

SecurLOCK™ Equip - Mobile App Procedures

July 2018

Empowering
the Financial World



SecurLOCK™ Equip – Mobile App Procedures

Introduction

- **Install application**
- **Register user**
- **Reset password**
- **Home screen**
- **View card details**
- **View transactions**
- **Set up control preferences**
- **Set up alert preferences**
- **Home Screen - Main menu options**

SecurLOCK™ Equip – Mobile App Procedures Objectives

- **Describe the basic functions of the SecurLOCK Equip Mobile Application.**
- **Identify how to perform multiple SecurLOCK Equip procedures from a user's viewpoint.**
- **Identify how a cardholder can use the application to contact her/his financial institution to provide feedback on the application or make a request for support.**

Communicate vs. Equip Quick Comparison

SecurLOCK™ Communicate

What is it?

SMS/E-mail auto case resolution features generated to consumers as a result of fraud alerts

How Does it Work?

- **Contact sent to cardholders via:**
 - 2-way SMS text alerts with an opt out (free to end user)
 - Interactive voice calls
 - 2-way e-mail alerts
 - Auto case resolution
- **Cardholder inbound calls:**
 - ANTI Spoofing detection to identify fraudulent callers and alert created

What are the Benefits?

- Stop fraud through real-time card engagement
- Create consumer loyalty

SecurLOCK Equip

What is it?

Gives your consumers the ability to control their own card settings with In-App Controls

How Does it Work?

- **Consumer's have access to:**
 - Switch card on/off
 - Set transaction size & type limits
 - Merchant control
 - Control by location
 - Instant transaction alerts
 - **Meets Visa/MC Mandates (Oct 2016)**

What are the Benefits?

- Reduce Fraud
- Create consumer loyalty
- Easy Deployment
- Admin access to manage tool

Communicate vs. Equip Quick Comparison

- SecurLOCK Communicate is connected to Falcon.
- SecurLOCK Equip is not integrated to Falcon or your core banking system.

Marketing Website Link

http://tools.cardholderadoption.com/SecurLOCK_Equip

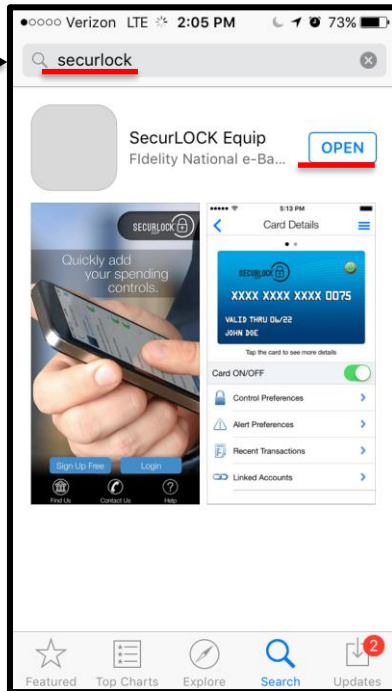
- Use the link above to access:
 - Marketing material
 - This training guide/deck
 - Frequently Asked Questions
 - How “My Regions” and “My Location” differ in detail

Install Application

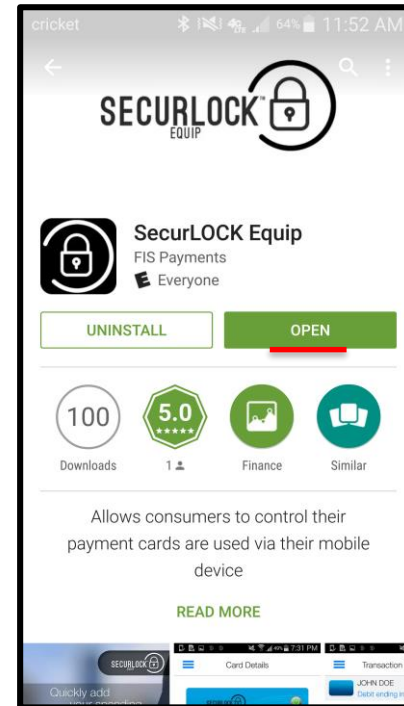
Start – Download the Application

Apple

Enter →



Android



- A cardholder will download the app from Apple thru the App Store or with Android thru the Play Store.
- The app can be used domestically and internationally. It can be downloaded within the US and US Territories and the following select countries: Venezuela, Colombia, Dominican Republic and Argentina.

Install Application

Start – iPhone Example



- A user with an iOS phone will need to access App Store to search for the SecurLOCK™ Equip App, download and install it.
- In this iPhone example, a grey spring board application icon will appear on the phone with an empty loading bar as the phone is “Waiting” to download the application.

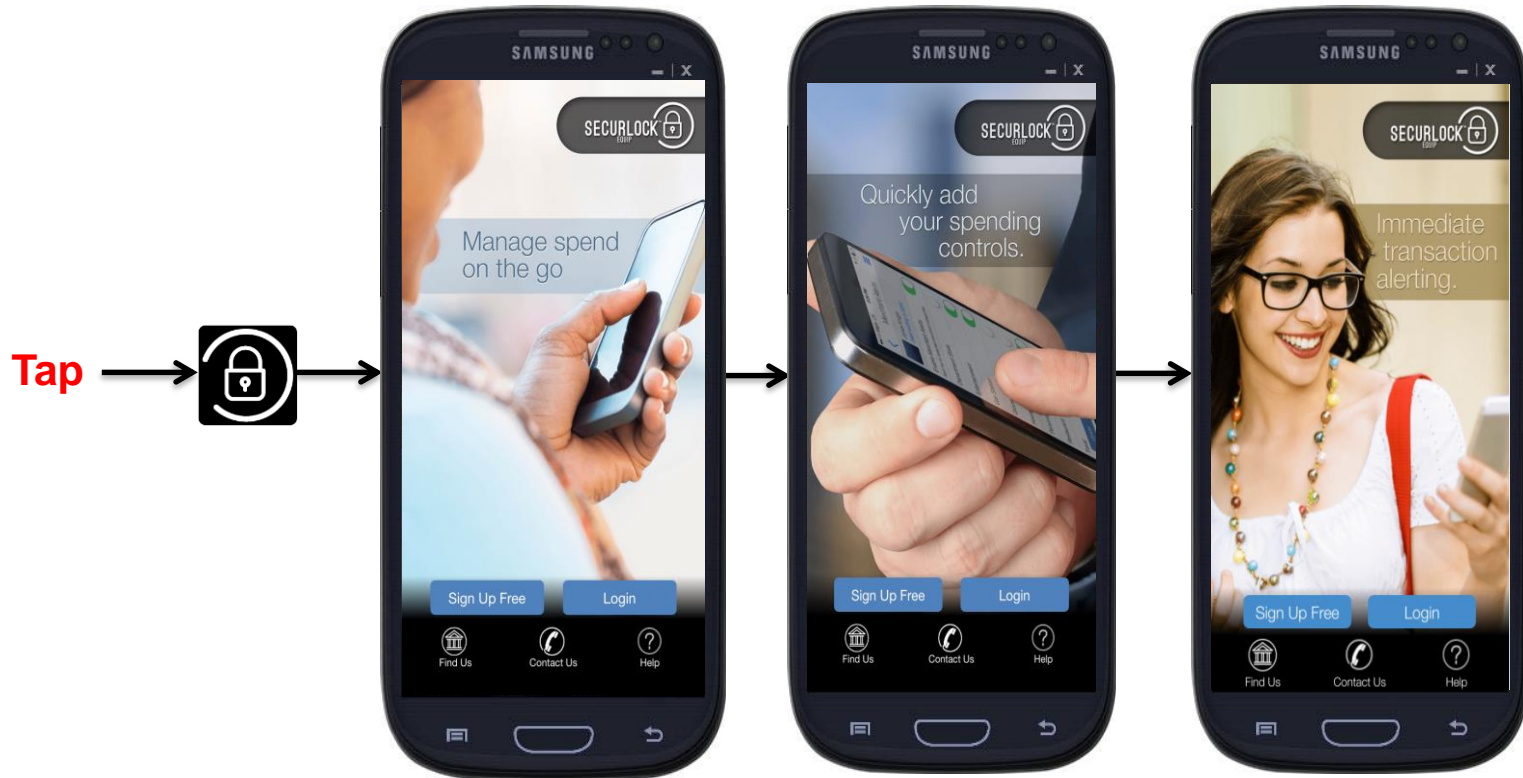
Install Application

Start – Android Example



- A user with an Android phone will need to access the Play Store to search for the SecurLOCK Equip app, download and install it.
- In this Android example, as the phone downloads the app, the word at the bottom of the spring board icon will change to “Installing” and the loading bar will fill.

Register User Launch App



- Once completely downloaded, the spring board icon will appear in the same brightness as all other spring board icons.
- Tap on the “App” icon to launch the app.
- A series of animation screens will appear.

Register User

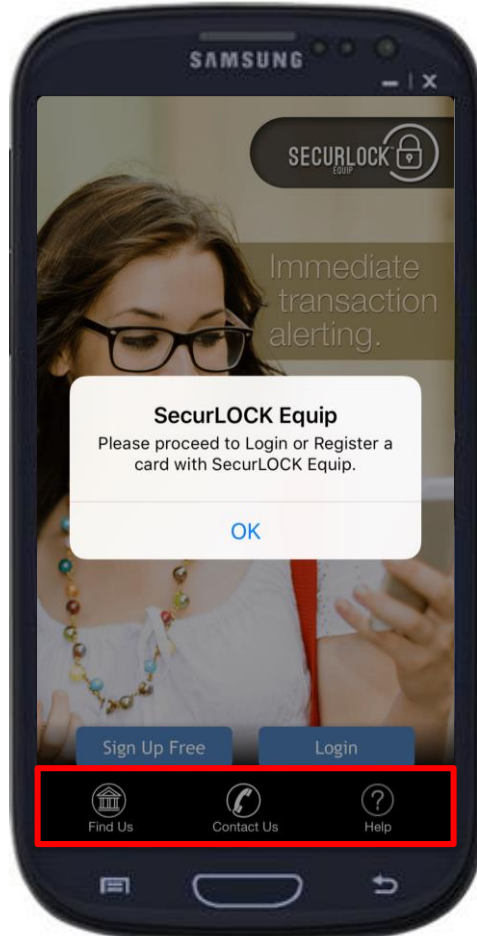
User Options

- **Upon opening the application, the user is provided with options to:**
 - Register as a new user (Sign Up Free)
 - Login to the application (if the user already has a login).



Register User

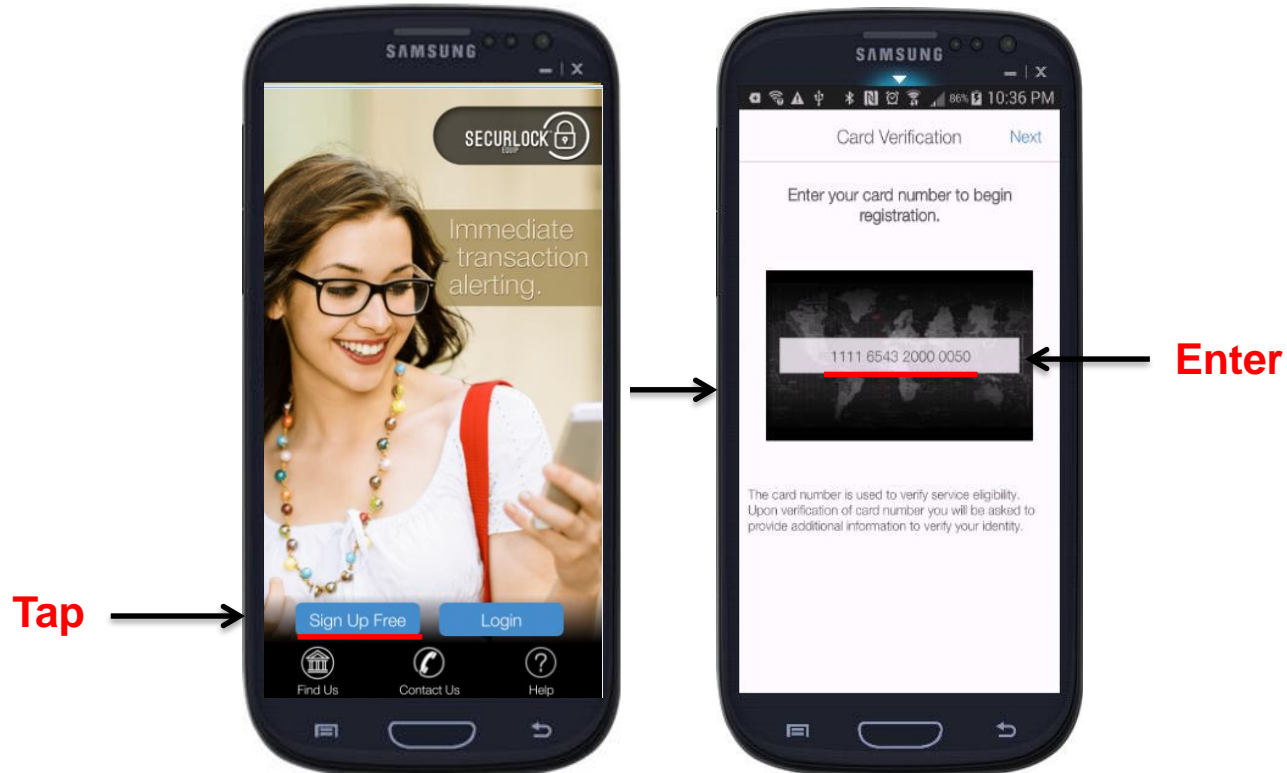
User Options



- **The bottom menu options allows registered users to:**
 - Find the Financial Institution ATMs/locations.
 - Contact her/his financial institution.
 - Get help on the app usage.
 - ☐ Help is a text document that covers all major functions of the application.
 - ☐ If Find Us and/or Contact Us data is not added to mConsole during implementations, then the corresponding icon will not display or be available in the app.
 - If the user selects one of these options before registering, an informal message will display.

Register User

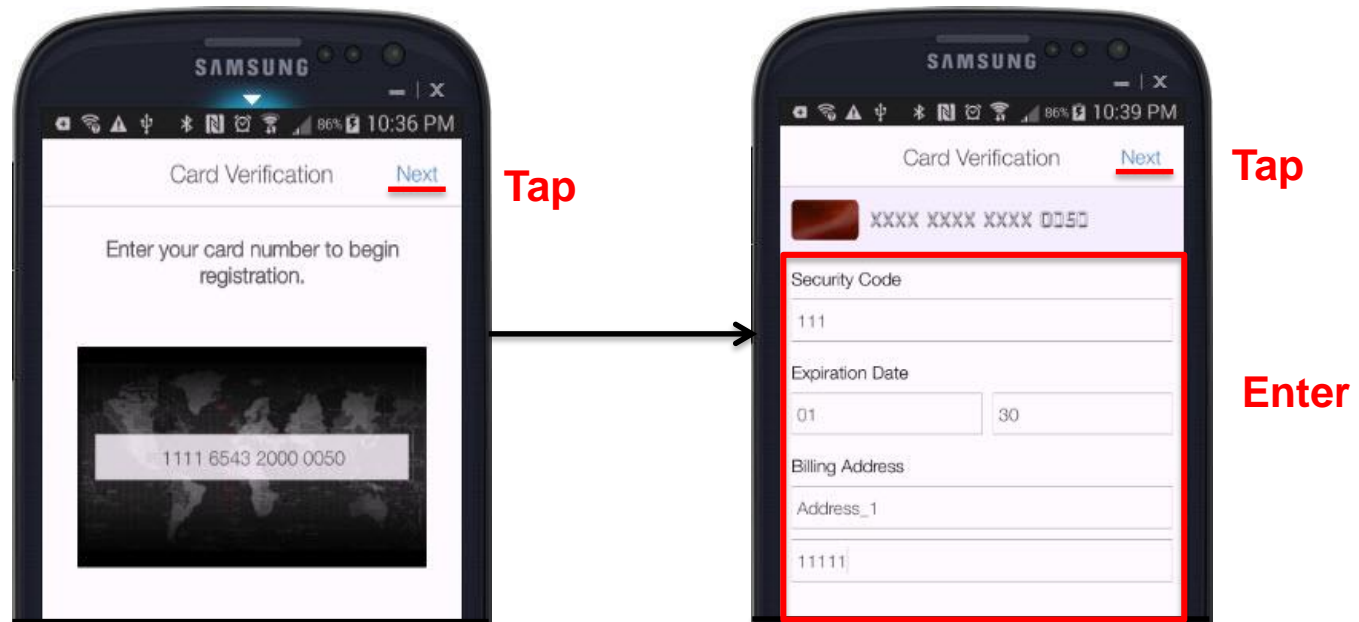
User Authentication



- To use the SecurLOCK™ Equip app, a cardholder must first register at least one card.
- Tapping on “Sign Up Free” button will start the registration process.
- The cardholder is prompted to enter her/his card number.
- Multiple users can register the same card number.

Register User

User Authentication (First Factor)



- After entering the card number, the user taps “Next” in upper right corner.
- The user is brought to the First Factor Authentication (FFA) page:
 - Security code (MasterCard[®] - CVC2 / Visa[®] - CVV2).
 - Expiration date (MM/YY).
 - Billing address (street address and zip code).
- After completing the FFA, the user taps “Next” in the upper right corner to go to Second Factor Authentication (SFA).

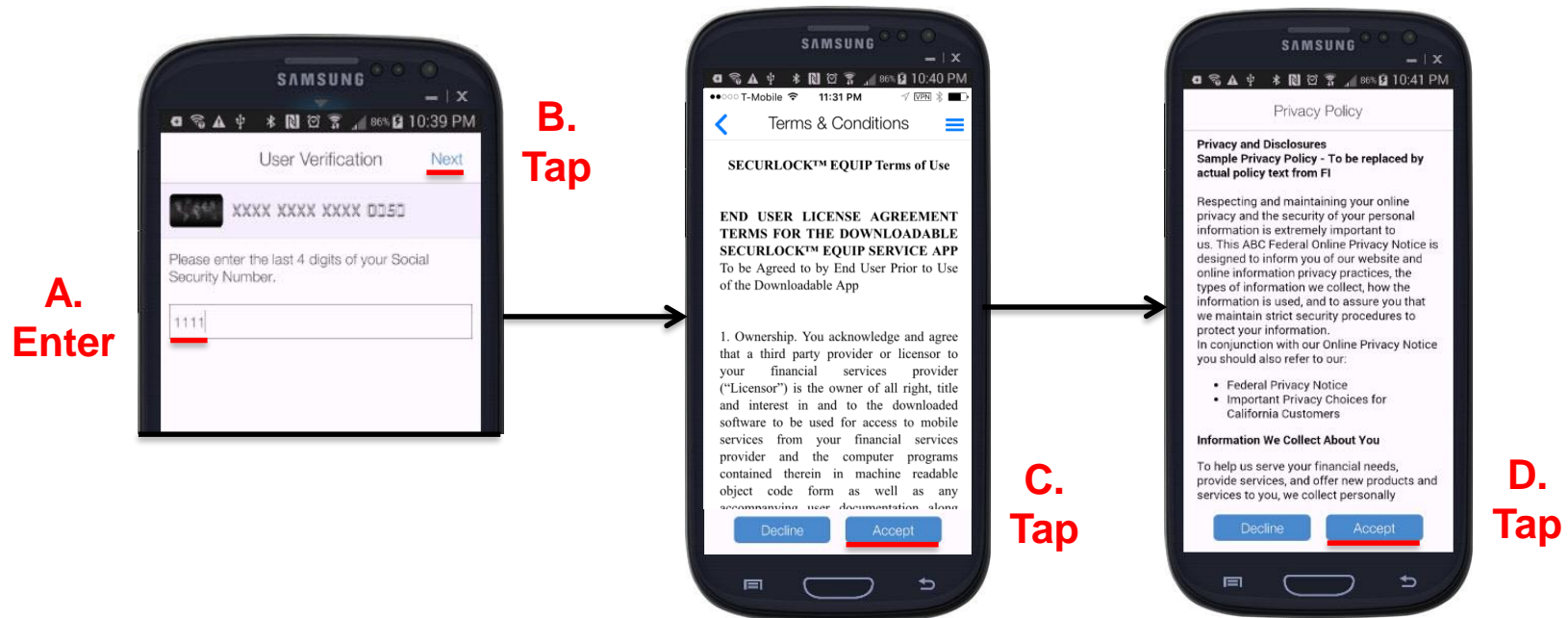
Register User

User Authentication (Second Factor)

- **Depending upon what information is returned from the system of record, SecurLOCK Equip SFA will present one of the following options:**
 - Norcross – Last 4 digits of the Social Security Number > Phone number.
 - BCFS – Last 4 digits of the Social Security Number or Date of birth.
 - St. Pete Debit – Last 4 digits of the Social Security Number or Date of birth > Phone number.
 - All credit cards – Last 4 digits of the Social Security Number or Date of birth > Mother's maiden name.
 - FISB - Last 4 digits of the Social Security Number or Date of birth.

Register User

User Authentication – Social Security Number Verification (Second Factor Authentication)



- After entering the SSN and tapping “Next”, the data is validated. After a successful validation, the user will be taken to the next two pages to accept the Terms & Conditions (FIS) and Privacy Policy (FI).
- If the data validation fails, the user will be prompted to enter the last four digits of the SSN again.

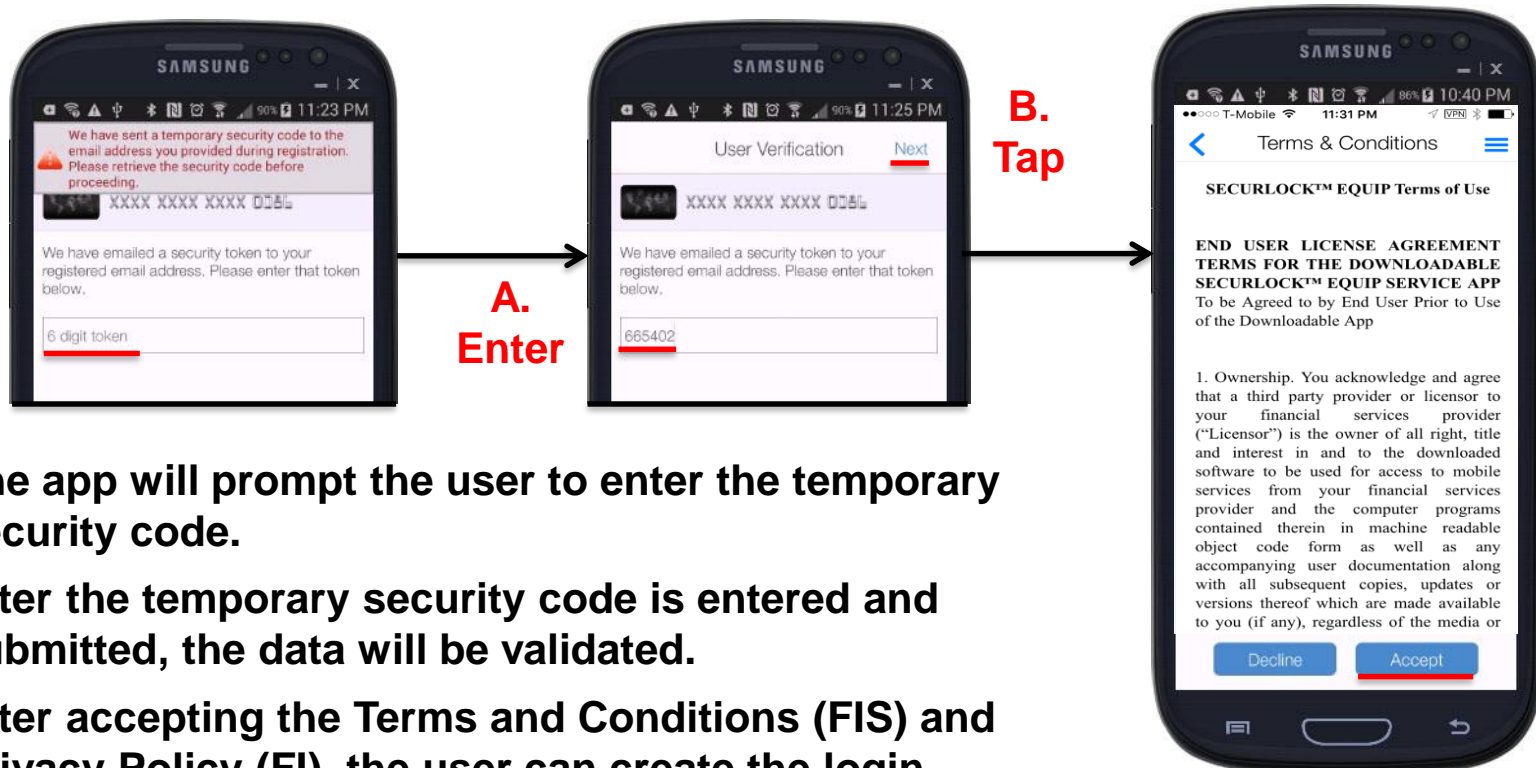
Register User

User Authentication – Security Code Verification (Second Factor Authentication)

- The Security Code authentication method will be used if criteria listed in Slide 15 is not available or SFA failed.
- If the user's email address is passed on to the SecurLOCK Equip application, the user will be sent an email with a temporary security code (see Slide #18).
- If an email is not available, then the “PIN-Based” transaction option should be used for debit card enrollment (see Slide #19).
- If it is a credit card, the cardholder will receive a message to contact their financial institution to update the cardholder's record.

Register User

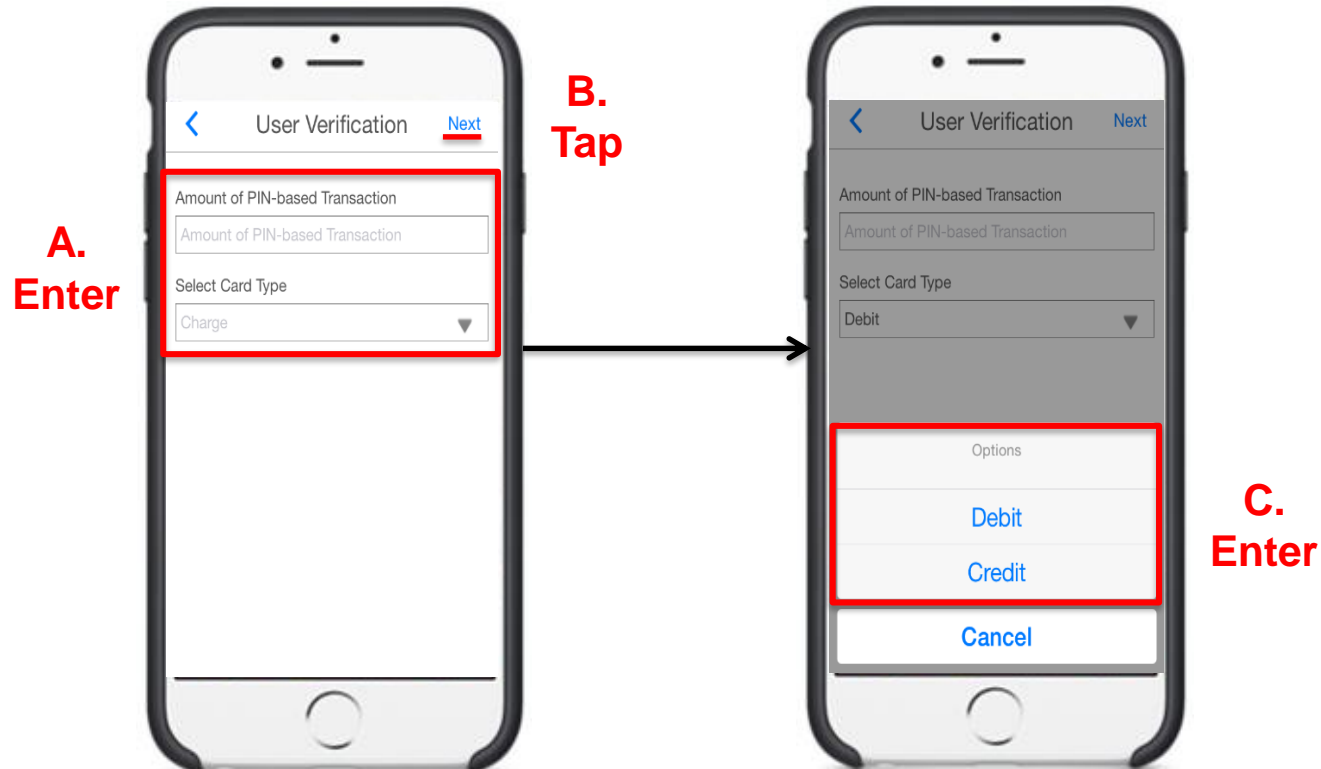
User Authentication – Security Code Verification (Second Factor Authentication)



- The app will prompt the user to enter the temporary security code.
- After the temporary security code is entered and submitted, the data will be validated.
- After accepting the Terms and Conditions (FIS) and Privacy Policy (FI), the user can create the login credentials.

Register User

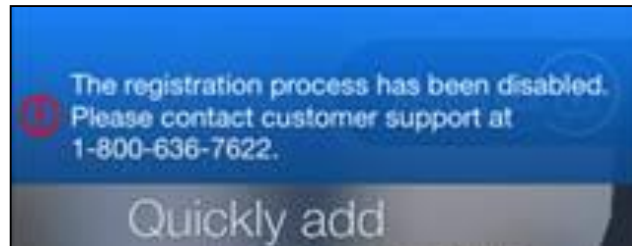
User Authentication- PIN-based Verification (Debit Cards Only) (Second Factor Authentication)



- The user must complete a new PIN-based transaction for any dollar amount within 72-hours of the attempted registration for validation purposes.

Register User

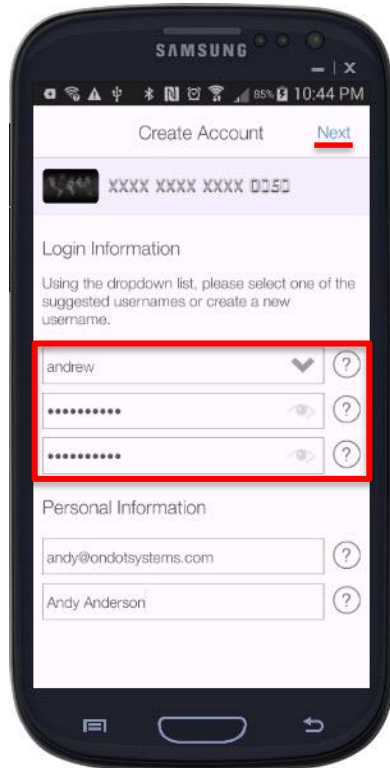
User Authentication - Unsuccessful Attempts



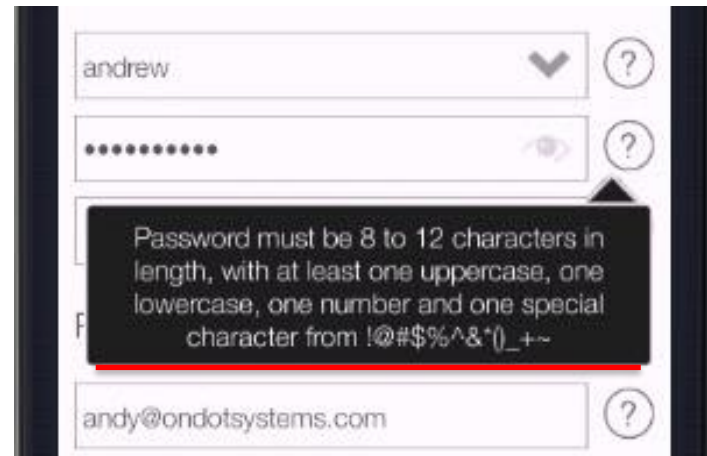
- Pictured above is the error message received when a user has made 3 unsuccessful registration attempts by either inputting the card number incorrectly or failing FFA.
- After three failed attempts, the user will be suspended from being able to register the card for the next 30 minutes.
- Once the suspension period expires, the user can attempt to register again; three more failed attempts will suspend the card again.
- The user can also call the financial institution's customer support group to have the card registration state reset (covered in mConsole training).
- If the card registration state is reset, the user can attempt to register again without having to wait for 30 minutes.
- The app will not indicate which field(s) was in error for security reasons.
- **SFA Failure – After three failed attempts the user will be suspended and brought back to the landing page. The only way to unlock the app is for the user to call into Customer Support to have the card registration state reset (covered in mConsole training).**

Register User

User Account Creation – Login Information



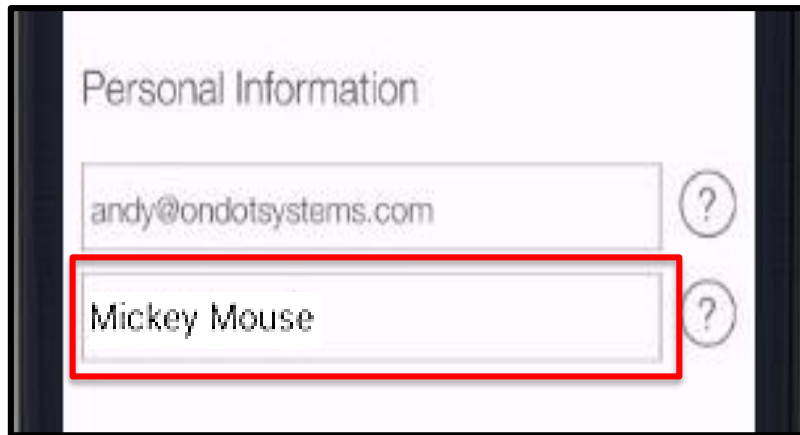
Tap



- On the Create Account screen, the user creates a Login and Password for logging into the app.
- Note that the system will make several recommendations for a Login based on a combination of the user's first and last name, or the user can create one.
- All Logins are stored in the same database so each one must be unique.
- The ? icons are informational and will be found throughout the app. Displayed above are the requirements for the Password.

Register User

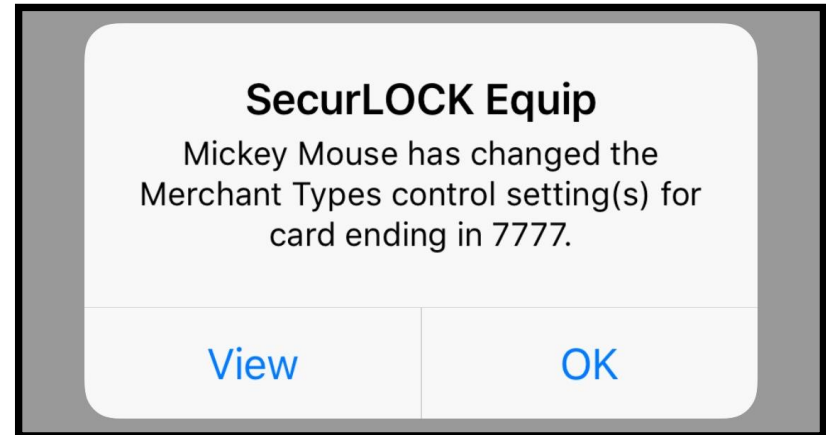
User Account Creation – Personal Information



Personal Information

andy@ondotsystems.com ?

Mickey Mouse ?



SecurLOCK Equip

Mickey Mouse has changed the
Merchant Types control setting(s) for
card ending in 7777.

View OK

- The email address entered here will be used for password resets. It **does not** go back to the system of record.
- The name entered here will be stored in mConsole and used for Notifications.
- Notifications are used if the same card number is shared with other users (covered later in this training).

Register User

User Account Creation



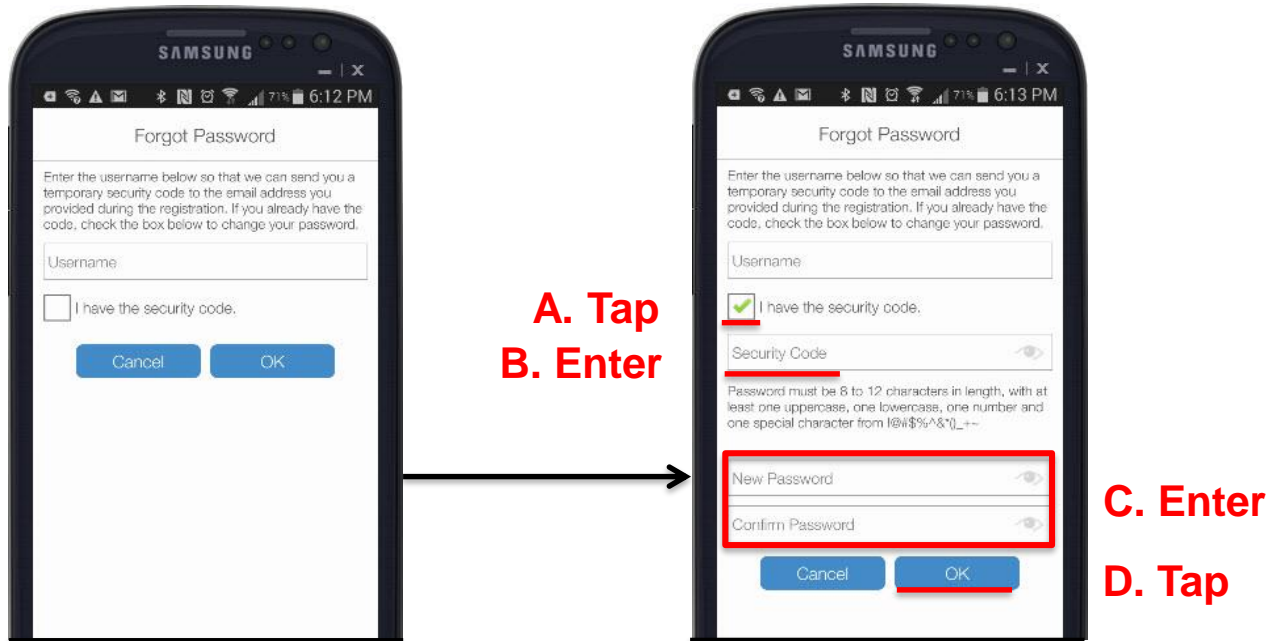
- After the user enters the personal information, the app will display a confirmation message.
- Tapping on “OK” will take the user to the Login page to login with their newly created credentials.

Reset Password Procedure – Request a New Password



- Tapping on the “Forgot Password?” link on the Login page will cause the Forgot Password page to display.
- The user enters his/her username and taps “OK” to have a security code sent to the email address s/he entered during registration.

Reset Password Procedure – Select New Password



- The user needs to check her/his email to retrieve the security code sent, then check the box “I have the security code” on the Forgot Password page.
- The user will be prompted to enter the security code, choose and confirm a new password, then select the OK button to proceed.
- The Security Code is valid for 30 minutes.

Reset Password

Password vs Passcode

Password (PW) - to login to the app, a user will need to enter the credentials (username and password). By logging in with the username and password, the app will create a session ID (20-minutes) where the user can remain idle and still be logged into the app. If the user closes the app and then reopens the app (within the 20-minutes session time), the app will just open. No password will be required.

Passcode (PC) - is an additional security setting provided by the app. If a user sets a passcode, each time the user navigates away from the app and comes back, the user will need to enter the passcode.

- The PW and PC never expire.
- The PW and PC values can be the same.

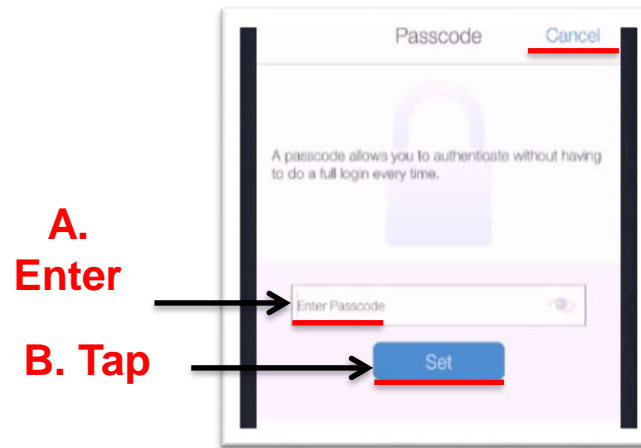
Reset Password

Password vs Passcode – Timing Scenarios

- **Timing Scenario #1**
 - Passcode enabled = Yes
 - Cardholder closes the application, but does NOT log out.
 - Cardholder re-opens the app and s/he will be prompted for the Touch ID/PC.
 - Result = this open app session will last for 30 days. Every 30-days the user will be prompted to enter her/his User ID and Password.
 - If there is a server outage, the user will need to re-authenticate by entering the Login and Password.
- **Timing Scenario #2**
 - Passcode enabled = No
 - Cardholder closes the application
 - Cardholder re-opens the app within 20 minutes of closing it
 - Result = the cardholder goes directly back to the app; if more than 20 minutes have elapsed, the cardholder must enter the Login and Password.
- **Note: A PC must be set in order to use Touch ID on an iPhone.**

Reset Password

Procedure - Set Passcode



- When logging in to a new device for the first time, the user will be asked to set a Passcode.
- A Passcode must have a minimum of four alphanumeric characters.
- Passcode setting at this stage is optional. The user can choose not to set the Passcode by clicking the “Cancel” button.
- A Passcode can be set anytime via **Settings > Personal Information** (covered later in this module).

Reset Password Procedure - Set Passcode



- The user can assign a Touch ID (or Face ID for X) to the Passcode if s/he is using an iPhone 5S and above. Touch ID allows the user to access the app using a fingerprint.
- When navigating away from the app and then coming back, the app will prompt the user to enter the Touch ID or Passcode.
- If the user enters the wrong passcode 3 times, s/he will be logged out of the app. At that point, the user will have to login with the Login name and Password.
- Upon successful login, the user can set up a new Passcode again and Touch ID.

Card Details Screen

General Information

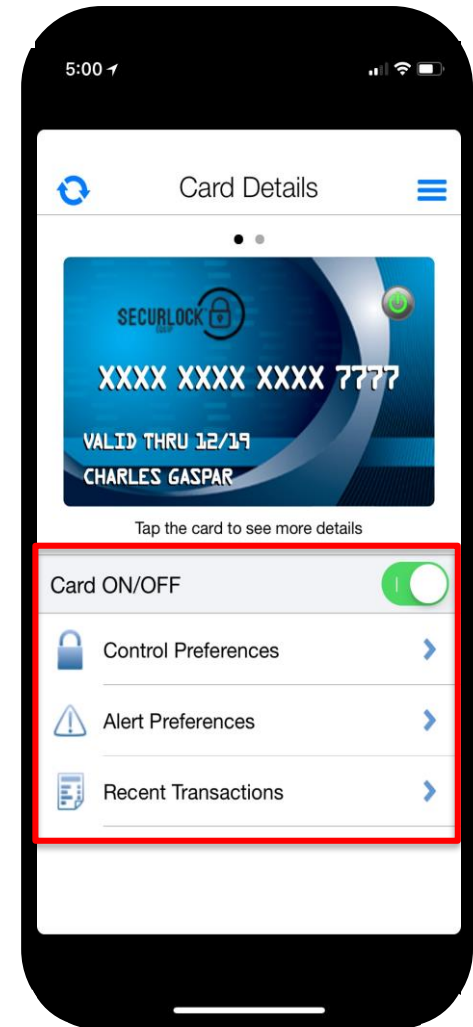


- The Card Details screen is the landing page once a user logs into the application. It shows the following information:
 - The Refresh (two circular arrows) and “Hamburger” Menu (three blue bars) icons
 - The menu will be upper right for iPhones, upper left for Android
 - The dots represent additional cards
 - An image of the card
 - Card status (green = ON, red = OFF).
 - Last 4-digits of the card
 - Expiration Date
 - Customer's name
 - Card On/Off
 - Preferences
 - Transactions

View Card Details

Front of Card

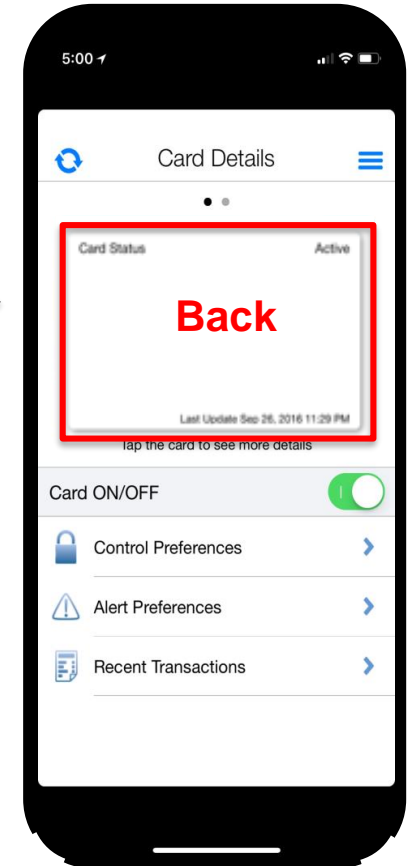
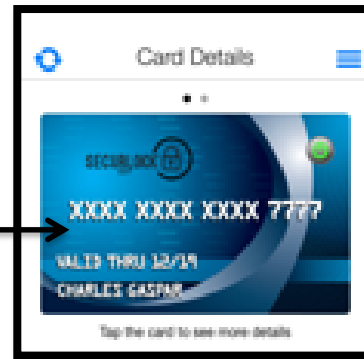
- To turn a card “On” or “Off”, the user taps on the “Card ON/OFF” slider. When a card is turned off, any transactions made on the card (other than recurring transactions and credits/deposits) will be denied.
- Tapping “Control Preferences” takes the user to the Control Preferences page.
- Tapping “Alert Preferences” takes the user to the Alert Preferences page.
- Tapping “Recent Transactions” takes the user to the transactions page, where the user can view transactions made on the card.
- The card’s expiration date is automatically updated when a new card is re-issued.
- If a card is reported as lost/stolen the new card would need to be added into the application by the user.



View Card Details

Back of Card

Tap



- The card image will rotate when tapped. The back of the card has additional card details:
 - Card status (based on actual card status from the system of record, not controls).
 - Last update time (cardholder's time zone).
 - Tap the card image again and the card will rotate back to the front.
- Swiping the card image from right to left will display any additional cards.

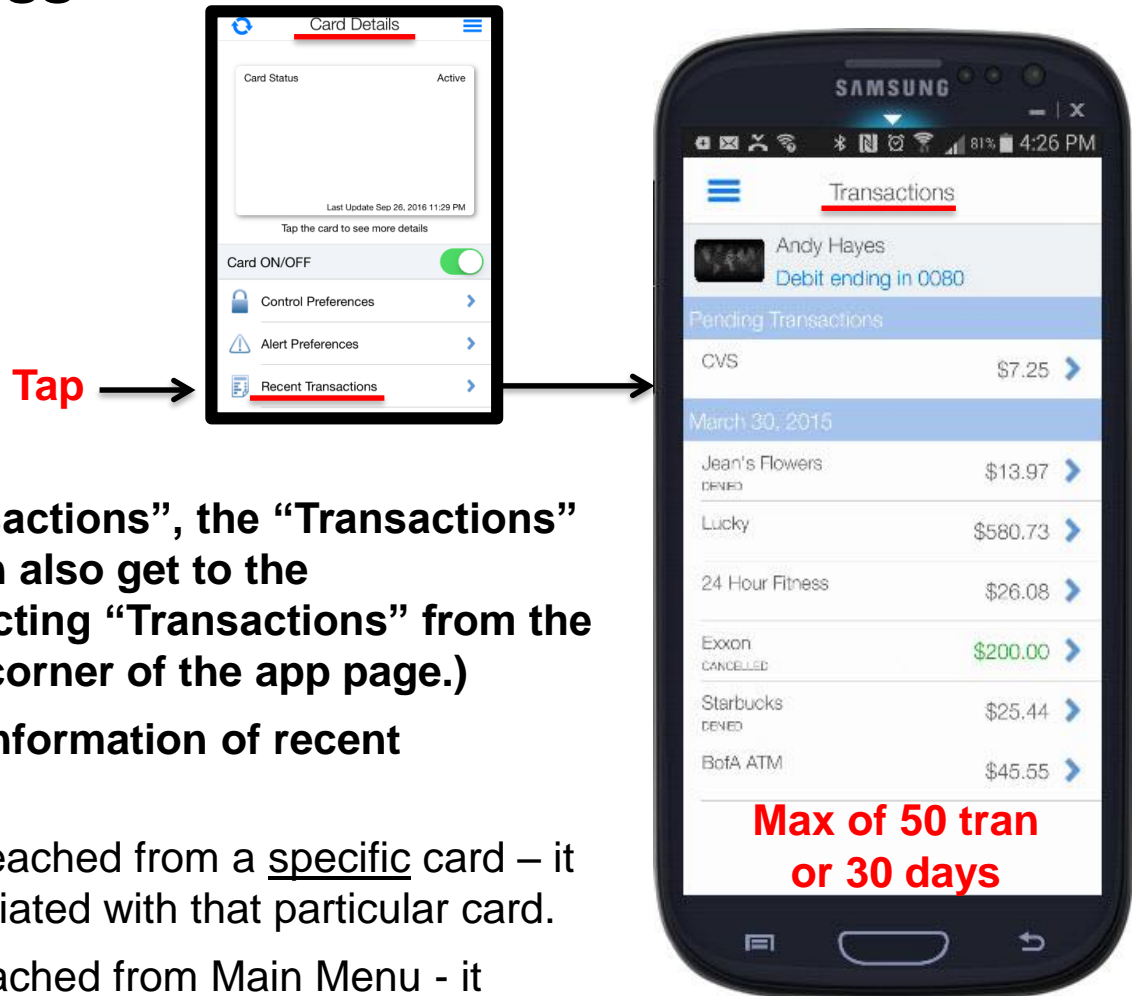


SWIPE



View Transactions

Transactions - Access

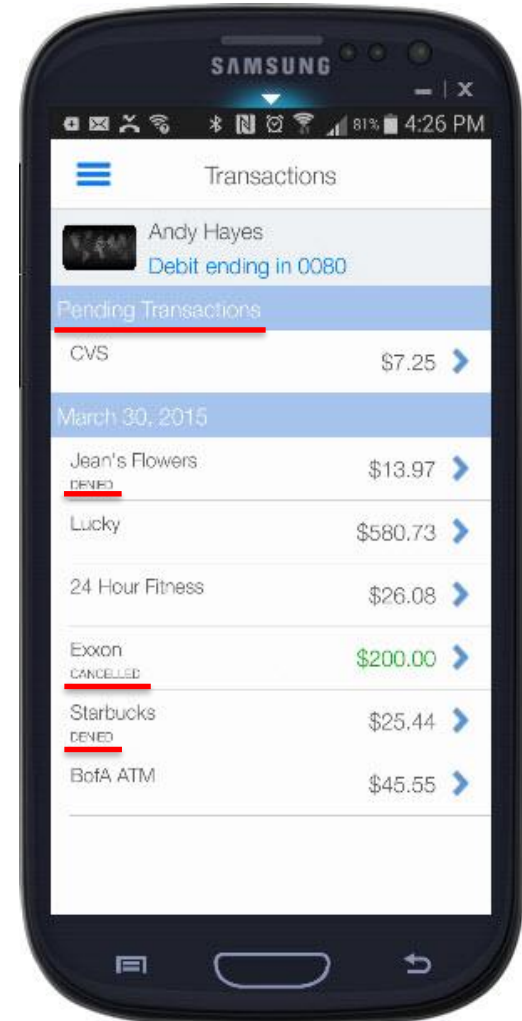


- By tapping on “Recent Transactions”, the “Transactions” page will display. (Users can also get to the “Transactions” page by selecting “Transactions” from the Main Menu in the upper left corner of the app page.)
- This page shows summary information of recent transactions:
 - If the transactions list is reached from a specific card – it shows transactions associated with that particular card.
 - If the transaction list is reached from Main Menu - it shows transactions for all the managed cards.

View Transactions

Transactions – Pending Transactions

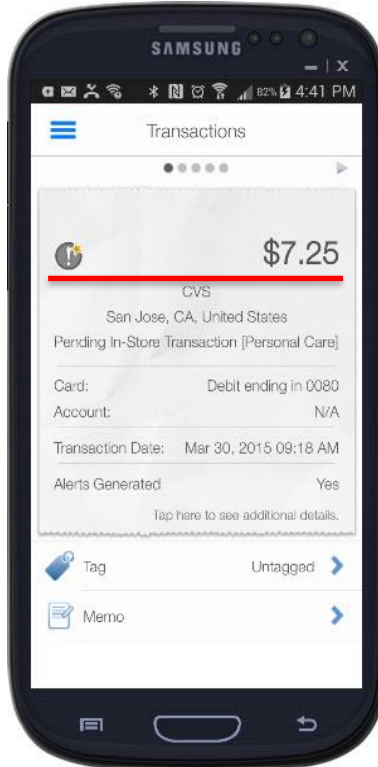
- Pending transactions (SecurLOCK Equip has not yet received the posted/financial advice message) are shown first in the list. Transactions with other statuses (Posted, Denied, or Cancelled) are shown chronologically.
- The summary information shown on this page includes:
 - Transaction Status
 - Merchant Name
 - Transaction Amount, where credit is shown in green text and debit is shown in black text



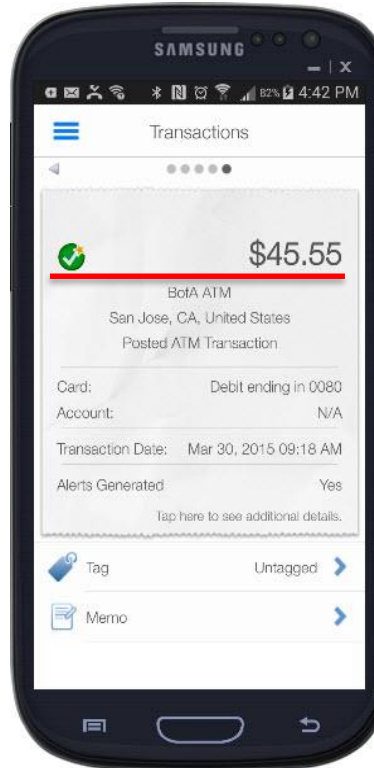
View Transactions

Transaction Details - Status

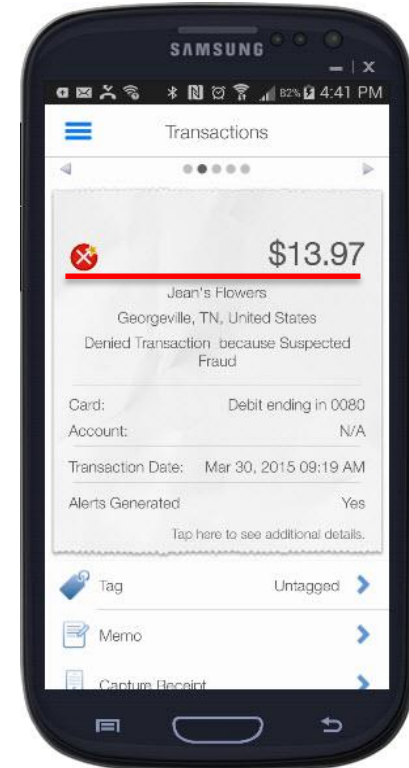
Pending



Posted



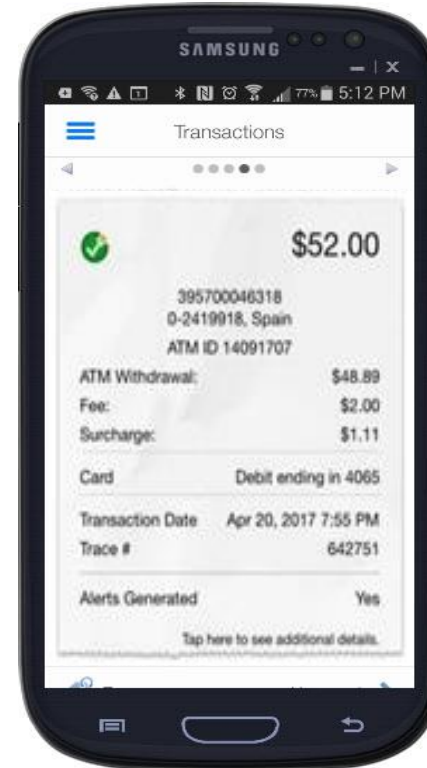
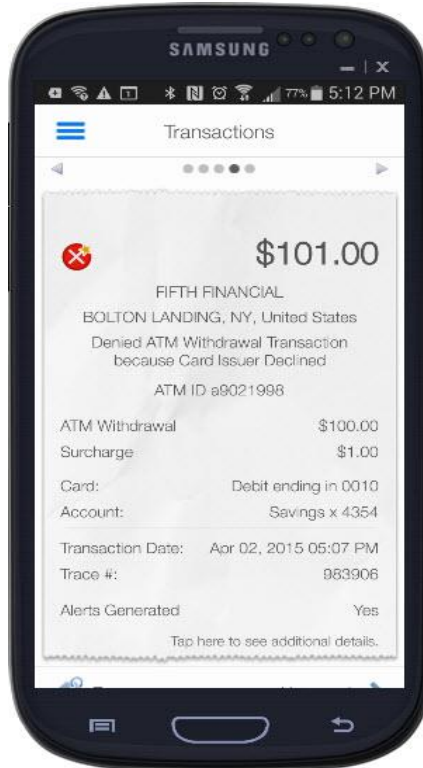
Denied



- Tapping on a transaction will cause the transaction details to display.
- A user can tap on the image to see additional details (see page 38).

View Transactions

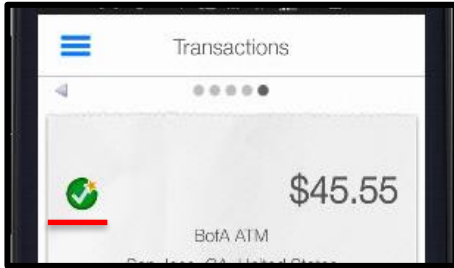
Transaction Details – Surcharge and Fees



- For transactions with fees and surcharge, the Transactions page will show the transaction amount, surcharge, and fee separately, as applicable.
- Transactions without a surcharge and fee will not have these fields shown on the Transactions page.

View Transactions

Transaction Details - Icons

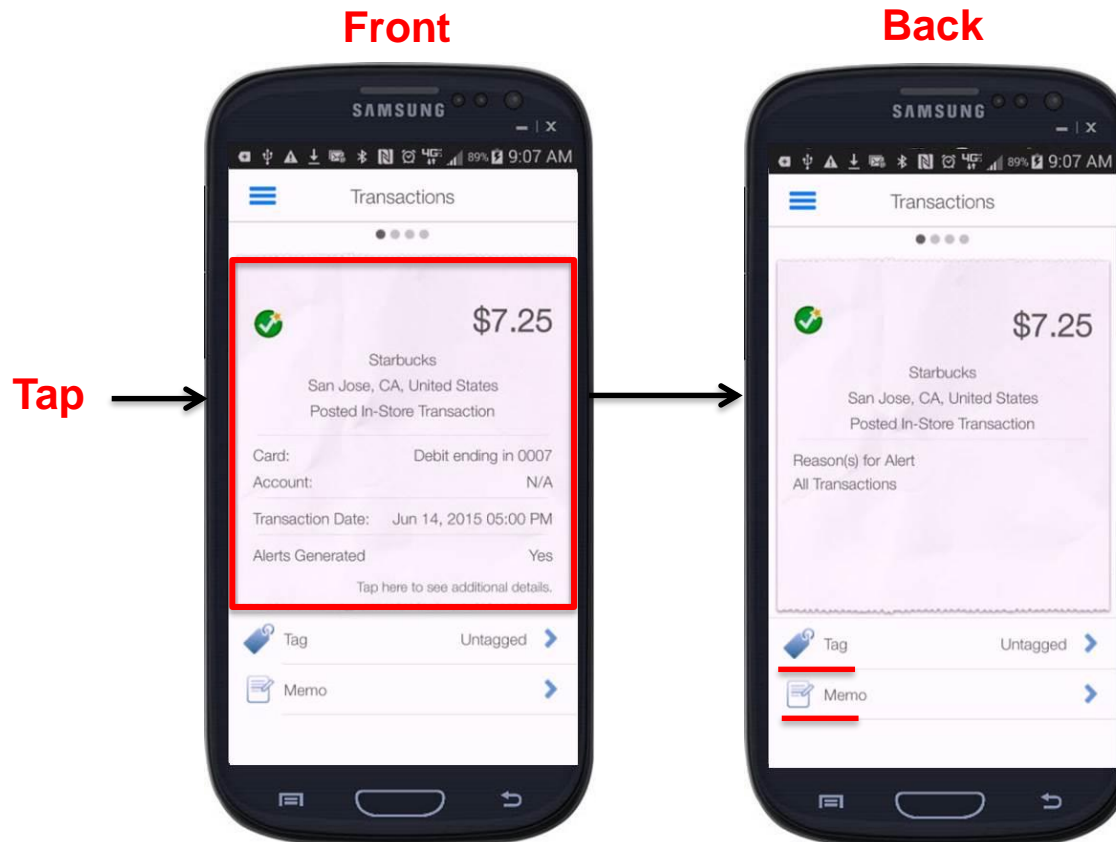


- On the Transactions page, the app displays a different icon for a transaction depending on the transaction status.
- A star in the upper right corner of an icon indicates that an alert has been generated for that transaction.

Icon	Meaning
	The transaction is posted and alert was not generated.
	The transaction is posted and alert was generated.
	The transaction is pending and alert was not generated.
	The transaction is pending and alert was generated.
	The transaction is denied and alert was not generated.
	The transaction is denied and alert was generated.
	The transaction is cancelled or reversed and alert was not generated.
	The transaction is cancelled or reversed and alert was generated.

View Transactions

Transaction Details - Reverse



- Tapping on the receipt image will cause the transaction details page to flip.
- The reverse side of the Transactions details page displays detailed information.
- The user is provided with the option to Tag or add a Memo to the transaction.

View Transactions

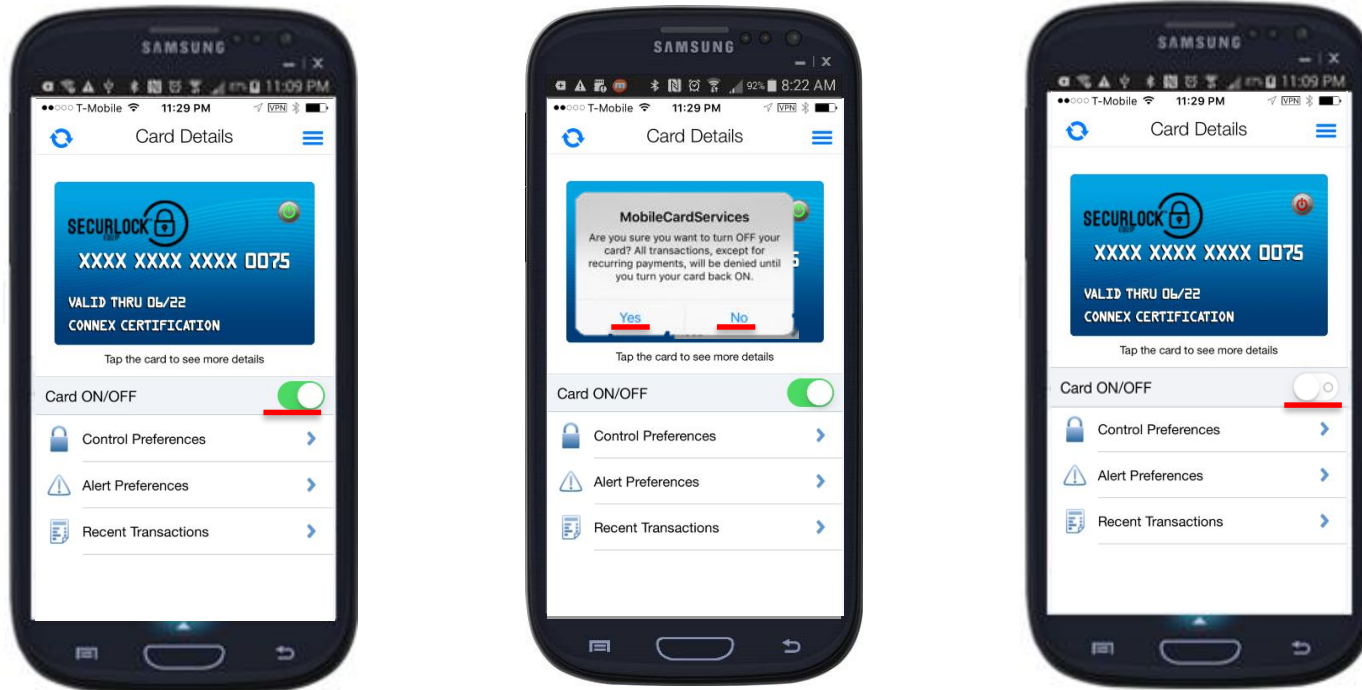
Transaction Details – Tags and Memos



- Tapping “Tag” takes the user to the “Tag” page.
- Tapping “Memo” takes the user to the “Notes” page, where the user can enter a short description about the transaction.
- The Tag and Memo functions allow users to categorize their transactions.

Set Up Control Preferences

Turn Card On/Off



- The simplest card control policy is to turn a card On or Off.
- To turn the card On or Off, tap the “Card ON/OFF” slider. An alert message appears for confirmation.
- Once the card is turned off, the power symbol on the card image changes from green (On) to red (Off) and the card ON/OFF slider turns to white.
- Note: Enabling/disabling works best if you tap rather than slide the control.

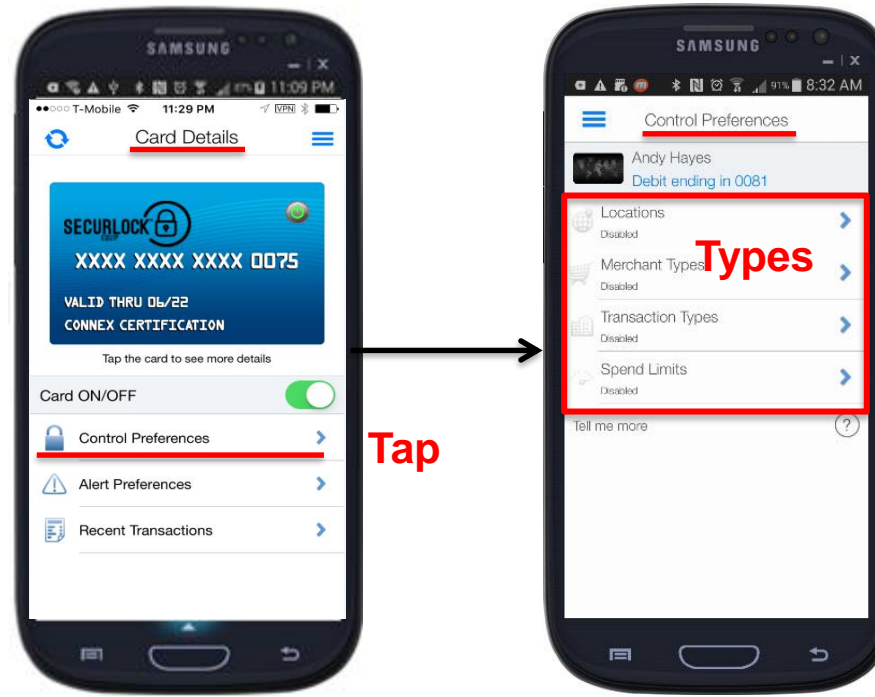
Set Up Control Preferences

Turn Card On/Off

- **When the card is turned off, a message pops up indicating all transactions will be blocked except for recurring transactions.**
- **Decline alerts will be pushed to the user. No other alerts will be sent.**
- **If the card status is changed (e.g., closed or hot carded or blocked by Falcon) in the system of record, the card status will not be changed to red.**
- **The On/Off feature only impacts the authorization stream and does not update the system of record.**
 - The user will receive a notification of a card status change when logging back into the application or after 10 minutes have elapsed with the app still open.

Set Up Control Preferences

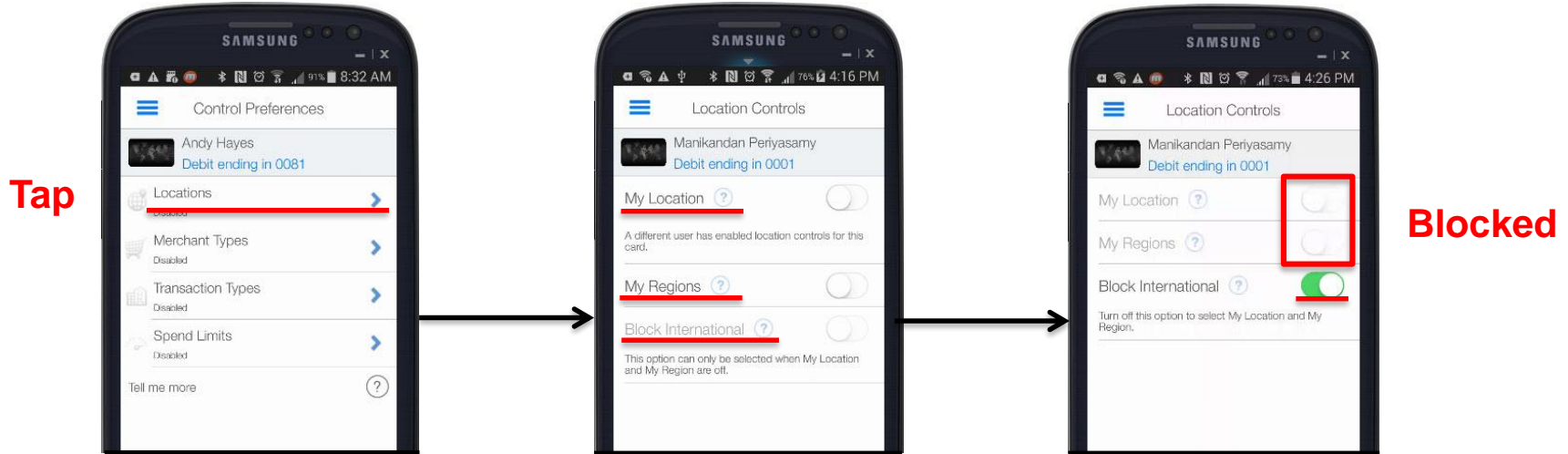
Advanced Controls



- To set up other advanced control policies, a user taps on “Control Preferences” on the Card Details page.
- The Control Preferences page appears, displaying multiple options for a user to set card control policies.
- Controls are applied immediately.
- SecurLOCK Equip cannot override a parameter or status on the system of record.

Set Up Control Preferences

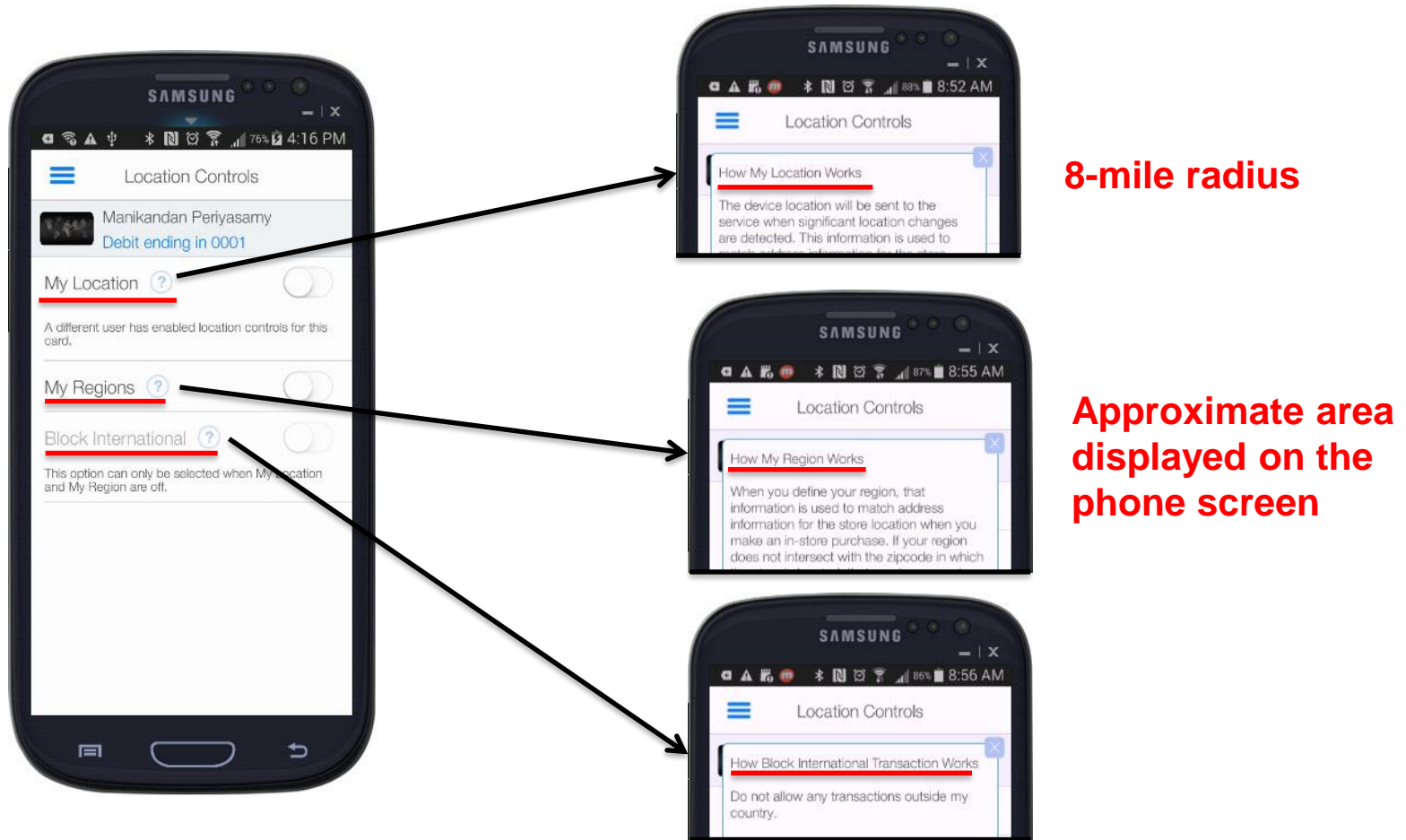
Location Controls



- A user can specify a location controls policy by selecting the “Locations” option.
 - The location policies only control in-store card present transactions. ➤
- Block International must be disabled when either the My Region and/or My Location option is enabled.
- Similarly, the My Region and My Location options must be disabled in order to enable Block International.

Set Up Control Preferences

Location Controls

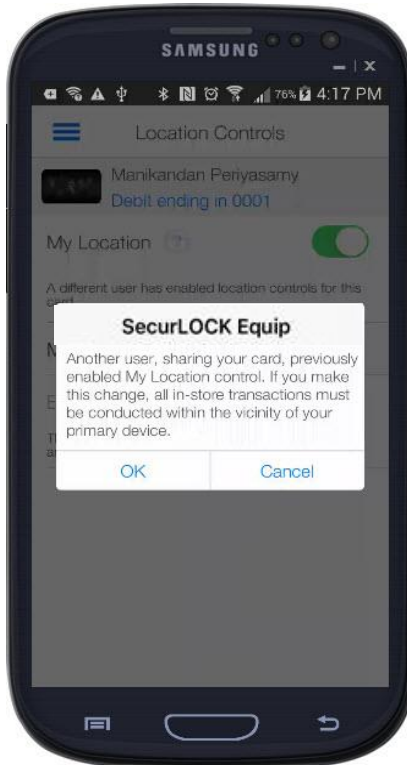


- To see more information on how each location control option works, a user can tap on the question mark next to each option.

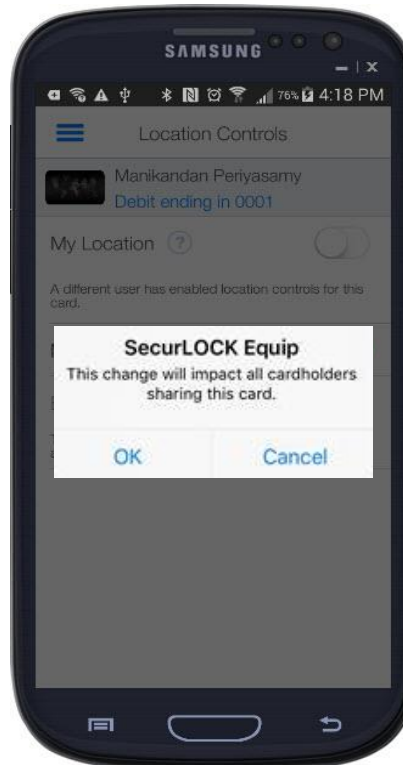
Set Up Control Preferences

Location Controls

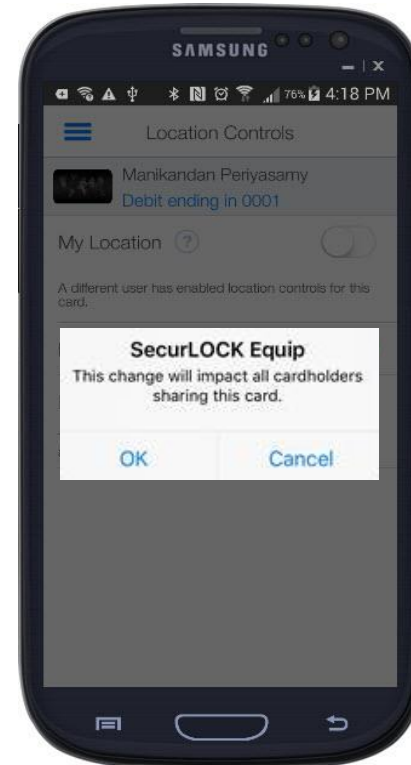
My Location



My Regions



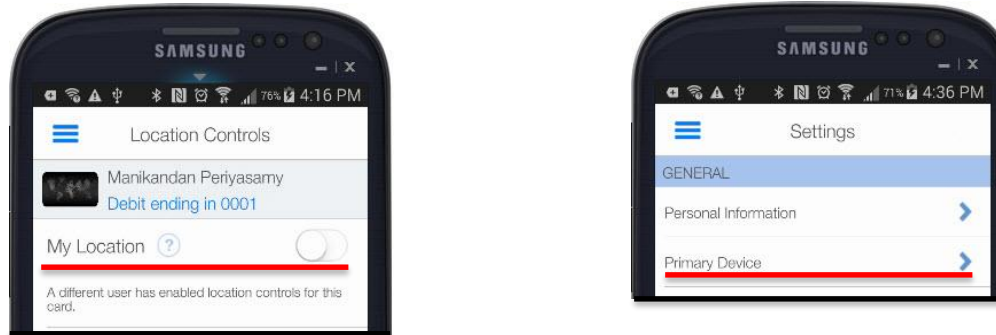
Block International



- The app will display an informational message, when a user selects each location control option.

Set Up Control Preferences

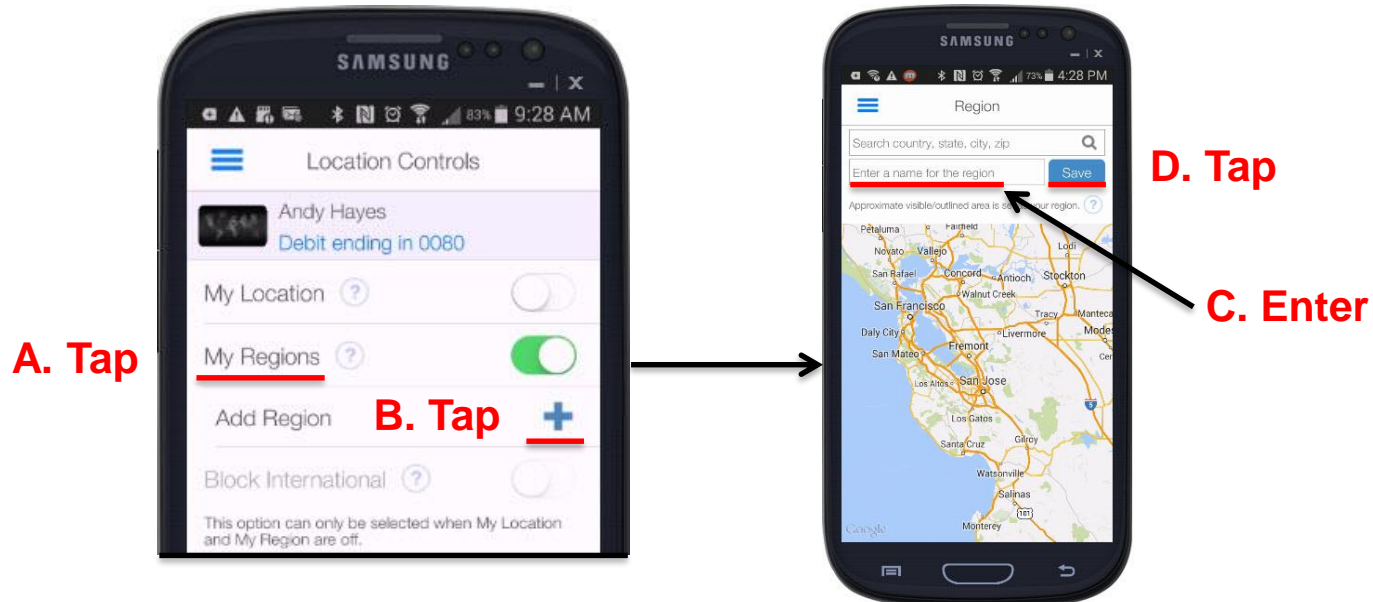
Location Controls – My Location



- When the “My Location” control preference is set, the app will compare the user location and the merchant location to decide whether to approve or deny the transaction.
- Transactions made at merchant locations that differ significantly from the user’s location will be denied.
- The app determines the user’s location by:
 - Assuming that the user will always carry the phone that has been set as “Primary Device”
 - Using the phone’s location as a proxy for the user’s location
- For “My Location” Control and Alerts preferences to work, the user must turn “On” the device’s Location Settings and enable location tracking.

Set Up Control Preferences

Location Controls – My Regions



- A user can select “My Regions” to set one or multiple geographical areas where in-store transactions can be made.
- A user can specify up to three control regions per card.
- Tapping the “Add Region” link brings up an interactive map where users can search for an area, then zoom in or out to specify the region.
- A user must enter the region’s name and tap “Save” after selecting the region.

Set Up Control Preferences

Location Controls

Additional information regarding Location Controls:

- Controls are exclusive to Card Present (CP) Transactions.
- Controls are dependent on the geofencing information the device captures.
- A devices Operating System (OS) or battery level may impact location information being captured by the device i.e. on “Low Power Mode” many OS functions are suspended to save power. This generally includes updating the devices location.
- Cellular network coverage and connectivity may impact the accuracy of location information.
- If the device was powered off while in transit then turned on for a transaction, the transaction might be denied as the app is using the last location captured by the device – the location in which the device was previously turned on.

Set Up Control Preferences

Location Controls

Additional information regarding Location Controls:

- **My Location and My Regions work independently or simultaneously.**
 - This means that if My Regions is set to Las Vegas and the mobile device is in Killen, TX with My Location enabled, a transaction made within either control area will be approved.
- **There are some occasions in which the app will by-pass a location control and approve a transaction.**
 - To avoid inconveniencing the customer and to allow a transaction to be made, there are some Merchant Category Codes (MCC) that are **excluded** from Location Controls (My Location AND My Regions). For instance, the MCC code for vending machines is 5814. This MCC is excluded from Location Controls as often the transaction is processed remotely - in another zip code. The next slide provides more details.

Set Up Control Preferences

Location Controls

Below is a list of the current MCC Codes that Equip excluded from location controls (My Location AND My Regions).

MCC	Short Description	MCC	Short Description
0780	Veterinary Services	4214	Motor Freight Carriers and Trucking
1520	General Contractors – Residential and Commercial	4215	Courier Services
1711	Heating, Plumbing, and Air Conditioning Contractors	4784	Tolls and Bridge Fees
1731	Electrical Contractors	4789	Transportation Services (Not Elsewhere Classified)
1740	Masonry, Stonework, Tile Setting, Plastering and Insulation Contractors	4900	Utilities – Electric, Gas, Water, and Sanitary
1750	Carpentry Contractors	5814	Fast Food Restaurants including Vending Machines
1761	Roofing, Siding, and Sheet Metal Work Contractors	5963	Door-To-Door Sales
1771	Concrete Work Contractors	5996	Swimming Pools – Sales and Service
1799	Special Trade Contractors (Not Elsewhere Classified)	7217	Carpet and Upholstery Cleaning
4111	Local and Suburban Commuter Passenger Transportation, Including Ferries	7342	Exterminating and Disinfecting Services
4119	Ambulance Services	7349	Cleaning, Maintenance, and Janitorial Services
4121	Taxicabs and Limousines	7549	Towing Services
4131	Bus Lines	7841	DVD/Video Tape Rental Stores

Set Up Control Preferences

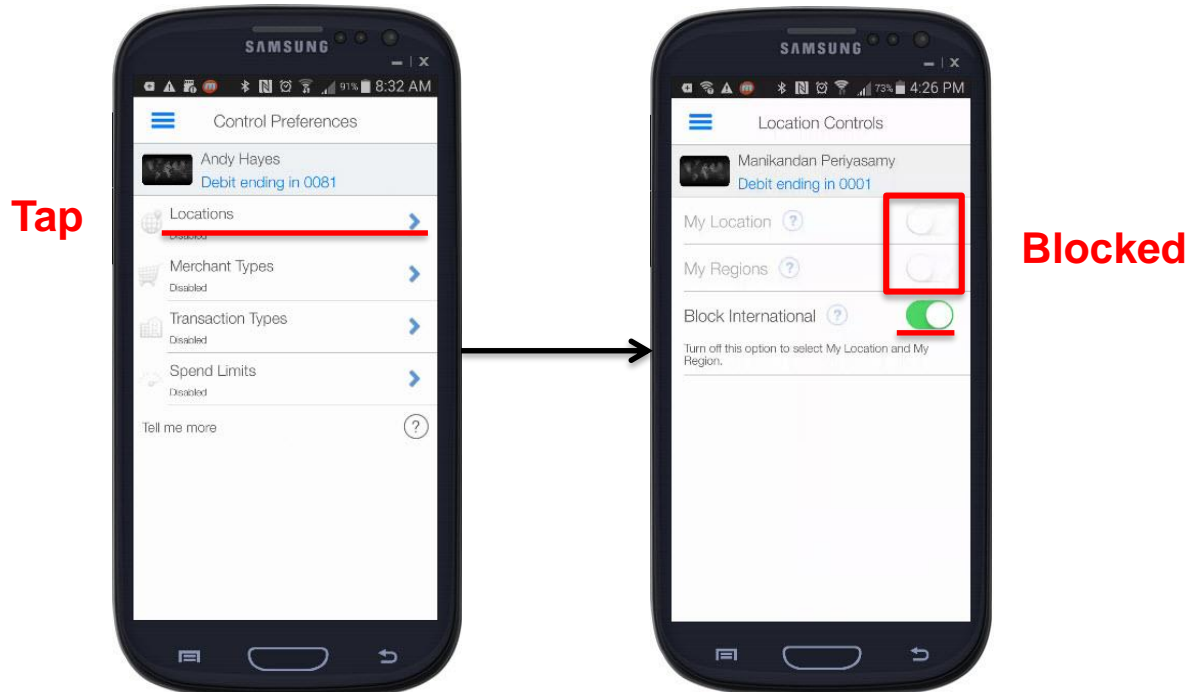
Location Controls

- The coverage area for a location control is a radius. For My Location the radius is 8-miles. For My Regions, the radius is whatever is set. Note the controlled area displayed in the device does not reflect the total coverage area.



Set Up Control Preferences

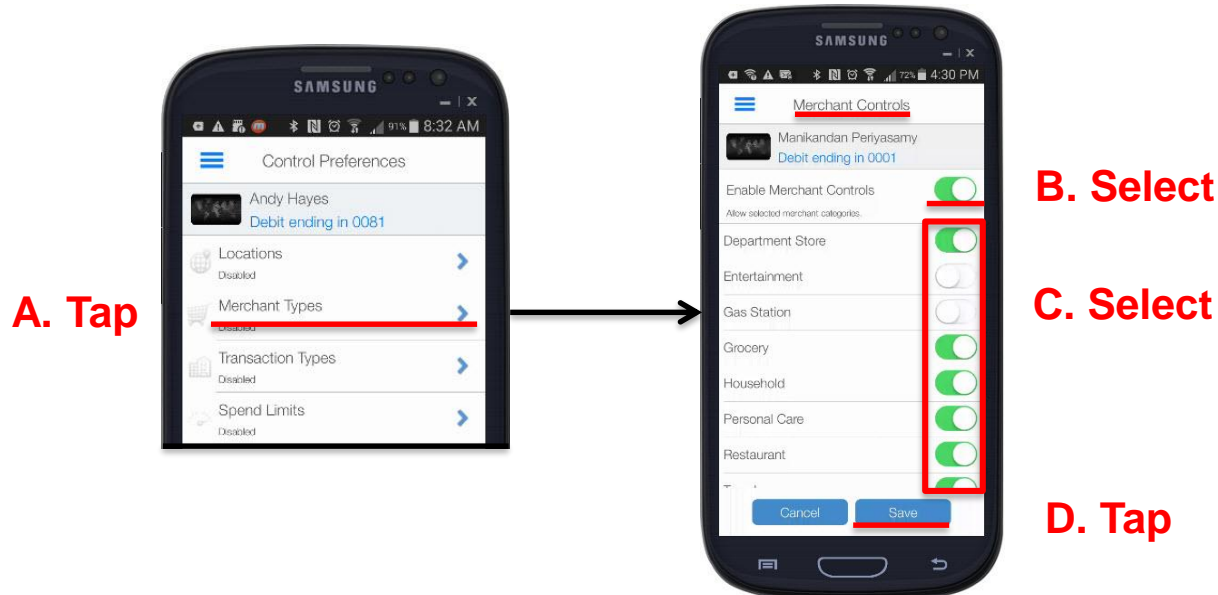
Location Controls – Block International



- To block transactions made outside of the user's home country, the user selects the "Block International" option by tapping the respective slider to the "ON" position.
- Both "My Location" and "My Region" sliders must be in the "OFF" position for the user to be able to select the "Block International" option.

Set Up Control Preferences

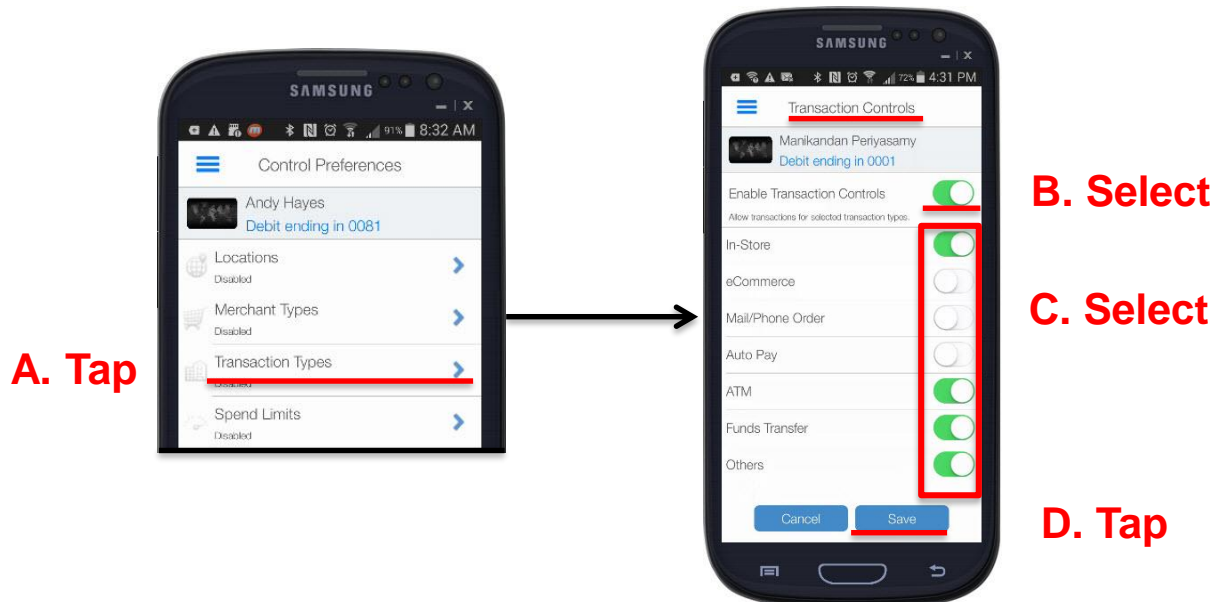
Merchant Controls – Merchant Type



- A user can specify merchant types for which transactions are allowed or denied.
- When “Merchant Types” is selected as “ON”, the individual types are shown. The first time a user selects “ON”, all of the Merchant Types will be enabled.
- Individual Merchant Types can be turned “OFF” by selecting the slide next to it.
- Selecting “ON” for a specific merchant type will allow a transaction to be permitted at that type of merchant. Selecting “OFF” will deny any transaction at that merchant type.
- If “Merchant Types” is turned “OFF” and then turned “ON” again, the last known settings will be displayed.

Set Up Control Preferences

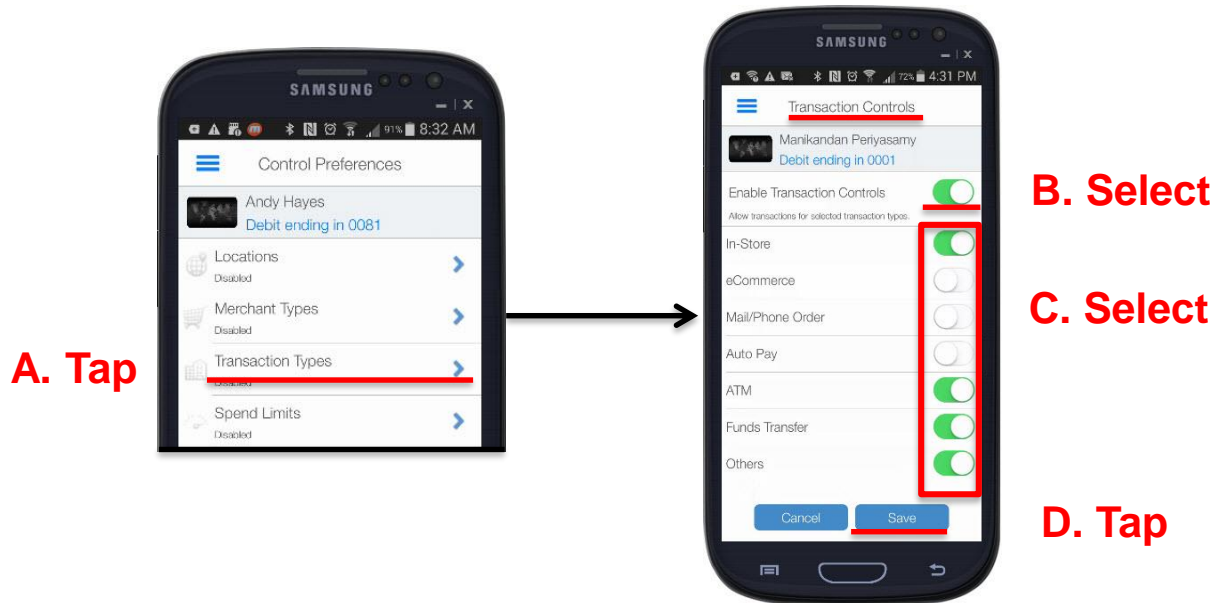
Transaction Controls



- The user can specify transaction types for which transactions are allowed or denied.
- When “Transaction Types” is selected as “ON”, the individual types are shown.
- The first time a user selects “ON”, all of the transaction types will be enabled.
- Individual transaction types can be turned “OFF” by selecting the slide next it.
- Selecting “OFF” will deny any transaction of that Transaction Type.
- If the Recurring option is “OFF” and the card is “OFF” everything is declined.
- If “Transaction Types” is turned “OFF” and then turned “ON” again, the last known settings will be displayed.

Set Up Control Preferences

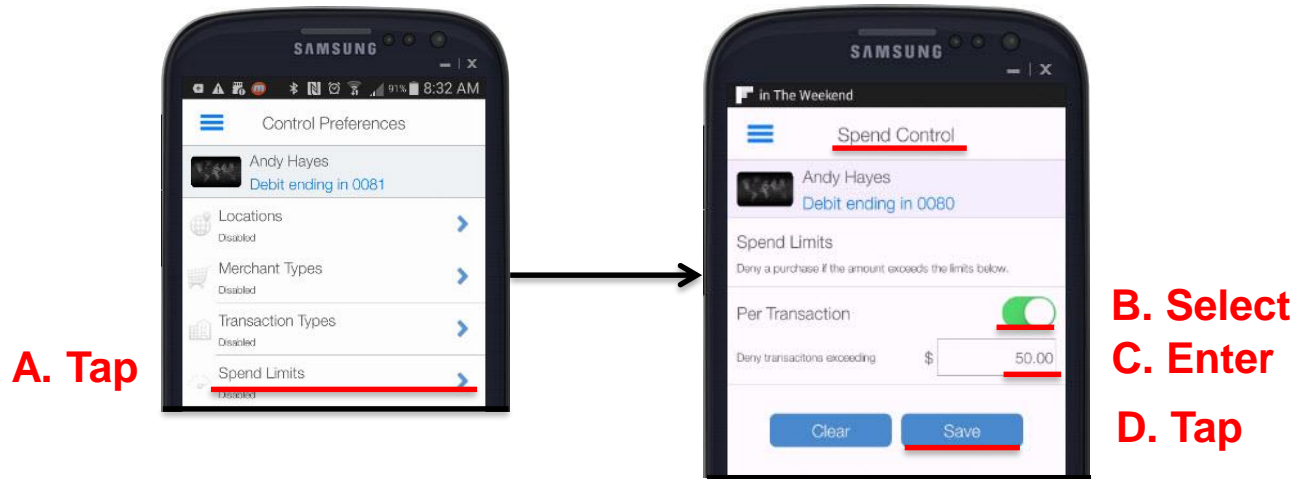
Transaction Controls



- Since “eCommerce” and “ATM” transactions are an increasing target to perpetrators, it is suggested that these controls are “Disabled” unless they are needed by the cardholder.
- If one of these transaction types is needed, it can be quickly activated and then deactivated after the transaction has been performed.

Set Up Control Preferences

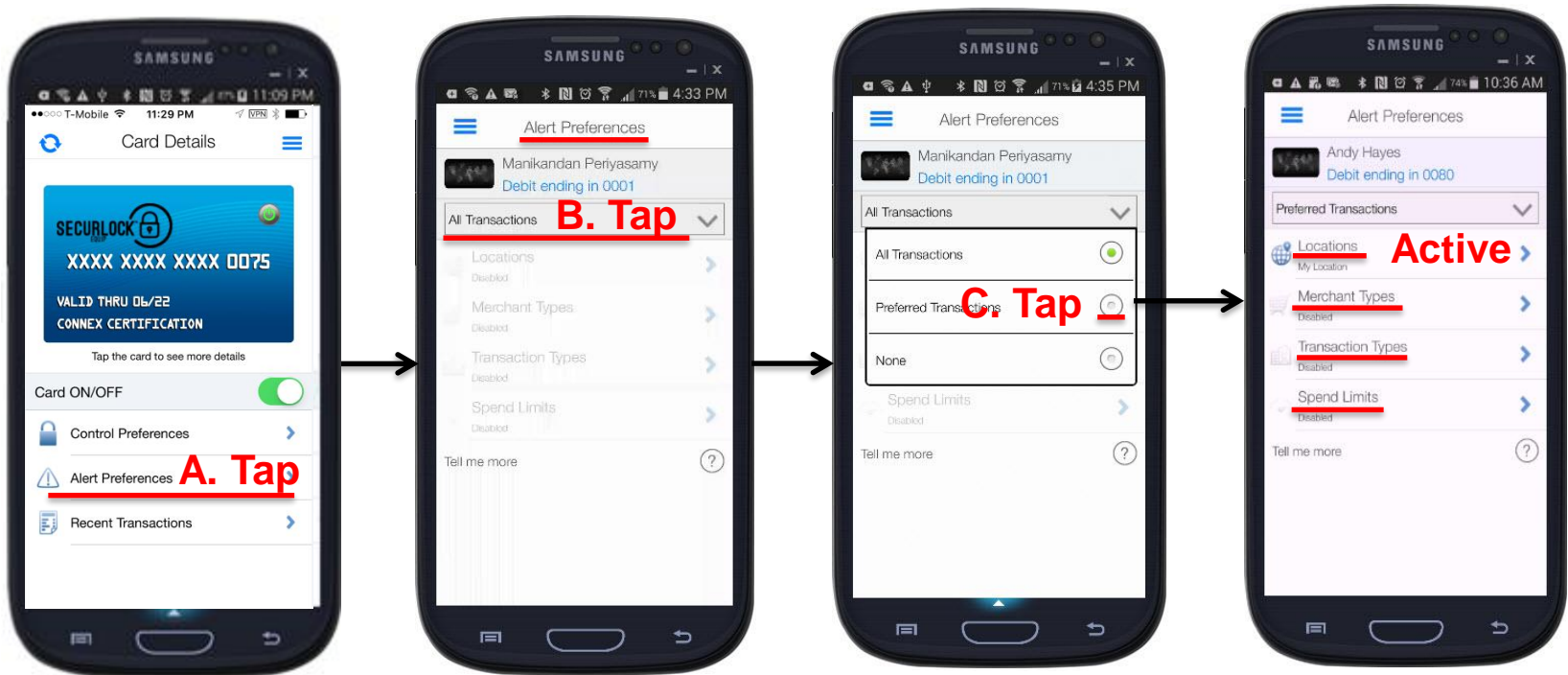
Spend Controls



- Tapping on “Spend Limits” on the Control Preferences page takes the user to the Spend Control page.
- Here a user can specify a transaction threshold amount (not transaction velocity), above which transactions will be denied.
- Tapping the “Per Transaction” slider to “ON” will display the amount field, where the user can enter the threshold amount.
- The user must tap on “Save” for the Spend Limits control policy to take effect.

Set Up Alert Preferences

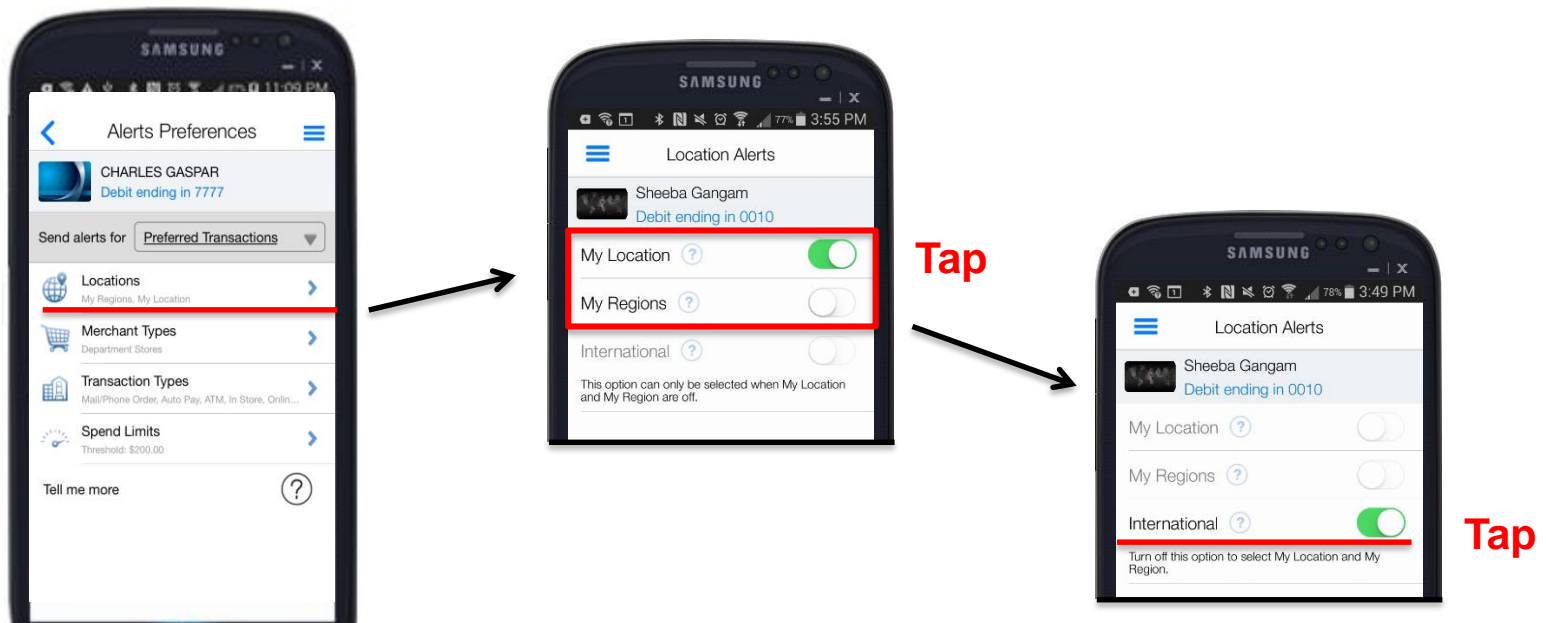
Preferred Transactions Option



- Selecting “Preferred Transactions” from the drop-down box on the Alert Preferences page presents the user with the several custom alert options.
- Once an alert preference is enabled, its icon changes from light grey to blue.
- All denied transactions will generate an alert, irrespective of the alert setting by the cardholder. Transactions can also be declined due to the status of the card on the system of record (the switch or the core).

Set Up Alert Preferences

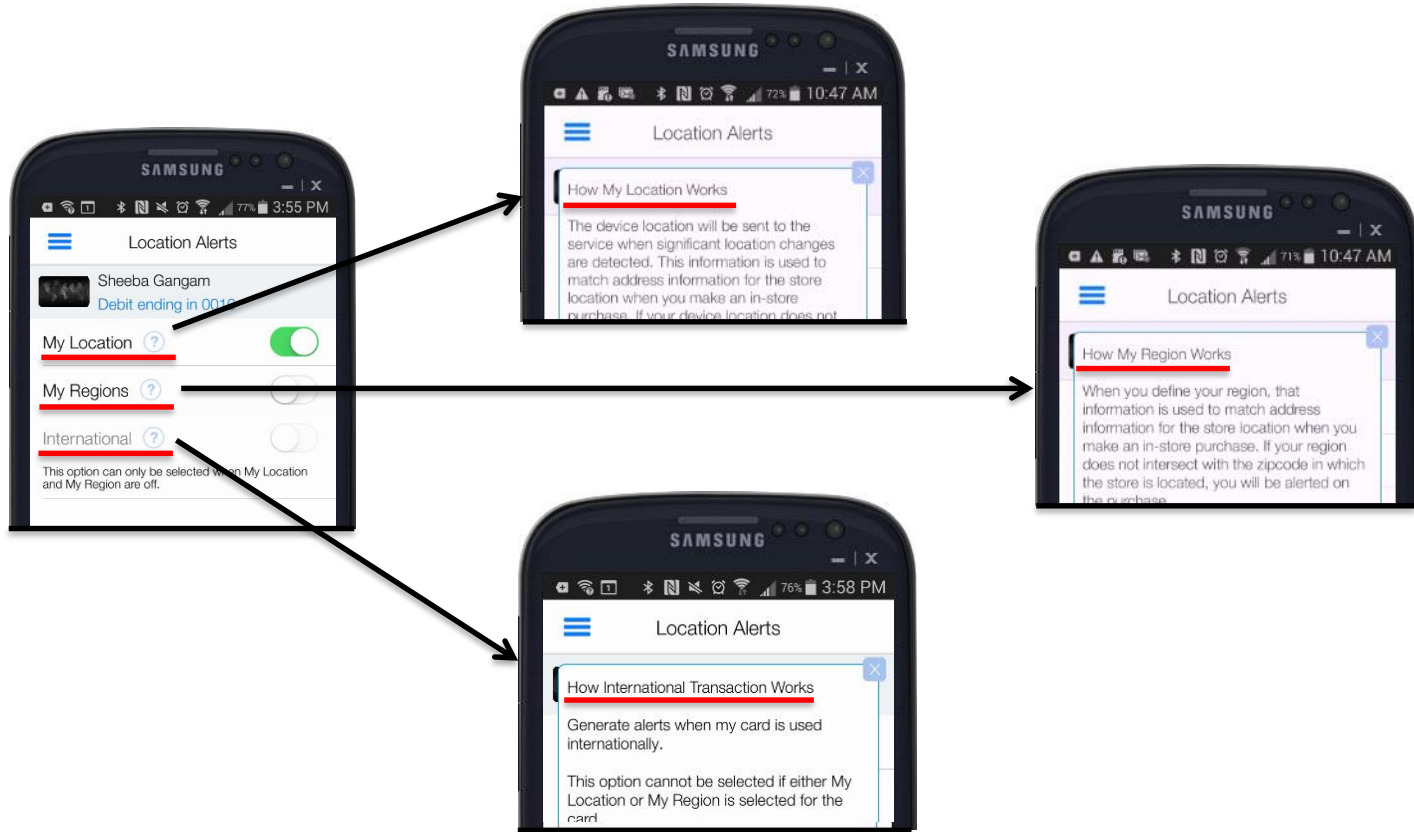
Location Alerts



- A user can specify a Location Alert by selecting the “My Location” option.
- Available Location Alerts are: My Location, My Regions, and International.
- Users can set multiple location alerts for each card.
 - “International” must be disabled, when either “My Regions” or “My Location” is enabled.
 - Similarly, “My Regions” and “My Location” must be disabled, in order to enable "International"

Set Up Alert Preferences

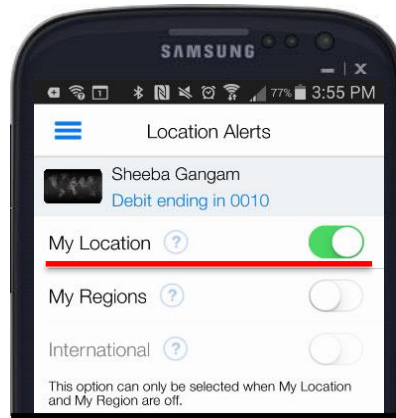
Location Alerts



- To see more information on how each location alert option works, a user can tap on the ? icon next to each option.

Set Up Alert Preferences

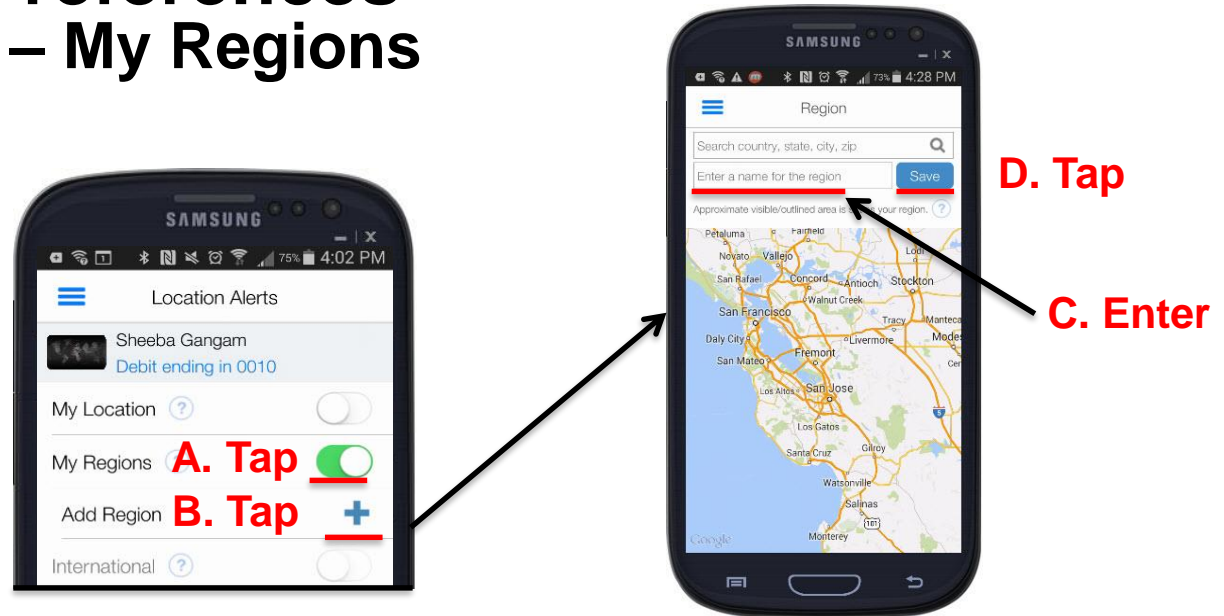
Location Alerts – My Location



- When the “My Location” control preference is set to “ON”, the app will compare the user and merchant locations in order to decide whether or not to trigger an alert.
- Transactions made at merchant locations that differ significantly from the user’s location will cause an alert to be sent to the user’s device.
- The app determines the user’s location by:
 - Assuming that the user will always carry the phone that has been set as “Primary Device”.
 - Using the phone’s location as a proxy for the user’s location (minimum 8 mile radius).
- For “My Location” Control and Alerts policies to work, the user must turn “ON” the device’s Location Settings and enable location tracking.

Set Up Alert Preferences

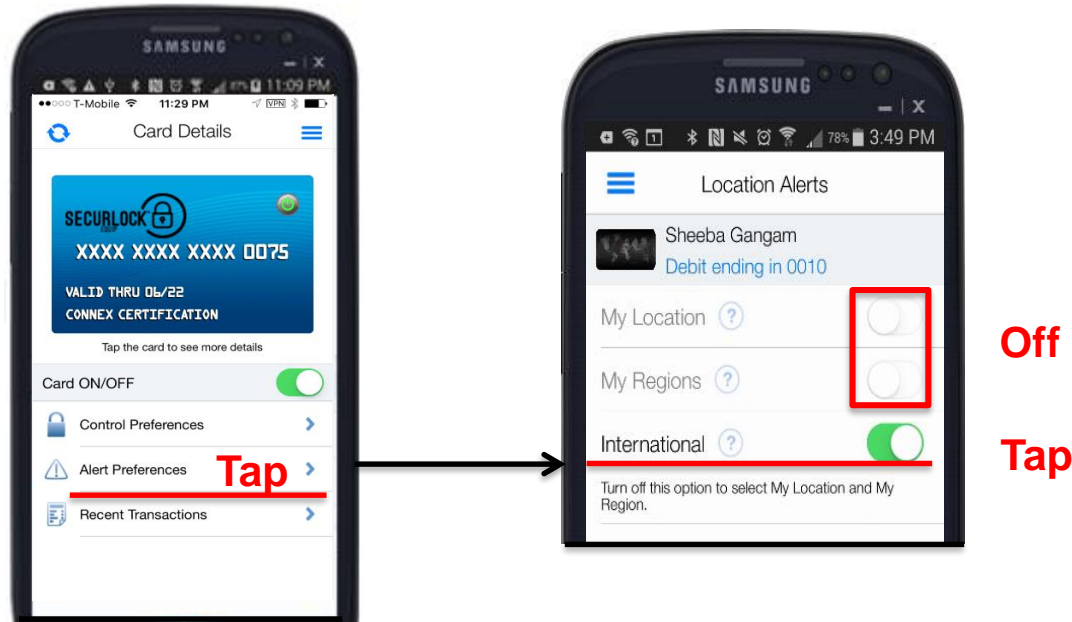
Location Alerts – My Regions



- A user can select “My Regions” to set one or multiple geographical areas where in-store transactions can be made. When “My Regions” alert is set to “ON”, any in-store transactions made outside the specified region(s) will trigger an alert to the user’s phone.
- A user can specify up to three Alert Regions per card. Each region is an approximate geographic area of the map displayed.
- Tapping the “Add Region” link brings up an interactive map where the user can search for an area, then zoom in or out to specify the region.
- The user must enter a region’s name and tap “Save” after selecting the region.

Set Up Alert Preferences

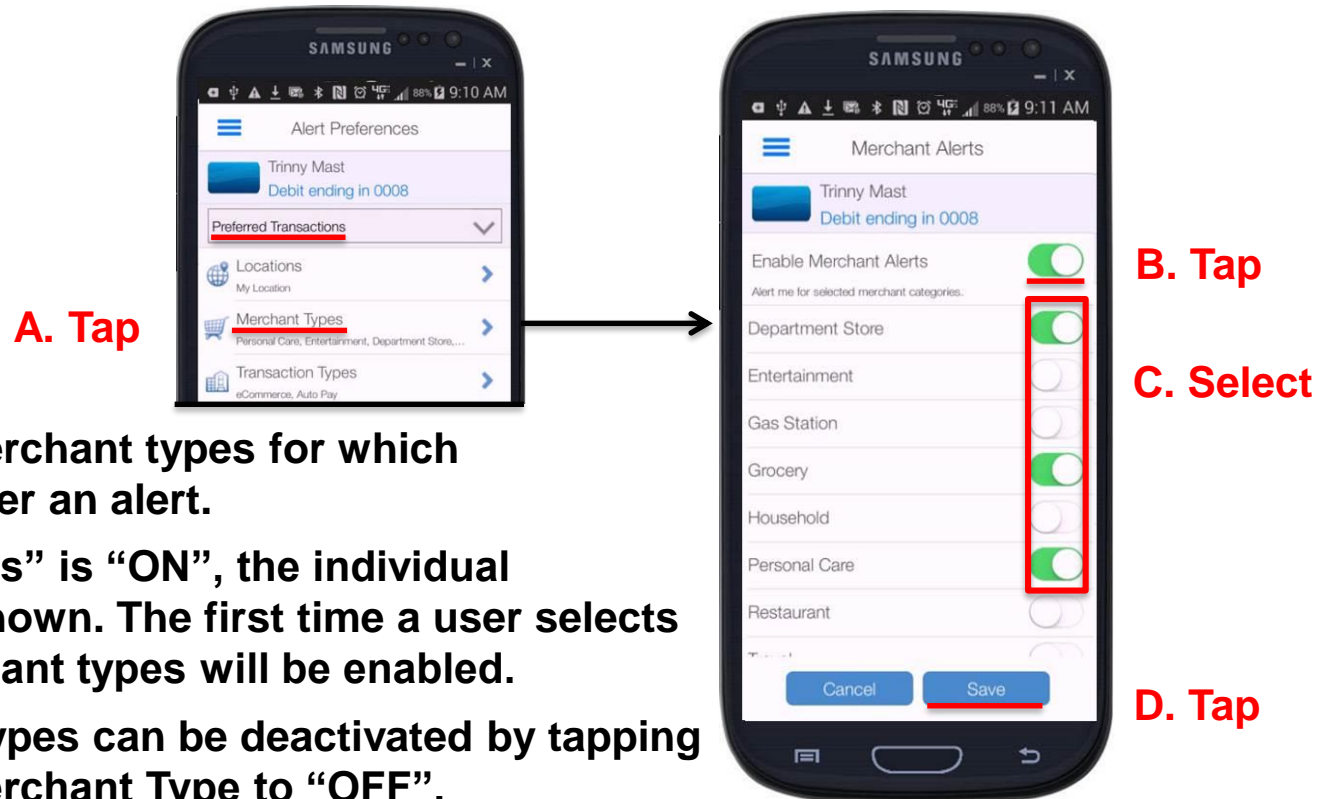
Location Alerts - International



- To get alerts for transactions made outside of the user's home country, a user selects the "International" option by sliding the respective slider to the "ON" position.
- Both "My Location" and "My Regions" sliders must be in the "OFF" position for a user to be able to select "International".
- Travel alerts are not integrated into SecurLOCK Equip; follow your normal procedures.

Set Up Alert Preferences

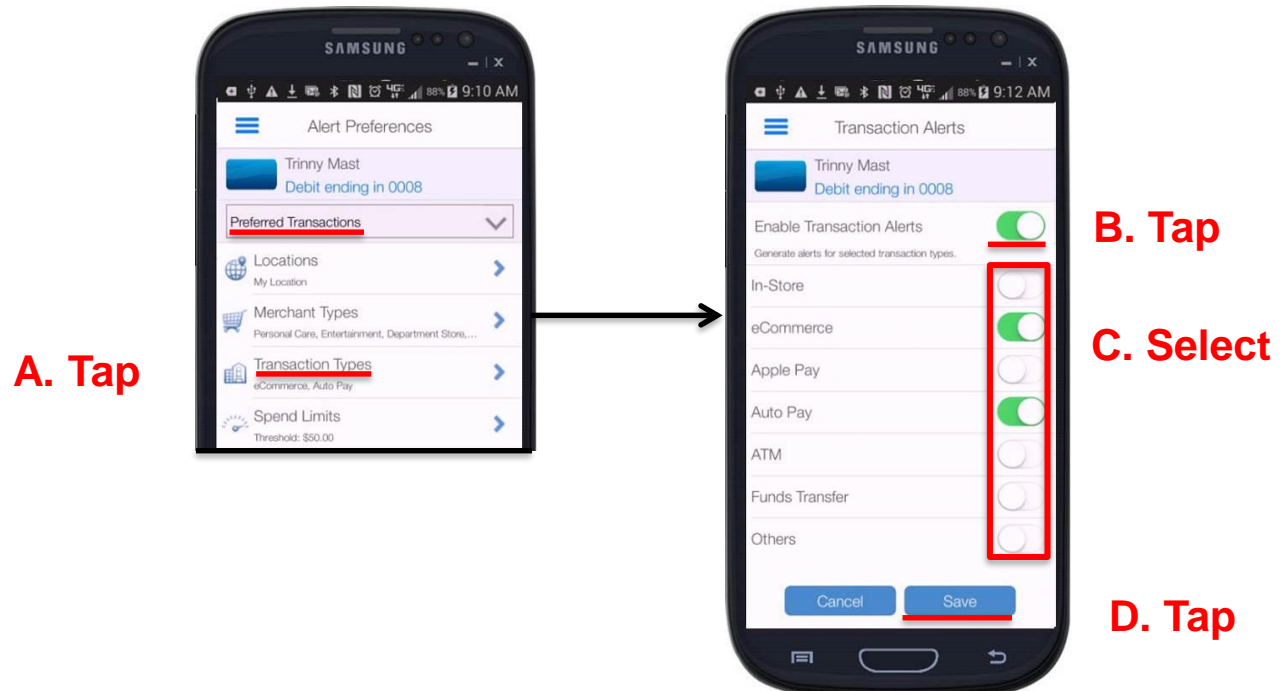
Merchant Alerts



- A user can specify merchant types for which transactions will trigger an alert.
- When “Merchant Types” is “ON”, the individual merchant types are shown. The first time a user selects “ON”, all of the merchant types will be enabled.
- Individual merchant types can be deactivated by tapping the slider next to a Merchant Type to “OFF”.
- Selecting “ON” for a Merchant Type will cause an alert to be triggered for transaction made at that Merchant Type.
- If Merchant Types is turned “OFF” and then turned “ON” again, the last known settings will be displayed.

Set Up Alert Preferences

Transaction Alerts – Transaction Types

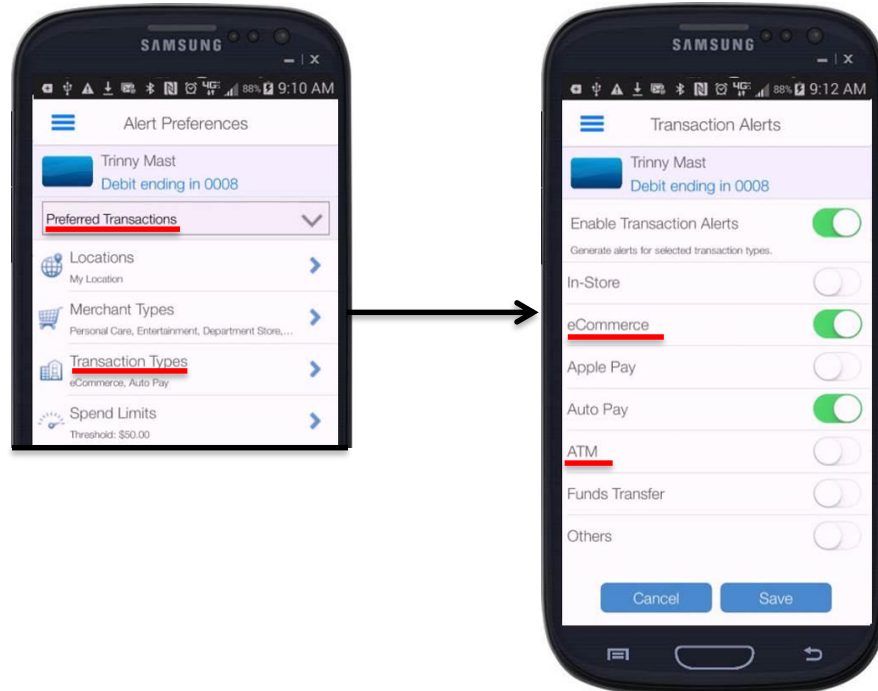


- The user can specify transaction types that will trigger an alert.
- When “Transaction Types” is selected as “ON”, the individual types are shown. The first time a user selects “ON”, all of the Transaction Types will be enabled. Individual Transaction Types can be turned “OFF” by tapping the slider next to each transaction type.
- Selecting “ON” for a Transaction Type will cause alert to be triggered for a transaction made with that transaction type.

Set Up Alert Preferences

Transaction Alerts – Transaction Types

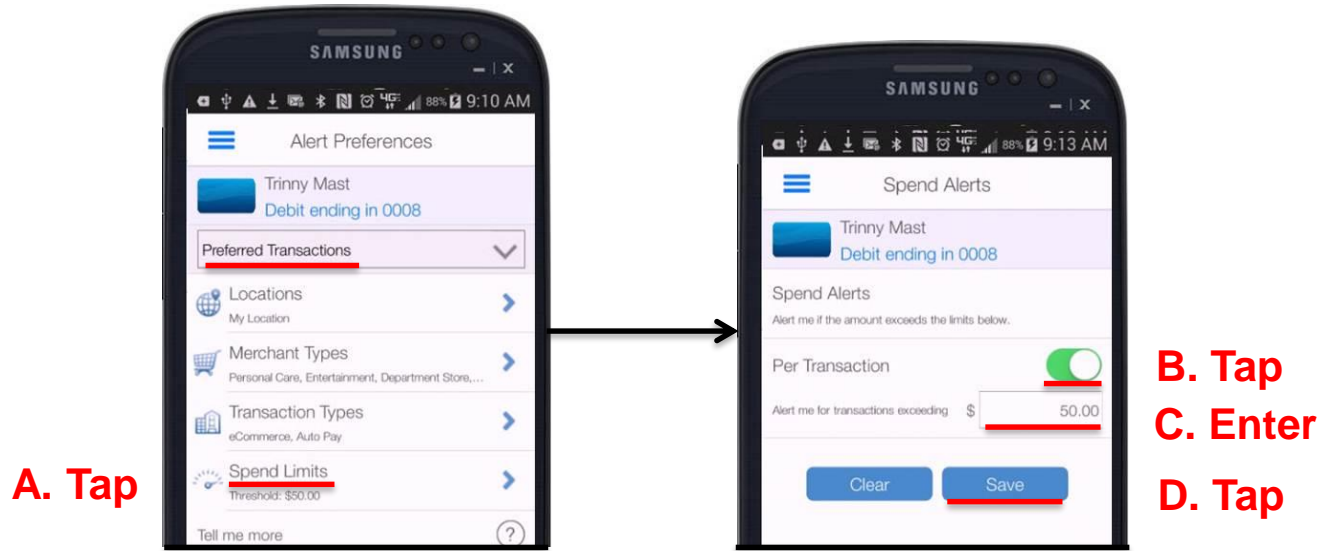
A. Tap



- If Transaction Types is turned “OFF” and then turned “ON” again, the last known settings will be displayed.
- Since “eCommerce” and “ATM” transactions are fraud targets, it is suggested that these alerts are enabled.

Set Up Alert Preferences

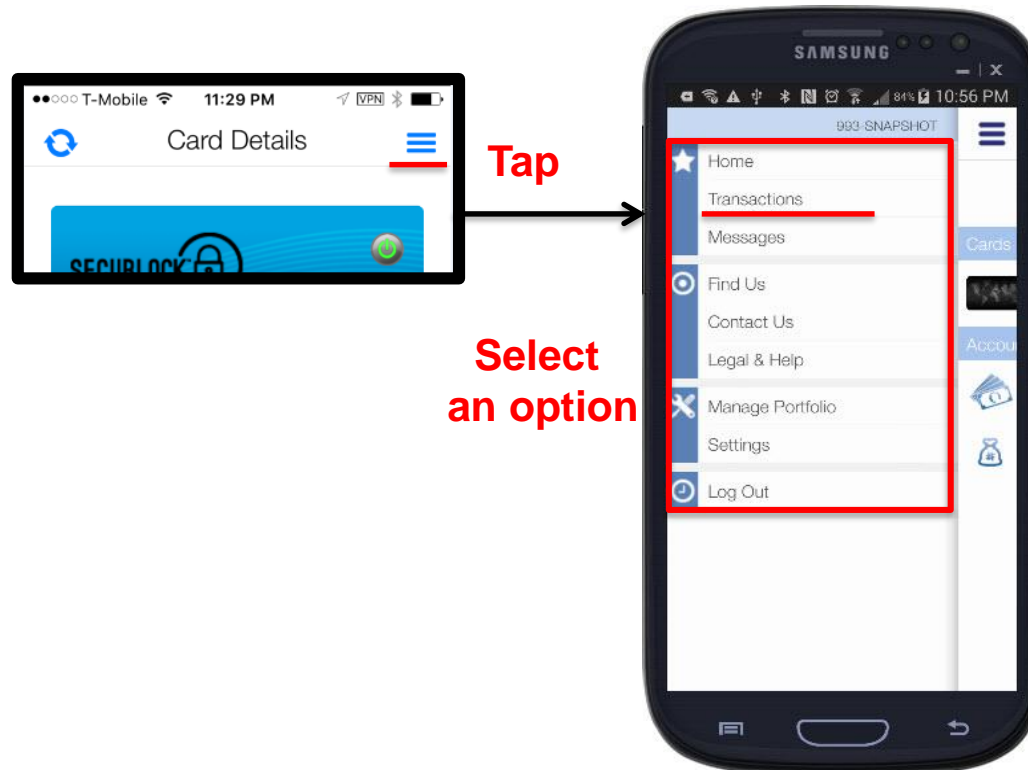
Spend Alerts – Spend Limits



- Tapping on “Spend Limits” on the Alert Preferences page takes the user to the Spend Alerts page.
- Here the user can specify a transaction threshold amount above which an alert will be triggered; the transaction will not be denied.
- Tapping the “Per Transaction” slider to “ON” will display the amount field, where the user can enter the threshold amount.
- A user must tap on “Save” for the Spend Limits alert policy to take effect.

Home Screen – Main Menu Options

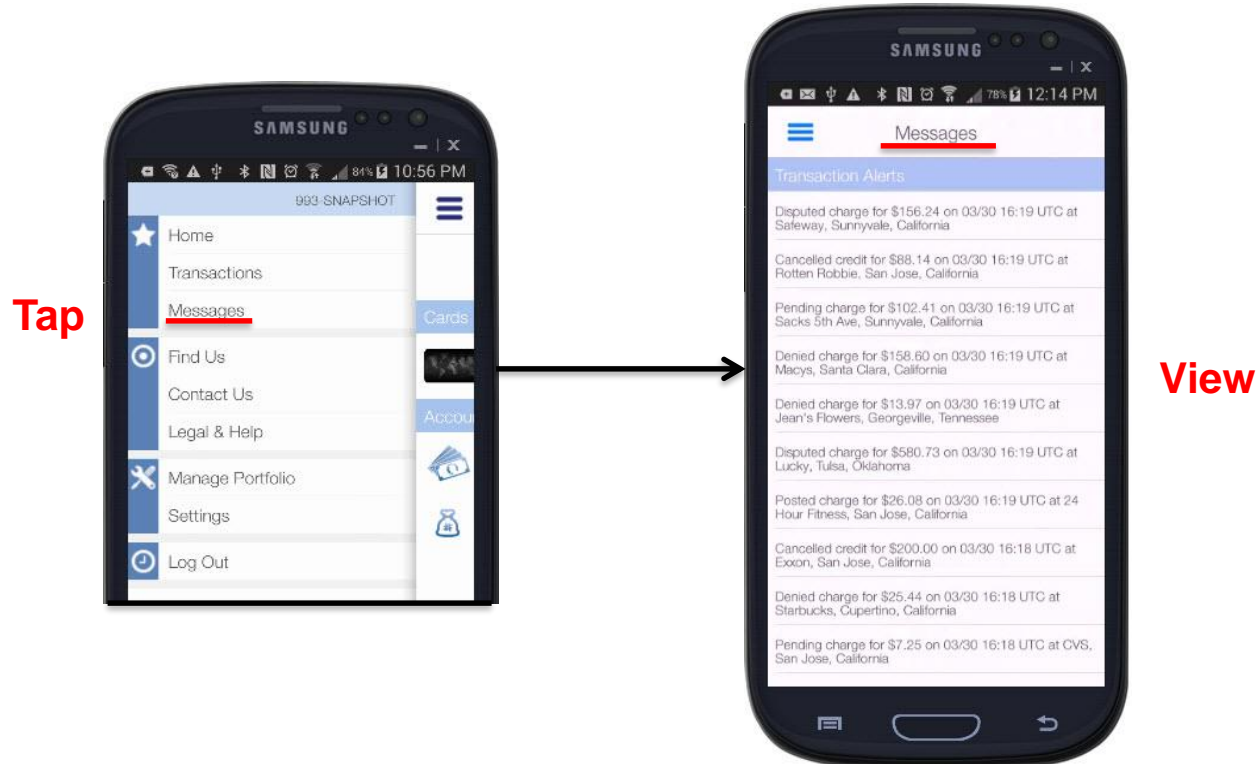
List of Options



- Tapping the Menu icon presents the user with a variety of menu options.
- This is another way to access Transactions.

Home Screen – Main Menu Options

Settings - Messages



- Tapping “Messages” on the Home Menu takes user to the “Messages” page.
- This page shows all transactions and card alerts sent to the user’s phone.
- All messages will fall off after 7 days.

Home Screen – Main Menu Options

Find Us (ATM Locations)



- This feature is configurable and may be turned off. This feature is also dependent upon the financial institution's Google Maps account.
- Tapping the “Find Us” icon on the Welcome page (or Home Menu) takes the user to the “Find Us” page. The app initially locates all ATMs based on the user's device location and displays them on a map.
- ATM locations are shown as red and green balloons on the map. Green balloons indicate locations of ATMs belonging to the user's financial institution. Red balloons indicate locations of all other ATMs – if these options are enabled.
- The user can narrow down the ATM search by entering the zip code or city information in the field provided. The app will bring up a list of financial institution ATMs in the area specified.

Home Screen – Main Menu Options

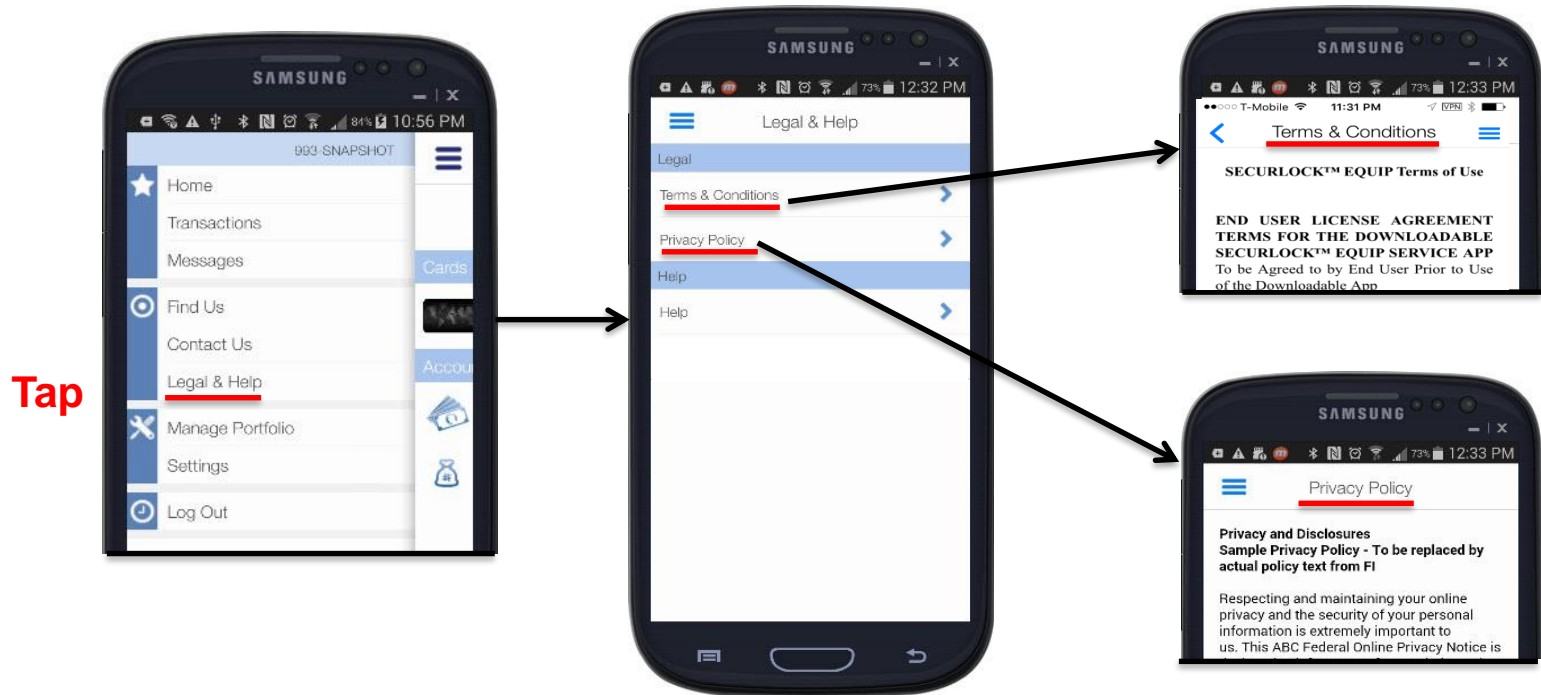
Contact Us



- By tapping the “Contact Us” icon from the Home Menu (and also from the Welcome screen), the user can see the contact information of the financial institution.
- Tapping the phone number and tapping “Call” enables the user to reach the financial institution for assistance.
- Tapping on “Email” provides user the ability to send an email directly to the FI.
- When the user taps on the email link, the app will activate the device’s default email to send a message to the FI; sensitive or personal information should not be sent.

Home Screen – Main Menu Options

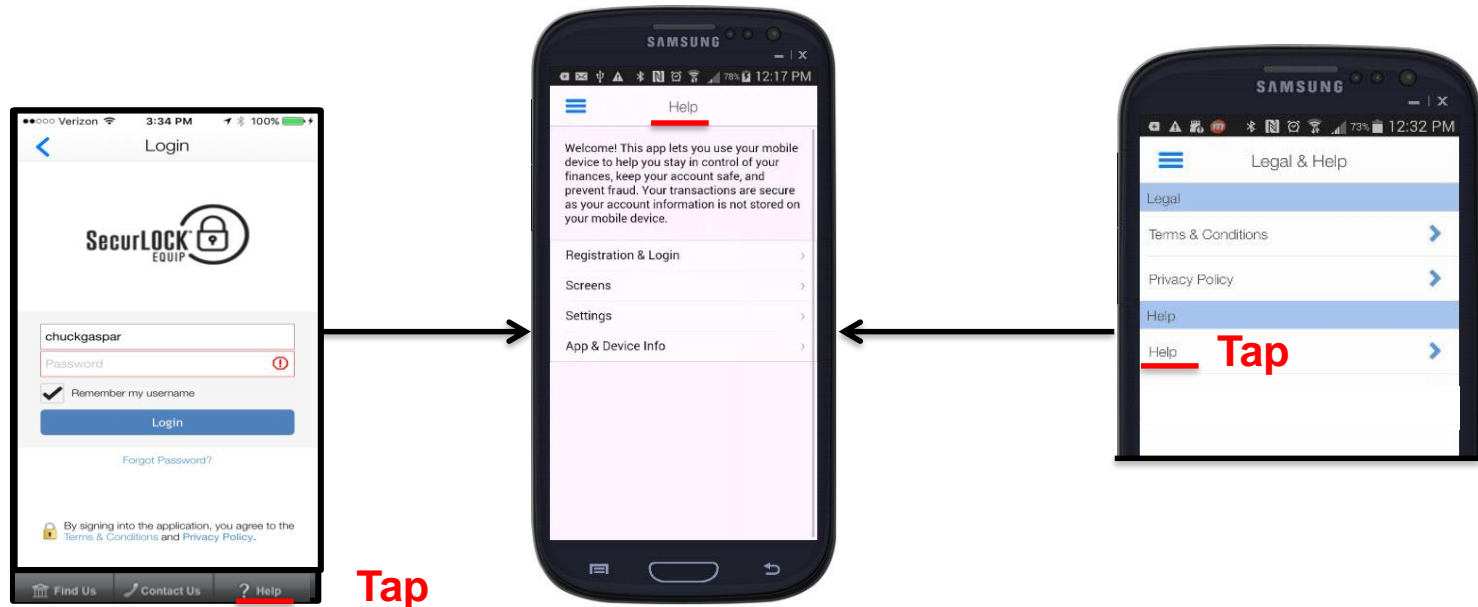
Legal and Help



- Tapping “Legal & Help” on the Home Menu takes user to the “Legal & Help” page.
- Here, user can tap on “Terms & Condition” or “Privacy Policy” to view the respective legal document that s/he accepted during the registration process.

Home Screen – Main Menu Options

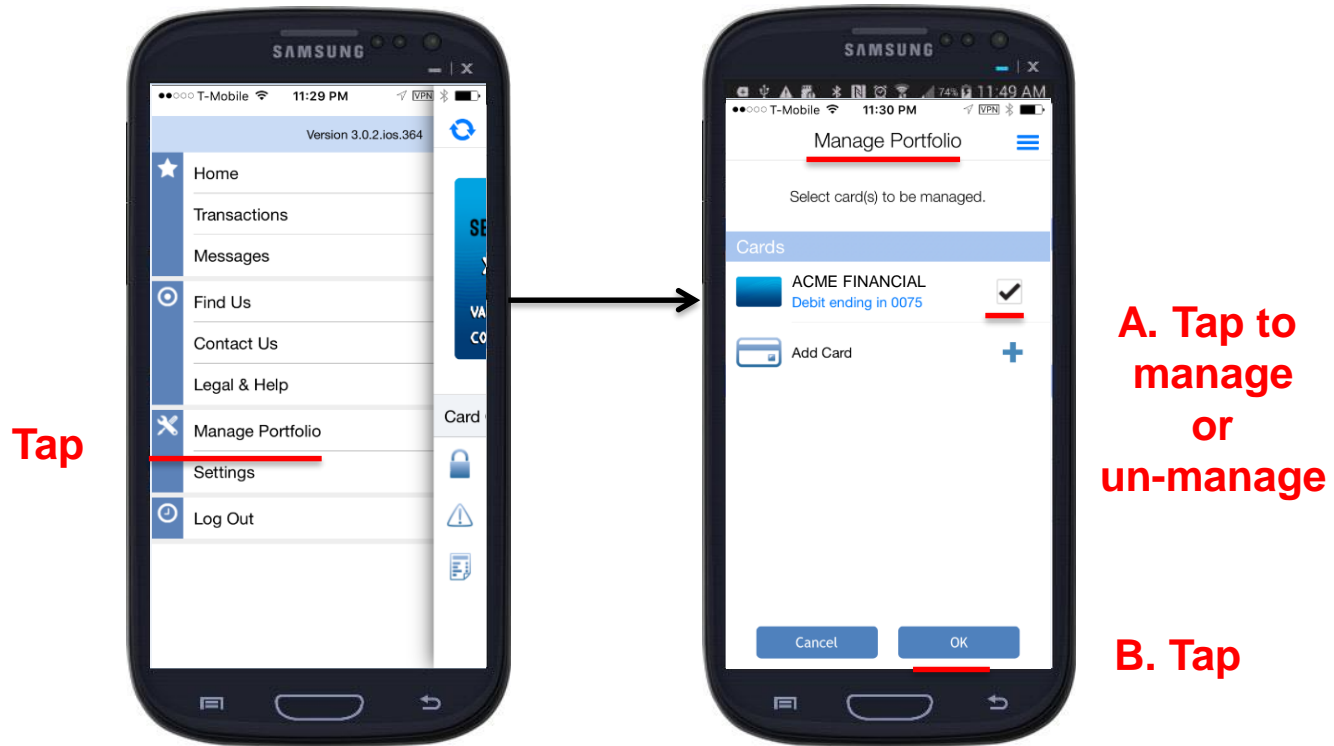
Help



- Tapping the question mark icon on the Welcome page will bring the user to the Help page.
- The Help page is a text document that covers all major functionalities of the app.
- On this page, a user can tap different sections to see more detailed information.
- Tapping “Help” from Legal & Help on the main menu (post login) also takes user to this page.

Home Screen – Main Menu Options

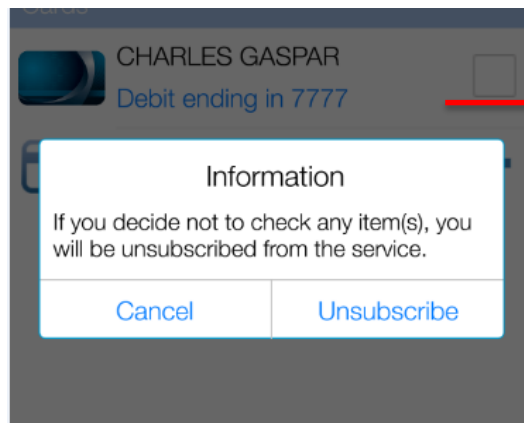
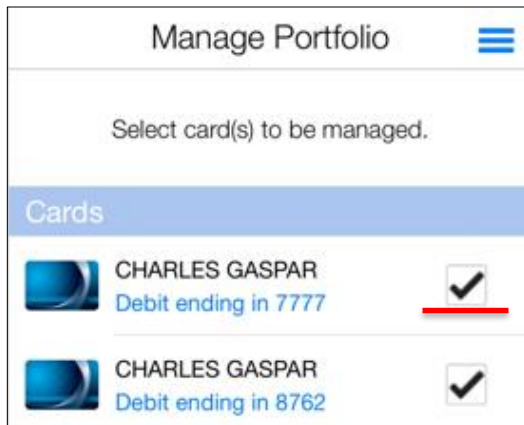
Manage Portfolio



- Tapping “Manage Portfolio” from the Home Menu takes a user to the “Manage Portfolio” page. Here, the user can select cards to be managed or unmanaged by the app.
- To un-manage a card, the user unchecks the box next to it, then taps “OK”.

Home Screen – Main Menu Options

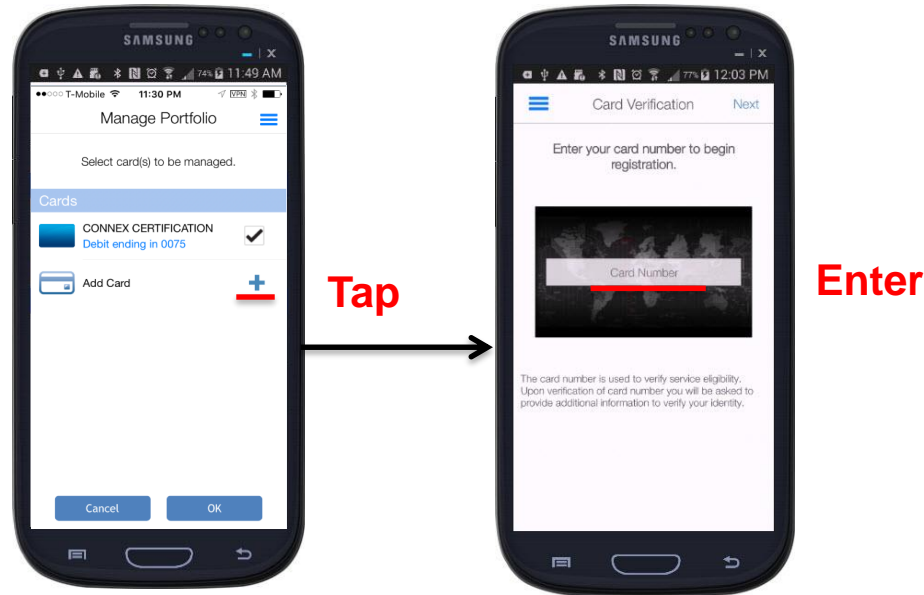
Manage Portfolio



- A card can only be unmanaged from within the app.
- An unmanaged card will no longer be viewable on the Card Details page.
- If a user chooses to un-manage all cards s/he will be asked if s/he wishes to unsubscribe from the service.
- If the user wants to use the app again after unsubscribing, s/he will have to register as a new user.
- Users are able to reuse a Login Name that was unsubscribed – as long as another user does not register with it.
- **No cardholder should ever be told to unsubscribe unless it is recommended by FIS. When a user is unsubscribed, data is purged that could help in researching an issue.**

Home Screen – Main Menu Options

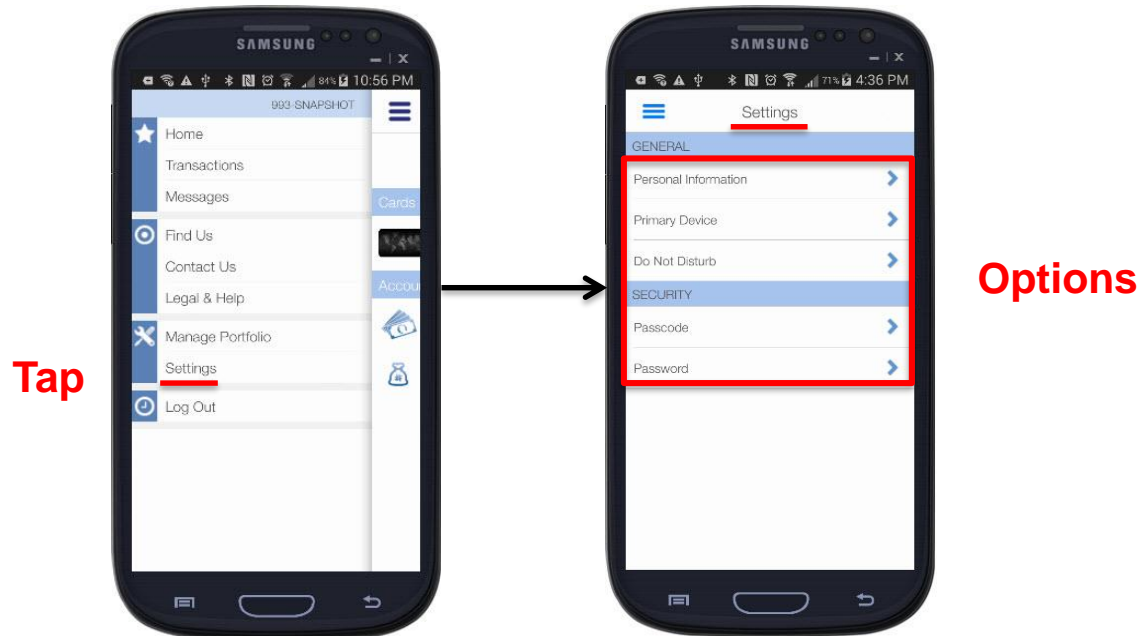
Manage Portfolio – Add a Card



- On the Manage Portfolio page, the user can add a new card(s) for management in the app by tapping “Add Card” (maximum of 15 cards).
- The Add Card process is similar to the Registration process, with the following exceptions:
 - A user is not asked to accept Terms and Conditions and Privacy Policy.
 - A user is not requested to create a new login account.
 - PIN Transaction is not available as an authentication option for “Add Card”.

Home Screen – Main Menu Options

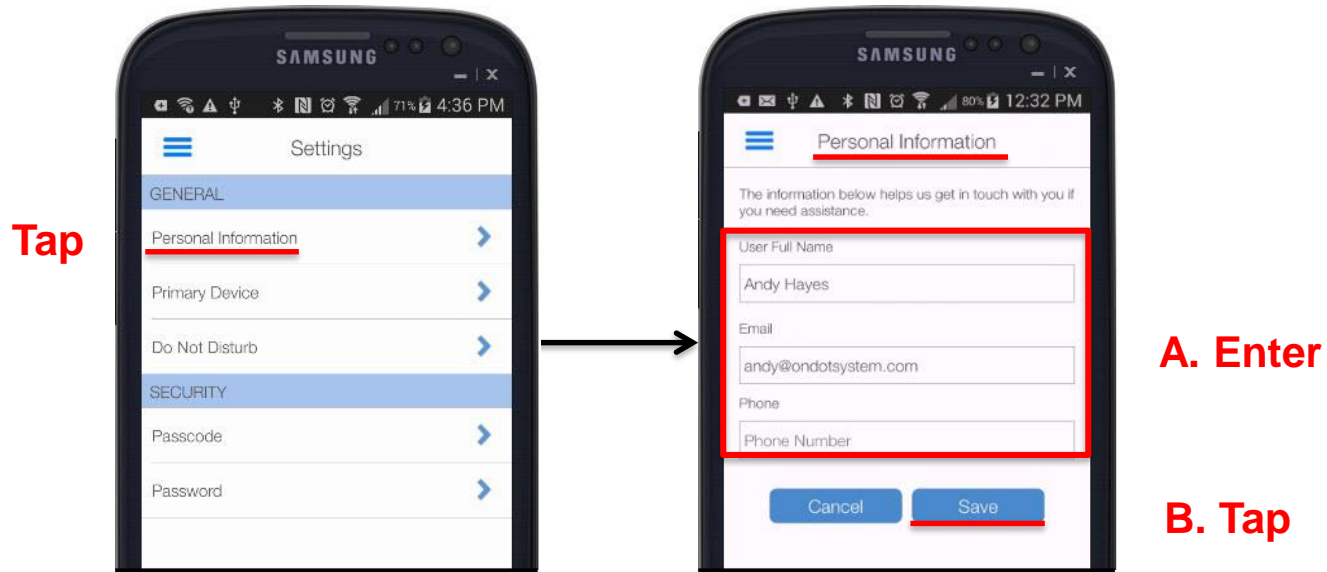
Settings



- Tapping “Settings” on the Home Menu takes a user to the “Settings” page.
- This page provides the user with the following options:
 - Update Personal Information
 - Set Primary Device
 - Set Do Not Disturb window
 - Set Passcode
 - Change Password

Home Screen – Main Menu Options

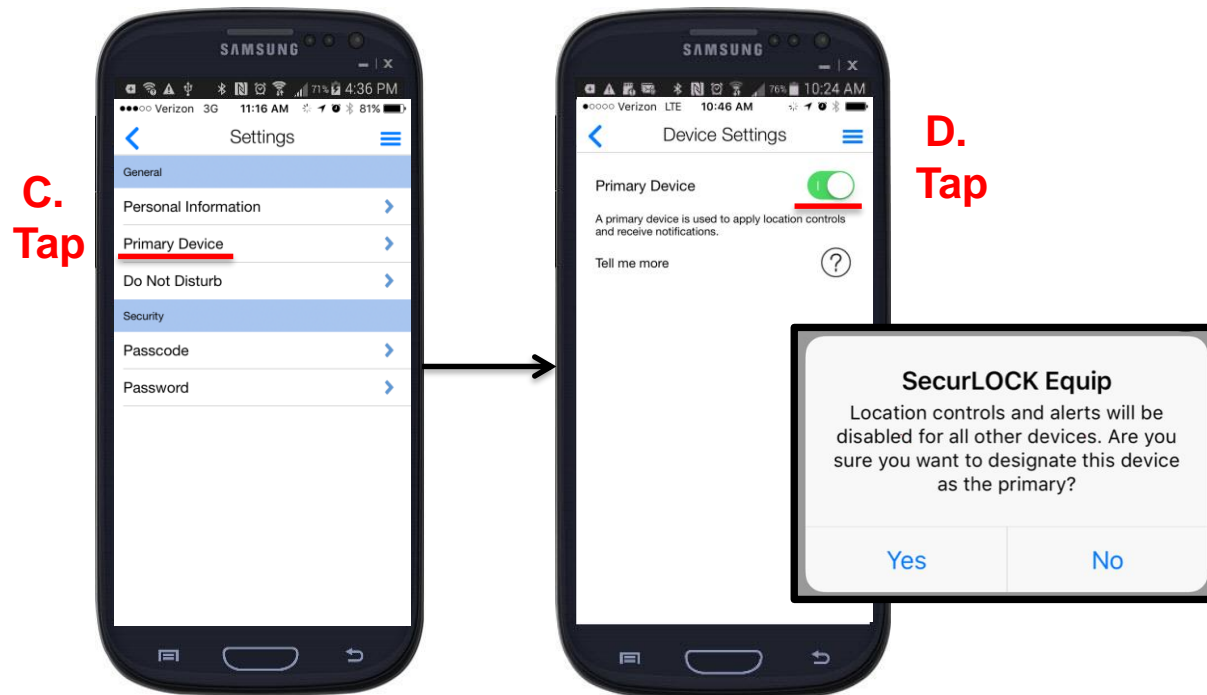
Personal Information



- Tapping “Personal Information” on the Settings page takes the user to the “Personal Information” page. This page enables the user to modify the following information:
 - User Full Name – this information is displayed in the Home page and also appears in notifications sent to other users.
 - Email – the email address that the app will send the security code email to when the user triggers the “Forgot Password” functionality.
 - Phone – this information will display in mConsole.

Home Screen – Main Menu Options

Primary Device

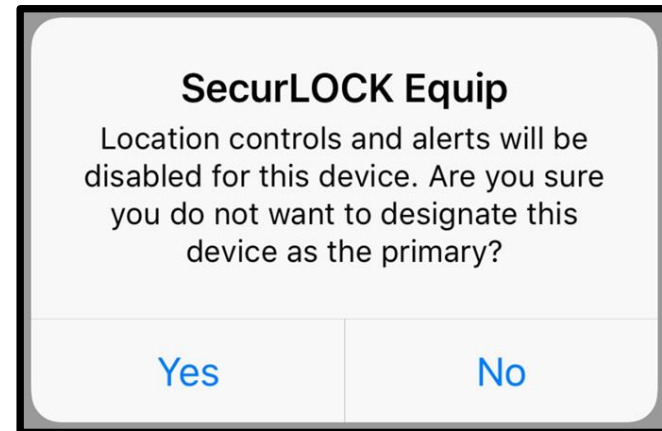
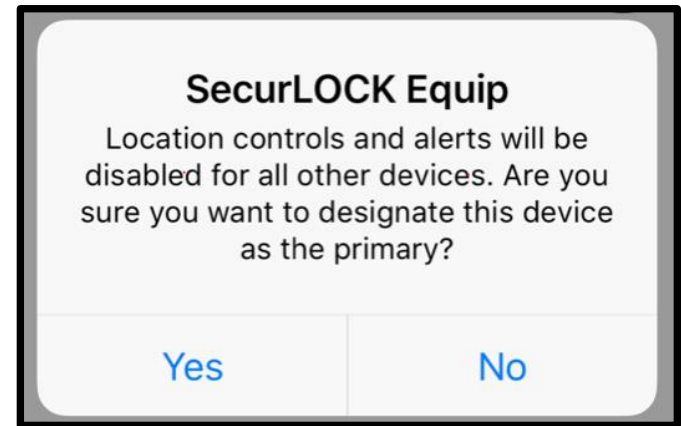


- In order to receive alerts, a user must set the phone s/he wants to receive alerts on as the Primary Device.
- To set a phone as the primary device, follow these steps:
 - Tap on “Primary Device.”
 - Tap the “Primary Device” slider to the “ON” position.

Home Screen – Main Menu Options

Primary Device

- The message that displays after the device is made primary indicates that if the same Login Name was used to login to another device, *that device* will no longer be primary.
- Only one device can be primary when logging into multiple devices with the same Login Name.
- When Primary Device is disabled, another message will display to ensure the user wants to make the change.



Home Screen – Main Menu Options

Primary Device

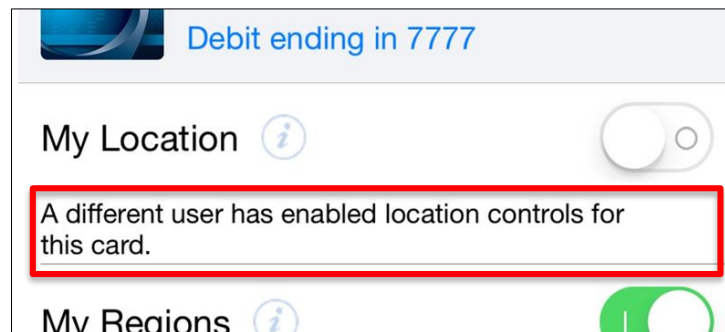
Additional information regarding the setup of Primary Device:

- **One Login / Multiple Devices / Shared Card Number:**
 - **The Primary is based on the DEVICE, not the user.**
 - **Only the Primary Device will get alerts and be used for location controls.**
- **If one Login Name is used on multiple devices (a husband and wife share one Login Name or one user logs into multiple devices with the same Login Name), only ONE device can be set to primary.**
- **When a device is set to primary, a message will display to confirm the action. See previous slide.**
 - **The Primary Device setting will be automatically disabled on the other device.**

Home Screen – Main Menu Options

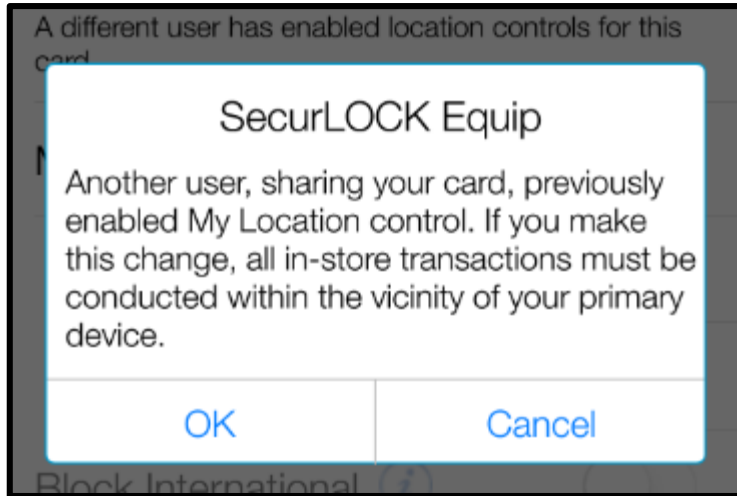
Primary Device

- **Multiple Logins / Devices & Shared Card Number:**
 - The Primary is based on the DEVICE, not the user.
 - Multiple users can register/add the same card number.
 - Multiple devices can be set as primary.
 - My Location controls can only be enabled on ONE primary device.
- **PAN (Primary Account Number) can be shared between multiple users.**
- **If multiple users select My Location for location-based control, then the app will track the location of the user who chooses My Location last. For other users, the app will display a message under the My Location control.**



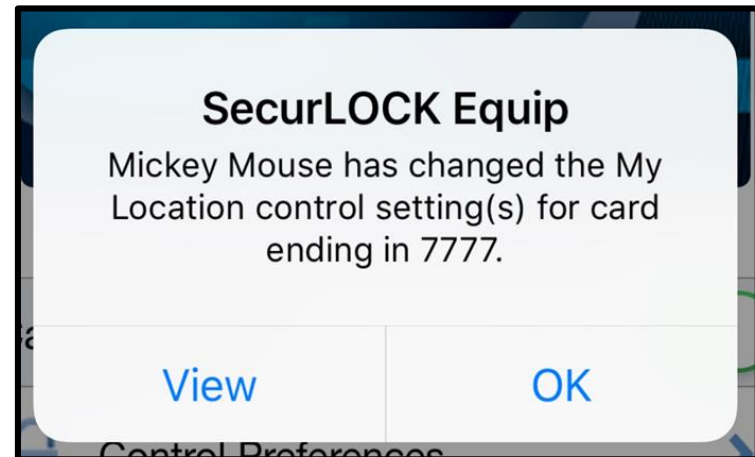
Home Screen – Main Menu Options

Primary Device



- When another user does decide to enable location controls, a message will display to ensure the user wants to make the change.

- When the change is made, the other user(s) will get a message indicating that another user made an update. In this example, Mickey Mouse's device is now being used for My Location.



Home Screen – Main Menu Options

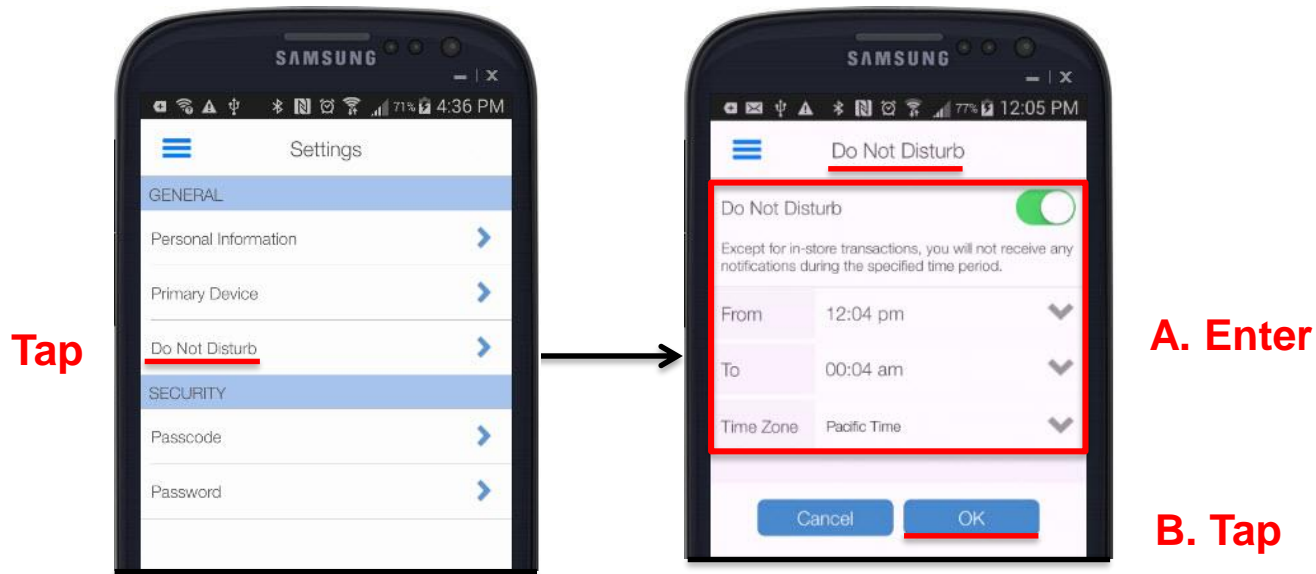
Primary Device

Additional information regarding the sharing of the same PAN:

- **Shared card users share control settings.**
- **If one user turns the card off, all other users will see the card status as “OFF” in their app. An alert is sent to other shared card users whenever a user changes control policies for the card.**
- **While control policies are shared, each user can set up his/her own separate alert preferences – as long as the device is Primary. The user will receive alerts based on the alert preferences set up individually.**
- **All users will receive alerts for denied transactions.**
- **If a user un-manages the shared card or unsubscribes from the app, NO alert is sent to the other card users who have registered or added the same card.**

Home Screen – Main Menu Options

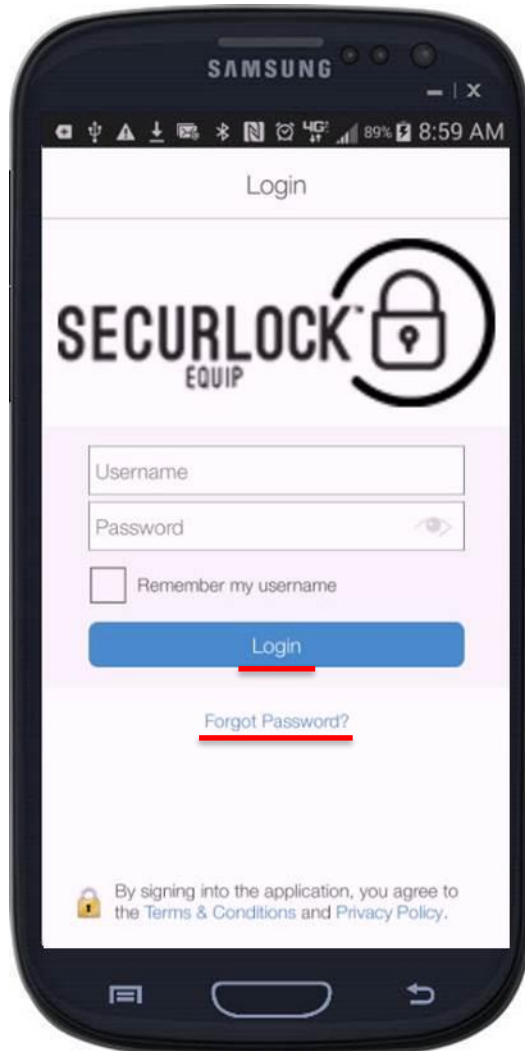
Do Not Disturb



- Tapping “Do Not Disturb” on the Settings page takes the user to the “Do Not Disturb” page. This page enables the user to set a specific time of the day during which the app would not send the mobile device any notifications.
- To set the “Do Not Disturb” window, the user taps the “Do Not Disturb” slider to the “ON” position, selects the time window and time zone and taps “OK”.
- Alerts for card present transactions during the “Do Not Disturb” window can later be viewed in Messages.

Home Screen – Main Menu Options

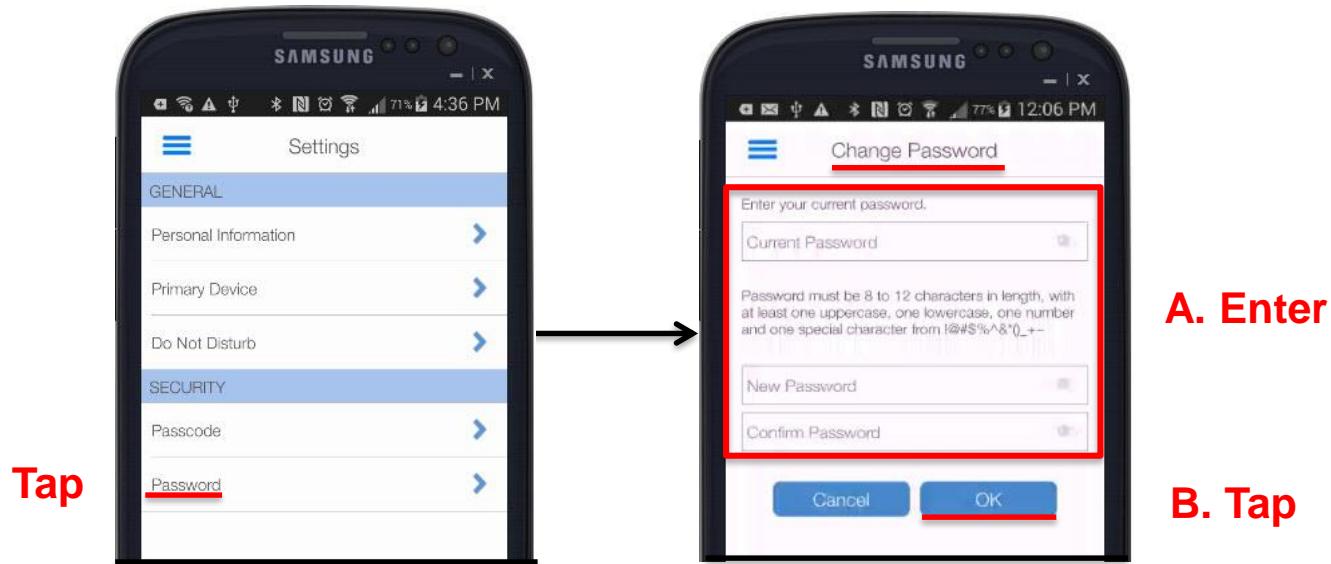
Change Password



- Upon opening the application, the user is provided with the option to:
 - Login to the application
 - Create a new password

Home Screen – Main Menu Options

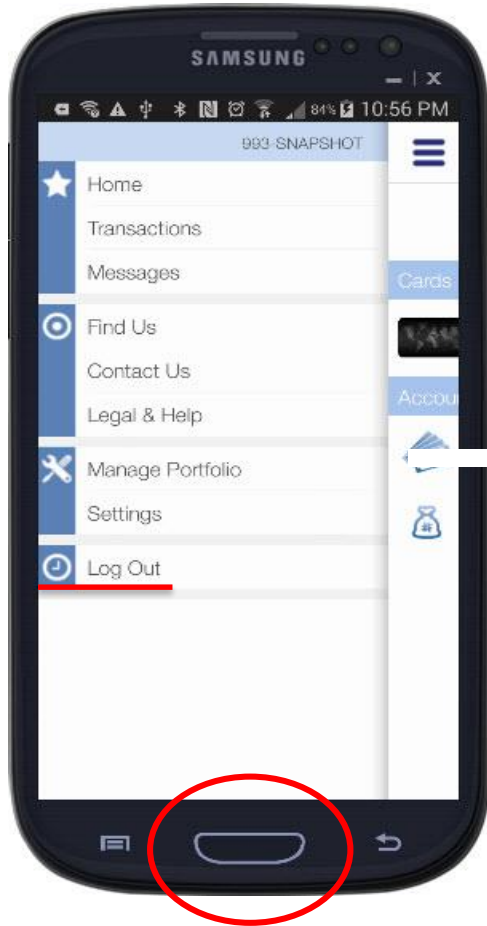
Change Password



- Tapping “Password” on the Settings page takes user to the “Change Password” page. This page enables the user to change the password for logging into the app.
- To change her/his password, the user needs to enter the old password and enter the new password twice to confirm the entry.
- A password must be 8 to 12 characters in length, with at least one upper case, one lower case, one number and one special character from !@#\$%^&*()_+~.
- To correctly enter the password characters, the user can tap the “Eye” Icon, which will make the password entered visible.

SecurLOCK™ Equip – Mobile App Procedures

Logout



There are two ways to exit the app:

1. By pressing the Home button
 2. By logging out.
- By pressing the Home button, the user is brought to the home page and can access the app again by Touch ID or Passcode.
 - By selecting “Logout” from the Menu, the user will be logged out of the application and brought to the Login page.
 - To log back into the application the user will need to enter their User ID and password.

SecurLOCK™ Equip – Mobile App Procedures Review

- **Install application**
- **Register user**
- **Reset password**
- **Home screen**
- **View card details**
- **View transactions**
- **Set up control preferences**
- **Set up alert preferences**
- **Home Screen - Main menu options**

Empowering
the Financial World



Copyright © 2017 by Fidelity National Information Services (FIS). All Rights Reserved.

This document is intended for use only by FIS Corporation customers in conjunction with products and services authorized by FIS Corporation. Any other use is prohibited.

©2016 FIS and/or its subsidiaries. All Rights Reserved. FIS confidential and proprietary information.