amounts that include the value. Below: If the alert is to be generated for amounts below the value. *In the second Amount Range field, enter a "ceiling" value for the alert. <ul style="list-style-type: none"> **Amounts that fall below a "floor" value <ol style="list-style-type: none"> Select the Notify me if Balance goes below radio button. Enter a balance "floor" in the associated field. **Amounts that rise above a "ceiling" value <ol style="list-style-type: none"> Select the Notify me if Balance goes below radio button. Enter a balance "ceiling" in the associated field. <p>* These features will be unavailable if Equal was selected from the first drop-down list.</p> <p>** These features are available only for certain alerts that use the Amount Threshold condition.</p>
Type & Date	Select a radio button to limit alerts to those transactions that are value-dated for the current day (select the Today radio button), some day in the future (select the Future radio button) or either (select the All radio button).		
Include Amount in Message	Select this checkbox if the transaction ID (if applicable) and transaction amount or balance are to be included in the alert message.		
Balance Type	Select the balance types for which alerts are to be generated. Hold down the Ctrl key while clicking to select multiple types.		
Message	Enter the text to be sent in the alert message.		
Date	Enter the date on which the free-form reminder alert is to be sent.		
Include Check # and Amount in Message	Select this checkbox if the check number and amount of the Positive Payment exception item are to be included in the alert message.		

Alerts (Cont'd)

Modifying Customer Alerts

All users who can create alerts can modify the alerts that they've created. No user may modify alerts created by another user.

Note: Alert modifications are processed at midnight EST. Your changes will become effective at that time.

To modify an alert:

1. On the Create tab, click the **modify** hyperlink associated with the alert to be modified. Alert details are displayed in the Alerts - Create pane.
2. Make the necessary changes. See the "Creating Alerts" topic for additional information about the fields used to configure alerts.
3. Click the **Save** button to save the alert and return to the alerts list.

Deleting Customer Alerts

All users who can create alerts can delete the alerts that they've created; users validated to view and delete alerts can also delete alerts created by other users at the location.

Note: Alert deletions are processed at midnight EST. Your changes will become effective at that time.

To delete an alert:

1. On the Create tab, do either of the following:
 - Delete a single alert
Click the **delete** hyperlink associated with the alert to be deleted.
 - Delete multiple alerts
 1. Select the checkboxes associated with the alerts to be deleted.
 2. Click the **Delete** button at the bottom of the screen.
A confirmation dialog box is displayed.
2. Click the **Yes** button. The selected alerts are deleted, and the alerts list is refreshed.

Suspending and Unsuspending Customer Alerts

Suspended alerts remain on the system, but no messages are sent even if the alert conditions occur.

Notes:

- Alert messages are not accumulated during suspension; designated recipients will receive only those messages generated while the alert is active.
- Alert suspensions and re-activations are processed at midnight EST. Your changes will become effective at that time.

All users who can create alerts can suspend the alerts that they've created; users validated to view and delete alerts can also suspend alerts created by other users at the location.

To suspend/unsuspend alerts:

On the Create tab, do either of the following:

- Activate a suspended alert

Click the **unsuspend** hyperlink associated with the alert to be activated.

- Suspend an active alert

Click the **suspend** hyperlink associated with the alert to be suspended.

The screen is refreshed, and the Status column is updated to reflect the change in status.

Note: Since the sorting of the alerts list is partially based on alert status, changes to an alert's status may cause the alert to change position on the screen or be moved to other pages of the list.

Maintaining the Customer Alerts Address Book

Alerts can be sent to any user listed in the Alerts module's address book. Any user validated to modify the Alerts address book may add recipients to the address book, modify an address book listing, or remove recipients from the address book.

Recipients added to the address book are available to all users at your location.

Notes:

- For security purposes, certain domains (@domain.com or @domain.net, etc.) may be banned from receiving alert messages; conversely, messages may be permitted only to certain domains.
- While modifications to the address book are immediately visible, changes to alerts themselves are processed at midnight EST, and will not become effective until that time.

Adding Recipients to the Address Book

At least one recipient must be available in the Address Book before an alert may be created.

To add users to the address book:

1. On the **Address Book** tab, in the blank fields at the bottom of the screen, enter a **First Name**, **Last Name**, and **Email Address** for the recipient.
2. In the Action column at the bottom of the screen, click the **add** hyperlink to add the recipient.

The recipient is immediately available for use when creating or modifying alerts.

Alerts (Cont'd)

Removing Recipients from the Address Book

For best results, if you are removing a recipient from the address book, be sure that all alerts addressed to that recipient are deleted, or that at least one other recipient exists for each alert addressed to the recipient.

Note: At least one recipient must be available in the Address Book before an alert may be created.

To remove a recipient from the address book:

1. On the **Address Book** tab, click the **delete** hyperlink associated with the entry. A confirmation message is displayed.
2. Click **Yes**. The entry is removed from the Address Book.

Alerts addressed to the deleted recipient will no longer be sent to that recipient. If the deleted recipient was the only recipient for an alert, the alert will no longer be sent, and alerts will not be accumulated for later sending.

Modifying Address Book Recipients

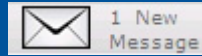
Changes to a recipient's details will change the details in all alerts addressed to that recipient.

To modify a recipient's record:

1. On the **Address Book** tab, click the **modify** hyperlink associated with the address book entry to be modified.
2. Make changes to the **First Name**, **Last Name**, and/or **Email Address** fields, as necessary.
3. Click the **update** hyperlink associated with the entry.

Alerts addressed to the recipient will be sent with the updated information.

Secure Messaging



The Secure Messaging module provides a quick, convenient way to send and receive correspondence regarding your accounts, transactions, and other services available to you.

Notes:

- The Secure Messaging module is not a POP/IMAP service; it is intended for use only in correspondence regarding your accounts and transactions, problems with the system, etc.
- Stored messages are periodically purged from the system, so be sure to print important messages, or copy their contents to a local drive!

The Secure Messaging module consists of the following tabs:

Inbox: Use this tab to access received mail. You can view all messages, or only those that have not yet been read.

Outbox: Use this tab to send mail that has been saved for later delivery.

Compose: Use this tab to create and send messages.

Sent Items: This tab archives sent messages.

Deleted Items: This tab archives messages deleted from the Inbox. Messages deleted from the Outbox and/or Sent Messages tabs are not archived.

Accessing Secure Messaging

To access Secure Messaging, click the the Secure Messaging icon, located on the right-hand side of the screen, beneath the Sign Out link. The Secure Messaging tabs are displayed.

The text accompanying the icon ([#] New Messages) indicates the number of unread messages.

Reading Incoming Messages

To read incoming messages:

1. Click the **Inbox** tab.
2. Click the **view** hyperlink associated with the message to be read. The message is displayed in a pop-up window.

From this screen, you can:

- Click the **Reply** button to reply to the message. The pop-up window closes, and the Compose tab is displayed. See the "Composing Messages" section of this document for additional instructions.
- Click the **Print** button to print the message.
- Click the **Delete** button to delete the message, then confirm your selection. The pop-up window closes, and the message is deleted. Deleted messages can be accessed from the Deleted Items tab, from where they can be "undeleted," if necessary.
- Click the **Close** button to close the pop-up window.

Note: Click the **View Unread Only/View All** hyperlink at the bottom right-hand corner of the mail tab to toggle the view between unread messages and all messages. When all messages are displayed, the link text is **View Unread Only**; when only unread messages are displayed, the link text is **View All**.

Deleting Messages

Messages deleted from the Inbox can be accessed from the Deleted Items tab; there, they can be "undeleted," if necessary. Messages on the Deleted Items tab are periodically purged from the system.

Messages deleted from other tabs are immediately purged, and are not available from the Deleted Items tab.

To delete messages:

- From the main window
 - Single message
 1. Click the **delete** hyperlink associated with the message. A confirmation dialog box is displayed.
 2. Click the **OK** button. The message is deleted.
 - Multiple messages
 1. Select the checkboxes associated with the messages to be deleted.
 2. Click the **Delete** button. A confirmation dialog box is displayed.
 3. Click the **OK** button. The selected messages are deleted.
- From the pop-up window
 1. Click the **Delete** button. A confirmation dialog box is displayed.
 2. Click the **OK** button. The selected messages are deleted.

Undeleting Messages

Messages deleted from the Inbox can be accessed from the Deleted Items tab. At any time, you can "undelete" them to return them to the Inbox.

Note: Please be aware that deleted messages are periodically purged from the system.

To undelete messages:

1. Select the messages to be undeleted.
 - Single message

Click the **undelete** hyperlink associated with the message.
 - Multiple messages
 1. Select the checkboxes associated with the messages to be undeleted.
 2. Click the **Undelete** button.A confirmation dialog box is displayed.
2. Click the **OK** button to return the message to the Inbox.

Secure Messaging (Cont'd)

Composing Messages

To compose a message:

1. Click the **Compose** tab.
2. In the **To** field, enter the recipient's name.
Note: Internet email addresses ("johnsmith@anycorp.com") are not supported.
3. From the **At** drop-down list, select a department name.
4. In the **Subject** field, enter a message subject.
5. *[Optional]* In the **CC** field, enter any additional recipient names.
6. Enter a message in the main text area.
Note: Total entry length must be less than 1,000 characters (about 160 words).
7. Click the **Send** button. A confirmation message is displayed.
Note: If the message is not delivered for any reason, it will be stored in the Outbox, and may be modified and/or manually submitted at a later time.

[Optional] Click the **Save** button to save the message in the Outbox for later editing and delivery.

Working with Archived Messages

Note: Archived messages are periodically purged from the system, so be sure to print important messages, or copy their contents to a local drive!

To work with a composed message saved for later editing and/or delivery:

1. Click the **Outbox** tab.
2. Use the hyperlinks associated with the desired message:
 - Click the **send** link to send the message.
 - Click the **modify** link to modify the message. The Compose tab is displayed, its fields populated with the message contents.
 - Click the **view** link to view the message in a pop-up window.
 - Click the **print** link to print the message.
 - Click the **delete** link to delete the message, then confirm the deletion in the confirmation dialog box.

Working with Sent Messages

Note: Archived messages are periodically purged from the system, so be sure to print important messages, or save their contents!

To work with a sent message:

1. Click the **Sent Items** tab.
2. Use the hyperlinks associated with the desired message:
 - Click the **view** link to view the message in a pop-up window.
 - Click the **print** link to print the message.
 - Click the **delete** link to delete the message, then confirm the deletion in the confirmation dialog box.