



# Mobile Banking Product Guide for Financial Institutions

*March 2016 (Mobile Banking Apps 5.1.0, Mobile Web Banking 2.7.5, Text Message Banking 3.2)*

---

# Mobile Banking Product Guide

---

## Table of Contents

<b>How to Use This Guide</b> .....	<b>3</b>
<b>Introduction to Mobile Banking</b> .....	<b>4</b>
<b>Mobile Banking Apps</b> .....	<b>5</b>
Log in.....	6
Core Features.....	15
Additional Features.....	36
<b>SmartWatch App</b> .....	<b>39</b>
<b>Mobile Web Banking</b> .....	<b>46</b>
Login.....	47
Core Features.....	52
Additional Features.....	58
<b>Text Message Banking</b> .....	<b>60</b>
Enrollment and Management.....	61
Setting Up and Receiving Alerts.....	66

# How to Use This Guide

## Overview

This comprehensive reference guide will help you learn about Mobile Banking and how to configure and enrich the experience for your users. You'll find:

- Instructions for using core features.
- Configuration options to tailor Mobile Banking.
- Tips to help support users.
- Additional solutions to provide greater functionality.

*Learn about product features, discover ways to customize Mobile Banking, and get quick tips to support your users.*

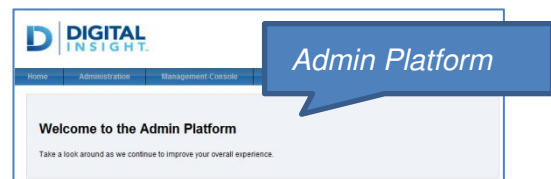
## Support Notes

Admin Platform provides a set of administrative tools, reports, and resources to help you support your Mobile Banking users. You will find references to the Admin Platform throughout this guide in the “Support Notes” sections.

Your financial institution's unique URL for Admin Platform is:

**<https://www.mydomain.com/connect>**

NOTE: The portion of the URL “[www.mydomain.com](https://www.mydomain.com)” is your Online Banking domain hosted by Digital Insight.



Key resources within Admin Platform to help you support Mobile Banking include:

- **New Support Dashboard** – Access user information and support tools.
- **Reports** – Access reports to track, troubleshoot and audit Mobile Banking activities.
- **KnowledgeBase** – Search this repository for answers to frequently asked questions.
- **Training** – Get on-demand tutorials and quick help guides, or register for virtual classes.
- **Marketing** – Utilize no-cost marketing resources to drive engagement and profitability.
- **Demos** – Tour Mobile Banking and see what's ahead on the Strategic Roadmap.
- **Communications Dashboard** – View product communications and materials, see a calendar of upcoming activities, and set your ongoing communication preferences.

For training on how to use the administrative tools referenced throughout this guide, review the in-depth training materials available within Admin Platform.

## Configuration Options

Each topic described in this document includes a summary of “Configuration Options” at the end of that section. Read the descriptions to learn about each feature then reference the “Configuration Options” list for more guidance on how to make changes to the Mobile Banking offering.

# Introduction to Mobile Banking

## Overview

The Digital Insight Mobile Banking Suite consists of Mobile Banking Apps, Mobile Web Banking and Text Message Banking. Our integrated Online and Mobile Banking solutions give you a competitive edge by delivering a consistent, connected experience across multiple channels.

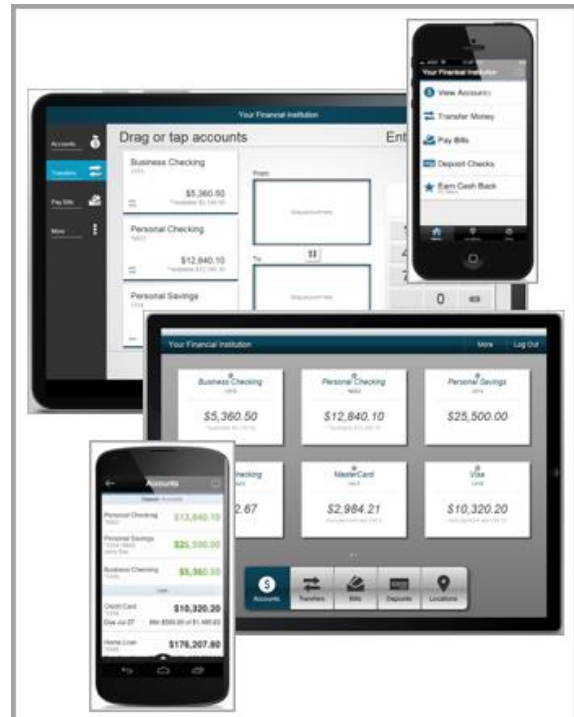
The Mobile Banking Suite supports multiple user interfaces that are optimized for a wide range of devices.

*For those Digital Insight consumers actively using digital banking to access their financial institution, 22.4 percent use only their mobile device to access their account information.<sup>1</sup>*

## Key Features

The features of Mobile Banking include:

- *Hosted by Digital Insight:* High availability, fast response time and network security are assured as Mobile Banking is hosted from the same SAS-70 certified data center that operates our Online Banking service.
- *Ease of use:* Make it easy for your users to perform key tasks in just a few clicks with our simple, intuitive user interface.
- *Complete security:* Mobile Banking is fully secure using industry-standard technologies and security certificates, with 128-bit encrypted communication. No personal or confidential information is stored on the device.
- *Ease of administration:* Provide enhanced service with support tools and reports in Admin Platform.
- *Adoption and engagement:* Drive adoption and increase active use with proven marketing campaigns launched on your behalf and self-serve marketing tools, including Mobile Banking demos.
- *Additional solutions:* Enrich the Online Banking experience with optional features like money management, cross-sell, money movement, and enhanced user support tools.



<sup>1</sup>Internal study of 7 Digital Insight financial institution users, August 2014.

# Mobile Banking Apps

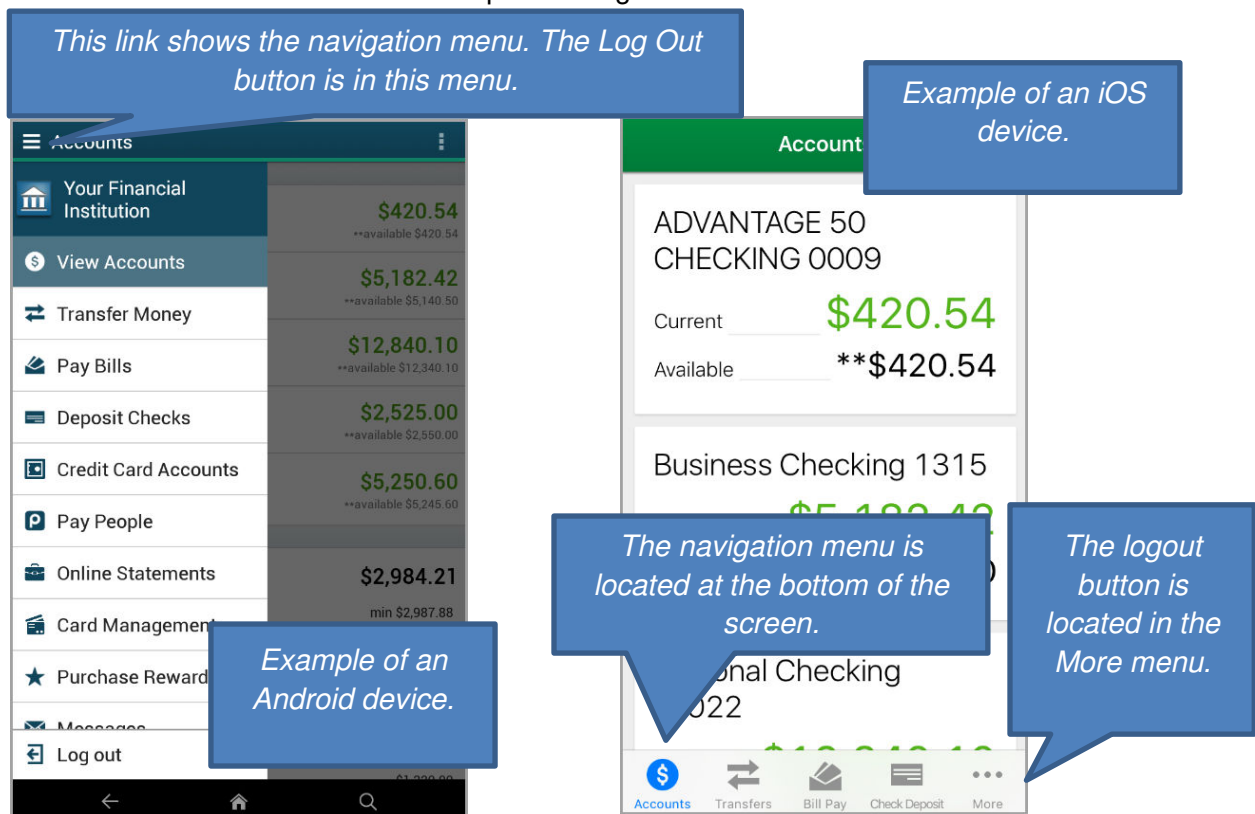
## Overview

Give your users ultimate freedom with access to account balances, transfers, payments and more through Mobile Banking Apps for iOS, Android devices. Users download your financial institution's specific free app via the iTunes App Store (iOS), Google Play Store (Android) or the Amazon Appstore (KindleFire).

Mobile Banking Apps contain the same functionality for all devices, except where specifically noted. There are features that look slightly different depending on the device and the user interface.

For example, Android and iOS devices are set up differently as shown below. The iOS menu appears at the bottom of the screen and the Android menu is accessed by tapping in the upper left corner. All devices are used as examples throughout this module.

*The Mobile Banking App has an average 4.6 star rating through Apple iTunes Store and Google Play.<sup>1</sup>*



The Mobile Branding Tool and the Admin Platform allows financial institutions to customize items within the Mobile Banking Apps. This feature offers the ability to set desired color/design palette for text, theme, button/icon, sub-headers and menu items within the App.

<sup>1</sup> Based on an April 2014 Digital Insight study of mobile banking providers with 235 or more reviews. Blended average of 4.6 stars from Digital Insight financial institution apps in both the Apple App Store and Google Play.

# Mobile Banking Apps: Log in

## Overview

The Mobile Banking App leverages a user's existing Online Banking credentials. No additional enrollment for Mobile Banking Apps is required.

### In this section:

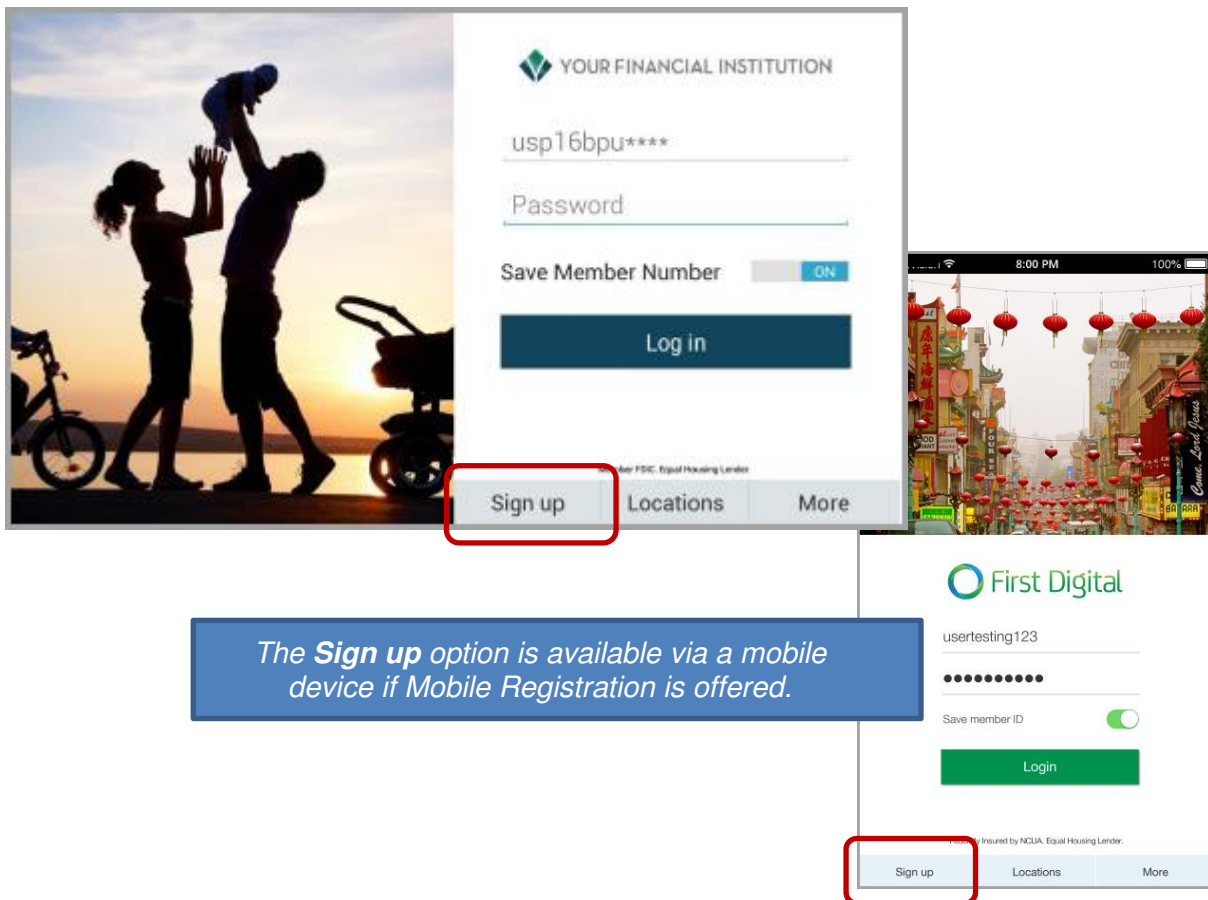
- Logging In
- Mobile Registration
- Multifactor Authentication

## Description

### Logging In: Existing Online Banking User

To access the Mobile Banking App the user simply enters their Online Banking username and password and clicks **Log in**. By swiping the **Save my User ID** or **Save Member Number** to the **ON** position, the user's username is saved and appears when the login screen is accessed.

Your financial institution has the option to place an image on the login page of the Mobile App and to update the image at any time. This can be done by using the Login Image Portlet in the Admin Platform.



*The **Sign up** option is available via a mobile device if Mobile Registration is offered.*

**Locations:** The user has access to view your financial institution’s ATM and branch locations, phone numbers and get directions. This feature is available before and after login. See page 35 for details.

**More:** The financial institution can customize this screen to contain contact information for the financial institution, as well as links to third-party vendors. This feature is available before and after login, however, additional links are available after logging in. See page 36 for details.

*\*Note: Users are locked out after five failed login attempts. This count is cumulative regardless of the device being used. Failed login attempts on the Mobile Banking App will also lock a user out of Online Banking on a PC.*

*\*\*Note: Your financial institution is able to generate one- time passwords via the Admin Platform for a user that is locked out. Once the user logs in they are required to create a new password.*

*\*\*Roadmap Preview: The Username Recovery and Password Reset feature guides users through a self-serve username recovery or password reset process when they have forgotten their login credentials. This feature will be available from the login screen. This feature is currently on the Roadmap.*

## Logging In: New Online Banking User

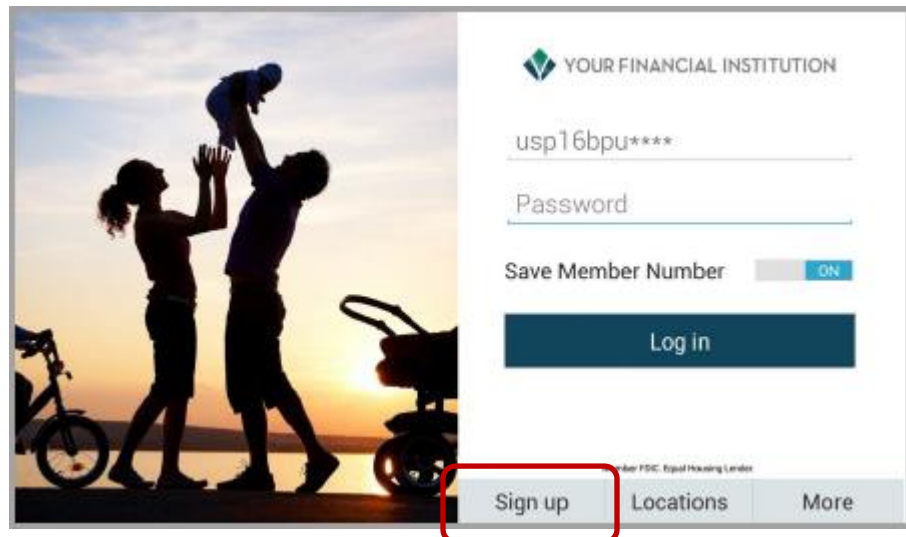
*\*\*Roadmap Preview: The following provides a preview of the new mobile registration experience that is currently on our Roadmap. Contact your relationship manager for more information.*

Engage the growing mobile-only user base by enabling your users to register for Online Banking from their mobile phone. Mobile Registration is a streamlined, easy-to-use registration experience.

In order to utilize the registration process via a mobile device, the user must have at least one account with your financial institution. If the user already has credentials for Online Banking, there is no need to go through this registration process. Users are able to access Mobile Banking using their existing credentials.

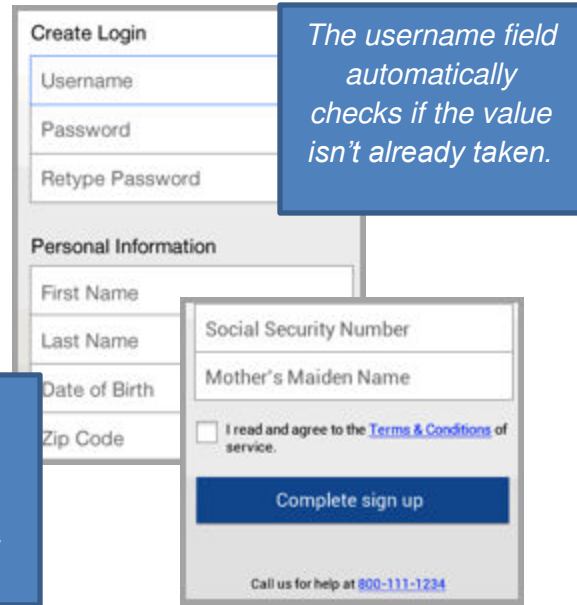
The specific registration process may differ what is represented below as many aspects depend on the registration type. The following is a high-level overview.

1. The user clicks the **Sign Up** link directly on the log in page.



2. The user is presented with the registration form. Depending on the device being used, they may need to scroll to see the entire registration form.

The user creates a username and password and then enters their validation information. The user will not be able to progress through the registration process until they agree to the Terms and Conditions.



The screenshot shows a registration form with the following sections:

- Create Login:** Username, Password, Retype Password.
- Personal Information:** First Name, Last Name, Date of Birth, Zip Code.
- Validation:** Social Security Number, Mother's Maiden Name.
- Agreement:** A checkbox for "I read and agree to the Terms & Conditions of service."
- Buttons:** "Complete sign up" and "Call us for help at 800-111-1234".

Two blue callout boxes provide additional information:

- One pointing to the Username field: *The username field automatically checks if the value isn't already taken.*
- One pointing to the Password field: *The password field automatically reveals two criteria the user has to fulfill with their password creation.*

If your financial institution has Auto-Approve for registration:

- The value entered for Social Security Number or Member Number is used for validation with what exists on the host processor. The result of this validation determines the outcome of the registration attempt.
- The only fields that appear are the validation fields. This is different than Online Banking where all fields are displayed.
- Specific fields for validation vary from institution to institution.

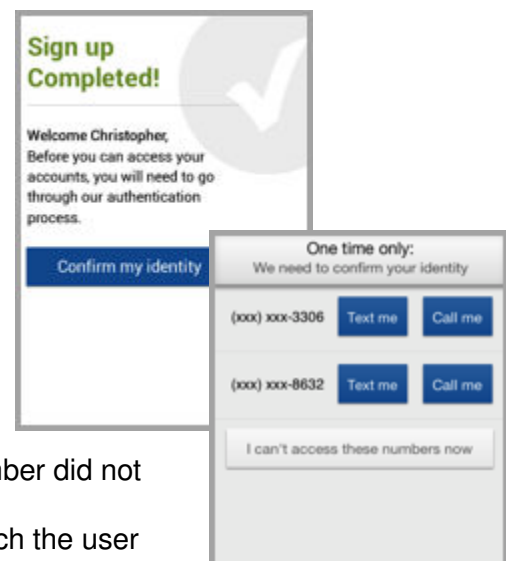
If your financial institution has Manual Approve for registration:

- All fields displayed on the Online Banking registration form is displayed on the mobile device, including optional sections such as Secondary Account Holder.
- Specific fields for validation vary from institution to institution.

3. The next steps depends on if your financial institution supports Auto-Approve or Manual Approve.

If your financial institution has Auto-Approve for registration:

- If the user's entries are successfully verified they will see a registration successful screen.
- By clicking **Confirm my identity**, the user is directed into the multifactor authentication workflow. Up to two numbers found for the user on the host are retrieved and listed as multifactor authentication numbers.
- After successfully completing the multifactor authentication workflow, the user is instantly logged into their Home Page.
- If the Social Security Number or Member Number did not match, the user is declined.
- If any of the other validation fields did not match the user registration is sent to the Admin Platform for manual review.



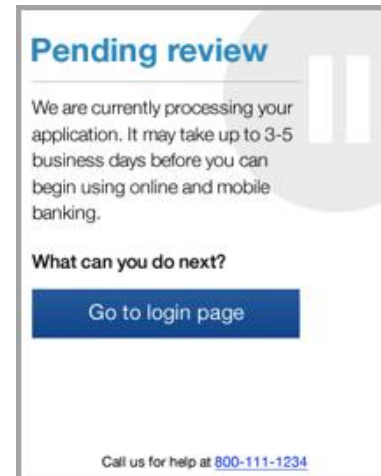
The screenshot shows a two-part interface:

- Top Section (Registration Completed):** A green checkmark icon, the text "Sign up Completed!", and a welcome message: "Welcome Christopher, Before you can access your accounts, you will need to go through our authentication process." Below this is a blue button labeled "Confirm my identity".
- Bottom Section (One time only):** A grey box titled "One time only: We need to confirm your identity". It lists two phone numbers: "(xxx) xxx-3306" and "(xxx) xxx-8632". Each number has "Text me" and "Call me" buttons next to it. At the bottom of this section is a link: "I can't access these numbers now".



If your financial institution has Manual Approve for registration:

- All registration attempts are sent to the approval tool in the Admin Platform for financial institution review.
- The user is given access to Online Banking once an administrator approves the registration.



## Logging In: Touch ID & Eyeprint ID

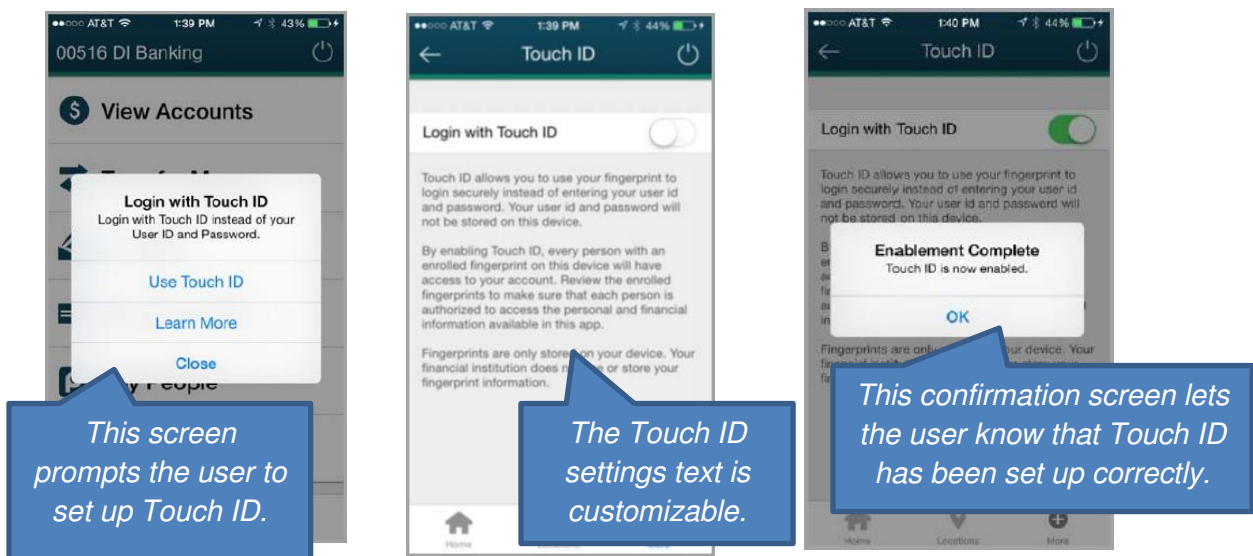
### Touch ID

iOS users are able to login to the Mobile App using the Touch ID function that exists on their device.

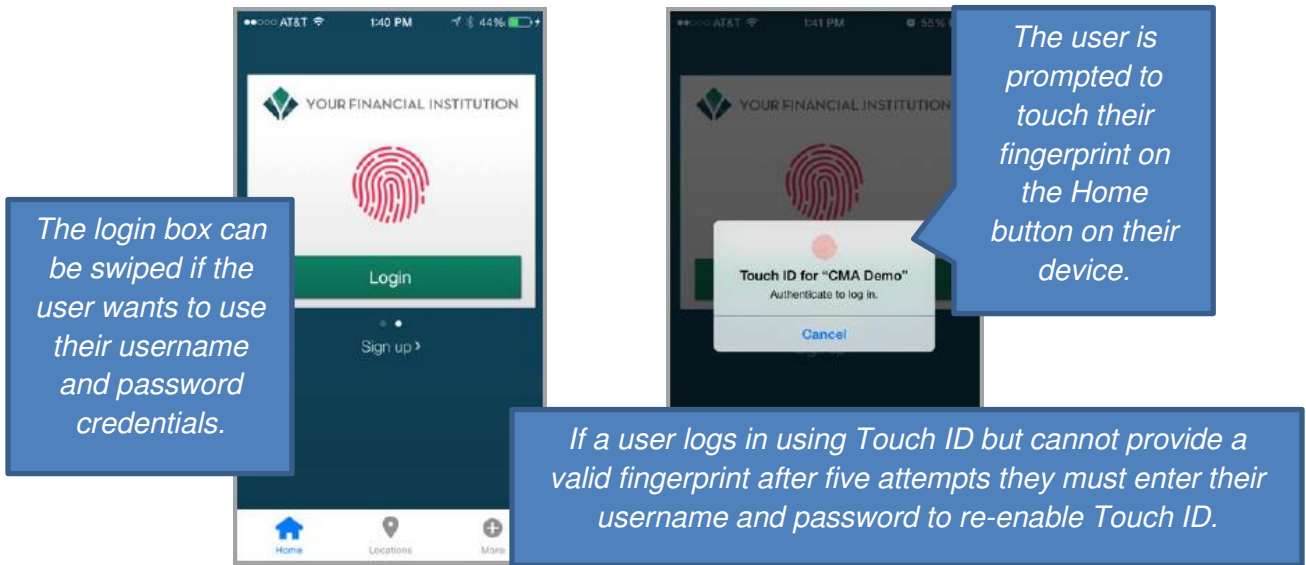
If the user has enabled Touch ID on their device, that feature can be used as an alternative login credential and to authenticate into the Mobile App. The user can turn this feature on or off at any time and can un-enroll fingerprints from with Settings menu of the Mobile App.

Once the user upgrades to a Mobile App version with the Touch ID feature on a Touch ID-enabled device, the user is prompted to set up this feature. On the prompt, if the user clicks:

- **Use Touch ID:** The user is prompted to place their Touch ID fingerprint on the device's home button. The user will see the settings page and Touch ID will automatically be enabled.
- **Learn More:** The user is presented with the Touch ID settings page and is able to turn the feature on from that screen.
- **Close:** The user is returned to the main menu of the Mobile App. After 30 days, the user is prompted one more time to take advantage of this feature.



Once Touch ID has been enabled, the user will see a Mobile App login page that shows a Touch ID theme. The user can click anywhere in the box to enable the Touch ID login prompt.

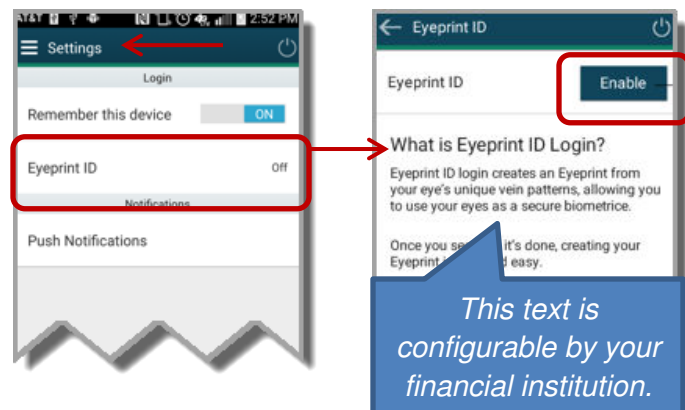


**\*\*Roadmap Preview: Android Fingerprint brings the Touch ID feature to relevant Android smart devices. Users are able to log into the Mobile App with just their fingerprint. This feature is currently on our Roadmap.**

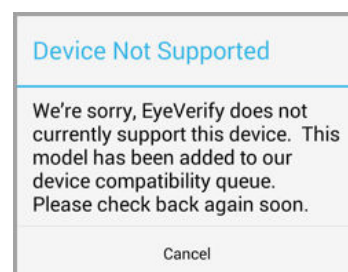
### *Eyeprint ID*

With Eyeprint ID™ from EyeVerify your users can log in to your Mobile Banking App by simply looking into the camera on their mobile device. By mapping the unique vein formation in the whites of the user’s eyes, this solution creates an authentication equivalent to a 50-character, complex password. This feature is available for Mobile and Tablet Banking Apps for iOS and Android. Eyeprint ID works on most devices that have a front-facing camera with a resolution of at least one megapixel.

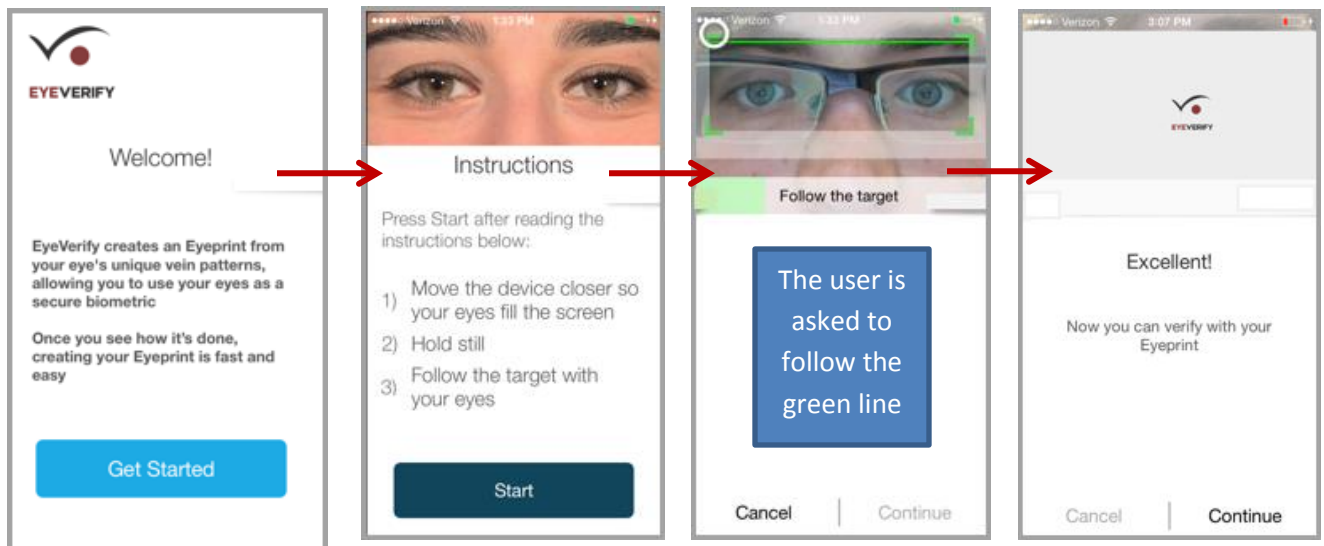
Eyeprint ID is enabled/disabled from the Mobile App’s Setting page. On the Eyeprint ID screen, the user taps **Enable** to turn this feature on.



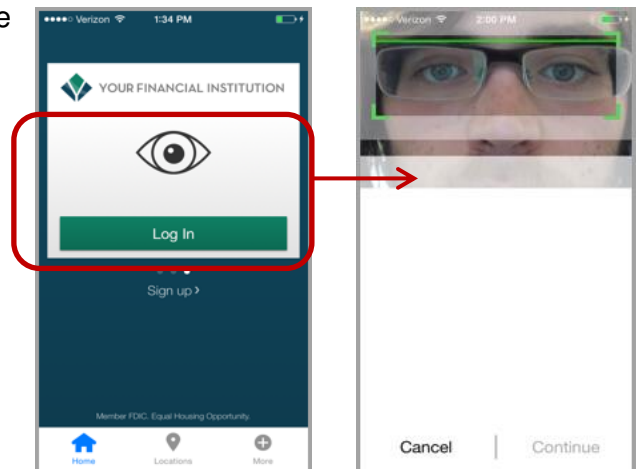
If the device does not support this feature then the user receives a **Device Not Supported** message.



Once this feature is enabled within the Mobile App the user is prompted to register for Eyeprint ID. The user follows the directions on the screens.



Once this feature has been enabled and set up, the user will see this feature on the login screen. The user taps **Log In** or the eye logo to start the login process. Swiping to the right on the login page allows the user to switch among the other login methods: Touch ID and Username and Password.



The user can disable this feature either before login or after login. Go to: **More > Settings > Eyeprint ID** and toggles the feature off. The user will see a confirmation message and taps **Disable**.



## Multifactor Authentication

Digital Insight's Mobile Banking Apps support the same type of multi-factor authentication, out-of-band authentication and device recognition, used with Online Banking. The Mobile Banking App automatically imports the registered phone number(s) the user uses for Online Banking authentication. For new mobile-only users the phone number(s) is pulled directly from the core processor.

If the user uses an unidentified device to access Online Banking via the Mobile Banking App they must go through a process to verify their identity. The user will only have to complete this process once per device. Users are able to have up to two devices authenticated to receive a text or phone call.

The following steps explain this process:

1. After successfully using their username and password to login, if a mobile device is unrecognized the user is presented with the options for receiving a code via text or phone call. The delivery options shown on screen are the phone numbers previously entered in Online Banking.

If the user selects **Call me** they will receive a phone call to confirm their identity via voice prompts.

If the user selects **Text me** they will receive a code via text to confirm their identity.

The first time a particular mobile device is used to access multifactor authentication, the user is able to enter a new phone number in order to complete process. This is done by tapping **I can't access these numbers now**. This gives them the opportunity to enter an additional phone number in order to receive a phone call. If a user has used this mobile device before and **I can't access these numbers now** is tapped, they are directed to update their phone numbers via Online Banking.



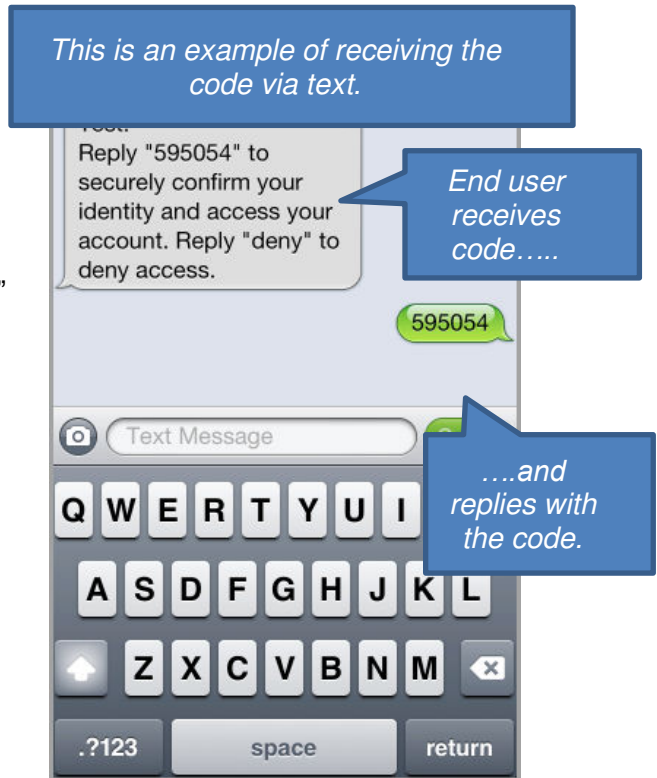
2. If receiving the code via text, the text is delivered within seconds. The user simply replies with the same code as instructed by the text.

If receiving the code via a phone call the user follows the prompts and presses “1” to confirm the login while on the phone.

Once the user’s identity has been confirmed they will receive the following message and are instructed to return to the App

Identity confirmed. Please go back to your app. Thank you!

*The user receives this message as a text.*



3. The user receives a success screen once they navigate back to the App. This gives the user confidence and assurance that their session and account is successfully authenticated.

Once the user taps **Go to my accounts** on the Multi-factor Authentication success screen, they are taken to the Home page of the Mobile Banking App. When using this same device, this is the screen that they will see upon login in the future.



## Support Notes

### What happens if a user tries to access the Mobile Banking App from a third unauthenticated device?

Users are able to have up to two devices authenticated in order to receive a text or phone call. If a new device is being used to access the Mobile Banking App, the user is challenged by the Multi-factor Authentication process, and will need to use one of the two devices already authenticated. The user will need to reply to the text message or receive a phone call from one of the two authenticated devices that are available to choose from. Once authenticated the user can return to using the third device to login to the app.

### Can the user choose to be challenged by Multifactor Authentication at every log in?

Yes. The user has the option to access the **More** section of the App and turn the **Remember Device** toggle **OFF**. This will challenge the user during every login of the App.

### Can my user change or update their username or password on their mobile device?

No. The end user's username and password is managed from within the full Online Banking site.

## Configuration Options: Mobile App Login

**Support for Languages:** Mobile Banking Apps support the Chinese and Spanish languages. Support includes all core screens (e.g. login page, Multi-factor Authentication page, accounts, transactions, transfers and Bill Pay). Static content is translated and information from the core processor remains in English.

The user sets this feature on their device by going to:

- Android: Settings>Language & keyboard>System language>select traditional Chinese/Spanish.
- iOS: Settings>General>International>Language> select traditional Chinese/Spanish.
- KindleFire: Settings>Language & Keyboard> Language>select traditional Chinese/Spanish.

**Reduce the number of failed login attempts:** Financial institutions can reduce the amount of times a user has to incorrectly login before becoming locked out. The default number is five. The financial institution needs to contact Customer Care at 877-462-3446 or go to **Admin Platform>MySupport** to submit a ticket.

**Mobile Banking App Customizations:** Financial institutions can update certain items within the Mobile Banking App by using the Mobile Branding Tool. A link to this resource is available in the within MySupport>Forms. Contact Customer Care at 877-462-3446 or go to **Admin Platform>MySupport** for additional information.

**Alternative Login Credentials in Admin Platform:** Your financial institution administrators can disable alternative login methods (Touch ID or Eyeprint ID) via the Support Dashboard in the Admin Platform. If a user's alternative login credentials are disabled then the user will no longer be able to use this method of login until registering again. The user is able to use the traditional username and password to login.

# Mobile Banking Apps: Core Features

## Overview

The Mobile Banking App allows your users to accomplish their most important banking tasks in just a couple clicks. They are able access the following areas (dependent on what your financial institution offers):

- View Accounts
- Transfer Money
- Pay Bills
- Deposit Checks
- Pay Other People
- Earn Cash Back

### In this section:

- View Accounts
- Transfer Money
- Pay Bills
- Deposit Checks
- Pay Other People
- Earn Cash Back

## Description

### View Accounts

Users are able to access the same accounts (deposit, loans and investment) that are available in Online Banking. Users can access their accounts within the App and also via the Quick Balance feature.

#### Account Information within the App

1. Deposit Accounts, Loan Accounts and Investment Accounts are available for viewing. Depending on the type of device being used, your users may have to scroll to view the entire list of accounts.

The account numbers are masked to only show the last 4 digits.

If an account is a joint account the account owner's name displays.

Deposit	
ADVANTAGE 50 CHECKING 0009	<b>\$420,541,871.87</b> <small>**available \$420,541,871.87</small>
Business Checking 1315	<b>\$5,182.42</b> <small>**available \$5,140.50</small>
Personal Checking +9022	<b>\$12,840.10</b> <small>**available \$12,340.10</small>
Personal Savings 1314	<b>\$25,525.00</b> <small>**available \$25,500.00</small>
Business Savings 23	<b>\$52,506.00</b> <small>**available \$52,456.00</small>
Loan	
MasterCard	<b>\$3,334.21</b> <small>min \$3,007.88 of \$250.00</small>

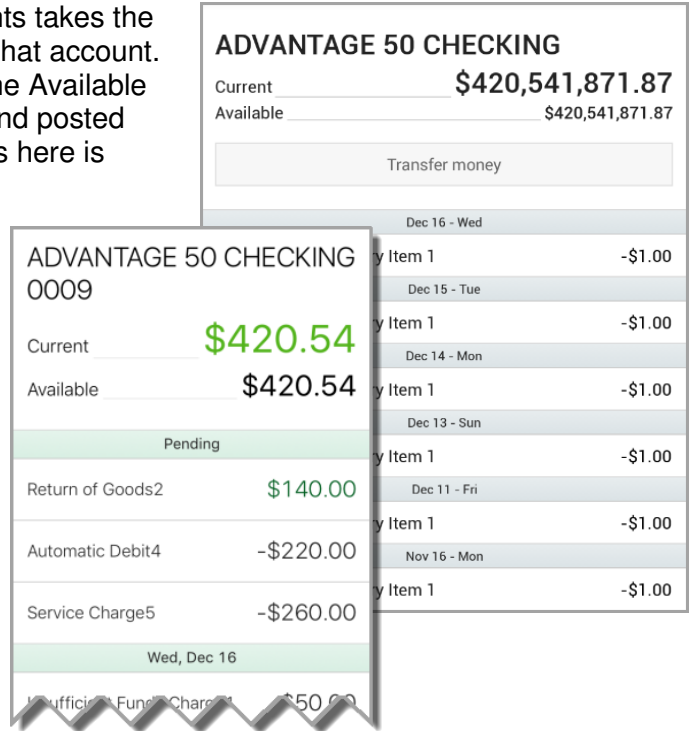
ADVANTAGE 50 CHECKING 0009	
Current	<b>\$420.54</b>
Available	<b>**\$420.54</b>
Business Checking 1315	<b>\$5,182.42</b>
	<small>140.50</small>

*If available, loan and credit card accounts show loan balances and next payment due dates. The user will may have to scroll to access all accounts.*

*The current balance is prominently displayed. Available balance is the secondary balance displayed, if available.*

- Tapping directly on any of the accounts takes the user to the Account History page for that account. From this screen the user can view the Available Balance, Current Balance, pending and posted transactions (information that appears here is dependent on the core processor).

The Account History screen automatically loads history as the user scrolls. The amount of history provided is dependent on how much history your financial institution provides.



- Users can view check images by clicking on the check icon next to a check transaction.

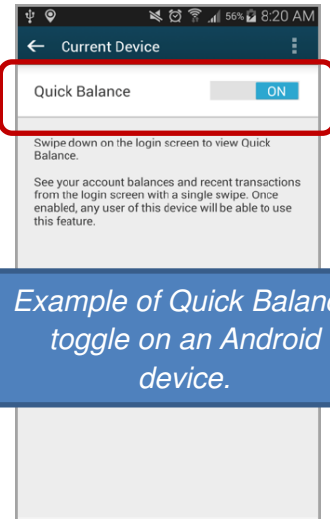




### Quick Balance

Quick Balance allows users to quickly access their financial information without the hassle of logging into the Mobile App. Once the feature is enabled in the App, the user's account balances and recent transactions are displayed on the Quick Balance page which can be revealed by swiping down on the App's login screen.

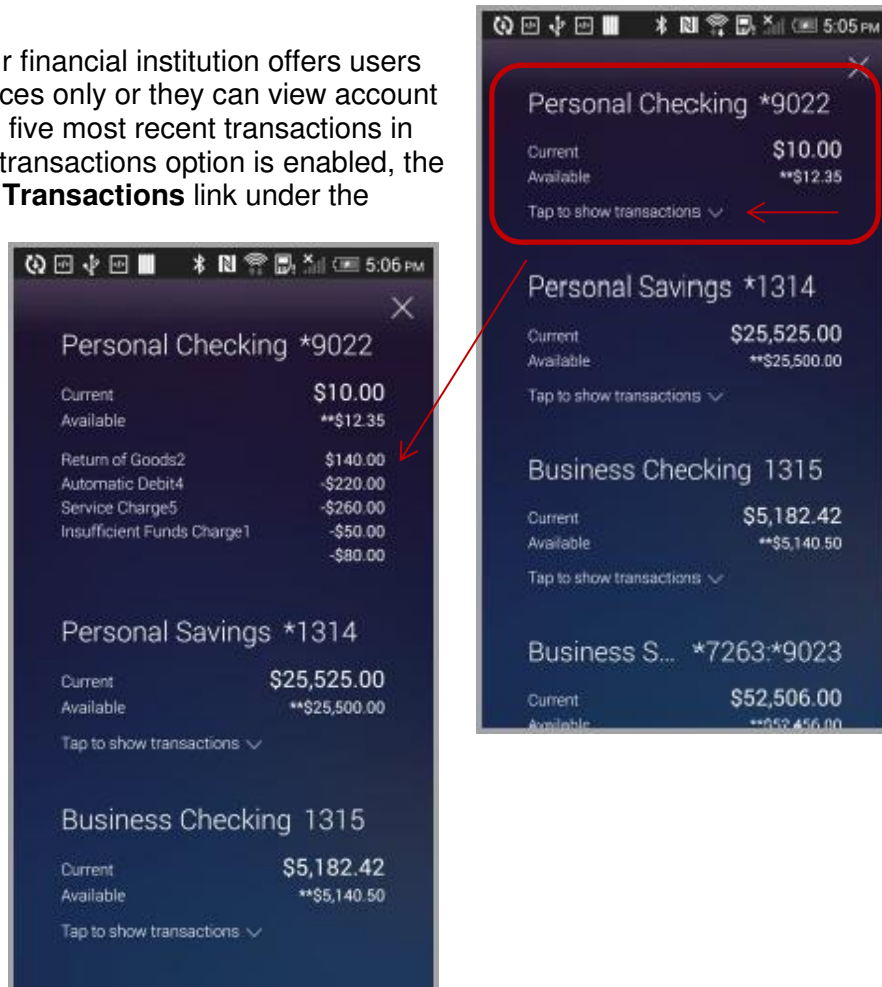
To enable Quick Balance the user must log into the app and go to Settings>Quick Balance>Current Device. On this screen, the user toggles Quick Balance to **ON**.



*Example of Quick Balance toggle on an Android device.*

The Quick Balance page displays the current and available balances for checking and savings accounts. For loan accounts and credit cards, the due date and minimum amount due is displayed.

Depending on what your financial institution offers users can view account balances only or they can view account balances along with the five most recent transactions in the past 30 days. If the transactions option is enabled, the user taps **Tap to show Transactions** link under the account.



**\*\*Note:** Quick Balance must be enabled on each device individually. If a user has both a phone and tablet, enabling Quick Balance on their phone will not enable the feature on their tablet. For users sharing a device, if the first user enables Quick Balance on the device, the second user will see the first user’s account balances. If the second user disables Quick Balance from the app, the first user will no longer see their Quick Balances.

## Configuration Options: View Account

**Quick Balance:** Your financial institution has the choice to offer users a view of only account balances, or account balances with the five most recent transactions in the past 30 days. This configuration request can be made at any time by contacting Customer Care at 877-462-3446 or go to **Admin Platform>MySupport** to submit a ticket.

### Transfers

Users are able perform a one-time, immediate transfer between accounts held at your financial institution.

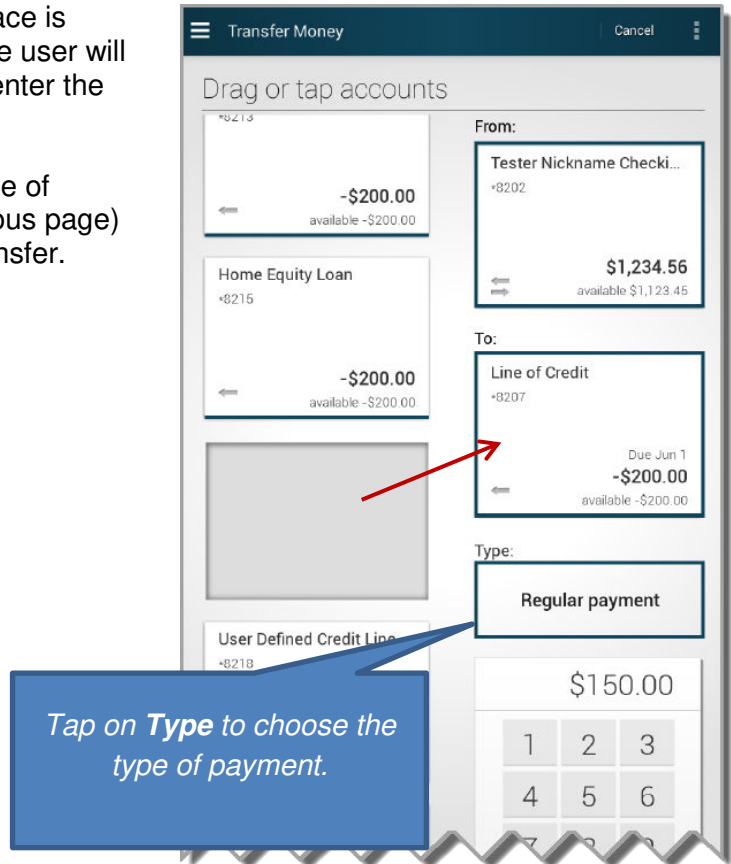
1. The user chooses the **From** and **To** accounts by tapping on that area. The accounts available for this type of transaction are dependent on the core processor. The available accounts reflect the same accounts the user is able to transfer to/from in Online Banking.
2. Enter the amount of the transfer.
3. If supported by the core processor and enabled by the financial institution, the user is able to choose the **Type** of transfer.(this is not shown in the screen shot) The options include the following
  - Regular payment
  - Extra to principal
  - Extra to interest
  - Pay principal only
  - Pay interest only
  - Pay escrow only
  - Pay fees

From	Personal Checking <b>\$12,340.10</b>
To	Personal Savings <b>\$2,550.00</b>
Amount	<b>\$250.00</b>
<div style="background-color: #0070C0; color: white; padding: 10px; display: inline-block; border-radius: 5px;">Transfer</div>	

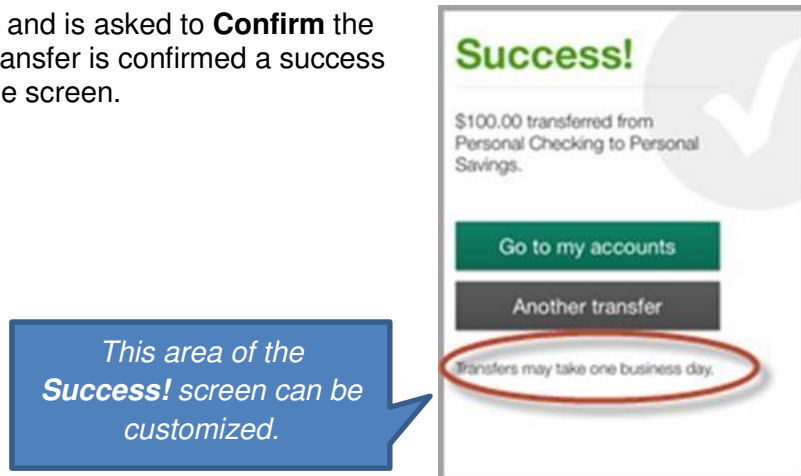
*The user clicks **Transfer** to process the transfer.*

**\*\*Note:** The Android user interface is slightly different in this area. The user will drag and drop the accounts to enter the **From** and **To** fields.

The user will then select the type of payment (as listed on the previous page) and enter the amount of the transfer.



4. The user taps **Transfer** and is asked to **Confirm** the transaction. Once the transfer is confirmed a success message appears on the screen.



**\*\*Roadmap Preview:** The ability for users to transfers funds to other users at your financial institution using the Mobile Banking App is currently on the Roadmap. The feature will be supported for the following core processors: OSI, Ultradata, Spectrum, Phoenix, Symitar and APEX.

## Configuration Options: Transfer Money

**Overpayment Options for Mobile Transfers:** Configuration for overpayments in the mobile product is separate from the Online Banking overpayment configurations. The financial institution will need to know which account types support which overpayment types by their core processor. To configure overpayment options, the financial institution needs to contact Customer Care at 877-462-3446 or go to **Admin Platform>MySupport** to submit a ticket.

**Success! screen customization:** In order to customize the last lines of the Success! screen the financial institution needs to contact Customer Care at 877-462-3446 or go to **Admin Platform>MySupport** to submit a ticket. This feature is included in the Mobile Banking Apps 4.3 release and is slated for availability beginning in December 2014.

## Pay Bills

The user is able to view and delete scheduled payments, set up new payees, as well as set up one-time payments.

*\*\*Note: If a user taps the Bill Pay button and is not a registered Bill Pay user, they are asked to submit a mobile optimized registration form. This is the same experience they would have if they accessed Bill Pay from within Online Banking on a PC.*

1. Once tapping the **Bill Pay** button, the user is presented with a list of scheduled payments.

The user can scroll to view pending and processed payments. The user able to delete payments that are still in a pending status. Processed payment cannot be cancelled.

To set up a new one-time payment, the user taps **Make a new payment** at the bottom of the screen.

*The Total on this screen gives users a quick snapshot of expected outflow of funds.*

Scheduled payments	
Processing	
Alison Test	\$1.00
Deliver by Dec 22	
American express cc	\$200.00
Deliver by Dec 23	
Sprint	\$200.00
Verizon Wireless	\$100.00
Walmart	\$25.00
<b>Total</b>	<b>\$526.00</b>
<b>Make a new payment ▶</b>	

2. To set up a payment the user taps the **Make a new payment** area. The user is presented with a list of payees that exist in **Bill Pay**.

In order to set up a payment for a payee that already exists, tap the desired payee. (Skip to step 5)

To set up a payment for a new payee the user starts to type in the name of the payee.

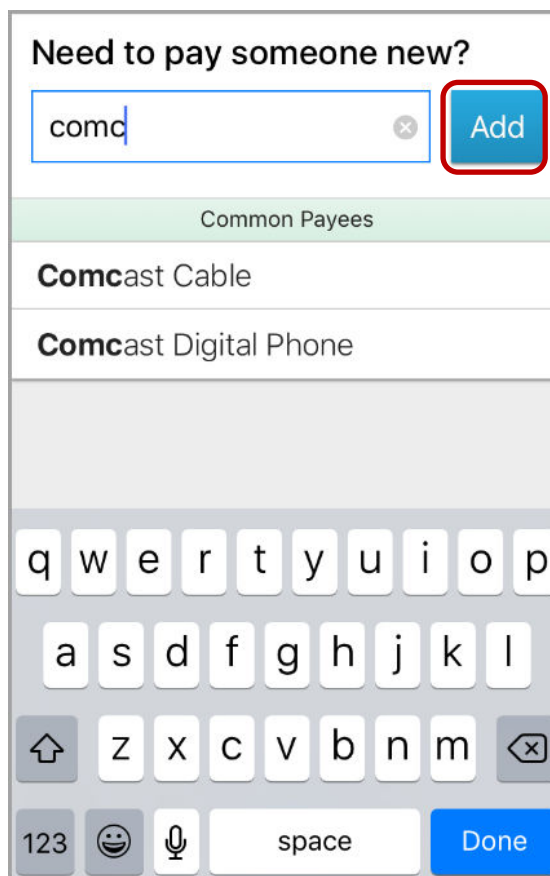
*This list of payees already exist in this user's Bill Pay module.*

**Need to pay someone new?**

Existing Payees	
<b>American express cc</b>	<b>*6780</b>
Last: \$25.00 on Nov 9	
<b>Comcast</b>	
Last: \$2.00 on Dec 9	
<b>enterprise</b>	<b>*1122</b>
Last: \$25.25 on Nov 16	
<b>GordonRogers</b>	<b>*5677</b>
No recent	

- When the user types in the name of the new payee the Bill Pay vendor database is searched and returns relevant merchants. If no matches occur, the user clicks **Add** to add the payee manually.

If a correct match is returned in the search results, the user taps that payee name.



- Depending on the payee and the information that is available in the Bill Pay database, the user may have to perform one of the following three scenarios:

Status of Payee	End User Action
1. The payee exists in the database and the address is on file.	The user enters in the Account Number, confirms the Account Number and taps <b>Add Payee</b> .
2. The payee exists in the database and there are multiple addresses for this payee.	The user is prompted to enter the ZIP code of where the payment should be sent so that correct payee address can be located. The user enters and confirms their Account Number and taps <b>Add Payee</b> . If no match is found the payee will need to be added manually.
3. The payee did not exist in the database.	The user will need to enter the payee information manually. This information includes, payee name, account number (optional), address and phone number (optional). The user then taps <b>Add Payee</b> .

Once a new payee has been added a success message will appear at the top of the Pay screen.

- On the Pay screen, verify the funding account, enter the amount of the payment and the delivery date.

If the payee has a scheduled payment amount and date then that information shows below the Payee name. If no payment is scheduled, then the last payment amount and date appears (not shown in screen shot)

Tap **Pay** to process this transaction.

<b>American express cc</b>	
🕒 Last: \$25.00 on Nov 9	
From	<b>Personal Checking</b>
Amount	<b>\$150.00</b>
Deliver by	<b>Dec 14</b>
<div style="background-color: #0099cc; color: white; padding: 10px; width: 100px; margin: 0 auto;">Pay</div>	

*The default funding account is pre-filled for the user, but can be changed.*

*The default send on or deliver date is set to the next possible date (based on payee and if available). Tap to*

- The user is presented with a **Success!** message. This message contains a confirmation number. The user has the ability to **Make another payment**, or **Cancel payment**.

✔ Success!

To ..... Kansas City Star

Amount ..... \$10.00

Send on ..... April 7

Deliver by ..... April 10

Conf # ..... X012385

**i** You can cancel until it processes.

Make another payment

Cancel payment

*This newly scheduled payment will now appear on the Scheduled Payments screen.*

*This area of the Success! screen can be customized.*

## Support Notes

### **When adding a payee my user gets a “More Information Required” message.**

This error occurs when the user enters an account number or ZIP code (scenario 1 or 2 from the chart above) and the payee is still not located in the Bill Pay database. The user must enter the payee manually.

### **When adding a payee my user gets a “Some information was missing or incorrect” message.**

This message appears when there are errors with the submitted fields. For example, if the account number was not entered twice or an address was not entered.

### **Does the user have to register for Bill Pay via Online Banking?**

Yes. Bill Pay registration via the Mobile Banking App is not yet available.

### **Can my user edit a pending payment?**

No. If a pending payment needs to be changed then the payment needs to be deleted and then set up again using the correct information.

## Configuration Options: Pay Bills

**Success! screen customization:** In order to customize the last lines of the Success! screen the financial institution needs to contact Customer Care at 877-462-3446 or go to **Admin Platform>MySupport** to submit a ticket. This feature is included in the Mobile Banking Apps 4.3 release and is slated for availability beginning in December 2014.



## Deposit Checks

The deposit check feature allows users to conveniently take a picture of a check they wish to deposit. Once captured, the check image is uploaded through the App to your financial institution.

Digital Insight offers this product from Vertifi and Ensenta. Both vendors' experience is the same from the user's point of view, which is included in this product guide.

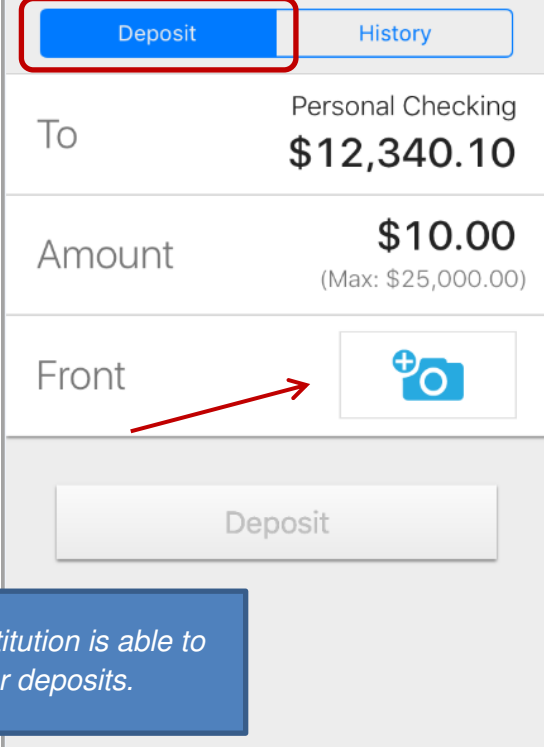
The first time a user accesses the Deposit Check feature, whether via Online Banking on a PC or via the Mobile Banking App, they are prompted to view and accept your financial institution's disclosure and agreement. Once the **Accept** button is tapped, the user will see one of the following screens:


- Deposit check screen
- Pending Approval Screen (Vertifi only)
- Denial Screen (Vertifi only)
- Unsupported Device Screen

### *Depositing a Check*

1. To deposit a check the user taps the **Deposit Check** option in the main menu.
2. On the Deposit screen, the user selects the account to deposit into and enters the amount of the check.

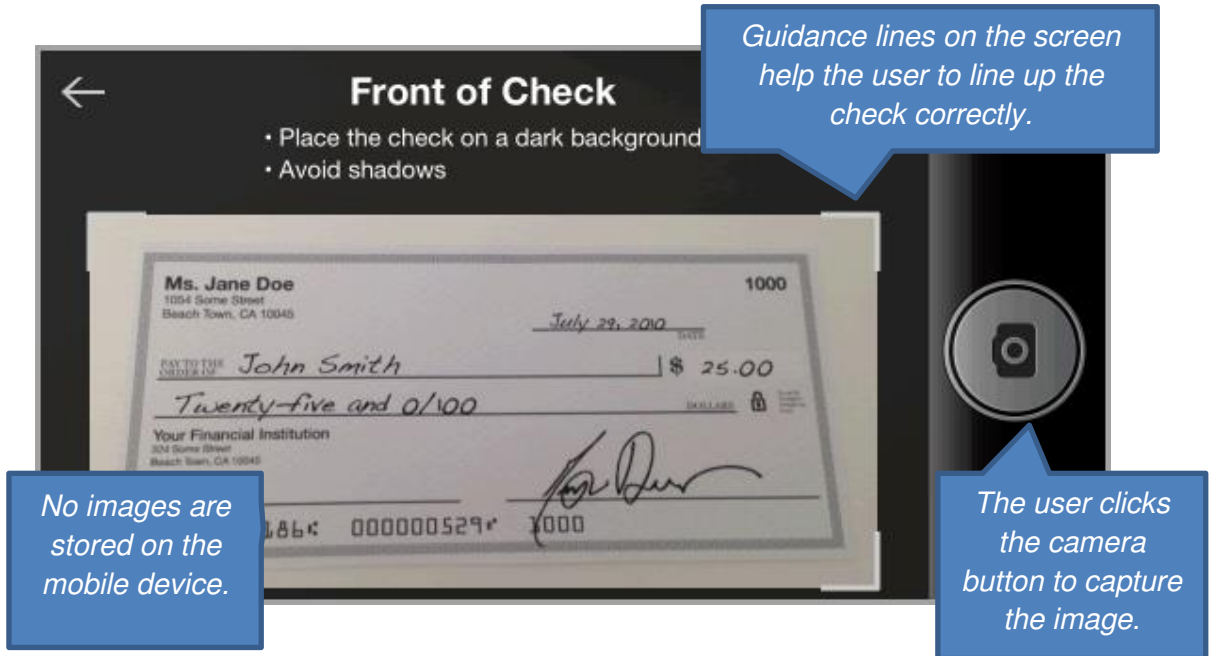
After the amount of the deposit is entered, the camera button appears.



<b>Deposit</b> History	
To	Personal Checking <b>\$12,340.10</b>
Amount	<b>\$10.00</b> (Max: \$25,000.00)
Front	
Deposit	

*The financial institution is able to set limits for deposits.*

- To take a picture of the front of the check, the user clicks the camera button. The camera on the mobile device is then opened. The user clicks the camera button or the screen on the device to capture that image.

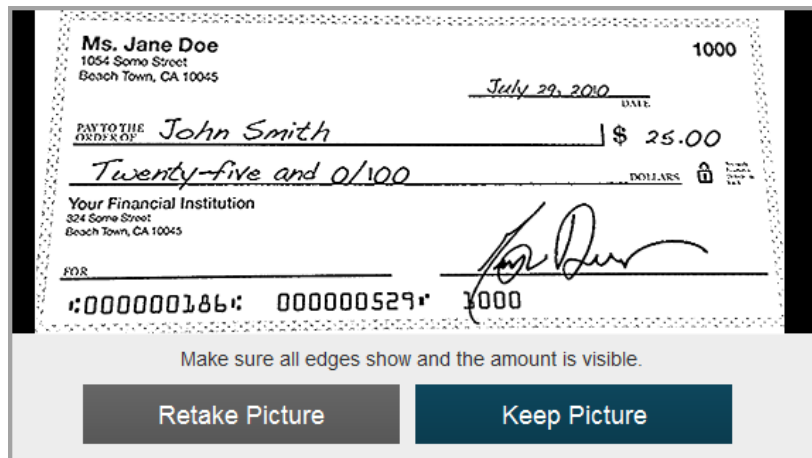


The check is scanned using Optical Character Recognition Technology (OCR). The OCR Technology scans certain items for validity, for example, the amount and overall image quality. If any problems are found with the image the user is asked to retake the picture. The financial institution can configure the product to manage risk factors for item quality.

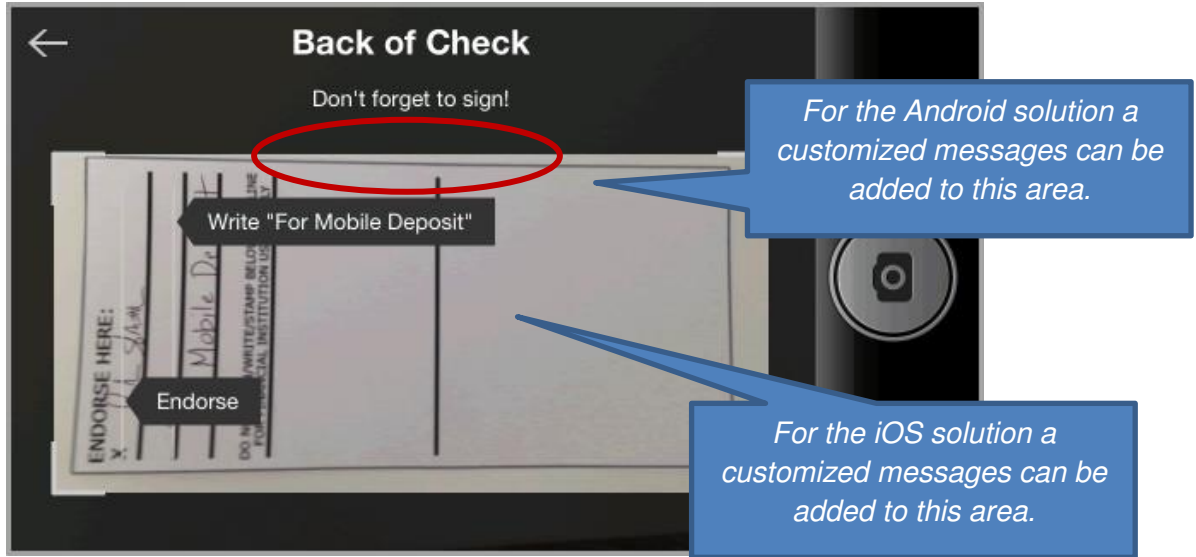
The user also has the option to turn on a flash feature. By default it is off, but the user can turn it on if they need additional light while taking the picture of the check.



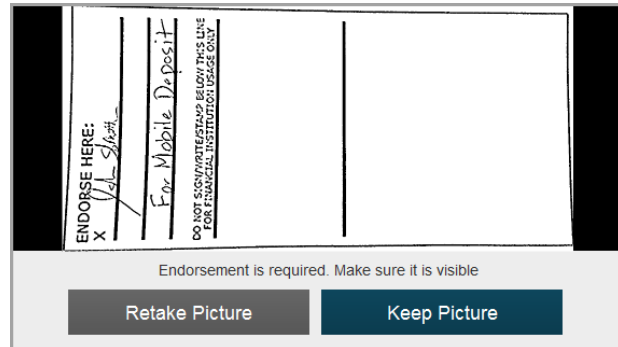
- Once the picture has been taken and appears on the screen, the user reviews the image. The user clicks **Keep Picture** to proceed or **Retake Picture** to retake the picture.



- The user is then prompted to take a picture of the back of the check. The user will need to endorse the check. Once the camera button or the screen on the device is tapped, the OCR Technology scans the check and give the user the option to process the check image or retake it.

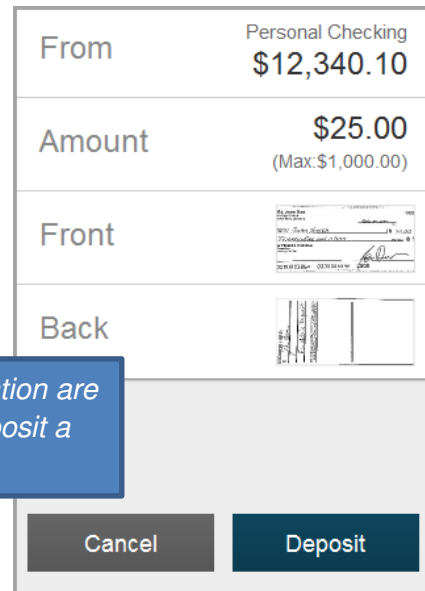


If the user is satisfied with the image, the user clicks **Keep Picture**. If the image is not clear the user can take another image by clicking **Retake Picture**.



- Once the user taps **Keep Picture**, a summary of the deposit appears on the screen.

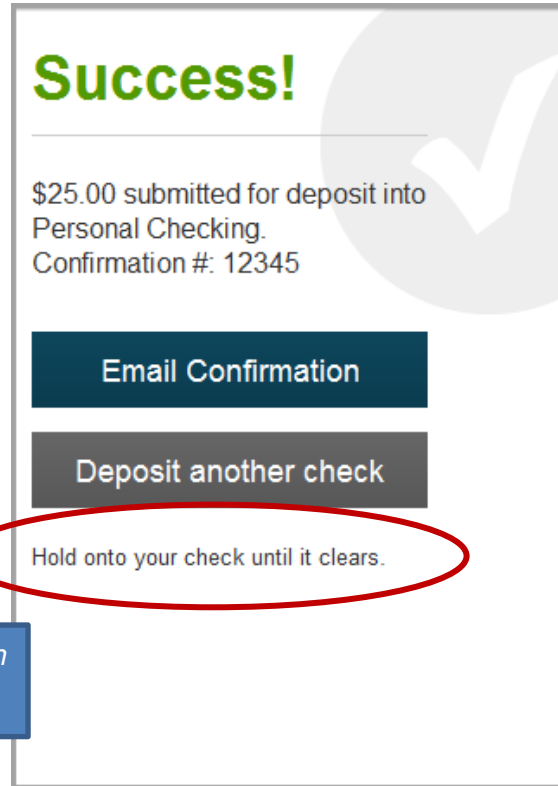
Clicking **Deposit** processes this transaction.



*All four pieces of information are needed in order to deposit a check.*

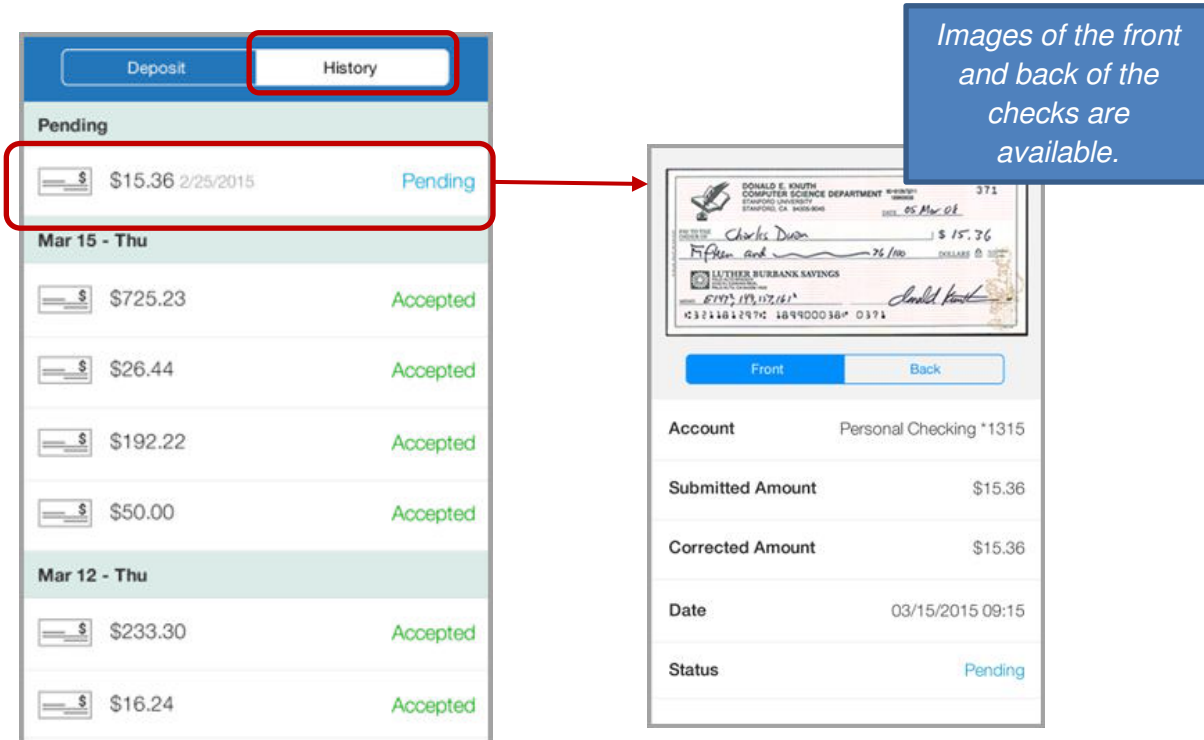
7. A **Success!** message appears on screen. The user is given the option of receiving an email confirmation or depositing another check.

To receive an email confirmation, the user taps **Email Confirmation**. An email is opened within the App and they enter an email address. The email automatically contains the same information as the Remote Deposit Capture confirmation page.



### Viewing Check History

The user is able to view up to 180 days of their mobile deposit history on the History screen. The user can view information about pending, cleared and rejected deposits by tapping directly on any of the deposits.



## Support Notes

### **My user cannot see an image of the deposited check on the history page. Why not?**

There is no option for the user to pull up the image of a deposited check on the history page. The user has the physical check and should hold on to this check, marked with “Mobile Deposit”, until they see that the deposit has cleared.

### **How can my user be sure that the check is not being manipulated after the image capture?**

The image captured by the Mobile Banking App is immediately sent to the Remote Deposit Capture Vendor. Furthermore, the image is not stored on the device itself so no manipulation can occur.

### **Will users have to accept new terms and conditions for phones and tablets?**

No. Once a user accepts the terms and conditions for a phone they do not have to accept terms and conditions for a tablet.

## Configuration Options: Deposit Checks

**Picture of Check Customized Messages (Back of Check):** Contact Customer Care at 877-462-3446 or go to **Admin Platform>MySupport** to submit a ticket to add a customized message when the user is taking a picture of the back of a check. This feature is included in the Mobile Banking Apps 4.4 release and is slated for availability starting in December of 2014.

**Success! screen customization:** In order to customize the last lines of the Success! screen the financial institution needs to contact Customer Care at 877-462-3446 or go to **Admin Platform>MySupport** to submit a ticket. This feature is included in the Mobile Banking Apps 4.3 release and is slated for availability beginning in December 2014.

**OCR Parameters:** The OCR parameters are originally set during implementations. If the financial institution needs to make adjustments to these parameters, contact Customer Care at 877-462-3446 or go to **Admin Platform>MySupport** to submit a ticket.

**Deposit Limits-** Making adjustments to the deposit threshold depends on the Remote Deposit Capture vendor:

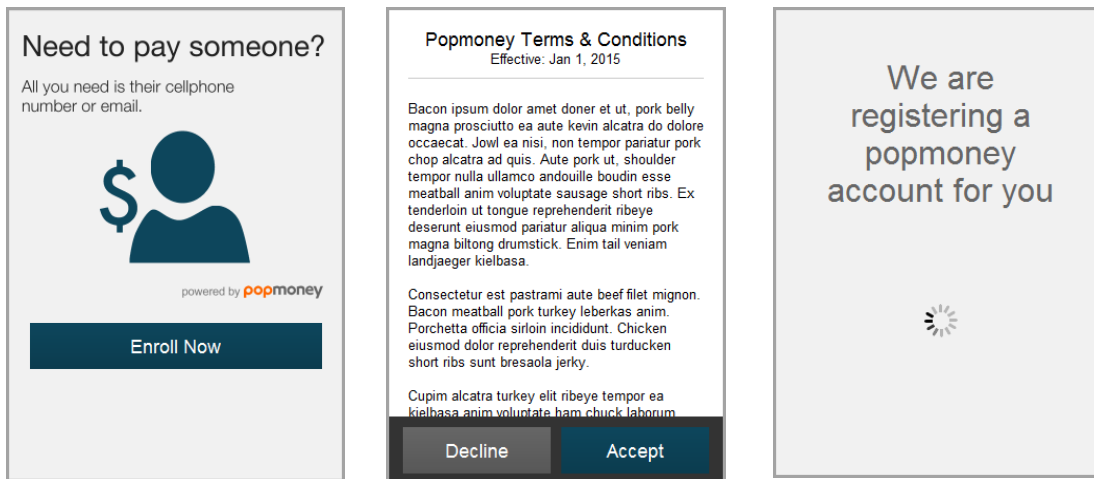
- With Verifi the financial institution is able to manage the deposit thresholds within the back end administrative platform at any time.
- With Ensenta deposit thresholds are set up during implementation and any changes after that point need to involve Customer Care (877-462-3446 or go to **Admin Platform>MySupport** to submit a ticket)

## Pay People

Pay People is a person-to-person payment service that allows your users to send secure electronic payment(s) to anyone using their email address or mobile phone number. Your financial institution must offer this product within Online Banking in order to offer it to your mobile users.

### Registration

If the user has never used Pay People, on a device or a PC, they are guided through a registration process as well as accepting the Terms & Conditions.



The user is only asked to register one time. If they have already registered for Pay People via Online Banking on a PC then they do not have to register again if accessing Pay People via a mobile device.

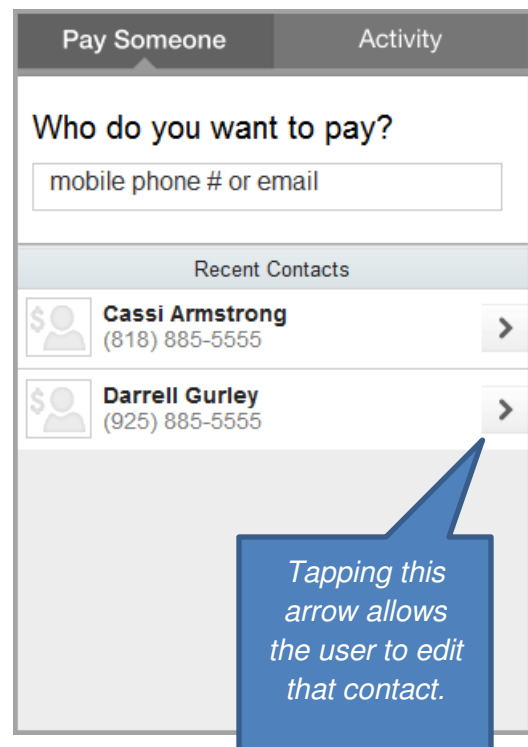
### Setting Up a Payment

1. The **Pay Someone** tab within **Pay People** lists the people and their mobile devices that have already been entered into the system. This list includes people that have been paid through Pay People on a PC (if applicable) as well as the user's contact list on their mobile device.

To pay someone that is already listed, simply tap their name.

To pay someone that isn't already listed, enter their mobile phone number or email in the space provided.

The user has the option of editing the contacts from this screen. By tapping the arrow beside the name the user is able to edit the contact's mobile number and email.



2. Enter the amount to pay, the funding account, and any message to be included with the payment.

The financial institution has the option of offering next-day delivery or a 3-day delivery. The financial institution will also be able to set the fees for these two options.

The user taps **Send Money** in order to process this transaction.

For every transaction over \$100 sent to an email there is an extra layer of security. The sender provides a phone number that the recipient must confirm when the payment is picked up.

*There is a 20 character limit in the message if the money is being sent to a phone number and a 250 character limit if the money is being sent to an email address.*

3. Once the user confirms the transaction the end user receives a **Success!** message letting them know the payment was successfully transmitted.

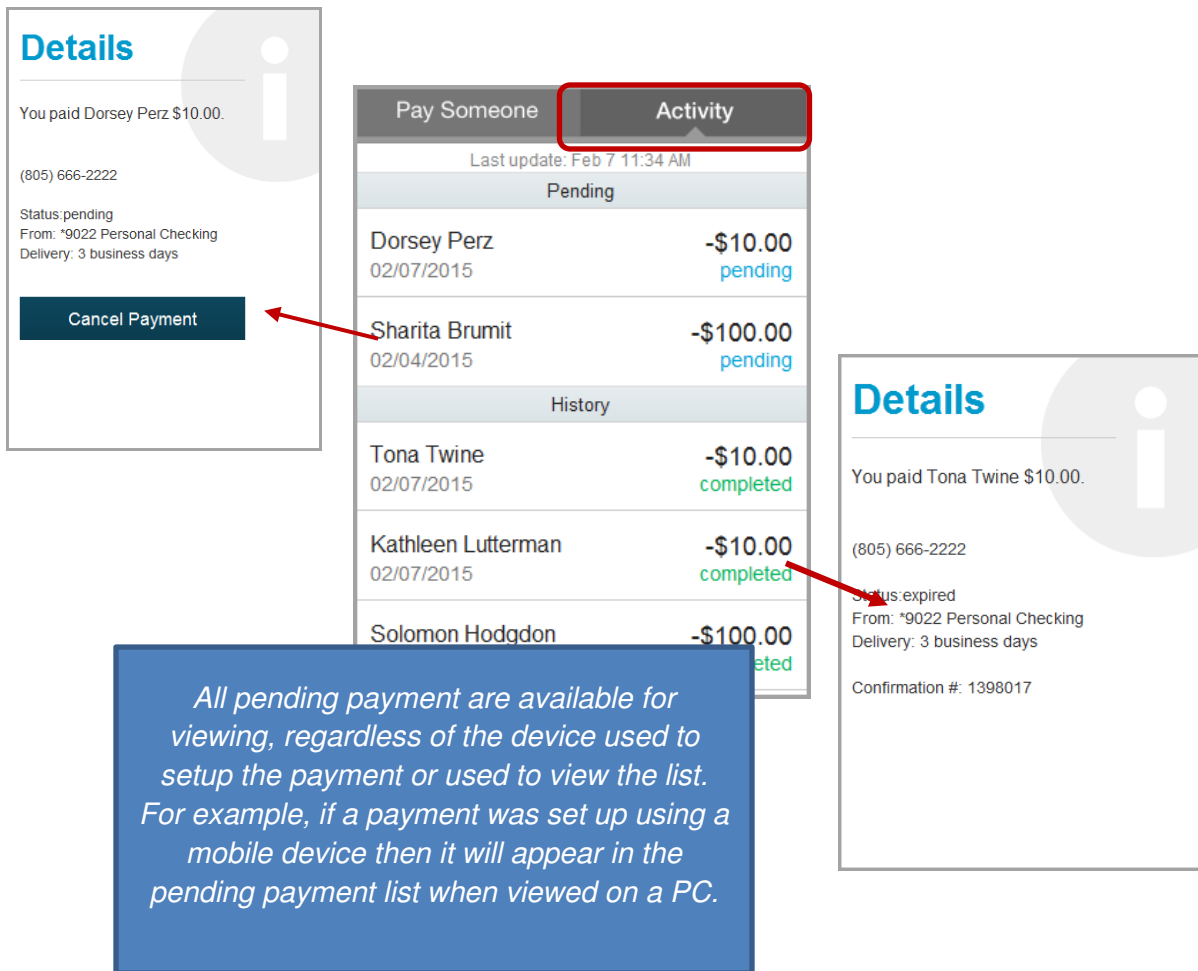
*Any applicable fees are shown to the user before they confirm the transaction.*

### View Activity and History

Under the Activity tab within Pay People the user is able to view pending and recent activity including details on that activity.

To cancel a pending payment, tap on the pending payment and tap **Cancel Payment**.

Tap on a completed payment to view details about that payment.



**Details**

You paid Dorsey Perz \$10.00.

(805) 666-2222

Status: pending  
From: \*9022 Personal Checking  
Delivery: 3 business days

**Cancel Payment**

Pay Someone	Activity
Last update: Feb 7 11:34 AM	
Pending	
Dorsey Perz 02/07/2015	-\$10.00 pending
Sharita Brumit 02/04/2015	-\$100.00 pending
History	
Tona Twine 02/07/2015	-\$10.00 completed
Kathleen Lutterman 02/07/2015	-\$10.00 completed
Solomon Hodgdon	-\$100.00 completed

**Details**

You paid Tona Twine \$10.00.

(805) 666-2222

Status: expired  
From: \*9022 Personal Checking  
Delivery: 3 business days  
Confirmation #: 1398017

*All pending payment are available for viewing, regardless of the device used to setup the payment or used to view the list. For example, if a payment was set up using a mobile device then it will appear in the pending payment list when viewed on a PC.*



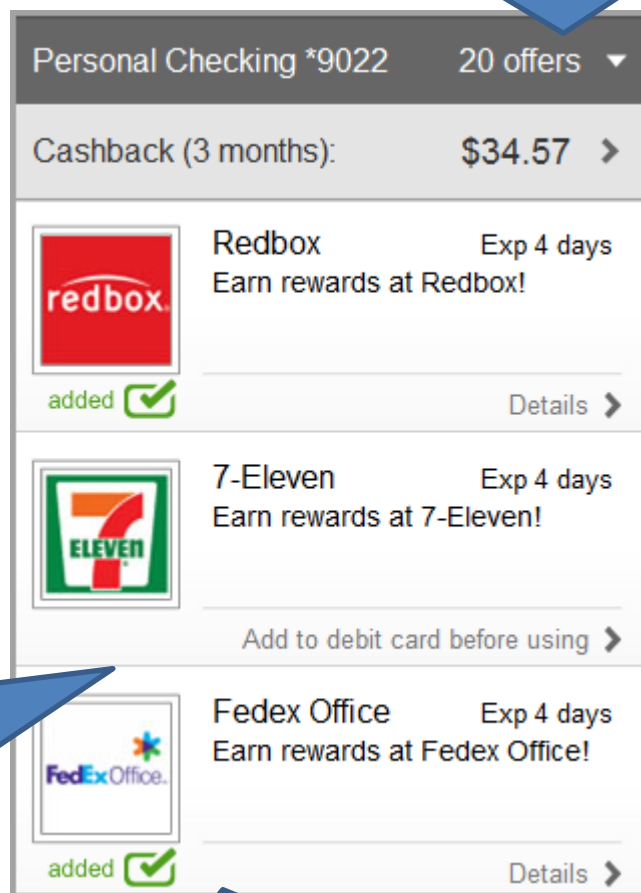
## Earn Cash Back

Build loyalty and satisfaction by helping your users save money with personalized cash-back offers via Purchase Rewards, provided in partnership with Cardlytics. Cash-back offers are based on user's location and debit card shopping history and can be used toward everyday debit card purchases.

1. The user initially views a summary of all available offers as well as a summary of the cash earned for the current month and the prior two months.

The user is able to view details regarding a particular offer or activate offer from this screen.

*Users are able to view the account that offers are attached to. If multiple accounts are tied to the rewards system this top bar is selectable.*



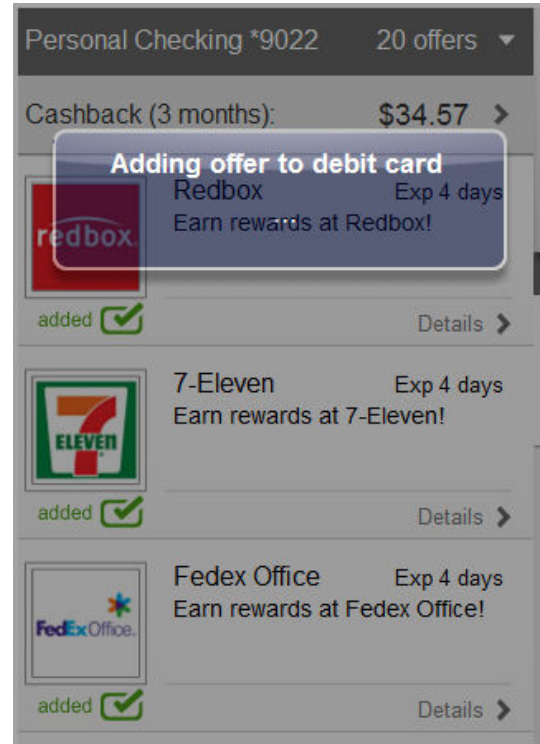
*The user taps **Add to debit card before using** to immediately add this reward to a debit card.*

*Tapping this line will direct the user to the redemption screen. This screen gives redemption details for each payment period.*

*Rewards that have **added** under the description have already been activated and are ready to be redeemed.*

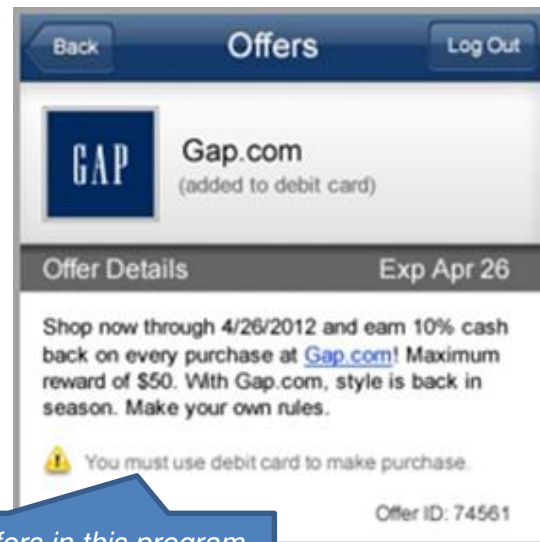
*The user clicks **Details** to view information about that offer.*

2. Once **Add to debit card before using** is tapped. The user sees a message saying the offer is being added to their debit card.



3. The user is taken to the details screen to view information about that offer. This screen contains the following information:

- Merchant name
- Offer status
- Link to map merchant location (available if in-store purchase only)
- Complete offer details
- Offer redemption instructions
- Offer ID



*There are some online offers in this program that require a purchase through the link provided in the details. In this case, additional language is displayed highlighting the need to use the link.*

## Support Notes

### **My user cannot view expired offers. Why not?**

Expired offers are not available for view in the mobile banking session. These can only be viewed by logging into Online Banking and visiting the rewards summary page.

### **When will my user see the reward deposited into their account?**

Qualifying purchases made in one month will be applied to the linked debit card account at the end of the following month. So, if you make a qualifying purchase in April, the amount will be deposited in your account at the end of May. The user will receive one credit for the cash back which will include all of the offers redeemed.

### **\*\*Roadmap Previews for the Mobile App:**

- *We are currently developing push notifications for the Mobile App. Users will be able to set up balance updates, as well as alerts for low balances, large withdrawals and large deposits from the Mobile App. This feature is currently on the Roadmap.*
- *The iPad Split Screen feature will allow users to run the Mobile Banking App at the same time they run another app. This feature will be available for iPad models that support the feature and run iOS9 or higher. This feature is currently on the Roadmap. This feature is not available for Android devices because the technology is not supported by Google.*
- *Card Management allows users to control when debit and credit cards are used directly from their Mobile App. This feature is based on card processors and is currently on the Horizon plan.*
- *The ability to sign up for and view integrated Online Statements via the Mobile App is currently on the Horizon Plan.*

# Mobile Banking Apps: Additional Features

## Overview

Leveraging the mobile devices' location technology, the Mobile Banking App has a **Locations** feature located in the main menu. In addition, the **More** button allows the financial institution to provide custom links.

The **Rate Our App** screen is available to users after a certain amount of activity.

### In this section:

- Locations
- More
- Rate Our App

## Description

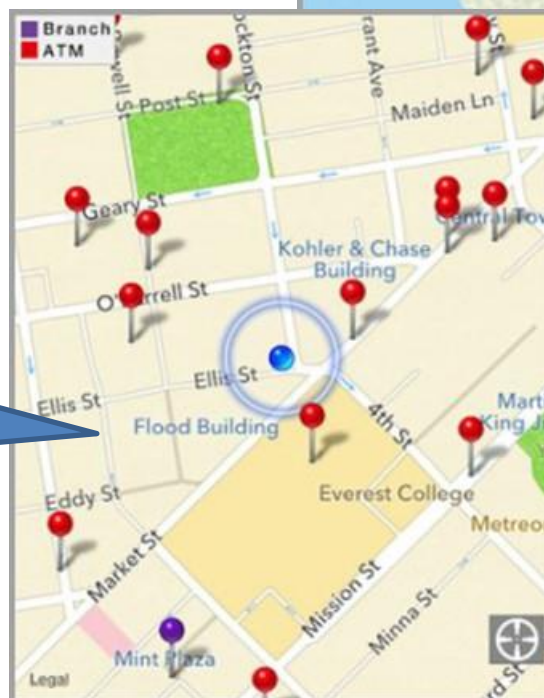
### Locations

Users enter a ZIP code or city and state to find their financial institution's locations.

A map with drop pins on all the financial institutions locations in that area appears. Red pins signify ATMs, purple for branches and blue for the user's current location.

A user is able to click on any drop pin location and view the address and phone number and business hours of that location.

In addition the user can use the mobile device's technology to receive directions to that location.



*The user clicks on any drop pin to view the address and phone number of that location.*

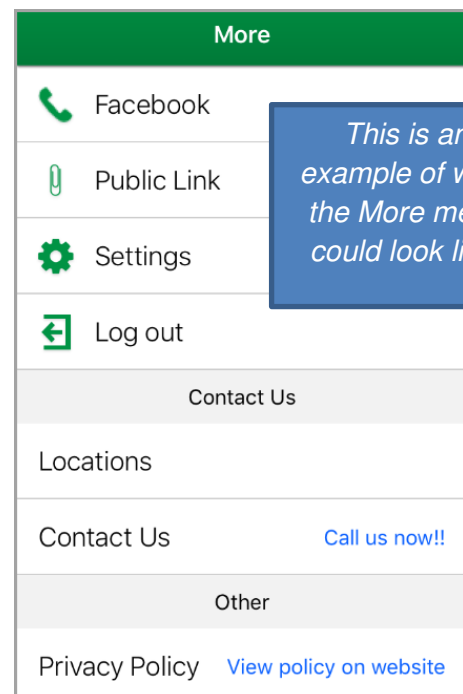
*The user clicks the **Find Me** button to automatically find to their current location.*

## More

The **More** area provides the opportunity for financial institutions to add links to non-single sign-on sites as well as single sign-on sites (available after the user has signed in).

The following information can be included in the **More** section:

- Create Your Own Page links. This feature empowers your financial institution or a third-party vendor to develop content as a page in the Mobile App. A link would be available in the Additional Links area of the More page, creating a seamless experience for your end users in order to give them additional functionality. Your financial institution is able to add up to 20 additional links. Contact your Relationship Manager for additional information.
- Messages: The Message area notifies user about new key features in the app and will display Push Notification history (Push Notifications is currently on the Horizon Plan). The “What’s New in this Version” section of the Messages area displays new features of an upgrade. The feature is displayed for 7 days or until it is tapped.
- A link to Customer Service information. Tapping the phone number automatically dials that number.
- A link to send an email to the financial institution. Tapping **Email Us** opens a new email in the user’s email app.
- A link to the website and privacy policy. Tapping **Website** or **Privacy Policy** launches a browser and takes the user directly to the financial institution’s website or privacy policy.
- Links to social media sites. Tapping on any of the social media sites opens a browser and take your user to the corresponding site.
- A link to open a new account. Tapping **Open new account** takes the user to a third party vendor site that provides a process for opening a new account online. This is dependent on the financial institution offering this product.
- Secure Support Email. Allow your users to contact support with secure emails. Emails are assigned ticket numbers and queued for the financial institution’s response. User can access replies through either Mobile or Online Banking. This product is part of the Desktopshare Bundle which includes Secure Support, Knowledgebase, Desktop Share and Secure Chat.

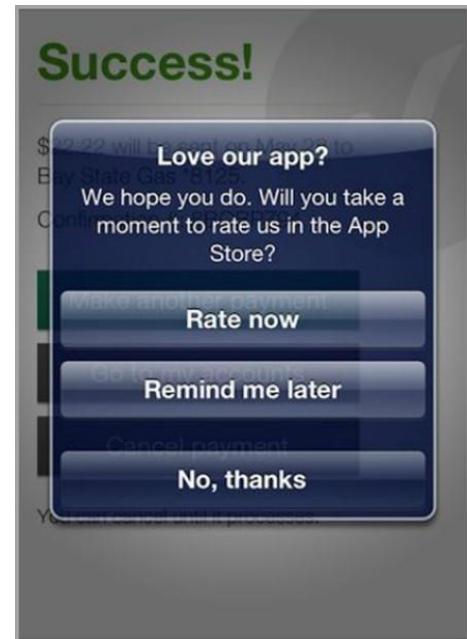


**\*\*Roadmap Preview: Secure Chat for Mobile Banking is currently on the Roadmap. This feature extends the Premier Secure Chat service to a user’s mobile channel allowing your user to chat with agents from a smartphone or tablet from within Mobile Banking Apps or Mobile Web Banking.**

## Rate Our App

The **Rate Our App** prompt appears when the user reaches a certain number of logins and activity within the App.

The type of smartphone will determine the destination of the rating system. The ratings are public information and are located in the App store or Google Play.



## Configuration Options: Additional Features

**Additional links on the More screen:** Contact Customer Care at 877-462-3446 or go to **Admin Platform>MySupport** to submit a ticket to request links added to the More screen. The financial institution is responsible for providing the destination URL and the title of the link. The character limit for the title link is 16 characters.

**Creating a single sign-on link on the More screen:** To add a single sign-on link to the More screen the financial institution will need to contact their Relationship Manager.

**Customizing ATM and branch info:** Contact Customer Care at 877-462-3446 or go to **Admin Platform>MySupport** to submit a ticket to customize the ATM or branch information that appears in the Locations area.

# SmartWatch App

## Overview

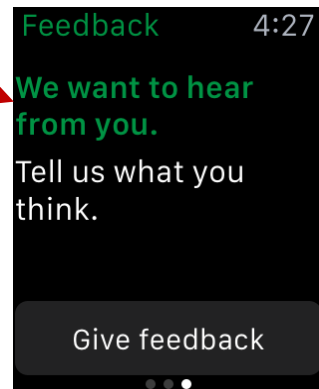
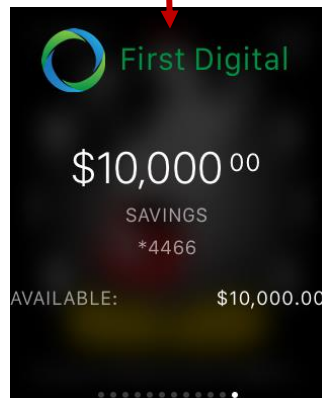
Smartwatch banking allows your users to access their important banking tasks via their Apple Watch or Android Wear. User can conveniently and securely check balances and transactions without needing to login. Users are able to determine which accounts can be viewed via the wearable as well as the order of the accounts. Using the geolocation feature, the wearables can provide branch locations as well.

The financial institution is able to brand certain components of the SmartWatch. Digital Insight will assist your financial institution with any customization during implementations. Digital Insight's Customer Care team can assist your financial institution with these types of changes once you are live.

*During the launch of our SmartWatch App one financial institution's logins by watch owners jumped more than 6x by the 3<sup>rd</sup> month. That's up to 6x more opportunities to connect with customers.*



*Customize with a watch-specific icon as well as a primary font color.*



## Description

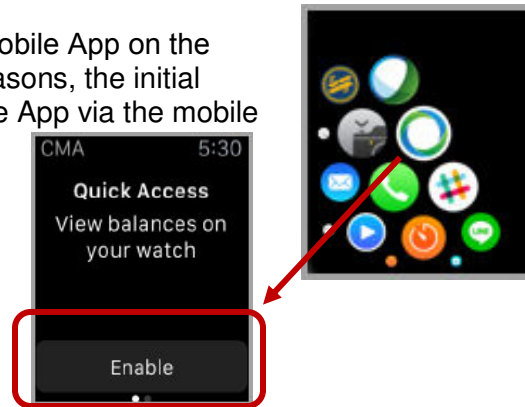
### First Use Experience (Apple Watch)

The financial institution's Mobile App automatically downloads to the SmartWatch from the corresponding phone. The user will need to have the latest financial institution Mobile App on their smartphone.

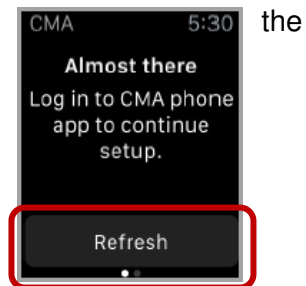
For security reasons, the SmartWatch must be enabled via the Mobile App on the mobile device. The user can initiate this process from the SmartWatch or directly from the Mobile App.

#### Access via the SmartWatch

1. The user clicks on the financial institution's Mobile App on the smartwatch and taps **Enable**. For security reasons, the initial screen instructs the user to login to the Mobile App via the mobile device.

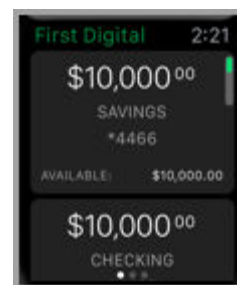


2. After a successful mobile device login, the user returns to watch and taps the Refresh button.



3. The user can then view account balances and transactions.

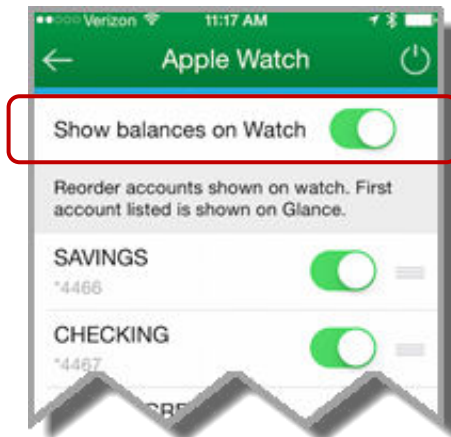
If enabled via the AppleWatch menu on the Mobile Device, the user is able to view the first account balance at a Glance screen.





### Access via the Corresponding Mobile Device

The user also has the opportunity to turn on functionality for the Apple Watch via the corresponding mobile device. Go to: **More > Settings > QuickBalance > Apple Watch** and turn on the toggle for Apple Watch. The user will need to tap **Refresh** on the SmartWatch in order to start using the features.



**\*\*Note:** For security reasons, the user is prompted to log into their Mobile App on the corresponding mobile device before being able to use their wearable if they have not logged into the Mobile App for 30 days or more.

### Viewing Accounts and Transactions (Apple Watch)

The user is able to control the accounts displayed and the order of the account balances in the SmartWatch. This is managed by the user via the Mobile App on the mobile device. The user navigates to: **More > Settings > Apple Watch > Edit**. Once any changes are made the user must tap the **Refresh** button on the SmartWatch to apply any changes. Changes take 10-15 seconds to appear.

*To view balances via the SmartWatch, toggle this option on.*

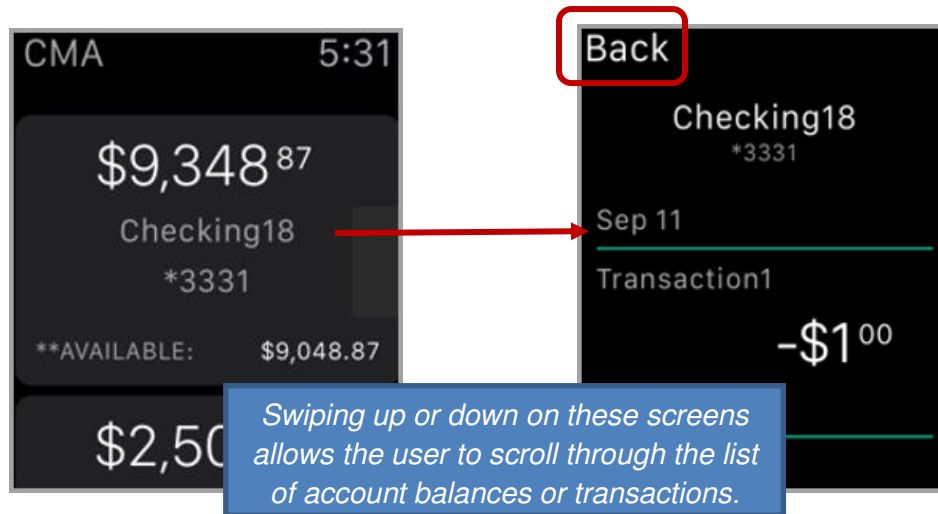
*The user taps Done to save any changes.*

*The user hide/unhides accounts by toggling them on/off.*

*The first account balance listed here is the account that is shown on the Glance view of the SmartWatch.*

*The user can rearrange the order of the accounts by dragging and dropping using the handles.*

To view transactions on the SmartWatch, from within the SmartWatch app, the user simply taps the account balance. The last 5 transactions from the past 90 days are available for viewing. The **Back** button returns the user to the list of account balances.



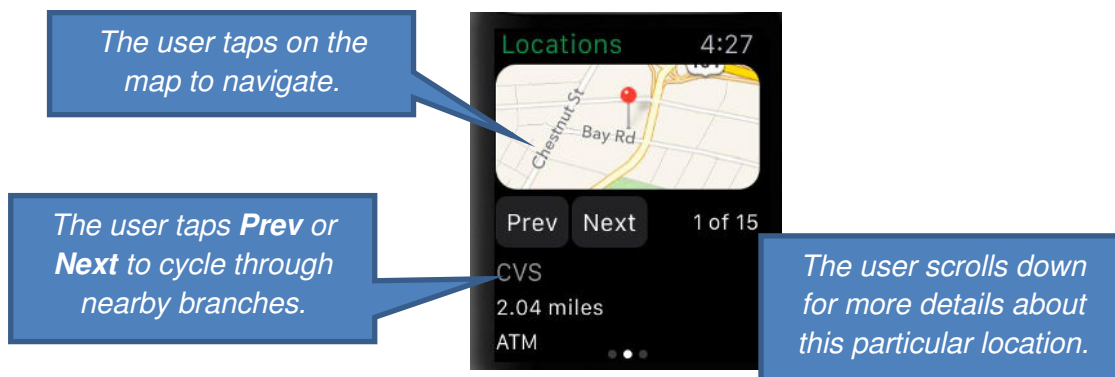
The user is able to set up a Glance view of the first account listed on the AppleWatch set up menu within the Mobile App (screen shot of this is on previous page). Within the AppleWatch app on the mobile device, within your financial institutions app, the user toggles the Glance View option to **ON**.



With this feature enabled, while on the Watch Face view of the Apple Watch, the user swipes up to scroll through any Glance views that may be set up.

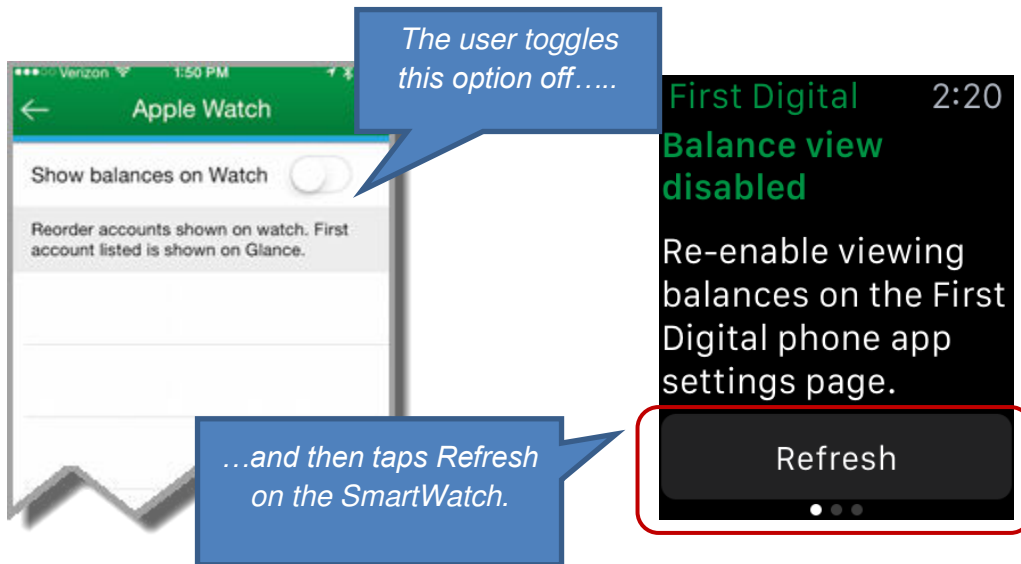
### Branch Locator (Apple Watch)

The user can access the Branch Locator feature by swiping left or right on the Glance or Accounts screen. The geo-location feature must be turned on within the device's settings.



## Turning Off Smart Watch Capability (Apple Watch)

The user can turn off SmartWatch capability at any time from the mobile device within the Mobile App. The user navigates to: **More > Settings > Quick Balance > Apple Watch**. The user toggles **Show balances on Watch** to off. The user will need to click **Refresh** on the wearable to apply the changes.



## First Use Experience (Android Wear)

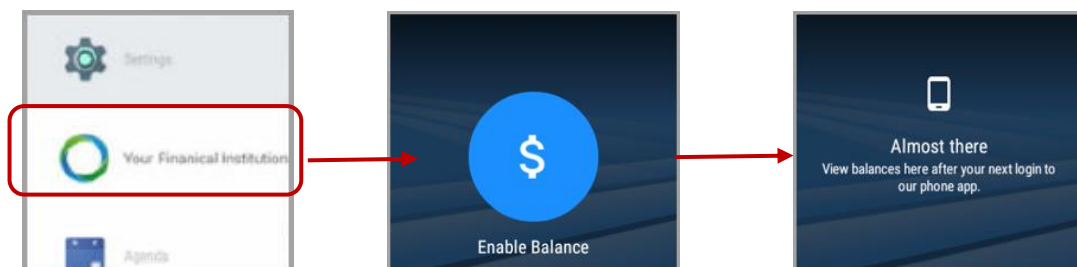
A first time Android user will need to have the latest financial institution Mobile App on their smartphone. The financial institution's Mobile App will then automatically download to the SmartWatch from the corresponding phone.

For security reasons, the SmartWatch must be enabled via the Mobile App on the mobile device. The user can initiate this process from the SmartWatch or directly from the Mobile App.

*Access via the SmartWatch*

1. The user clicks on the financial institution's App on the SmartWatch and taps the **Enable Balance** button.

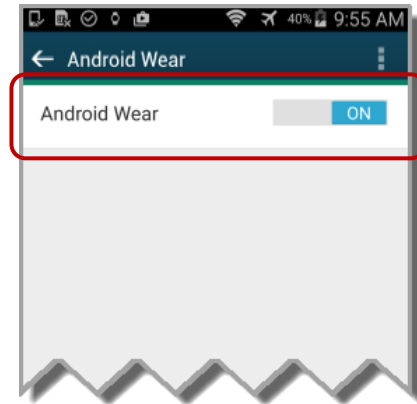
For security reasons, the initial screen instructs the user to login to the mobile device and confirm the ability to view balances via the smartwatch.



2. After a successful mobile device login, the user returns to the watch and is able to view balances.

### Access via the Corresponding Mobile Device

The user also has the opportunity to turn on functionality for Android Wear via the corresponding mobile device. Go to: **Menu > Settings > Quick Balance > Android Wear** and turn on the toggle for Android Wear.



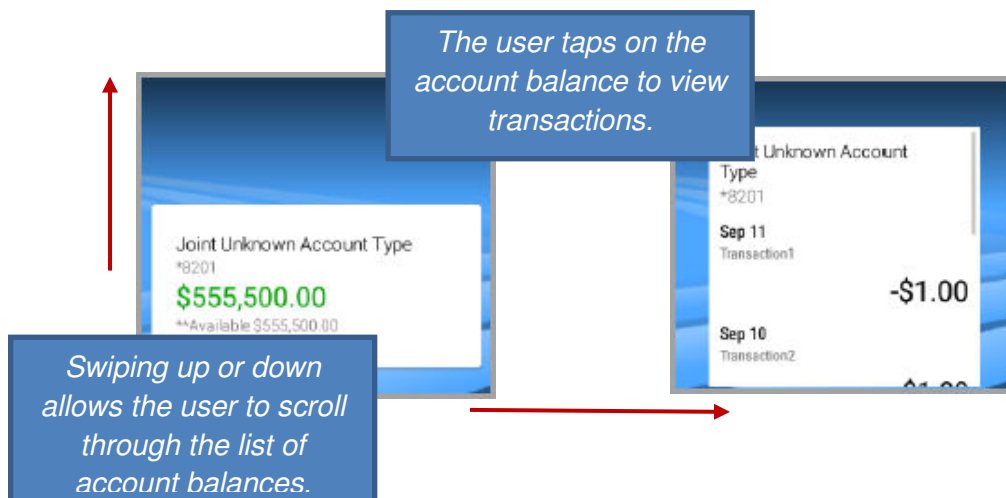
The user will need to tap **Refresh** on the SmartWatch in order to start using the features.

**\*\*Note:** For security reasons, if the user hasn't logged into the Mobile App for 30 days or more, then they are prompted to log into their Mobile App before being able to use their wearable.

### View Transaction History (Android Wear)

The user is able to control the accounts displayed and the order of the account balances in the SmartWatch. This is controlled by the user via the Mobile App on the mobile device. The user navigates to: **Menu > Settings > Quick Balance > Android Wear > Edit**. Once any changes are made the user must tap the **Refresh** button on the SmartWatch to apply any changes. Changes take 10-15 seconds to appear.

To view transactions on the SmartWatch, the user simply taps the account balance. The last 5 transactions from the past 90 days are available for viewing.



**\*\*Note:** The Android watch backgrounds can be configured by your financial institution. By default, a background template using your financial institution's primary color is uploaded. This default background can be changed by contacting Customer Care. The image must be a 300 x 300 px PNG.

### **Turning Off Smart Watch Capability (Android Wear)**

The user can turn off SmartWatch capability at any time from the mobile device within the Mobile App. The user navigates to: **Menu > Settings > Quick Balance > Android Wear**. The user toggles **Show balances on Watch** to off.

### **Smart Watch Reporting**

Reporting is available for financial institutions via the Admin Platform. Go to: **Admin Platform > Reports > Activity Report**.

This report is scheduled to be available in Spring 2016. More details to follow.

# Mobile Web Banking

## Overview

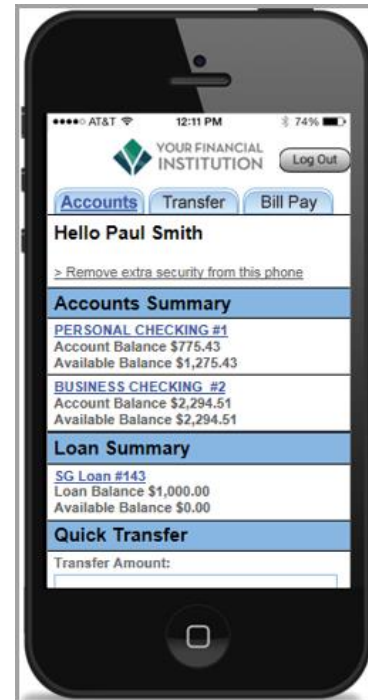
Capture and keep your most profitable users with the on-the-go convenience of Mobile Web Banking. Get all the key features of Online Banking – but optimized for your mobile phone. Users only need a mobile phone that has browsing capabilities. Mobile Web Banking provides access to account information, transfers and Bill Pay.

Online users connect 148 times per year and mobile users connect up to 211 times per year.<sup>1</sup>

The solution gives automatic access to Mobile Banking from your existing website with our mobile device detection capability. Any user going to your regular financial institution website is automatically taken to the mobile version of the site. This mobile redirect filter is standard with Mobile Web Banking.

Mobile Web Banking features include:

- *No mobile device compatibility gaps:* Mobile Web Banking works on any mobile phone with a data plan and browser, and works across any cellular service provider.
- *Superior usability:* No separate Mobile Banking sign-up required for Mobile Web Banking. Users enter your main website URL into the browser on their mobile phone, log in with their existing Online Banking credentials, and start using Mobile Banking on a user interface (UI) matched to their mobile device.
- *Consistent branding:* The mobile website matches your other online channel branding logos and colors.
- *UI tailored for individual phones:* With optimization for different mobile devices. The screen and layout automatically change based on the mobile device to give the optimal user interface.
- *Complete end-to-end security:* Mobile Web Banking is fully secure using industry standard technologies (SSL, WTLS) and security certificates, with 128-bit encrypted communication. No personal or confidential information is stored on the mobile device.
- *Digital Insight hosted:* High availability, fast response time, and network security is assured as Mobile Web Banking is hosted in the same SSAE 16 certified Data Center that operates our Online Banking service.
- *Multifactor authentication:* Mobile Web Banking uses two-way, out-of-band authentication. This enables greater security while keeping the user experience delightfully easy.



is

<sup>1</sup>Internal study of 75 Digital Insight financial institution users, July 2009 through August 2014 based on Digital Insight online end users; Internal study of 47 Digital Insight financial institution users, July 2009 through August 2014; claim based on comparison to Digital Insight non-mobile end users.

# Mobile Web Banking: Login

## Overview

Mobile Web Banking leverages a user's existing Online Banking credentials. No additional enrollment for Mobile Web Banking is required.

### In this section:

- Logging In
- Mobile Registration
- Multi-factor Authentication

## Description

### Logging In: Existing Online Banking User

The financial institution has the option of placing a redirect on their Online Banking URL. If a user enters your financial institution's URL into the browser of their mobile device they are automatically redirected to the Mobile Web Banking site. The financial institution can also offer a link, located on their Online Banking URL, to the mobile site.

The user is presented with the Mobile Web Banking log in screen. Users use their current Online Banking username and password in order to gain access to Mobile Web Banking.

**Contact Us:** The financial institution can customize this screen to contain contact information for the financial institution as well as links to third party vendors. This feature is available before and after login. See page 70 for details.

**Locations:** The user has access to view financial institution's ATM, branch locations, phone numbers and directions. This feature is available before login and after login. See page 70 for details.

**Rates:** The financial institution is able to provide a list of the current rates. This feature is available before and after login (dependent on if your financial institution offers this feature).

**More:** This provides a screen that can contain links including opening a new account, social media as well as a link to the financial institution's full website.

YOUR FINANCIAL INSTITUTION

### Banking Access

Customer Number

Password

Log In

[Sign up](#)

[Contact Us](#) | [Locations](#) | [Rates](#) | [More](#)

*\*\*Note: Similar to Online Banking, users are locked out after five failed login attempts. Failed login attempts on Mobile Web Banking will also lock a user out of Online Banking on a PC.*

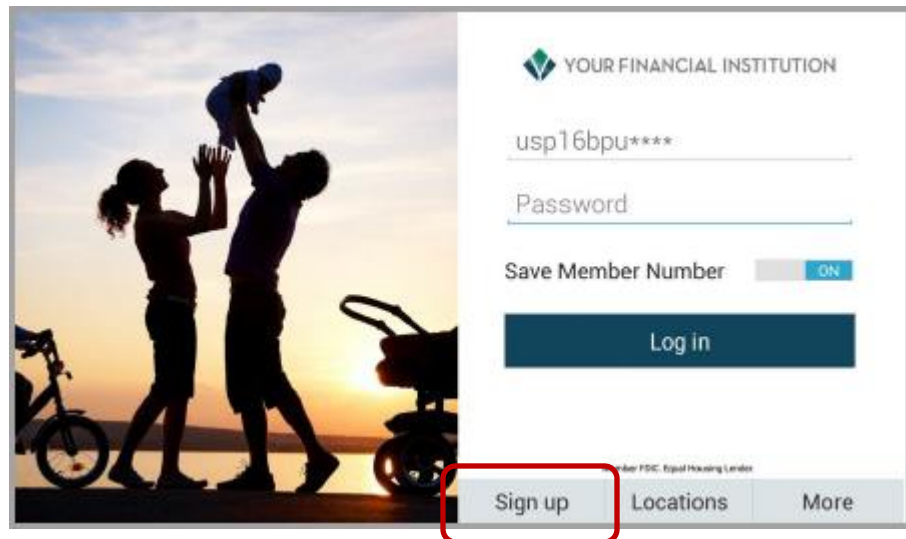
## Logging In: New Online Banking User

**\*\*Roadmap Preview: The following provides a preview of the new mobile registration experience that is currently on our Roadmap. Contact your relationship manager for more information.**

Engage the growing mobile-only user base by enabling your users to register for Online Banking from their mobile phone. Mobile Registration is a streamlined, easy-to-use registration experience.

In order to utilize the registration process via a mobile device, the user must have at least one account with your financial institution. If the user already has credentials for Online Banking, there is no need to go through this registration process. Users are able to access Mobile Banking using their existing credentials.

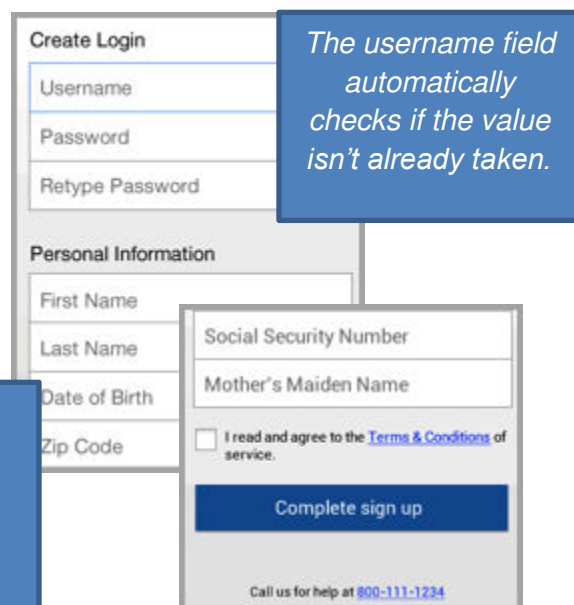
- The user clicks the **Sign Up** link directly on the log in page.



- The user is presented with the registration form. Depending on the device being used, they may need to scroll to see the entire registration form.

The user creates a username and password and then enters their validation information. The user will not be able to progress through the registration process until they agree to the Terms and Conditions.

*The password field automatically reveals two criteria the user has to fulfill with their password creation.*





If your financial institution has Auto-Approve for registration:

- The value entered for Social Security Number or Member Number is used for validation with what exists on the host processor. The result of this validation determines the outcome of the registration attempt.
- The only fields that appear are the validation fields. This is different than Online Banking where all fields are displayed.
- Specific fields for validation vary from institution to institution.

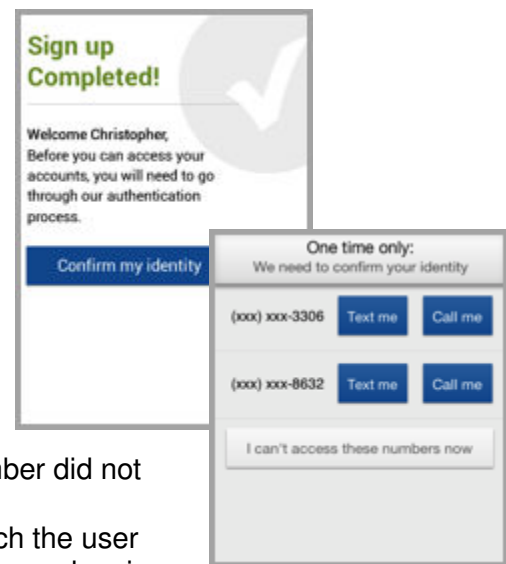
If your financial institution has Manual Approve for registration:

- All fields displayed on the Online Banking registration form is displayed on the mobile device, including optional sections such as Secondary Account Holder.
- Specific fields for validation vary from institution to institution.

6. The next steps depends on if your financial institution supports Auto-Approve or Manual Approve.

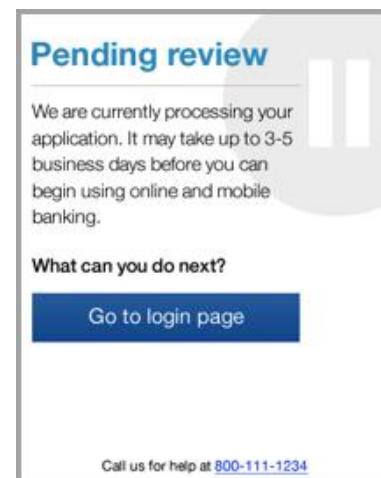
If your financial institution has Auto-Approve for registration:

- If the user's entries are successfully verified they will see a registration successful screen.
- By clicking **Confirm my identity**, the user is directed into the multifactor authentication workflow. Up to two numbers found for the user on the host are retrieved and listed as multifactor authentication numbers.
- After successfully completing the multifactor authentication workflow, the user is instantly logged into their Home Page.
- If the Social Security Number or Member Number did not match, the user is declined.
- If any of the other validation fields did not match the user registration is sent to the Admin Platform for manual review.



If your financial institution has Manual Approve for registration:

- All registration attempts are sent to the approval tool in the Admin Platform for financial institution review.
- The user is given access to Online Banking once an administrator approves the registration.



## Multi-factor Authentication

Multi-factor Authentication for Mobile Web Banking is the same experience as Online Banking. Both solutions utilize out-of-band authentication and device recognition. Mobile Web Banking imports the registered phone number(s) the user uses for Online Banking authentication.

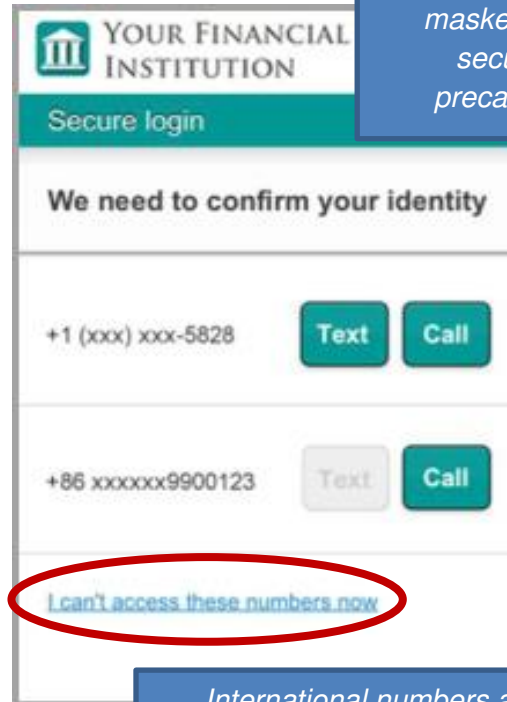
The user only has to go through this procedure once per device.

1. After a successful login, if the user is using an unidentified device, they are asked to confirm their identity. The phone numbers that are already registered for this user via Online Banking will appear on screen.

If the user selects **Call** the user receives a phone call to confirm their identity via voice prompts.

If the user selects **Text** the user receives a code via text to confirm their identity.

The first time a particular mobile device is used to access multi-factor authentication the user is able to enter a new phone number in order to complete the process. This is done by tapping **I can't access these numbers now**. This gives the user the opportunity to enter an additional phone number in order to receive a phone call. If a user has used this mobile device before and **I can't access these numbers now** is tapped, they are directed to update their phone numbers via Online Banking.

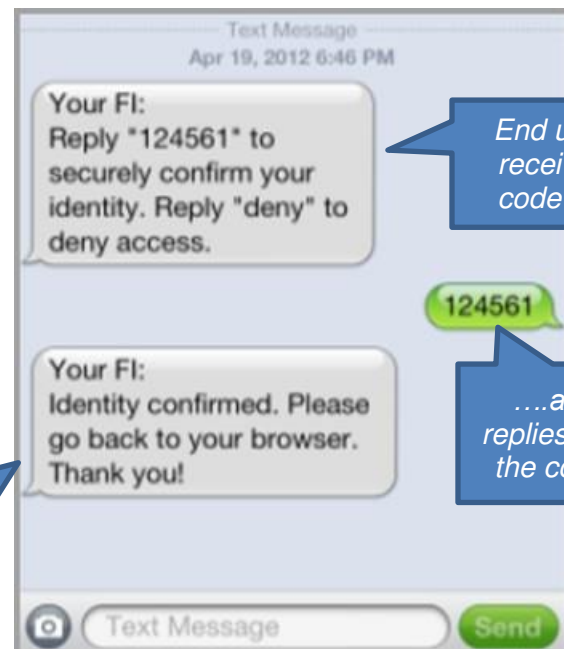


*Numbers are masked as a security precaution.*

*International numbers are supported for voice calls only.*

2. If receiving the code via text, the text is delivered within seconds. The user simply replies with the same code as instructed by the text.

If receiving the code via phone call the user follows the prompts and presses "1" to confirm their identity while on the phone.



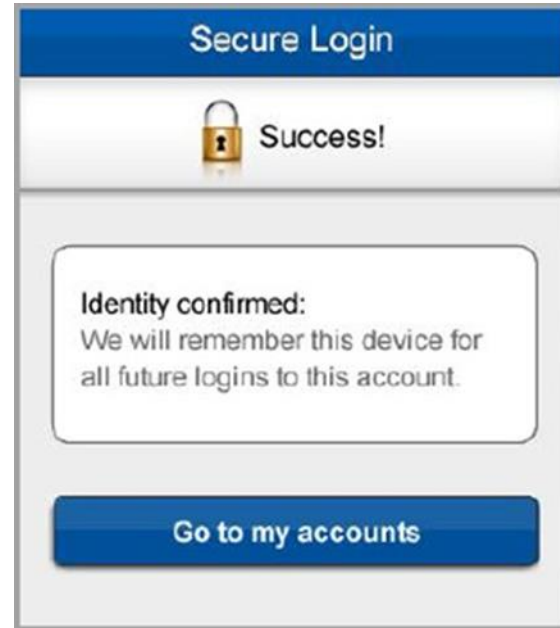
*End user receives code.....*

*....and replies with the code.*

*Once the user's identity has been confirmed they are instructed to return to their browser.*

- The user receives a success message once they navigate back to their browser. This gives the user confidence and assurance that their session and account is successfully authenticated.

Once the user taps **Go to my accounts** on the multifactor authentication success screen they are taken to the Home page of Mobile Web Banking. This is the screen that they will see immediately upon login in the future.



### Support Notes

#### Will users be able to change the phone number(s) they use for authentication?

Yes. The user can manage the multifactor authentication phone numbers via Online Banking. However, during first-time use of mobile authentication, consumers are able to change the phone number(s) they use for authentication. This will allow a Mobile Web Banking-only user to add a new number or change an old number.

#### Does the user need a registered phone number in order to log in?

Yes. The user can use the same approach as the authentication setup in Online Banking. The user is prompted to enter a phone number if he or she is a Mobile Web Banking-only user and hasn't registered a phone number for use with Online Banking. The user uses this new phone number for login attempts on other devices.

## Configuration Options: Mobile Web Banking Login

**Updating the Full Site link:** If the financial institution needs to update the Full Site link located on the Mobile Web Banking Login screen they will need to contact Customer Care at 877-462-3446 or go to **Admin Platform > MySupport** to submit a ticket.

# Mobile Web Banking: Core Features

## Overview

Mobile Web Banking provides maximum access to account balances, history, transfers, Bill Pay and more.

### In this section:

- View Accounts
- Transfer Money
- Pay Bills

## Description

### Accounts

Users are able to access the same accounts (deposit, loans and investment) that are available in Online Banking.

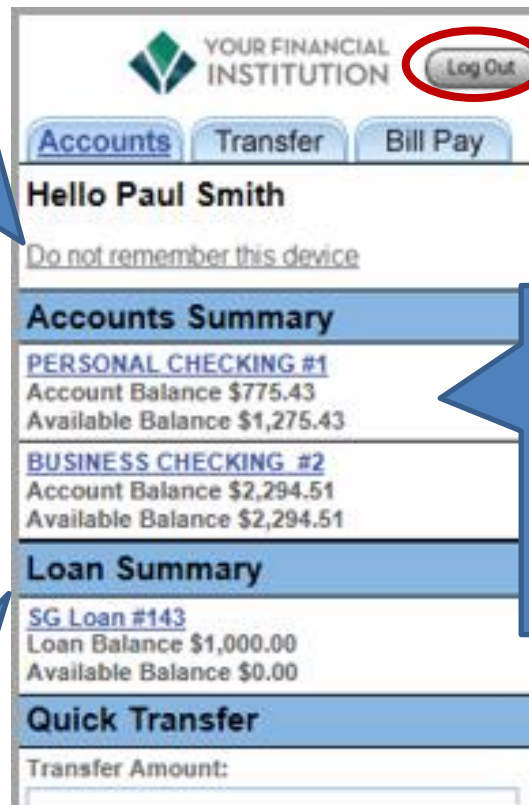
1. All of the user's active Online Banking account are displayed along with the current and available account balance. Your users may have to scroll to view the entire list of accounts.

The same account nicknames from Online Banking are displayed.

The **Log Out** button allows the user to log out quickly and securely.

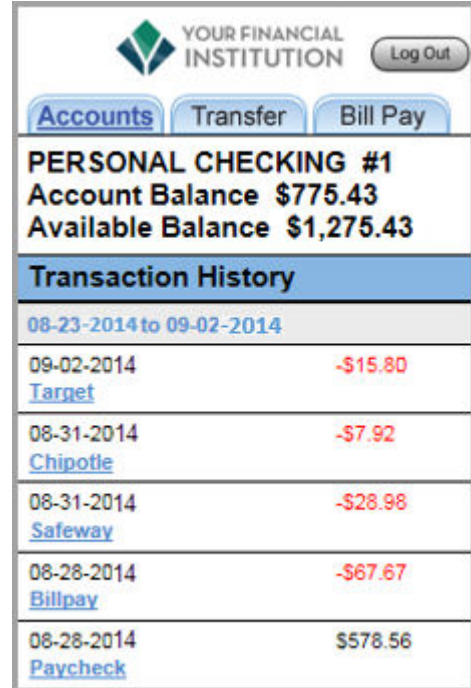
For additional security, the user can tap Do not remember this device and the user will be prompted for multifactor authentication during every login.

If available, the loan and credit card accounts show loan balances. The minimum amount due and due date will appear as well (not shown in screen shot).



The current balance is listed first. Available balance is displayed as well, if available.

- Tapping directly on any of the accounts takes the user to the Transaction History page for that account. From this screen the user can view the Account Balance, Available Balance and posted transactions (information that appears here is dependent on the core processor).



- By scrolling to the bottom of the Transaction History screen a user is able to see additional history, change the date range as well as choose to view information on a different account.

Mobile Web Banking defaults to the last 30 days of account history but will allow as much history as the core processor allows. A user can view additional history by selecting a custom date range (at the bottom of the history screen) and tapping **Go**. When choosing a custom date range, 15 transactions appear at a time. Additional history is also available by tapping **More History**.

*The user clicks on **More History** to see additional transaction history.*

*If the user scrolls to the bottom of the Transaction History screen they see these additional options.*

*The user can enter in a date range here to view more or less history. The user clicks on the date fields to enable a calendar and use this calendar to choose the desired dates.*

*View account history for another account by choosing the account from the dropdown and tapping **View Different Account**.*

08-19-2014 <a href="#">Fiesta Del Sol</a>	-\$18.32
08-18-2014 <a href="#">Safeway</a>	-\$16.97
08-28-2014 <a href="#">Transfer</a>	\$50.00
<a href="#">More History</a>	
Change Date Range (mmdyyy)	
<input type="text" value="08082014"/>	
~	<input type="text" value="08222014"/>
<a href="#">Go</a>	
1: PERSONAL CHECKING	
<a href="#">View Different Account</a>	
<a href="#">Contact Us</a>   <a href="#">Locations</a>   <a href="#">Rates</a>   <a href="#">Log Out</a>	

- Tapping on any individual transaction will give the user additional information about that transaction.

*Information that appears here is exactly what appears for this transaction within Online Banking. This information comes directly from the core processor.*

YOUR FINANCIAL INSTITUTION Log Out

[Accounts](#) [Transfer](#) [Bill Pay](#)

**PERSONAL CHECKING #1**  
**Account Balance \$775.43**  
**Available Balance \$1,275.43**

**Transaction Detail**

09-02-2014 -\$15.80  
 TARGET STORES 0322 032  
 Debit Card Sep. 02, 2014 04:07 Ref: 524862.

[Back to Transaction History](#)

[Contact Us](#) | [Locations](#) | [Rates](#) | [Log Out](#)

- From the Accounts Summary screen the user can perform a Quick Transfer. This is a one-time immediate transfer.

*The user enters the amount of the transfer and choose the **From** and **To** account from the dropdown menus.*

Account Balance \$775.43 Available Balance \$1,275.43
<b>BUSINESS CHECKING #2</b> Account Balance \$2,294.51 Available Balance \$2,294.51
<b>Loan Summary</b>
<b>SG Loan #143</b> Loan Balance \$1,000.00 Available Balance \$0.00
<b>Quick Transfer</b>
Transfer Amount: <input type="text" value="100.00"/>
From Account: 1: PERSONAL CHECKING; 775.43 ▼
To Account: 2: BUSINESS CHECKING; 1,294.5 ▼
<a href="#">Transfer Funds</a> <a href="#">Clear</a>
<a href="#">Contact Us</a>   <a href="#">Locations</a>   <a href="#">Rates</a>   <a href="#">Log Out</a>

*Accounts available for transfer To and From are the same as what is available in Online Banking.*

*The user clicks **Transfer Funds** to process this one-time immediate transfer. The end user is asked to confirm the transfer and will receive a success message that contains a confirmation number.*

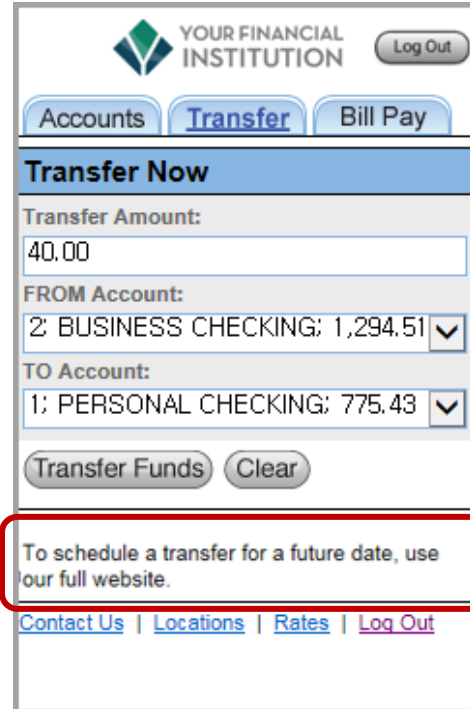
## Transfers

Users are able to process a one-time immediate transfer.

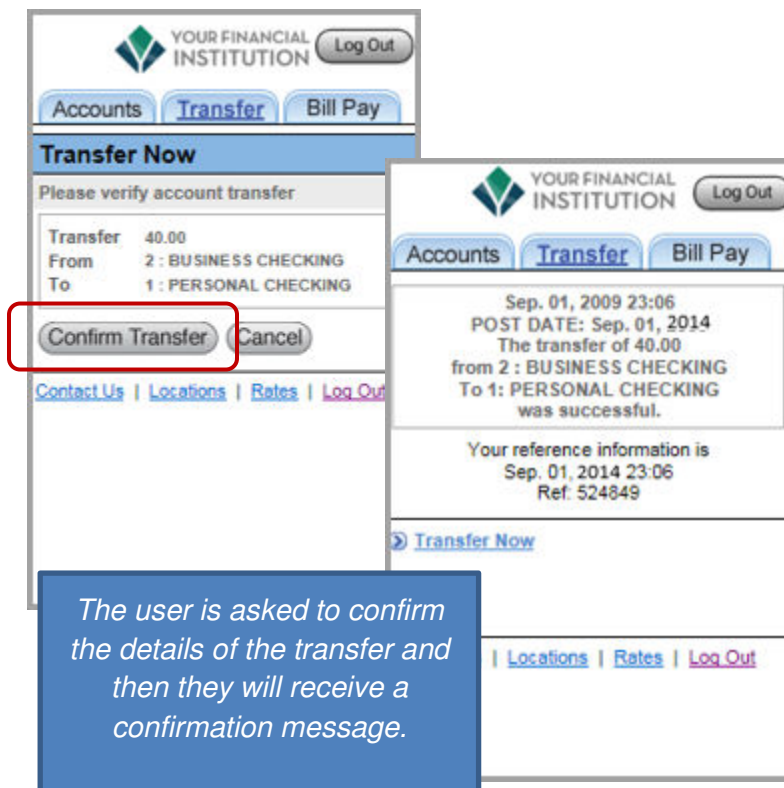
1. On the **Transfer** tab, the user enters the transfer amount, the **From** Account and the **To** Account.

The accounts that are available to transfer **To** and **From** are the same accounts that are available in Online Banking.

In order to schedule a transfer for a future date, the user is directed to use the full website



2. Once the user processes the transfer they are asked to confirm the transaction and then they will receive a success message that contains a confirmation number for that transaction.



*\*\*Note: Account holders are able to transfer funds to other account holders at your financial institution. Recipients must be set up within Online Banking. This feature is core dependent.*

## Bill Payment

The user is able to make single payments, view/delete pending payments and view payment history via the Bill Pay module.

1. To set up a payment select the funding account from the drop-down menu and select a payee from the payee list.

*The payees listed here are the existing payees that have been set up within Online Banking.*

2. The user enters the **Amount** of the payment and the **Send On** date, then taps **Pay**.

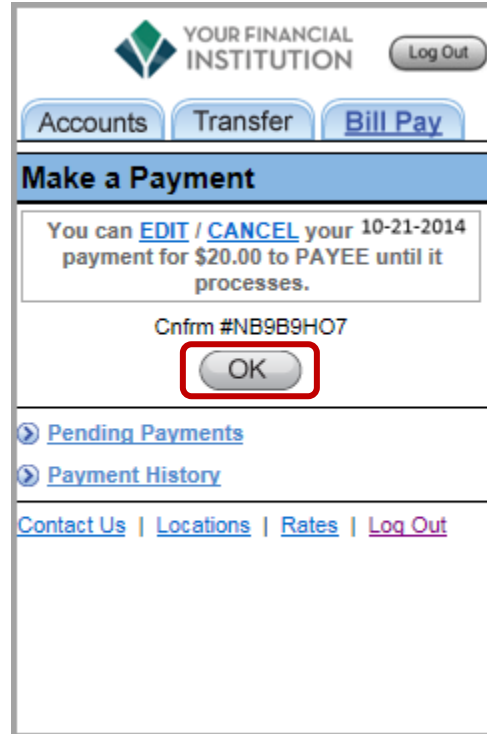
*When the user clicks on the date field a calendar appears. The user can use the calendar to choose the correct date.*

*\*\*Note: For the FIS Process Date model, when the user selects the Send On date the Delivery Date will automatically appear below the date field.*

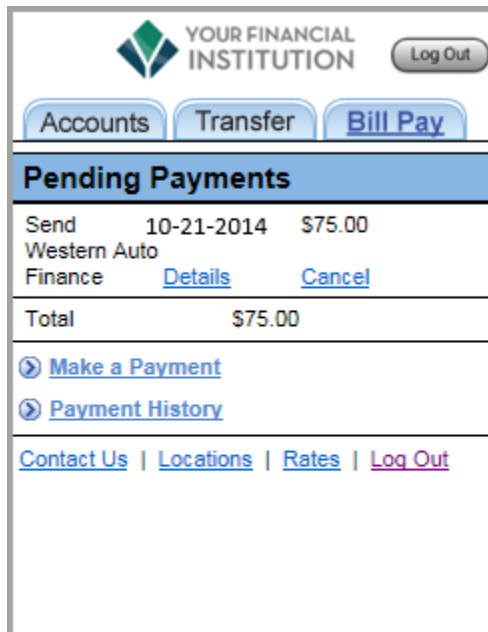


- The user receives a confirmation message regarding the new bill payment and is prompted to click **OK**.

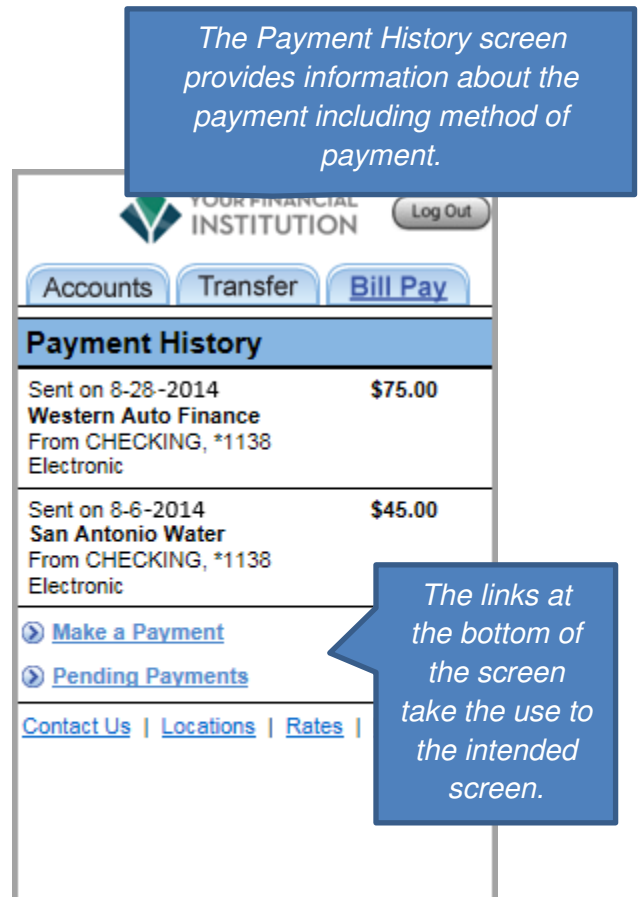
This new payment will now appear on the pending payments screen.



- Throughout the Bill Pay screens, the user is able to access pending payments as well as payment history.



*From the Pending Payments screen users are able to view details about a pending payment as well as cancel that payment.*



*The Payment History screen provides information about the payment including method of payment.*

*The links at the bottom of the screen take the user to the intended screen.*

# Mobile Web Banking: Additional Features

## Overview

Additional features are available for the user before and after log in. This includes Contact Us, Locations, Rates and Log Out.

## Description

### Contact Us

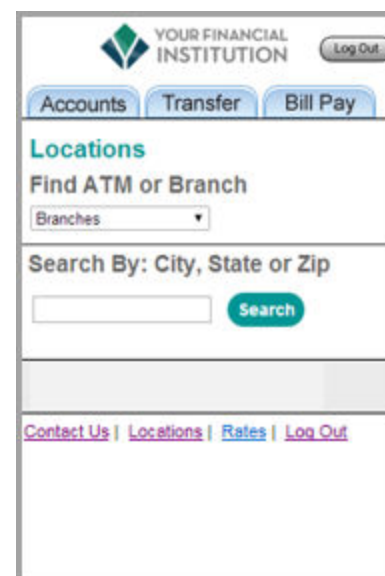
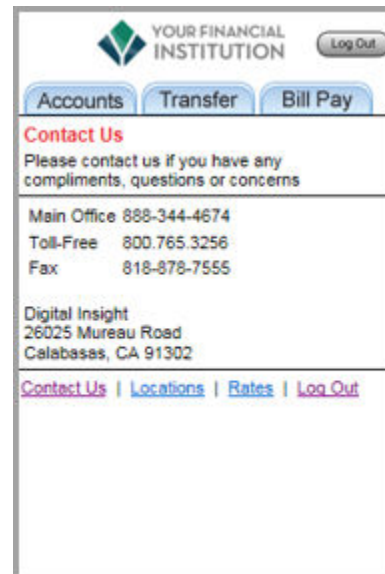
The financial institution is able to place custom customer service contact information in this area. This can include multiple phone numbers, email addresses and a physical address. When the user clicks on the phone number it will direct the user to the dialing screen of the mobile device.

### Locations

The user is able to search for ATM locations and branch locations. Simply use the pull-down menu to choose the type of location and enter a city, state or ZIP code.

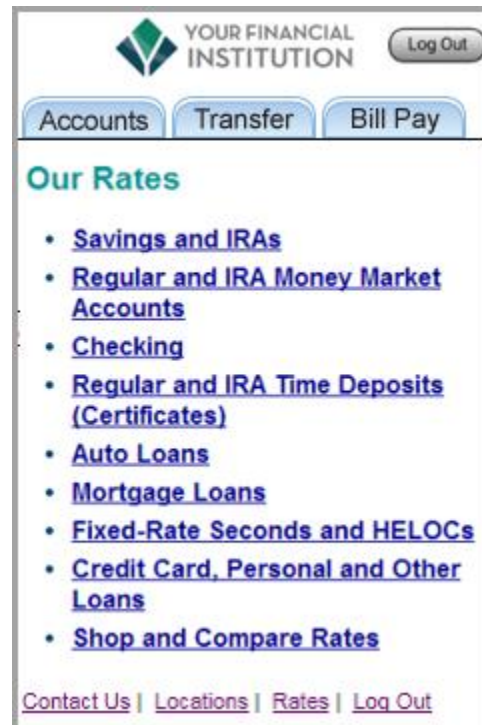
### In this section:

- Contact Us
- Locations
- Rates
- Log Out



## Rates

Financial institutions can provide easy-to-access rate information to users.



*\*\*Roadmap Preview: Secure Chat for Mobile Banking is currently on the Roadmap. This feature extends the Premier Secure Chat service to a user's mobile channel allowing your users to chat with agents from a smartphone or tablet from within Mobile Banking Apps or Mobile Web Banking.*

## Configuration Options: Mobile Web Banking Additional Features

**Changes to Rates:** To update rates on the Mobile Web Banking rates page, the financial institution needs to contact Customer Care at 877-462-3446 or go to **Admin Platform>MySupport** to submit a ticket.

# Text Message Banking

*NOTE: This section of the guide reflects the new Alerts and Notifications experience rolling out to financial institutions in the beginning of 2016. Contact your Relationship Manager for more information about this upgrade.*

## Overview

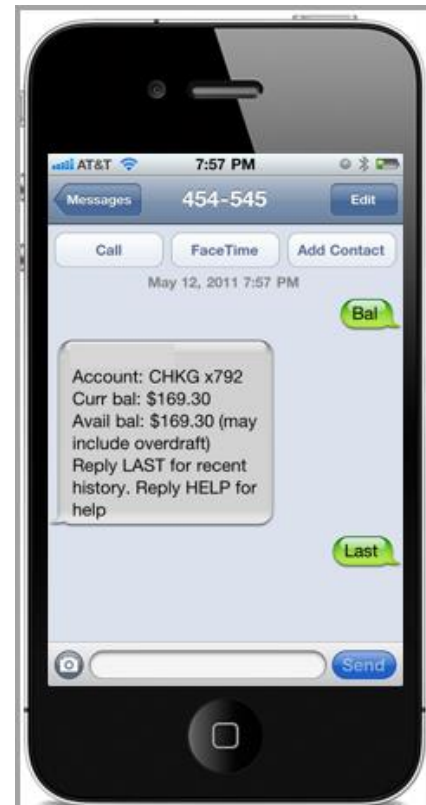
Attract and retain your most profitable users by giving them on-the-go access to account balances and transactions via simple SMS text messages. Text Message Banking can be used from any mobile phone with SMS capability.

**59 percent of Mobile Bankers receive one or more SMS text messages per month.**

Users can access their account information in seconds and receive account notifications. Text Message Banking is an important complement to the browser-based Mobile Banking solution and Mobile Banking Apps because it simplifies users' access to account balance and transaction information. Text Message Banking is free, however, standard rates and fees from an end user's wireless carrier may apply.

Text Message Banking features include:

- *Optimized for most mobile phones:* Most text message-enabled phones can use Text Message Banking. There is no need for Web access, a large phone screen or a keyboard on the phone.
- *Up-to-date account information:* The information provided via Text Message Banking is as current as the account information within Online Banking.
- *Ease of use:* Users simply send a text message to the designated shortcode with the appropriate banking command and immediately receive the requested information.
- *Simple end-user enrollments:* From within Online Banking, users complete a simple, three-step process to enable their mobile phones.
- *Robust security:* Text Message Banking is secure. Enrollment is completed within the user's password-protected Online Banking account. During their Online Banking session, users receive, via text, a one-time activation code.
- *Alerts:* Low balance alerts and account alerts help increase profit per user and reduce call volume by keeping users informed of key banking-related events.



# Text Message Banking: Enrollment and Management

## Overview

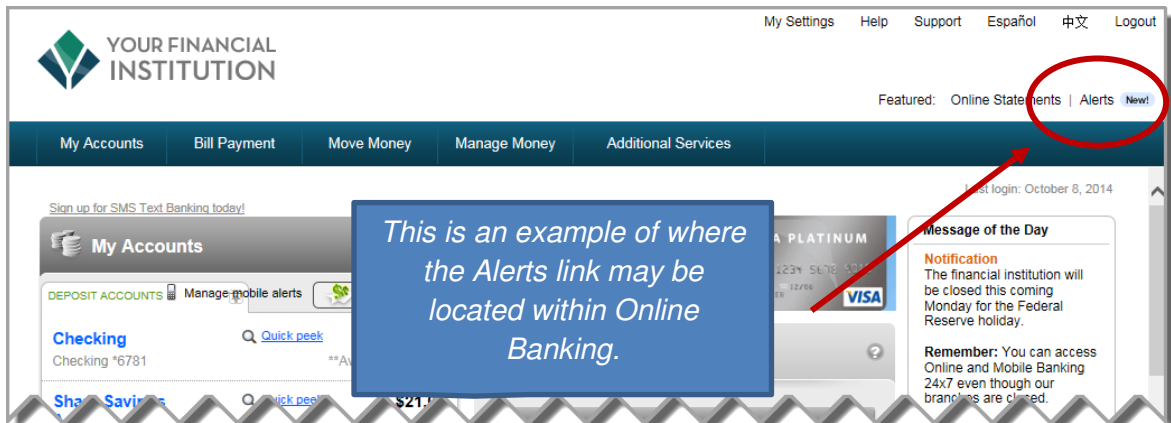
Enrollment for Text Message Banking is fully integrated within the Alerts area of Online Banking. Text Message Banking enrollment is a quick three-step process that typically takes just a few minutes to complete.

### In this section:

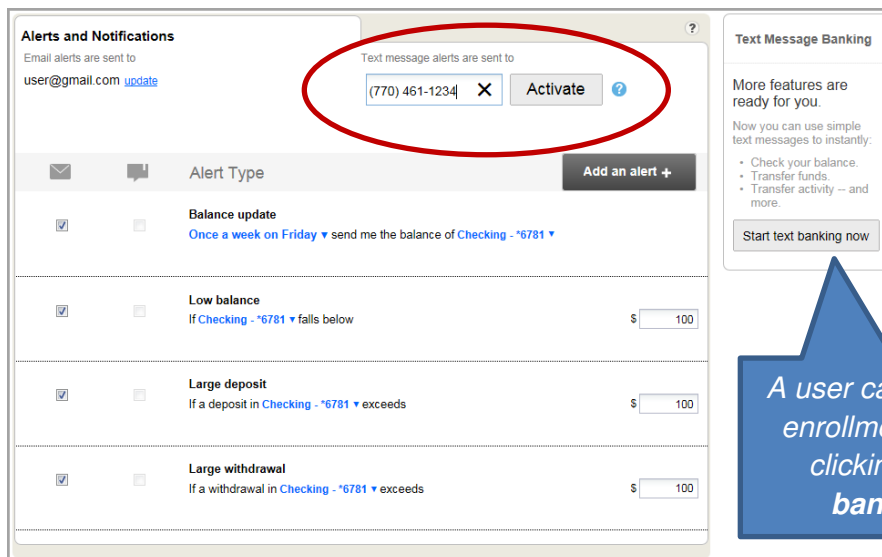
- Enrollment
- Managing

## Description

1. To enroll in Text Message Banking, users simply log into Online Banking and navigate to the Alerts link. Users must have their mobile device in their possession in order to complete the enrollment process.



2. On the Alerts and Notifications screen enter the phone number of the mobile device and click **Activate**.



3. The

user will receive an activation code on their mobile device and will be asked to enter that code on the pop-up screen.

*[FI branding tag]  
Code: #####  
Text HELP for help or call ###-###-####.  
Msg&data rates may apply. Msg freq  
based on settings.*

*This is an example of the  
activation code text that  
is sent to a user.*

**Set up (770) 461-1234 for text** ×

Within a minute, you'll receive a verification code by text

[Send it again](#)

When you receive it, just type it in

**Verify** **Cancel**

*The user can click  
**Send it again** if  
another code needs to  
be sent.*

*Once the activation code is entered the user clicks  
**Verify**. If the activation was successful the mobile phone  
will receive an activation success message.*

- The activated phone number is now set up and can be managed from the main Alerts and Notifications screen. Up to two mobile phones and one email address can be set up to receive texts.

*The email address associated with this account is listed and can be managed here.*

*An additional mobile number can be added by clicking **Change or add number**.*

*A summary of the "pull" text commands are available.*

**Alerts and Notifications**

Email alerts are sent to  
user@gmail.com [update](#)

Text message alerts are sent to  
(770) 461-1234  
[Change or add number](#)

**Text Message Banking**

Activated numbers  
(770) 461-1234  
[Add a second number](#)

Primary account ?  
Checking \*6781

Transfer account ?  
Transfers disabled

[Update](#)

**Text Commands**

Text the following commands to 454545

**BAL** Primary balance  
**LAST** Last 5 transactions  
**TRANS** Transfer funds to primary account  
**STOP** Deactivate service  
**HELP** Help keywords

Alert Type	Frequency	Amount
Balance update	Once a week on Friday	send me the balance of Checking - *6781
Low balance	If Checking - *6781 falls below	\$ 100
Large deposit	If a deposit in Checking - *6781 exceeds	\$ 100
Large withdrawal	If a withdrawal in Checking - *6781 exceeds	\$ 100

- Once a mobile phone number is activated, the column for that text message channel is activated as well. If there are two mobile numbers activated then there will be two columns for the text message channel.

**Alerts and Notifications**

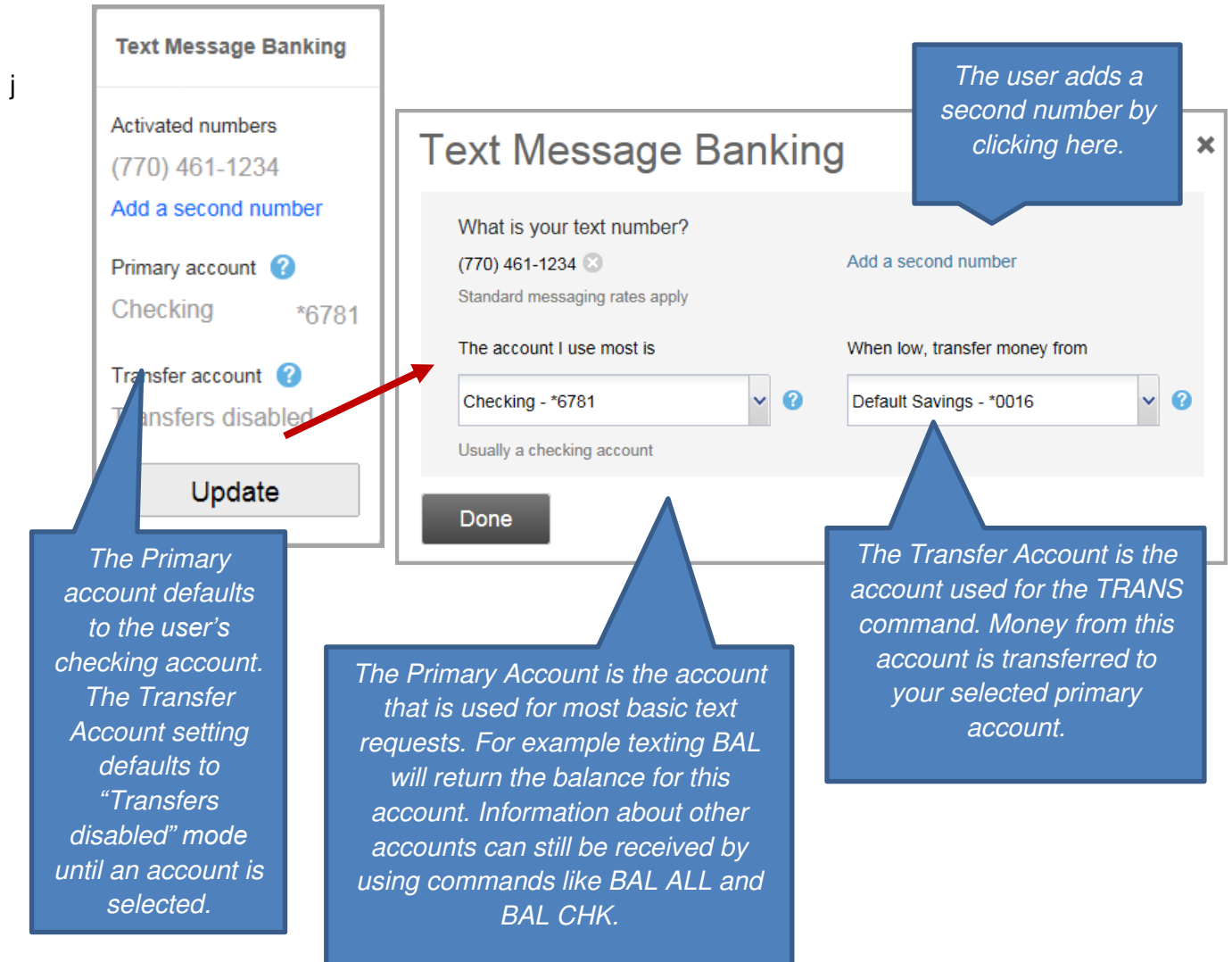
Email alerts are sent to  
firstname.lastname@email.com [update](#)

Text message alerts are sent to  
(415)555-1234  
(415)555-5678  
[Change numbers](#)

Alert Type	Frequency	Amount
Balance update	Once a week on Friday	send me the balance of checking *3243
Low balance	If Checking *7799 falls below	\$ 1500.00
Large withdraw	If a withdraw in Checking *7799 exceeds	\$ 500.00
Large deposit	If a deposit in Checking *7799 exceeds	\$ 500.00

6. The Text Message Banking area on the upper right corner of the Alerts and Notifications screen gives the user a quick glance at the following:
- Phone numbers set up for text message banking
  - The primary account to which text message commands will apply
  - The designated transfer account (source) for transfers made via Text Message Banking.

Click on **Update** to manage any of these settings.



The image shows two overlapping screenshots of the 'Text Message Banking' settings screen. The left screenshot shows the summary view with an 'Update' button. The right screenshot shows the configuration form with callouts explaining the 'Primary account' and 'Transfer account' settings. A red arrow points from the 'Update' button in the left screenshot to the configuration form in the right screenshot.

**Text Message Banking**

Activated numbers  
(770) 461-1234  
[Add a second number](#)

Primary account ?  
Checking \*6781

Transfer account ?  
Transfers disabled

**Update**

**Text Message Banking**

What is your text number?  
(770) 461-1234 ✕  
Standard messaging rates apply

Add a second number

The account I use most is  
Checking - \*6781 ?

When low, transfer money from  
Default Savings - \*0016 ?

Usually a checking account

**Done**

*The user adds a second number by clicking here.*

*The Primary account defaults to the user's checking account. The Transfer Account setting defaults to "Transfers disabled" mode until an account is selected.*

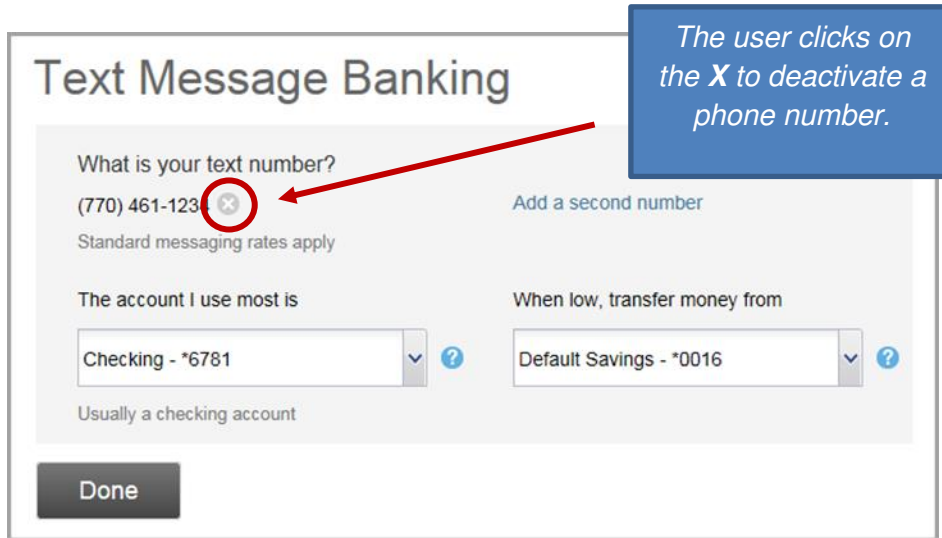
*The Primary Account is the account that is used for most basic text requests. For example texting BAL will return the balance for this account. Information about other accounts can still be received by using commands like BAL ALL and BAL CHK.*

*The Transfer Account is the account used for the TRANS command. Money from this account is transferred to your selected primary account.*



7. If a user wants to no longer receive text message on a particular phone number they must click the X to the right of the phone number on the Text Message Banking pop-up. They are prompted to confirm this action. In addition a text is sent to the deactivated phone number with a deactivation successful message.

Once a phone number is deactivated it will no longer show up on the main Alerts and Notifications screen. The text message column associated with that phone number will be in a deactivated mode.



*The user clicks on the X to deactivate a phone number.*

*This is an example of the deactivation text that is sent.*

*[FI branding tag]  
Deactivation successful. You will no longer receive txt message banking msgs. Go to [website] to reactivate.*

# Text Message Banking: Setting Up and Receiving Alerts

## Overview

Text Message Banking supports two types of alerts.

- Push alerts are set up and sent to a user when an activity happens or when the notification is scheduled to be sent.
- Pull alerts are requests made by the user to receive immediate information or perform an activity in real time.

### In this section:

- Push Alerts
- Pull Alerts

## Description

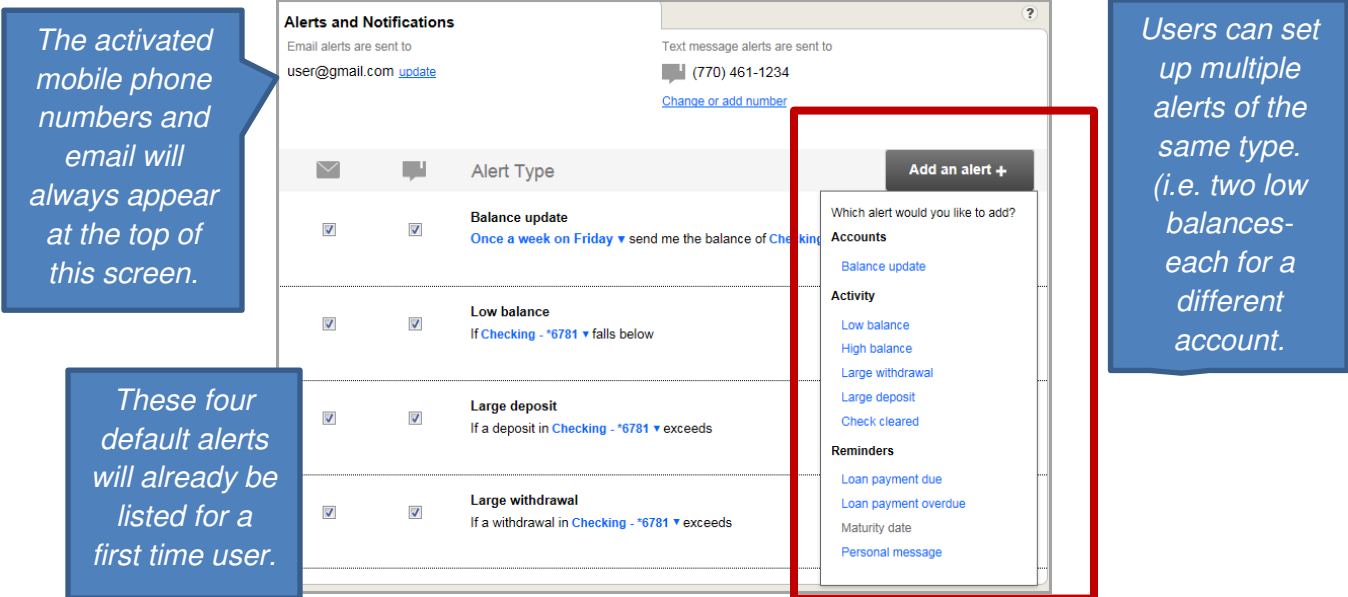
### Push Alerts

Users can receive a text message for the following actionable or scheduled alerts (some alerts are core processor dependent):

Alert	Functionality
Balance Update	This alert provides regular updates on the account balance of a chosen account. It sends the account balance according to the selected frequency.
High Balance	Sends an alert when account balance is at or above threshold.
Low Balance	Sends an alert when account balance is at or below the threshold. Threshold can be set to 0.
Large Deposit	Alerts is sent whenever there are deposit transactions with amounts equal to or above the user-specified threshold.
Large Withdrawal	Alert is sent whenever there are withdrawal transactions with amounts equal to or above the user-specified threshold.
Loan Payment Due	This alert lets users know when a loan payment is coming due.
Loan Payment Overdue	This alert lets users know when a loan payment is overdue. The alert will be sent when the payment date is past and the loan balance has not changed.
Maturity Date	This alert lets users know when their investment accounts are maturing so they can take action on the account.
Check Cleared	Alert is sent when the specified check number has cleared the account.
Personal Message	Sends the user a specified message according to the selected frequency.

*\*Note: Balance Update and Personal Reminder alerts are sent between 8-10 a.m. on the day scheduled. All other alerts are processed three times a day, 8 a.m., 12 p.m. and 4 p.m. (local to the financial institution).*

- To add a new alert, the user clicks **Add an alert** on the Alerts and Notification page within Online Banking. A list of the available alerts appears and the user clicks on the alert to add.



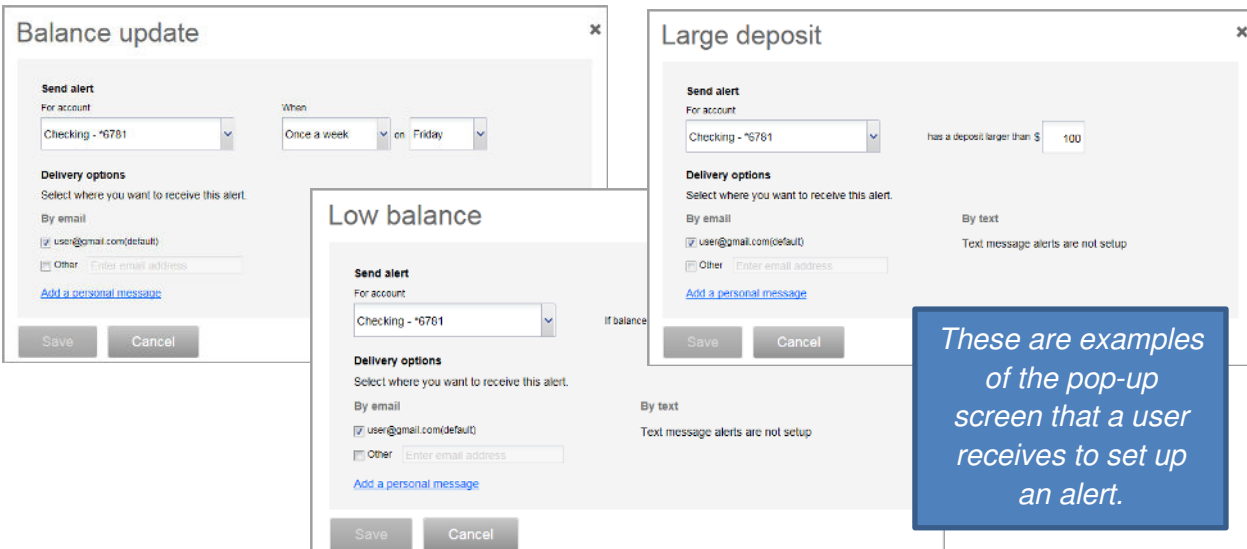
*The activated mobile phone numbers and email will always appear at the top of this screen.*

*Users can set up multiple alerts of the same type. (i.e. two low balances- each for a different account.)*

*These four default alerts will already be listed for a first time user.*

- Each alert supports certain configuration options depending on that alert.

- Alerts can be configured to go to specific channels by checking and un-checking the individual delivery channels that have been set up (text or email).
- Different accounts can be chosen by clicking the account menu and choosing the appropriate account.
- Different schedule recurrences can be chosen by clicking on the schedule links to show the list of available recurrence types.
- Thresholds and other input can be changed directly in the text boxes.
- A personal message can be added. Note- personal messages are only included in notifications set as an email.



*These are examples of the pop-up screen that a user receives to set up an alert.*

- Once an alert is set up it will appear immediately on the main Alerts and Notification page. An alert can be edited by clicking **More Options** or deleted by clicking **Remove**. These links become visible when the mouse hovers on that alert.

The screenshot shows the 'Alerts and Notifications' page. At the top, it displays contact information for email alerts (user@gmail.com) and text message alerts ((770) 461-1234). Below this is a table of alerts with columns for delivery method (email and text) and alert type. The 'Alert Type' column includes 'Balance update', 'Low balance', 'Large deposit', and 'Large withdrawal'. Each alert has a threshold value of \$100. A red circle highlights the 'More Options' and 'Remove' links for the 'Low balance' alert. Two blue callout boxes provide additional context: one on the left explains that delivery options are managed directly from this screen, and one at the bottom right explains that thresholds are managed directly on this screen.

*Options for text or email delivery are managed directly from this screen.*

*Thresholds are managed directly on this screen.*

## Pull Alerts

Users have the option of sending commands to a Digital Insight provided short-code in order to receive an immediate answer via text message. These commands include:

Command	Definition
• BAL	Primary account balance
• BAL ALL	All account balances
• LAST	Last 5 transactions from the primary account
• BAL CHK	Balances of all checking accounts
• BAL SAV	Balances of all savings accounts
• STOP	Un-enroll from the service
• HELP	Get information on commands and the financial institution's phone number.
• TRANS	Transfer from a source account to the primary account

*\*Note: The primary account and the transfer accounts mentioned above are managed from within Online Banking in the Alerts & Notifications area.*

For example, the user texts "BAL ALL" to the financial institution's short code they will receive all of their active account balances. An example is what they might see is below:

### Financial Institution Banking:

**CHKG12 x442 \$10091.55**

**CHKG12 x4271 \$2991.32**

**SAVG4 x639 \$2891**

**ORTG x358 \$199848**

**Reply STOP to cancel**

*The account number is truncated in all messages.*

**\*\*Roadmap Preview: Financial institutions will have the option of having their own customized short codes instead of using Digital Insight's universal short code. This feature is currently on the Roadmap. This feature will be provided for a monthly fee.**

## Configuration Options: Text Message Banking

**Current Balance or Available Balance Used for Alerts:** Financial institutions are able to designate whether the current balance or the available balance is used for the low balance, high balance or balance update alerts. The financial institution needs to contact Customer Care at 877-462-3446 or go to **Admin Platform>MySupport** to submit a ticket.

## Record of changes for the Mobile Banking Product Guide

Date	Changes/Additions Made
Feb 2015	1. Changes reflect Jan 2015 Roadmap <ul style="list-style-type: none"> <li>• Remote Deposit Check History (Roadmap Preview)</li> <li>• Create Your Own Page (Roadmap Preview)</li> <li>• Remote Deposit for Android (Roadmap Preview)</li> <li>• Mandatory Password Change (Roadmap Preview)</li> <li>• Secure Support Email (Roadmap Preview)</li> <li>• Spanish Language (Roadmap Preview)</li> </ul>
June 2015	1. Changes reflect CMA 4.5 release <ul style="list-style-type: none"> <li>• Touch ID</li> <li>• The ability to view RDC history for tablets in the Fall of 2015</li> <li>• Temporary Password Reset</li> </ul> 2. Changes reflect the April 2015 Roadmap <ul style="list-style-type: none"> <li>• Eyeprint ID (Roadmap Preview)</li> <li>• Quick Balance (Roadmap Preview)</li> </ul>
August 2015	1. Changes reflect MWB 2.7.4 <ul style="list-style-type: none"> <li>• Loan accounts show min amt due and due date on Account Summary screen</li> <li>• Delivery By date showing in BP for FIS Process Date only.</li> </ul>
November 2015	1. Changes reflect CMA release 4.6.3 <ul style="list-style-type: none"> <li>• Touch ID enhancements</li> <li>• Alternative Login Credential control in AP</li> <li>• Message Center</li> </ul> 2. Change reflects MWB 2.7.5- Intra-institution transfers supported. 3. Changes reflect Oct 2015 Roadmap
December 2015	1. Changes reflect CMA release 5.0 <ul style="list-style-type: none"> <li>• Branded Login Page</li> <li>• Added Quick Balance</li> <li>• Navigation controlled via AP</li> <li>• Added Registration section- more detail</li> </ul>
February 2016	1. Changes reflect the CMA release 5.1.0 <ul style="list-style-type: none"> <li>• Android fingerprint feature</li> </ul> 2. Changes reflect Jan 2016 Roadmap <ul style="list-style-type: none"> <li>• Adjustments to items moved to Roadmap from Horizon</li> <li>• Added extensive info regarding Eyeprint ID</li> </ul> 3. Added Smartwatch module