FIAT Registration and User Login/MFA Workflow

The registration process is covered below. The screens that a user sees upon subsequent logins are described at the end of this document.

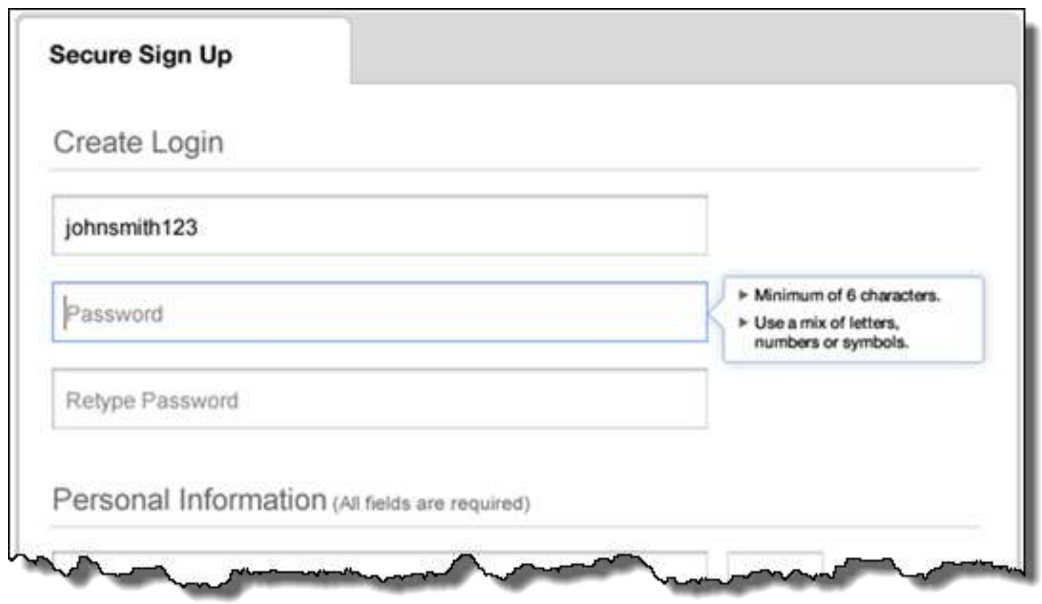
Step 1: Click Enroll Link

New users will begin the registration process by clicking the Enroll link.

FIAT with PIN: The host requires a PIN to process the registration. Your financial institution may choose to either auto-generate the PIN (ex. last 4 of SSN) or to have a PIN field on the registration form where the user will enter the PIN upon initial registration only. **Note:** The registration PIN is different from the password created by the user (shown in Step 2 below). The password (and User ID) are used each time the user logs into Online Banking.

Step 2: Create Username and Password

The user will be prompted to create their username and password.

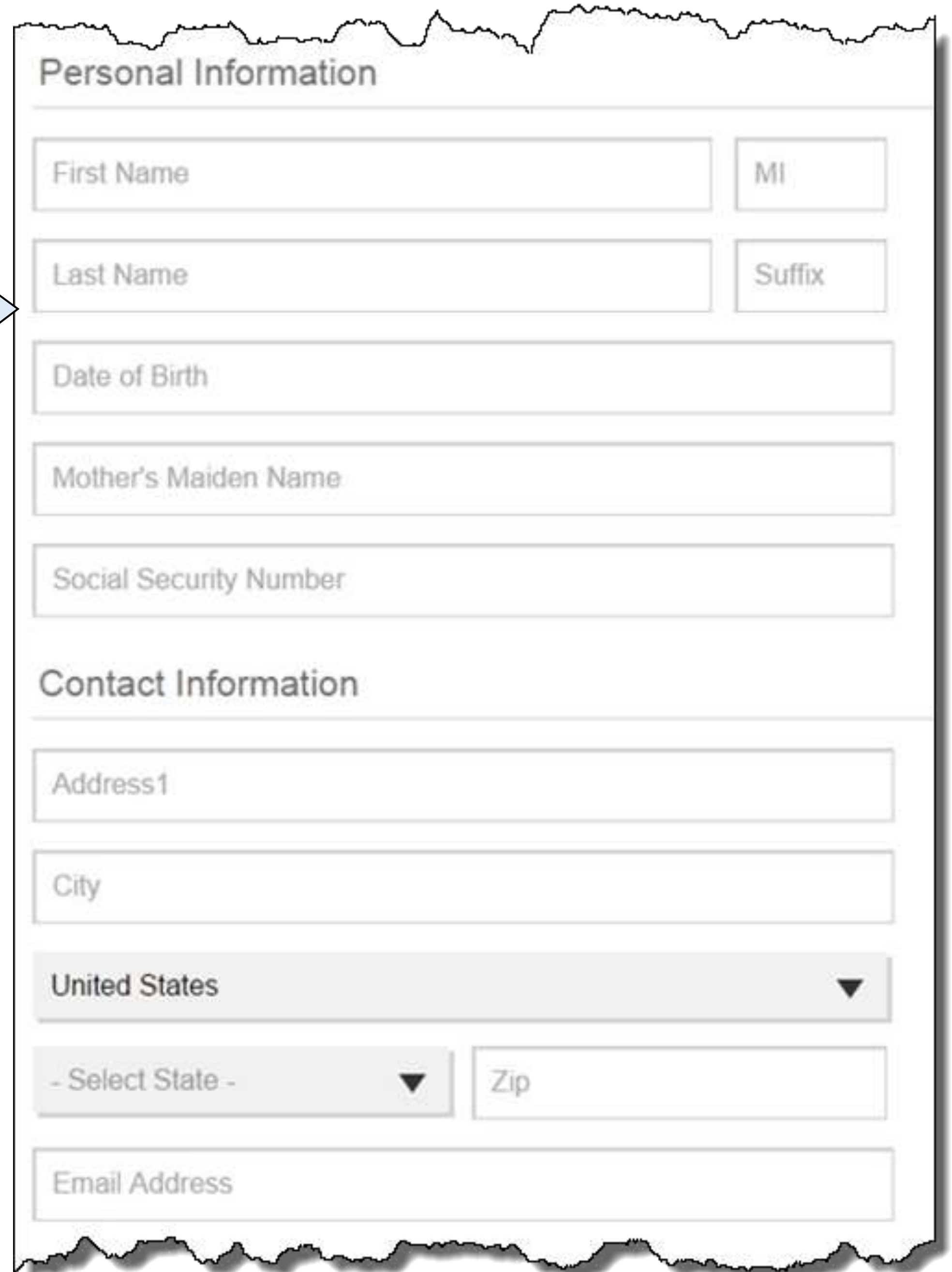


Step 3: Complete Remaining Fields

Fields shown at right are required. Additional fields are configurable and may vary based on your financial institution.

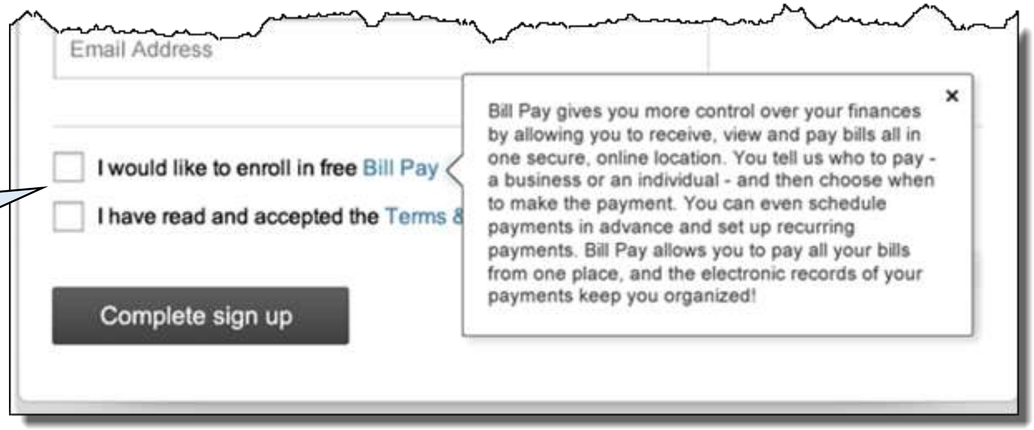
Your financial institution will create fields on the registration form that will be used to validate the user. Upon the user submitting the registration form, these fields will be validated with the information on your host system to facilitate automatic approval of the registration.

Note: At least one phone number is required. Up to three phone numbers may be collected if desired by contacting NCR's Digital Insight™ Solutions Software Support.



Step 4: Bill Pay Enrollment

The user may enroll in Bill Pay through combined enrollment (if offered by your financial institution) and must accept all terms and conditions.

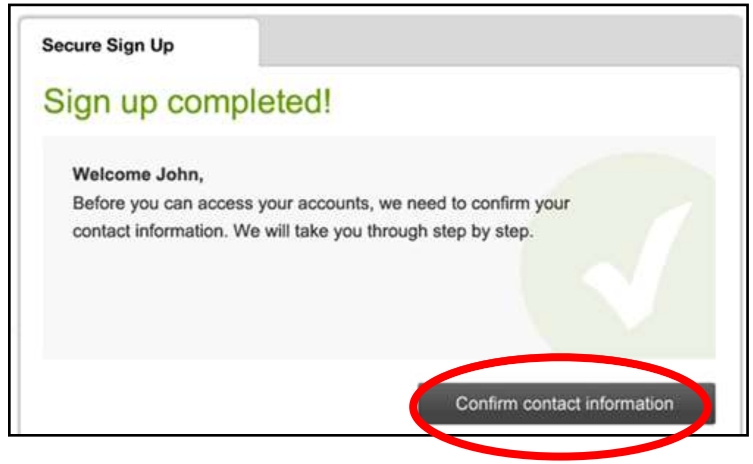


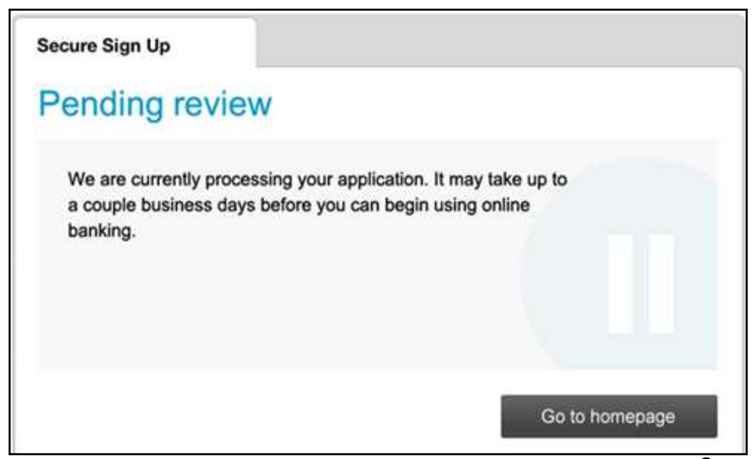
Step 5: Secure Sign Up Screens

Financial Institutions with Real-Time Interface
If the user's entries for the validation fields on the form are successfully verified against what is listed on the host, they will see the **"Sign up completed"** screen and the registration will be automatically approved. An email is not sent to the user if initial validation is successful. See Step 6 for the MFA screens that the user will see upon clicking "Confirm contact information".

Financial Institutions with Hybrid or Batch Interface
If your financial institution uses a batch connection to communicate with your host/DPV, a new user (newly opened account) would need to have his/her data included in your financial institution's batch upload before the Online Banking application can be validated. If the user data is already on the core and successfully validated, the user will see the **"Sign up completed"** screen at the time of registration.

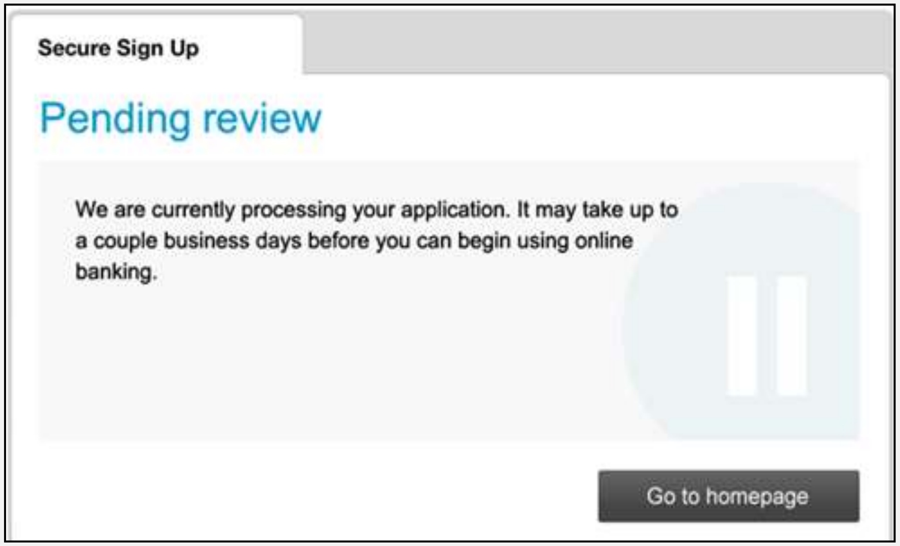
Otherwise, the user will need to wait up to one full day (depending on the timing of the batch run(s) for your financial institution) before logging in to complete MFA setup as outlined in Step 6. During this time, the **"Pending review"** screen is displayed. The text on this screen may be customized to display timing that applies to your financial institution.





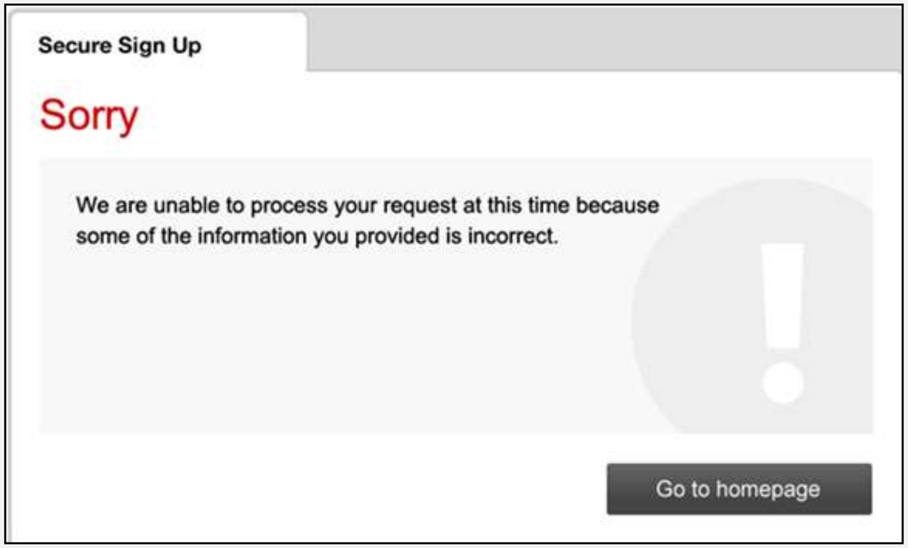
Validation Soft Fail

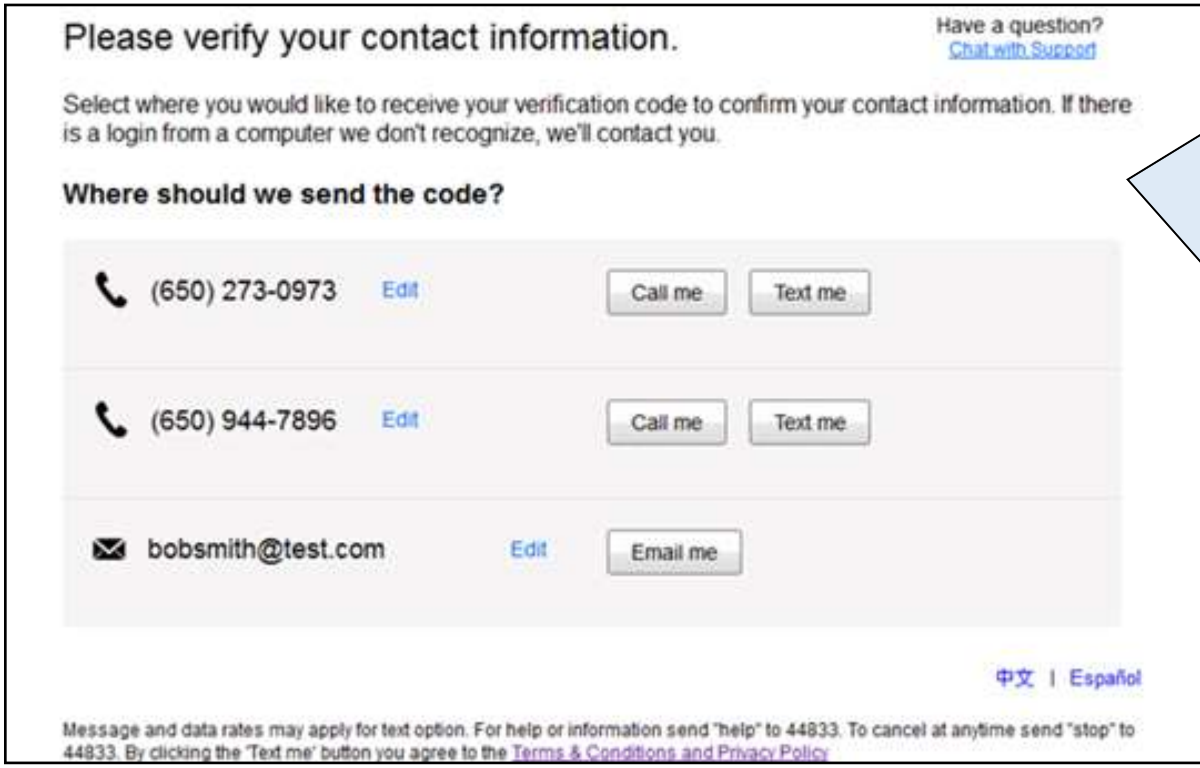
- If any of the validation fields that the user enters are different than what is listed on the host, the user's Online Banking registration will be placed in the "Pending" queue in the Registration Approval tool in Admin Platform.
- The financial institution will then have to review the user's entry against the host to approve or decline the user (covered in the Registration Processing course).
- Once the user has been approved by the financial institution, they will receive an approval email (not customizable). The user will login and be prompted with the MFA process (see Step 6).



Validation Hard Fail

- If the social security number or member number that the user enters is not found on the host, the user's registration is declined.
- No further action is necessary from the user or the financial institution. For the user to register again, verify that the data on the host is correct.
- Failed registrations are captured in the Activity Report (event type = registration), but are not located in the Registration > Queue tool for Online Banking.



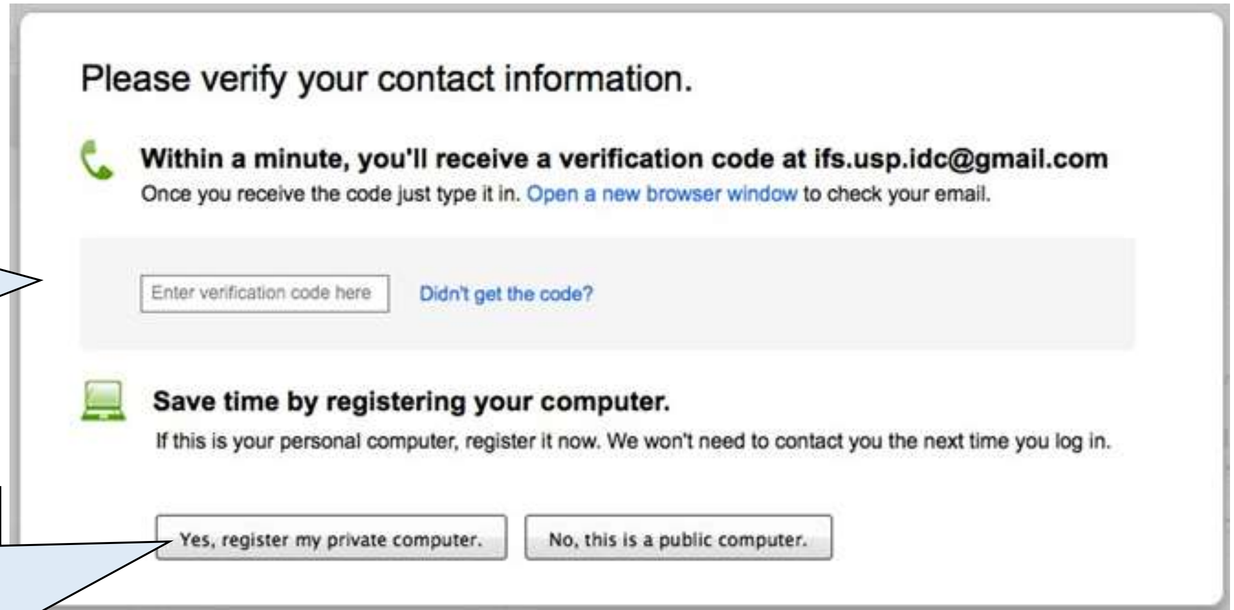


Step 6: Verify MFA Details

- Upon a successful registration, up to two phone numbers will be retrieved from the host and will be listed as the user's MFA numbers.
- These numbers will then be used for authenticating any future unrecognized devices.
- The email address that the consumer entered on the registration form will also be available as an MFA option if the FI has configured email as an MFA option.
- During subsequent logins, the user will be unable to edit their contact info on this screen.
- Forgotten password can only be retrieved via phone (not email), so it is important to confirm that the phone number(s) used are correct.
- If the user doesn't see an option for email, your financial institution might have chosen to disable the use of email for this user (via AP > Home > Support Dashboard) or chose to disable the email option either altogether for all users.

Step 7: Enter Verification Code

Codes expire after 10 minutes and consist of 6 random digits.



Step 8: Register the Computer

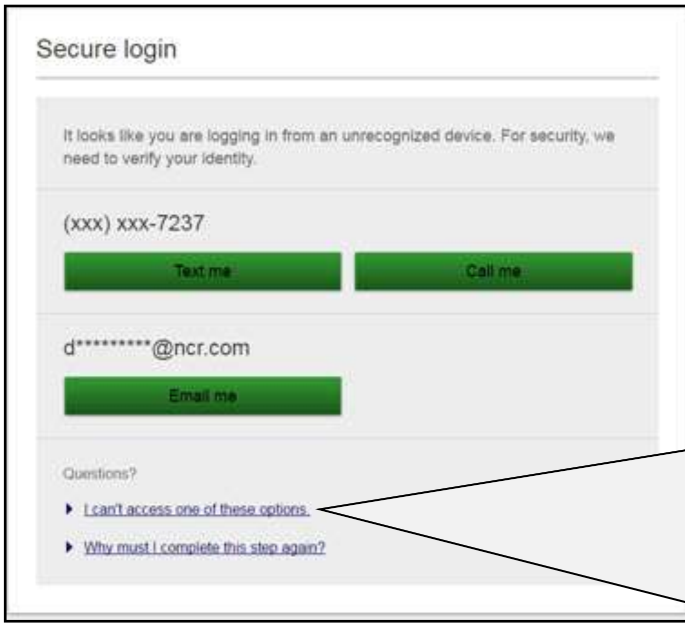
If the user is on their personal computer, they should register it (by clicking "**Yes, this is a private computer**") so that they don't get the MFA challenge screen upon next login. If they are on a public computer, they should choose "**No, this is a public computer**". Either button takes them in to Online Banking.

Device Identifier

When selecting '**yes**', a device identifier is left in several places within the user's browser. If cookies are deleted, for example, the presence of the identifiers in other places could still allow the computer to be identified.

Upon subsequent logins, the user may get prompted to verify their identity.
Why? Because there was no device identifier found on the device (cell phone, tablet, computer). This can be due to:

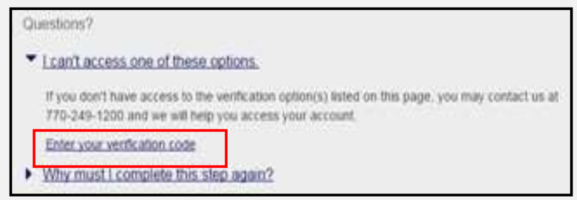
- the user deleting their cache/cookies
- anti-virus software and/or the browser is set to automatically delete cache/cookies
- the identifier was corrupt (clearing cache/cookies will remove the corrupted identifier)



User Can't Access Any Option?

If the user does not have access to either of their phones or their email, the financial institution can generate a code on behalf of the user (via Admin Platform > Home > Support Dashboard).

The user should click on the first link under "**Questions?**". Then click the **"I can't access one of these options"** link to get to the screen where they can enter the code generated by the financial institution.



IMPORTANT: If the user is already at the verification screen (because they choose a delivery method), the financial institution generated code can be entered there and is considered valid. However, if the user attempts to enter a code that they generated, it will not be accepted on the screen that is designed for the financial institution provided code.