

# SecurLOCK™ Equip - Mobile App Procedures

Version 3.8

**April 2019**

Empowering  
the Financial World



# SecurLOCK™ Equip – Mobile App Procedures

## Introduction

- [Objectives](#)
- [Communicate vs. Equip Quick Comparison](#)
- [Marketing Website Link](#)
- [Install Application](#)
- [Register User](#)
- [Logging In to the Mobile App](#)
- [View Card Details](#)
- [View Transactions](#)
- [Set Up Control Preferences](#)
- [One-time Override](#)
- [Set Up Alert Preferences](#)
- [Home Screen - Main menu options](#)
- [Reset Password](#)
- [App Rating](#)

# **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 view point**
- **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**

# SecurLOCK™ Equip – Mobile App Procedures 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 all Visa/MC Mandates

### What are the Benefits?

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

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

# SecurLOCK™ Equip – Mobile App Procedures

## Marketing Website Link

[http://tools.cardholderadoption.com/SecurLOCK\\_Equip](http://tools.cardholderadoption.com/SecurLOCK_Equip)

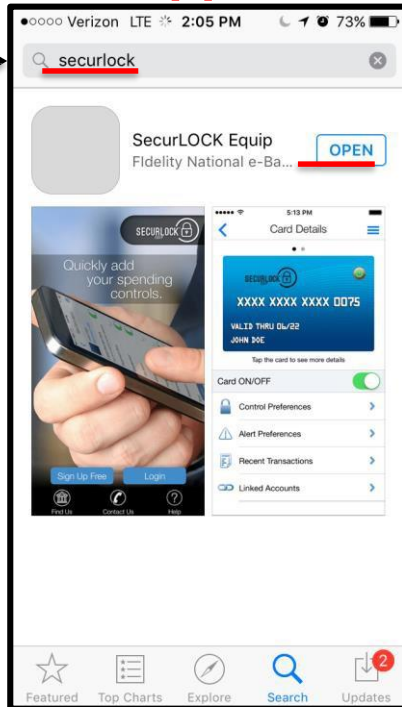
- Use the link above to access:
  - Marketing material
  - This training guide/deck
  - Frequently Asked Questions
  - How 'My Regions' and 'My Location' differ in detail

# Install Application

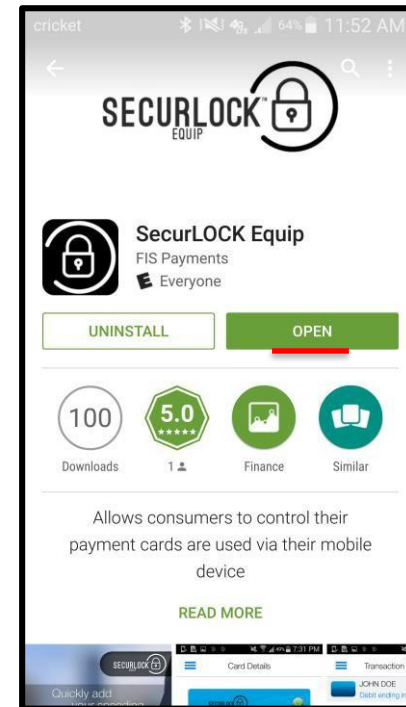
## Start – Download the Application

### Apple

Enter



### Android



- A user will download the app for their iPhone via the App Store or for their Android device via the Google Play Store.
- The app can be used and downloaded both domestically and internationally.

# Install Application

## Start – iPhone Example

- A user with an Apple phone will need to access the 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

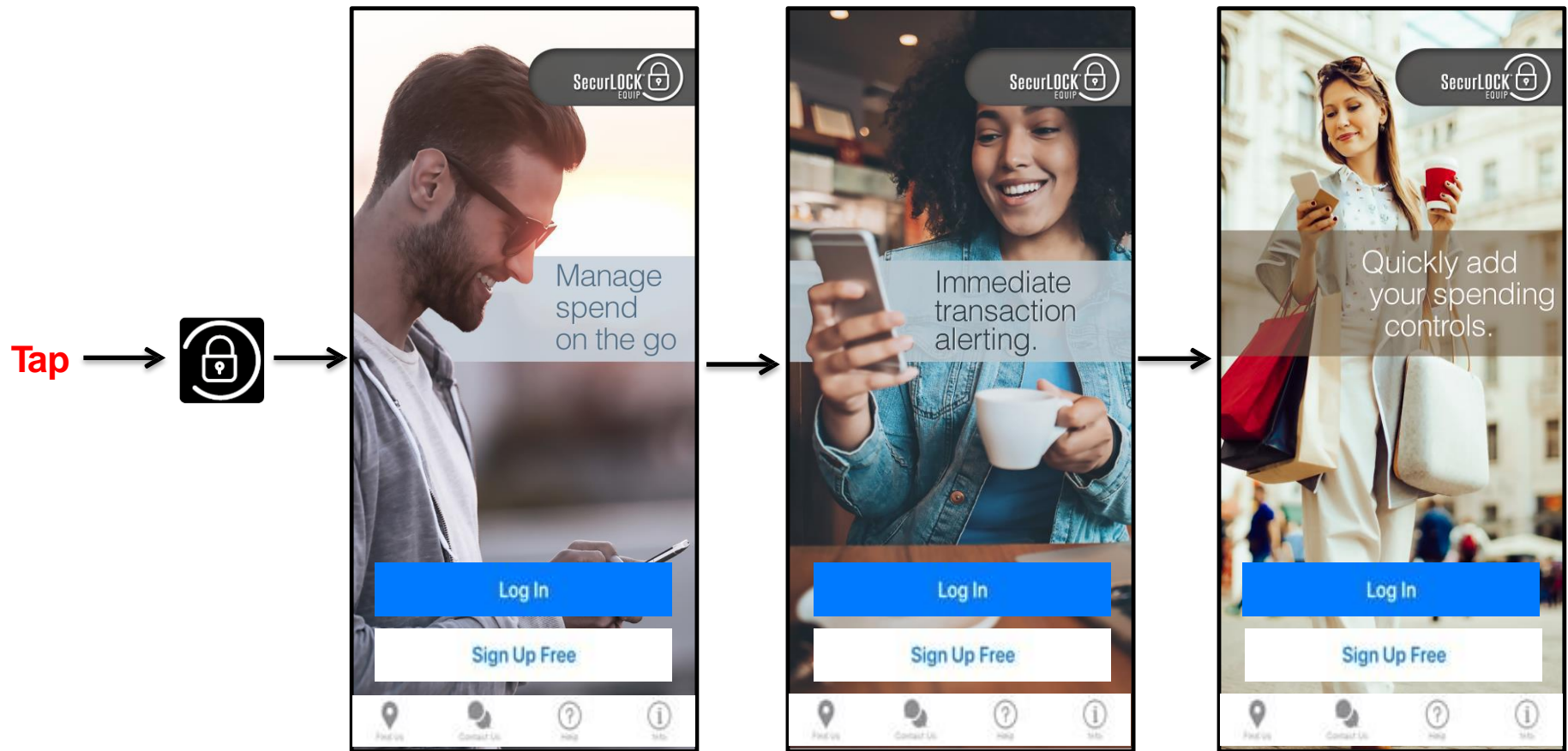
- A user with an Android phone will need to access the Google Play Store to search for the SecurLOCK Equip app, download and install it.
- In this Android example, as the phone downloads the app, the word at the bottom of the spring board icon will change to 'Installing' and the loading bar will fill.

**View**





# Register User Launch App

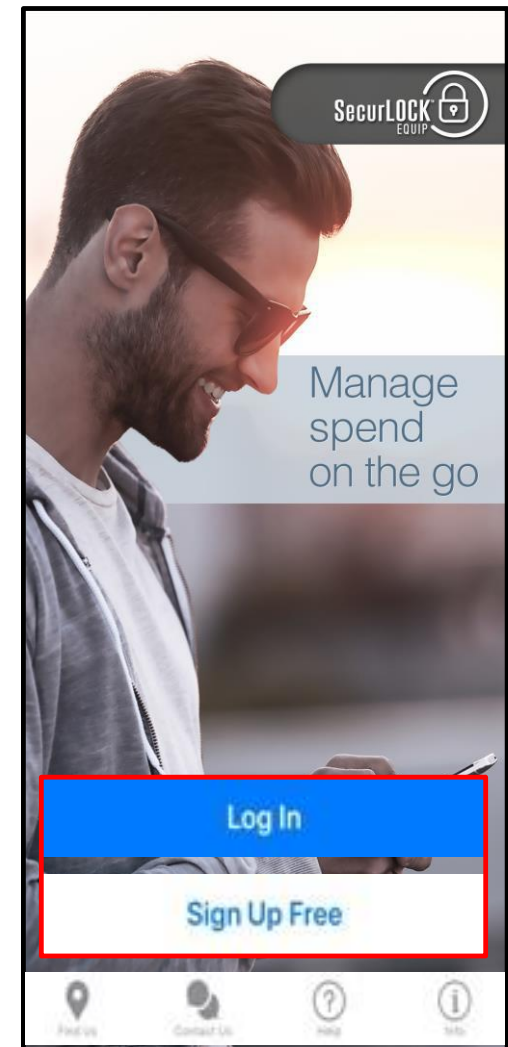


- Once completely downloaded, the spring board icon will disappear and be replaced with the "SecurLOCK Equip" app icon.
- Tap on the 'App' icon to launch the app.
- Users will see the above splash page once the app launches.

# Register User

## User Options

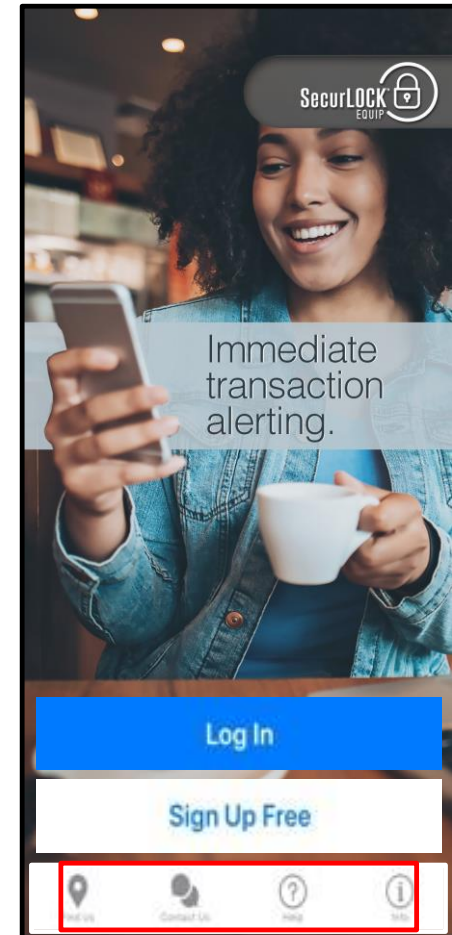
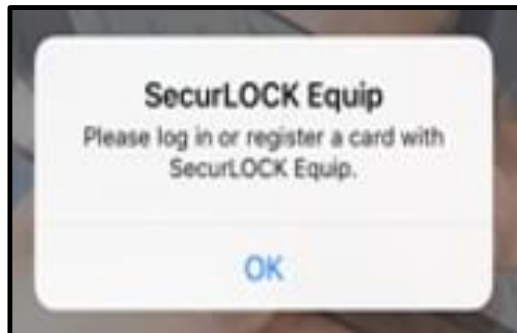
- **Upon opening the application, the user is provided with options to:**
  - Sign Up Free (Register as a new user)
  - Log In to the application (if the user already has a login).



# Register User

## User Options

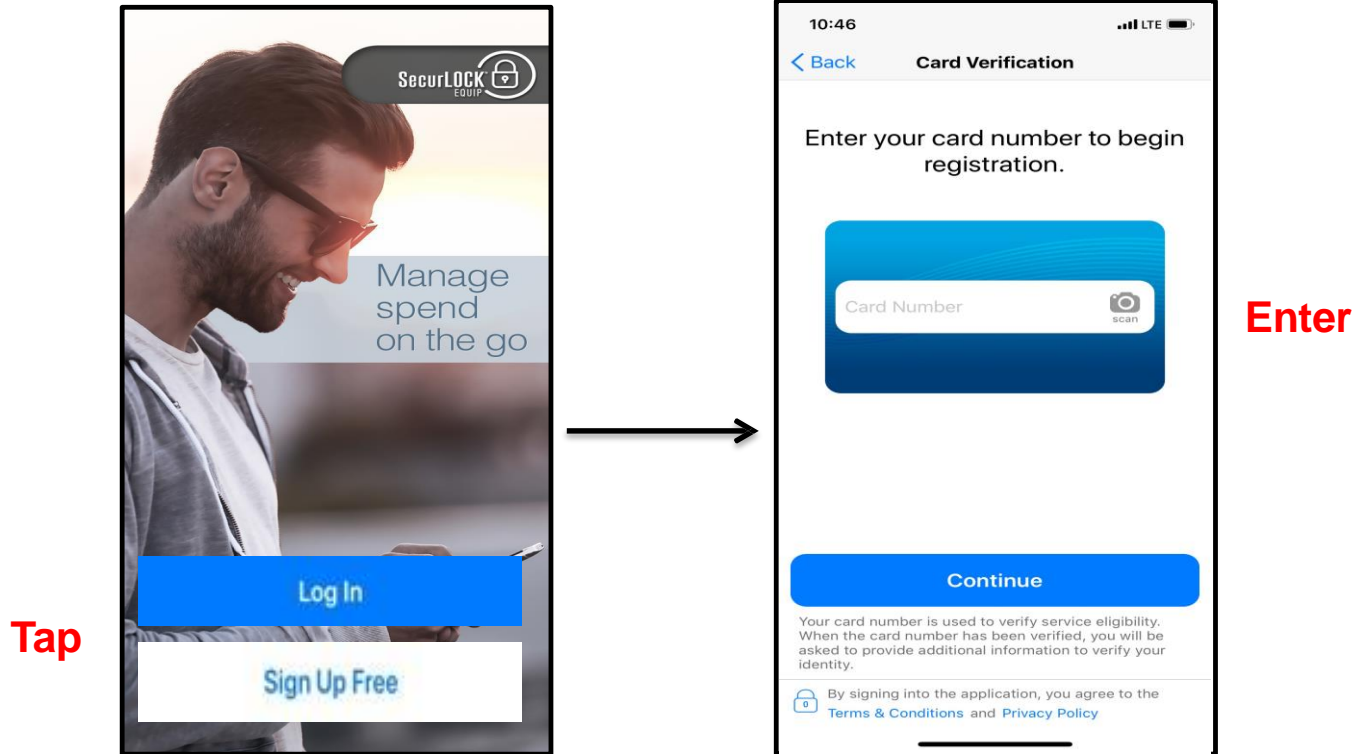
- The bottom menu options allow registered users to:
  - Find ATMs in a specific area
  - Contact the user's financial institution
    - ❑ If Find Us and/or Contact Us data is not added to mConsole during implementation, then the corresponding icon will not display or be available in the app.
  - Get help on the app usage
    - ❑ 'Help' is a text document that covers all major functions of the application.
  - If the user selects one of these options before registering an informal message will display:



**Tap**

# Register User

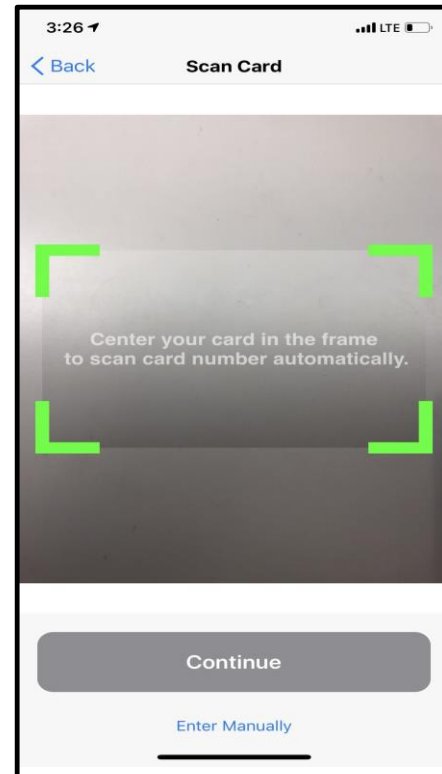
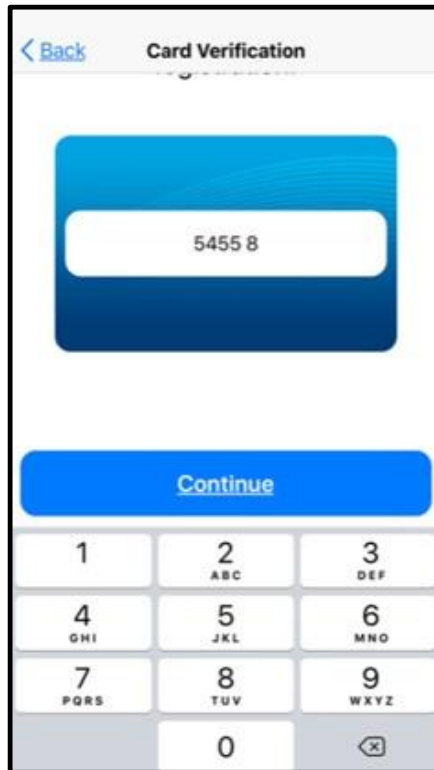
## User Authentication



- To use the SecurLOCK™ Equip Mobile App, a user must first register at least one card.
- Tapping on 'Sign Up Free' button will start the registration process.
- User is prompted to enter or scan the card number.
  - Please note: non-embossed cards cannot be scanned.
  - Multiple users can register the same card.

# Register User

## User Authentication (First Factor)



- After entering the full card number or scanning the card, the user taps 'Continue'.

# Register User

## User Authentication (First Factor)

The image shows two sequential screenshots of a mobile application's 'Card Verification' screen, connected by a right-pointing arrow. Both screens have a title bar 'Card Verification' and a card number field 'XXXX XXXX XXXX 1538'. The left screen displays the instruction 'Please enter your address and your security code and expiration date.' followed by input fields for 'Security Code (CVC2/CCV2)', '3 Digit Code at the back of your card', 'Street Address', 'Zip Code', and 'Expiration Date'. The right screen shows the same fields but with a different layout: 'Security Code (CVC2/CCV2)' is at the top, followed by '3 Digit Code at the back of your card', 'Street Address', 'Zip Code', and 'Expiration Date'. Both screens feature a blue 'Continue' button and a smaller 'Cancel' link at the bottom.

- **The user is brought to the Card Verification page for First Factor Authentication:**
  - Security code (MasterCard - CVC2 / Visa - CCV2)
  - Street address and Zip Code
  - Expiration date (MM-YY)
- **After completing FFA, the user taps 'Continue' to go to the Second Factor Authentication (SFA).**

# Register User

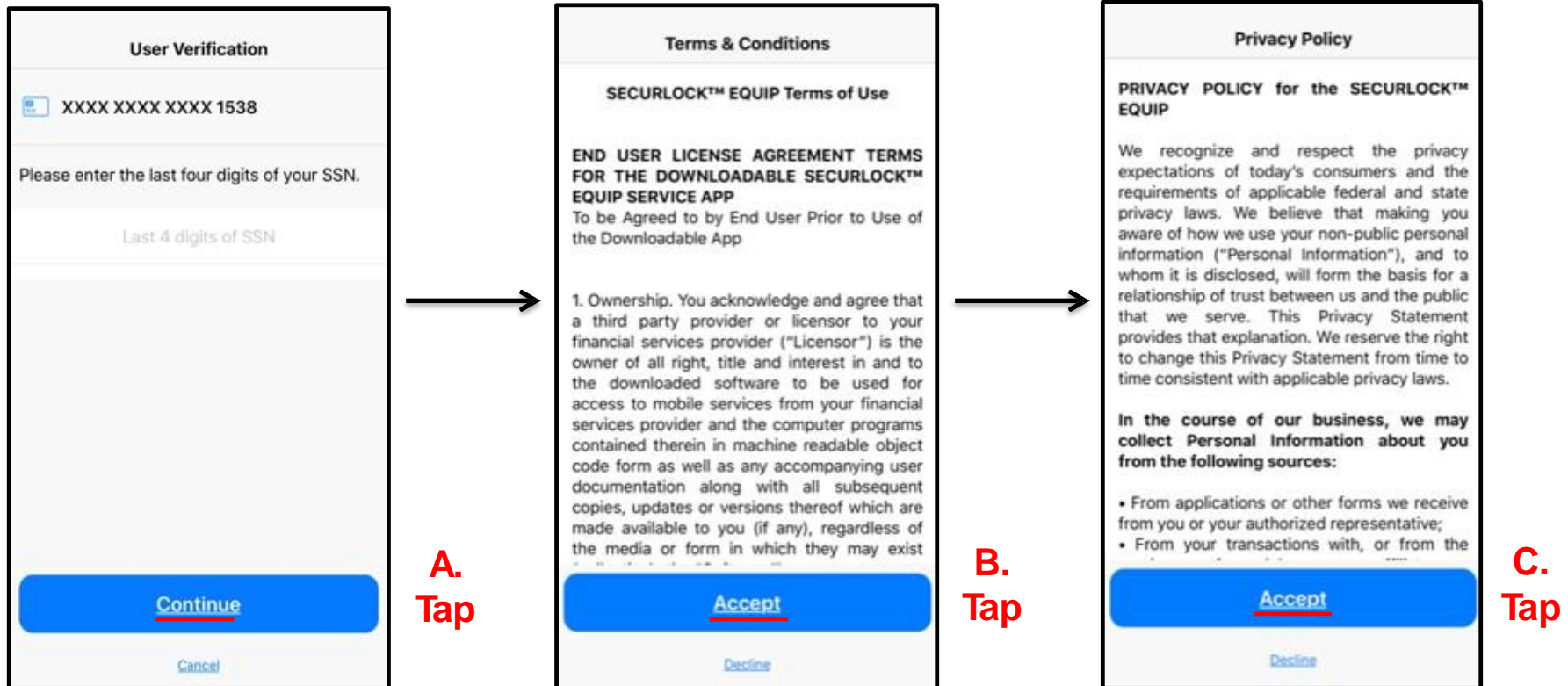
## User Authentication (Second Factor)

- **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 'Continue', 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 corresponding SSN again.



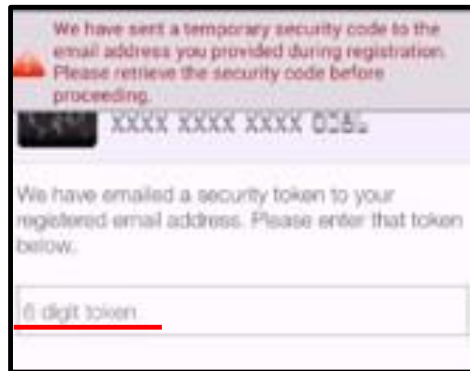
# Register User

## User Authentication – Security Code Verification (Second Factor Authentication)

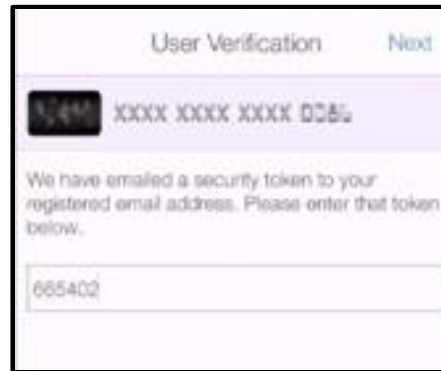
- The Security Code authentication method will be used if criteria listed in Slide 14 is not available.
- If the user's email address is passed on to the SecurLOCK Equip application, the user will be sent an email with a OTP/One Time Password (see Slide #18).
- If an email is not available, then the 'PIN-Based' transaction option will be used for debit card enrollment (see Slide #19).
- If an email isn't available for a credit card, the user will receive a message to contact their financial institution to update the card record.

# Register User

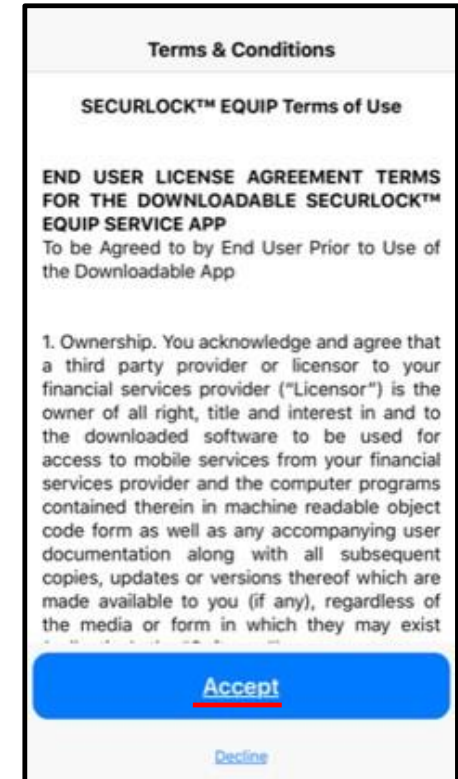
## User Authentication – Security Code Verification (Second Factor Authentication)



**A.**  
**Enter**



**B.**  
**Tap**

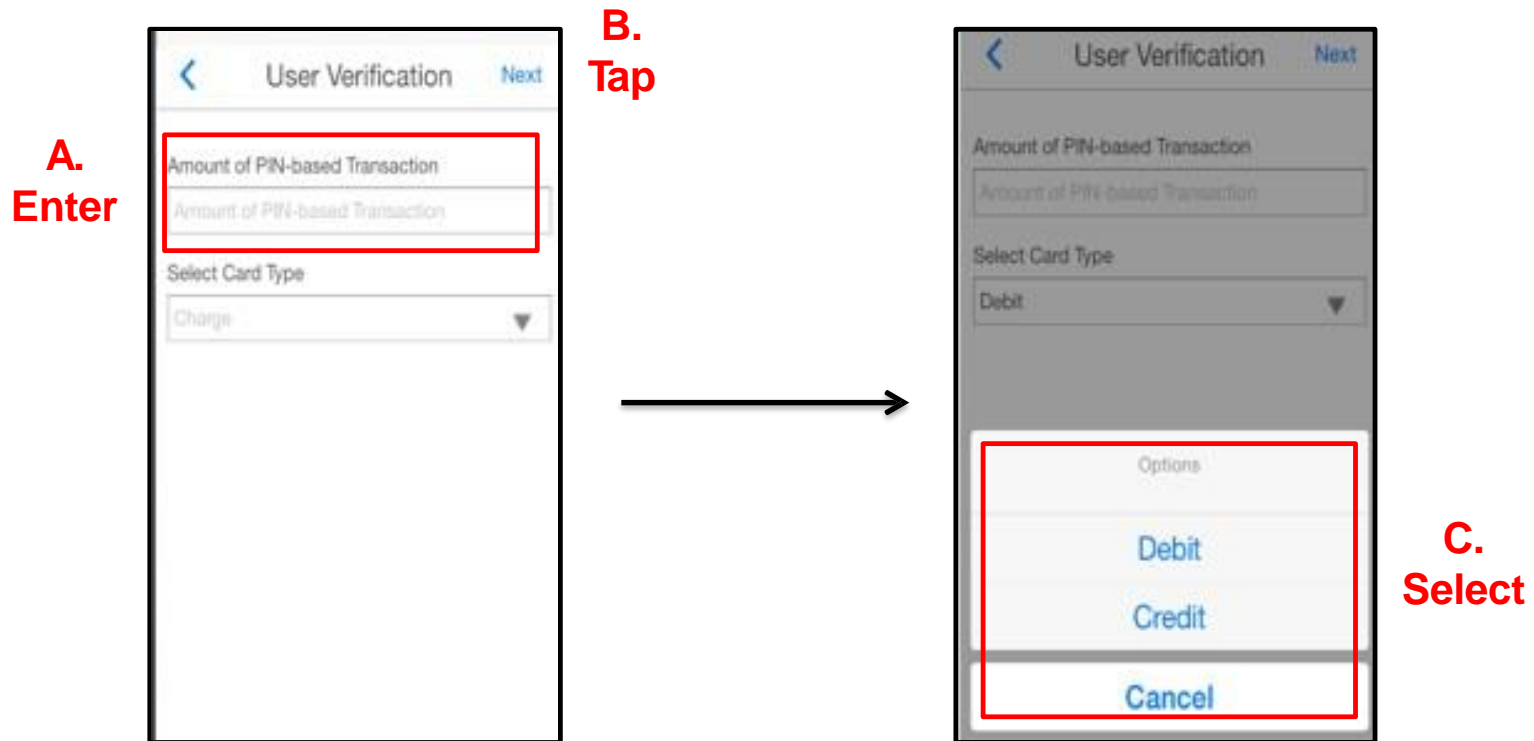


**C.**  
**Tap**

- Email with one time password will also detail OTP expiration timeframe (e.g. token will expire at 10:15am ET).
- The app will prompt the user to enter the one time password.
- After the OTP 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)



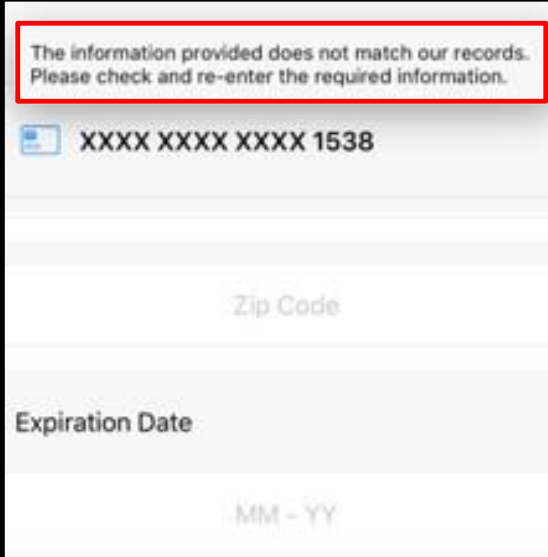
- The user must complete a new PIN-based transaction for any dollar amount within 72-hours of the attempted registration for validation purposes.

# Register User

## User Authentication - Unsuccessful Attempts

- This is the error message received when a user has makes an unsuccessful registration attempt by failing First Factor Authentication.
- 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) caused the error for security reasons.

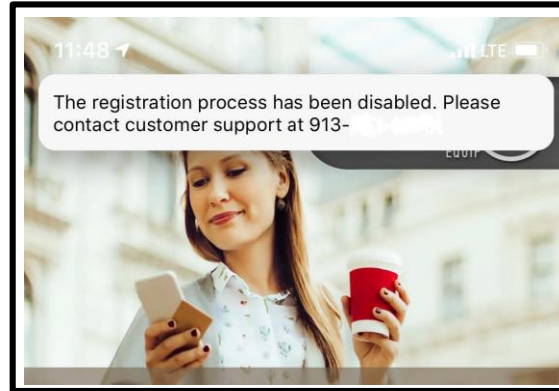
**View**



The screenshot shows a registration form with a red-bordered error message at the top: "The information provided does not match our records. Please check and re-enter the required information." Below the error message, the form contains a card number field with the placeholder "XXXX XXXX XXXX 1538", a "Zip Code" field, and an "Expiration Date" field with the placeholder "MM - YY".

# Register User

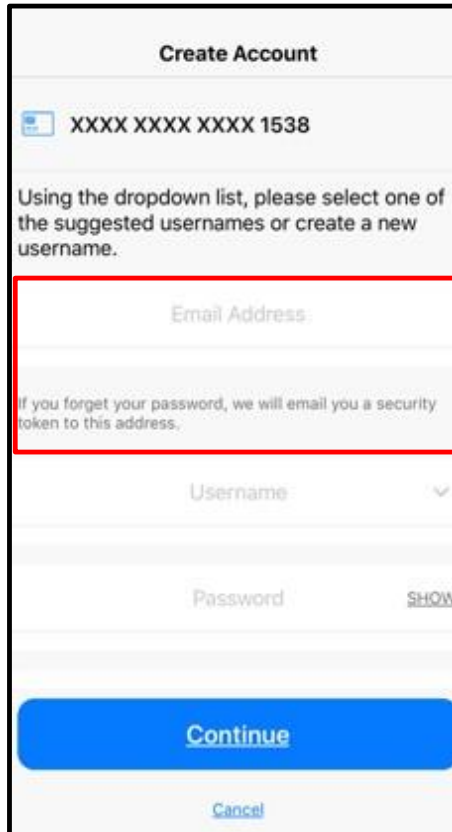
## User Authentication - Unsuccessful Attempts



- **With Second Factor Authentication Failure, after three failed attempts the user will be suspended and brought back to the landing page.**
- **The only way to be reset is for the user to call the financial institution's customer support to have the card registration state reset (covered during mConsole training).**

# Register User

## User Account Creation



The image shows a mobile app screen titled "Create Account". At the top, there is a header "Create Account". Below it, there is a text input field containing "XXXX XXXX XXXX 1538". Below that, there is a paragraph of text: "Using the dropdown list, please select one of the suggested usernames or create a new username." Below this text, there is a red rectangular box highlighting the "Email Address:" input field. Below the red box, there is a small text note: "If you forget your password, we will email you a security token to this address." Below this, there is a "Username:" dropdown menu. Below that, there is a "Password:" input field with a "SHOW" link to its right. At the bottom, there is a large blue "Continue" button and a smaller "Cancel" link below it.

A.  
Enter

- On the Create Account screen, the user enters their email address.
- The email address entered here will only be used for password resets. It **does not** go back to the system of record.

# Register User

## User Account Creation

The image shows two sequential screenshots of a mobile application's 'Create Account' screen, connected by a right-pointing arrow. Both screens have a title bar 'Create Account' and a card number 'XXXX XXXX XXXX 1538' with a card icon. Below the card number, a message reads: 'Using the dropdown list, please select one of the suggested usernames or create a new username.'

**Left Screenshot (Step B):** A red box highlights the 'Username' dropdown menu and the 'Password' field with a 'SHOW' toggle. To the left of this box is the red text 'B. Enter'. Below the highlighted fields is a blue 'Continue' button and a smaller 'Cancel' button at the bottom.

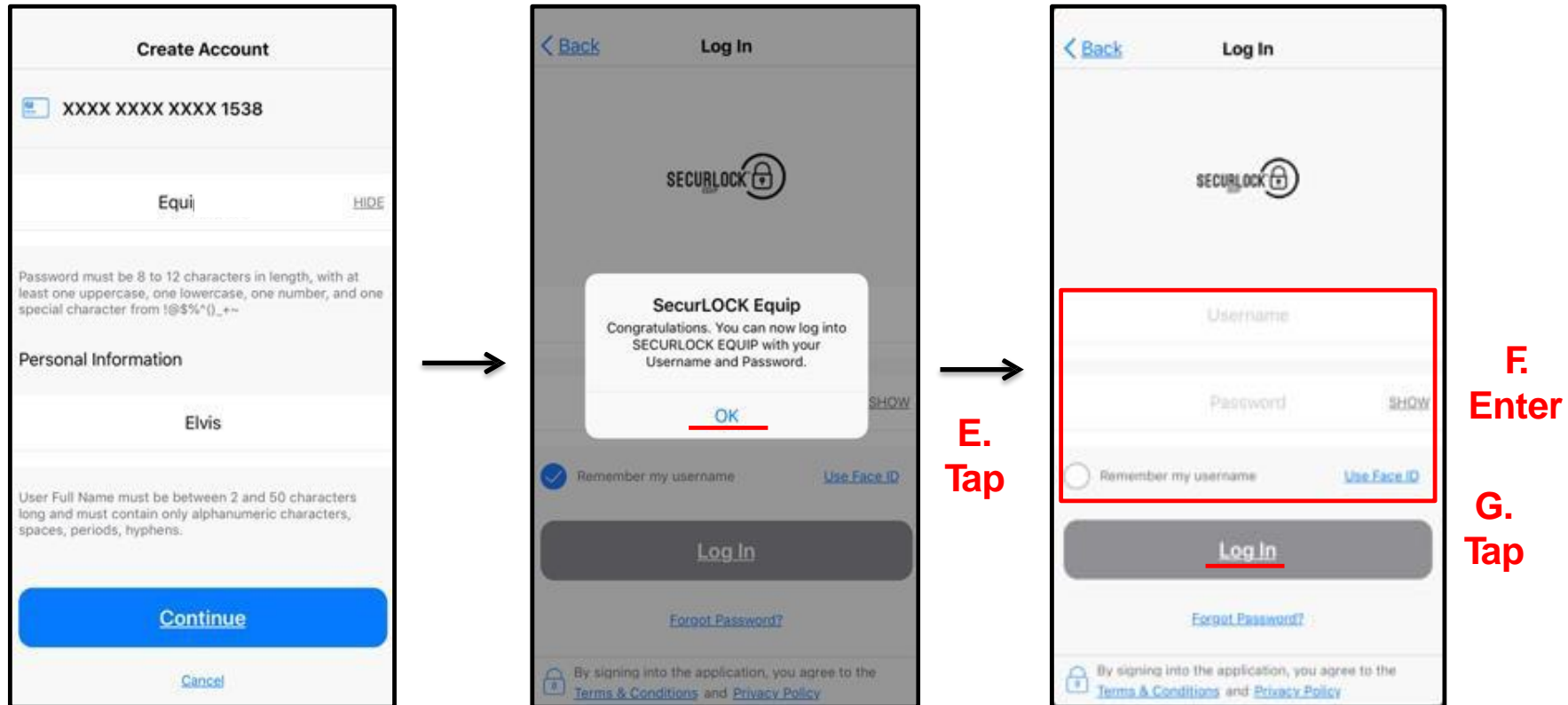
**Right Screenshot (Step C):** A red box highlights the 'Re-Enter Password' field with a 'SHOW' toggle, the 'Personal Information' section header, the 'User Full Name' field, and the 'User Full Name' validation text: 'User Full Name must be between 2 and 50 characters long and must contain only alphanumeric characters, spaces, periods, hyphens.' To the right of this box is the red text 'C. Enter'. Below the highlighted fields is a blue 'Continue' button and a smaller 'Cancel' button at the bottom.

**Step D:** To the right of the right screenshot is the red text 'D. Tap', indicating the final action to complete the registration.

- The user then creates a Username and Password for logging into the app.
- The user may use the drop-down list to select one of the suggested usernames or create a new username. Note: Usernames must be between 6 - 16 characters.
- All Usernames are stored in the same database, so each one must be unique.
- The 'User Full Name' 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 the newly created credentials.

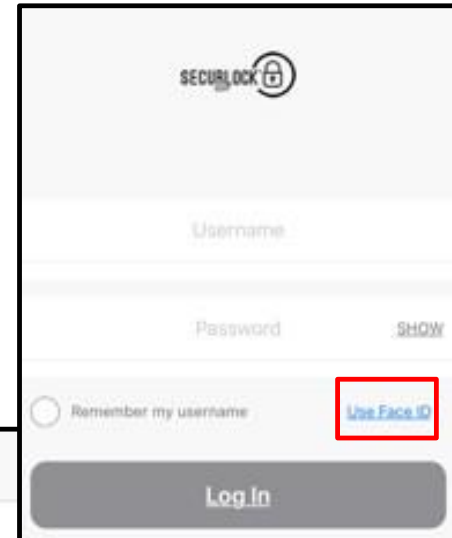


# Logging In to the Mobile App

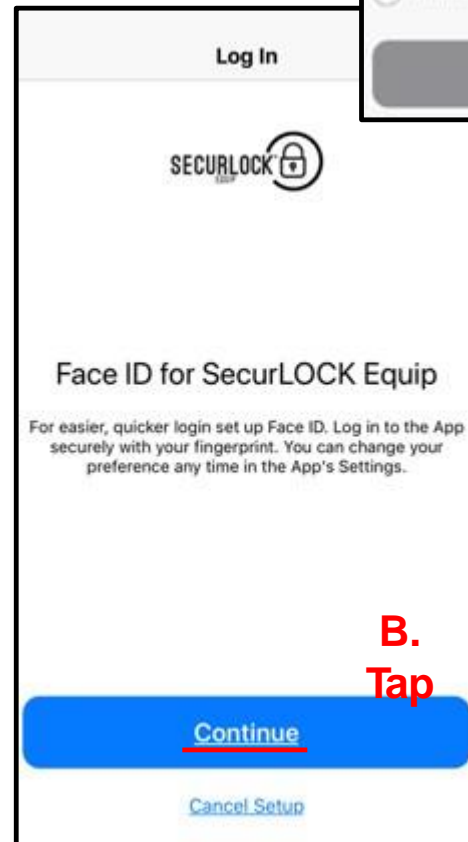
## Touch ID/Face ID (Biometrics)

- SecurLOCK Equip utilizes Apple's Touch ID/Face ID and Android's Fingerprint\* features to authenticate users.
- A user can enable Touch ID/Face ID/Fingerprint on the login screen or via the 'Settings' section after logging in.
- If the user enables this feature, they are prompted to log in to the app by placing their finger on the device's fingerprint scanner or holding the device up to their face.
- A user can dismiss the prompt at any time and enter their password to log in.

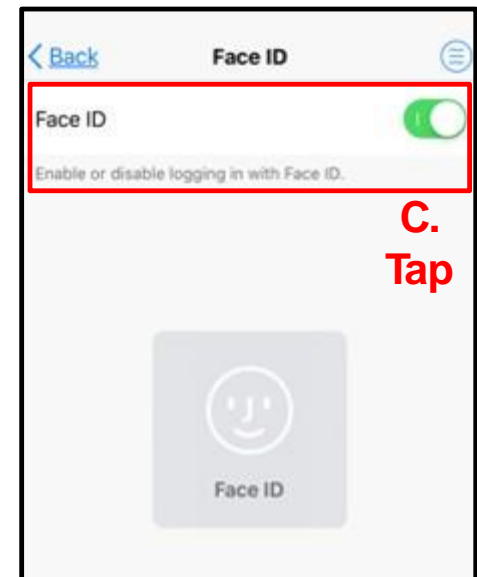
\*Apple's Touch ID/Face ID and Android's 'Fingerprint' features are collectively referred to as 'biometrics' or 'biometric login'



A.  
Tap



B.  
Tap

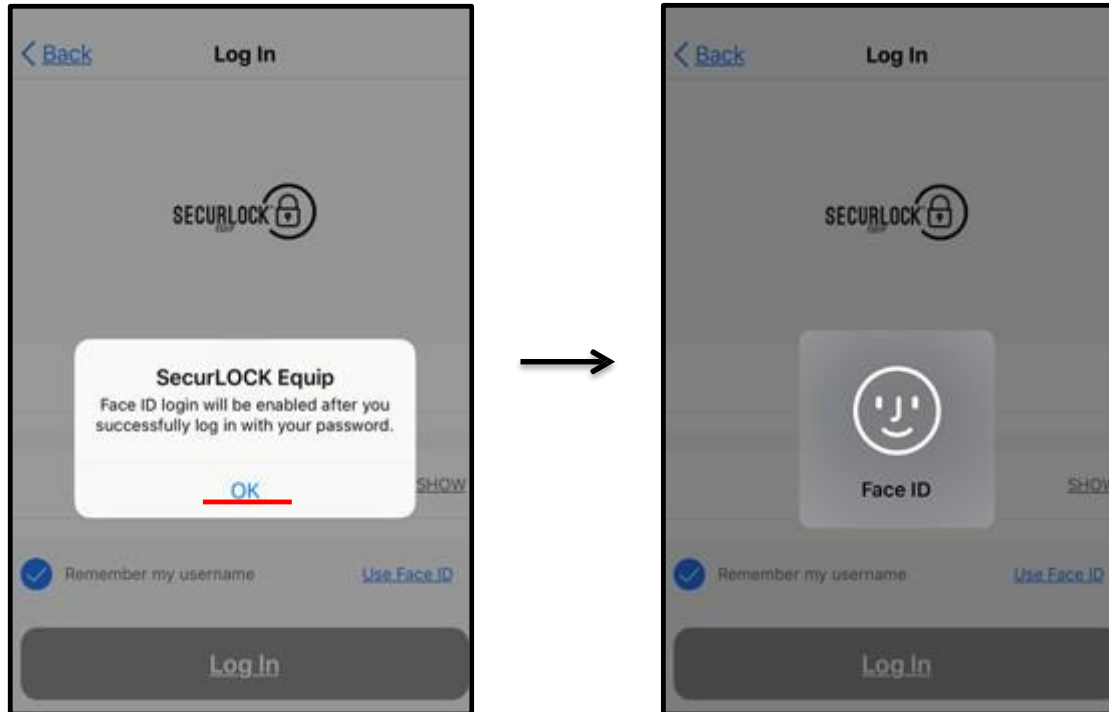


C.  
Tap

# Logging In to the Mobile App

## Biometrics

**D.**  
**Tap**



- The option to enable Touch ID/Face ID on iOS or Fingerprint on Android is available on the login screen.
- Once a user selects the option and successfully logs in with a username and password, biometric login is enabled.
- When biometric login is enabled, users are prompted with the Touch ID/Face ID or Fingerprint (Android) option when they attempt to log in.
- When a match is found with the biometrics stored on the mobile device (authenticated by the OS), the user is logged in to the Mobile App.

# Logging In to the Mobile App

## Password vs Passcode

- Users with mobile devices that do not have biometric capability are given the option to utilize a numeric Passcode instead of Touch ID/Face ID/Fingerprint. When this feature is enabled, these users can use that numeric Passcode to extend sessions.
- Users with a biometrics-capable mobile device will not be offered the Passcode option. They are presented only with the option to set up Touch ID/Face ID/Fingerprint.
  - **Password (PW)** - to login to the app, a user will need to enter the credentials (username and password) or login using biometrics. By logging in via this method, the app will create a session ID (20-minutes) in which 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 reauthentication will be required.
  - **Passcode (PC)** - is an additional security setting provided by the app specifically for users without biometrics capable mobile devices. If a user sets a passcode, each time the user navigates away from the app and comes back, the user will need to re-enter the passcode.

# Logging In to the Mobile App

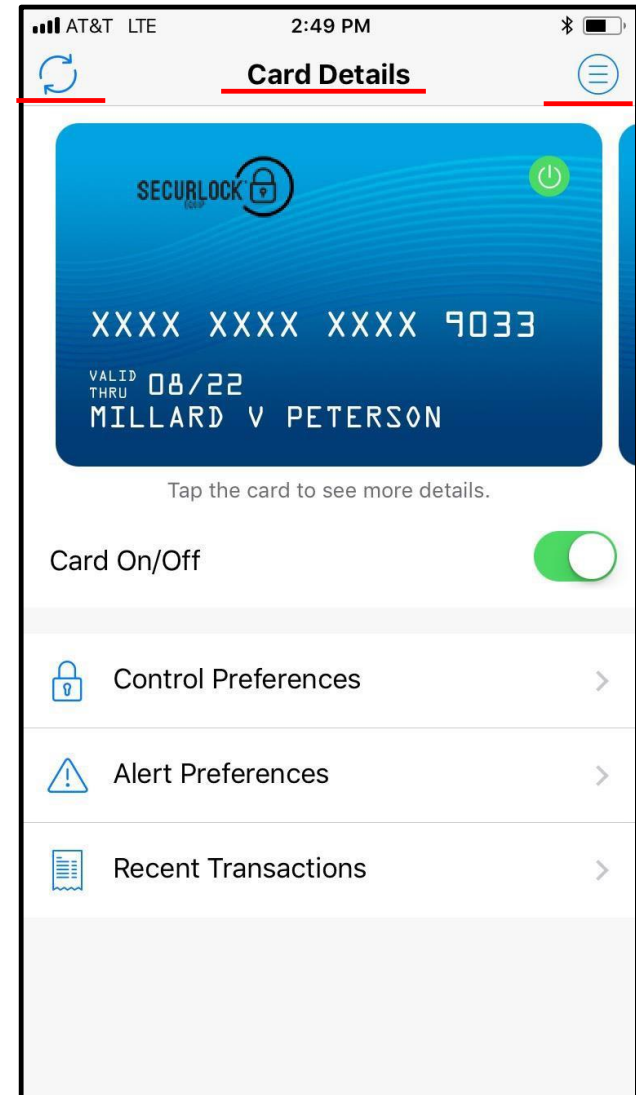
## Password vs Passcode – Timing Scenarios

- **Timing Scenario #1**
  - Passcode enabled = Yes
  - User closes the application, but does NOT log out.
  - User re-opens the app and s/he will be prompted for biometrics/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.
- **Timing Scenario #2**
  - Passcode enabled = No
  - User closes the application
  - User re-opens the app within 20 minutes of closing it
  - Result = the user goes directly back to the app; if more than 20 minutes have elapsed, the user must enter the Login Name and Password or biometrics.

# View Card Details

## General Information

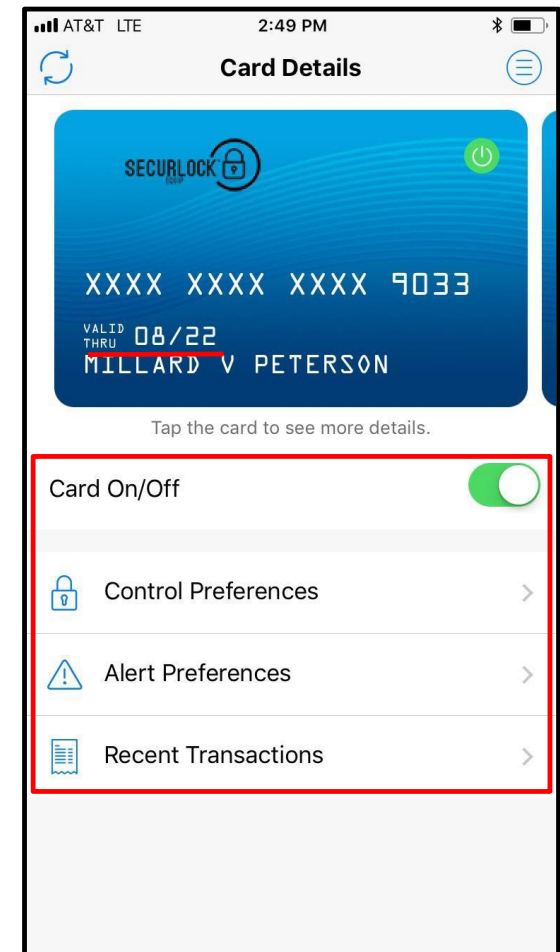
- The Card Details screen is the landing page once a user logs into the application. It shows the following information:
  - Refresh (two circular arrows) and “Hamburger” Menu (circle surrounding three blue bars) icons
    - The menu will be upper right for iPhones, upper left for Android
  - Swipe to show additional cards being managed within the Mobile App
  - Card Front Image
    - Card status (green = ON, red = OFF).
    - Last 4-digits of the card number
    - Card Expiration Date
    - Cardholder Name
  - Card On/Off
  - Control and Alert Preferences
  - Recent Transactions



# View Card Details

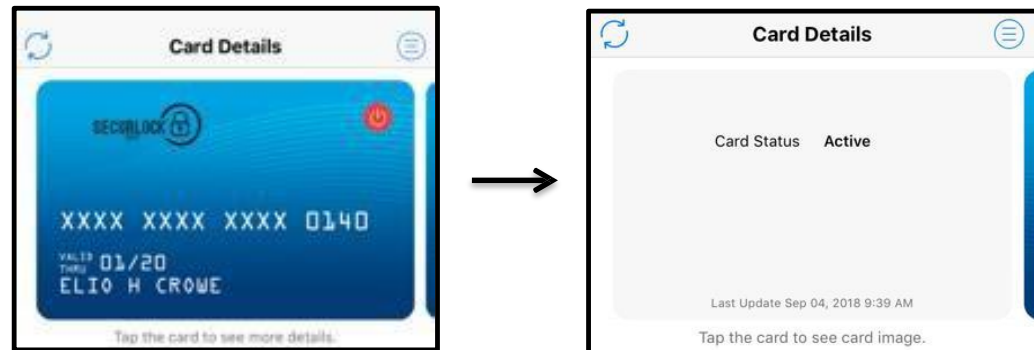
## Front of Card

- 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 payments that were setup prior to turning the card off and credits/deposits) will be denied.
- Tapping 'Control Preferences' takes the user to the Control Preferences screen to define how and where the card may be used.
- Tapping 'Alert Preferences' takes the user to the Alert Preferences screen to specify the kinds of transactions that should generate an alert.
- Tapping 'Recent Transactions' takes the user to the transactions screen, 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 Mobile App by the user. The previous card should be unmanaged by the user at this time.



# View Card Details

## Back of Card



- The card image will rotate when tapped. The back of the card has additional card details:
  - Card status
  - Last updated time
  - 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.

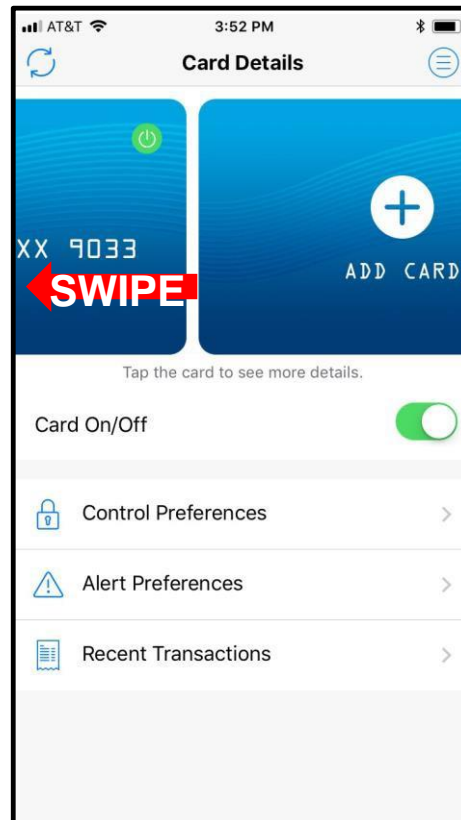


# View Card Details

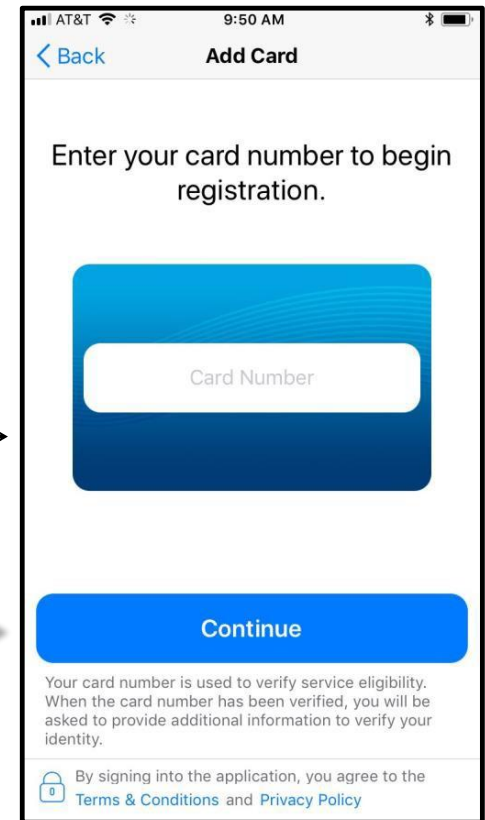
## Add a Card

- On the Card Details screen, swiping the card image from right to left will also allow the user to add a new card for management in the app.
- This process can also be done via 'Manage Portfolio' in the app.
- The 'Add Card' process is similar to the registration process, with the following exceptions:

- A user is not asked to accept the 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'.



A.  
Tap



B.  
Enter

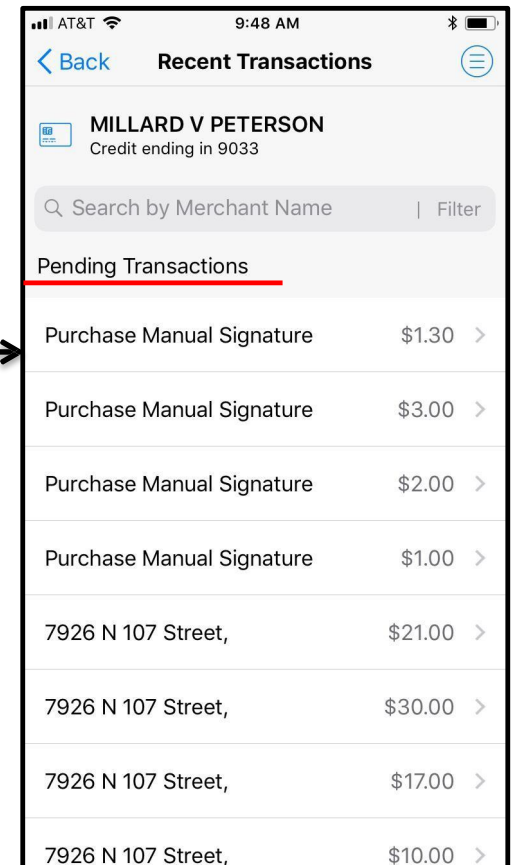
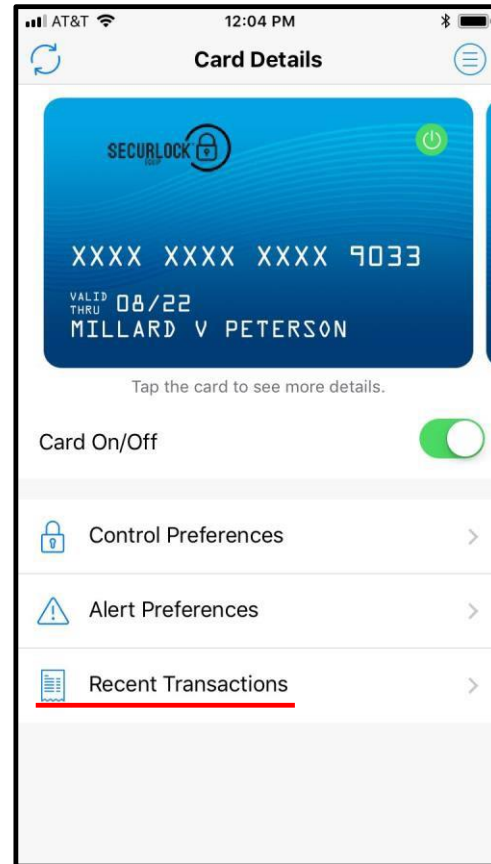
C.  
Tap



# View Transactions

## Recent Transactions

- Tap 'Recent Transactions' to view the 50 most recent transactions made in the past 30 days.
- Main Menu – Transactions will also take the user to the same screen.
- This page shows summary information of recent transactions:
  - If the transactions list is reached from a specific card, it only shows transactions associated with that particular card.
  - If the transaction list is reached from Main Menu, it shows transactions for all the managed cards.

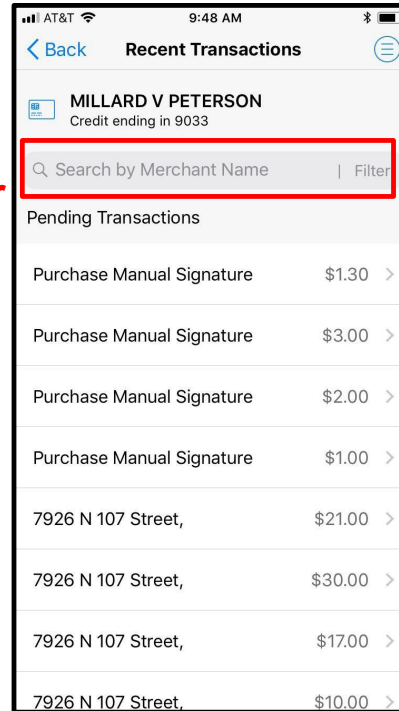


# View Transactions

## Recent Transactions

- Transactions can be searched and filtered.
- The 'Search by Merchant Name' field can be used to find recent transactions from a specific merchant.
- Tap 'Filter' to bring up the 'Transaction Search' screen where a user can search by:
  - Transaction Tag
  - Transaction Start Date
  - Transaction End Date
  - Transaction Amount
- On Android, the 'Search' feature can be found in the upper-right:

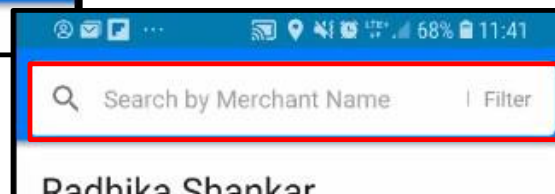
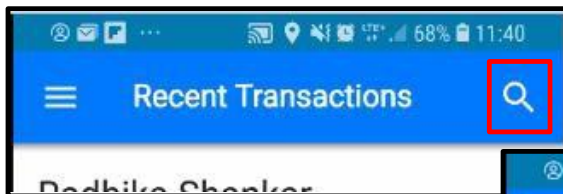
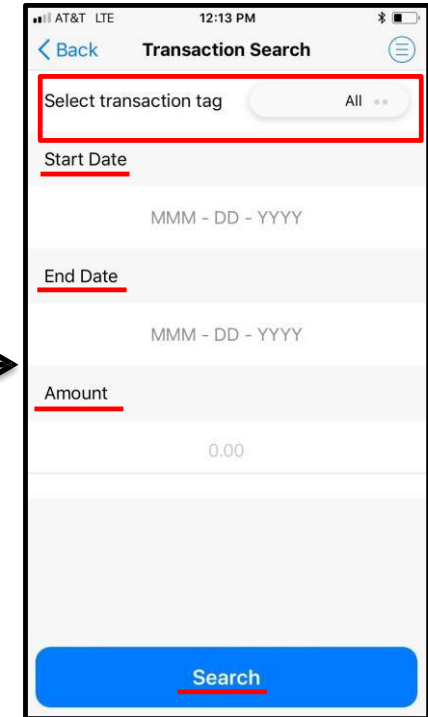
A.  
Enter



B.  
Select

C.  
Enter

D.  
Tap

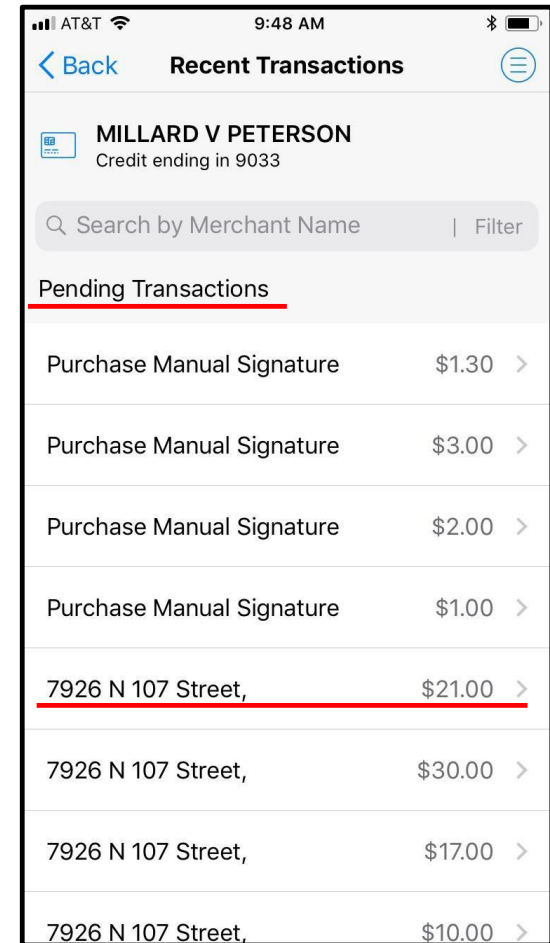


# View Transactions

## Recent 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
- Tapping on a transaction will cause the transaction details to display.

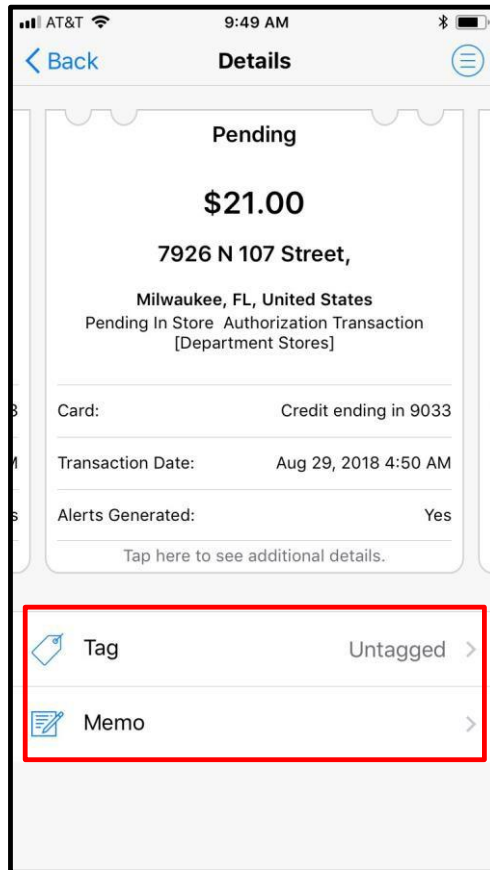
Tap



# View Transactions

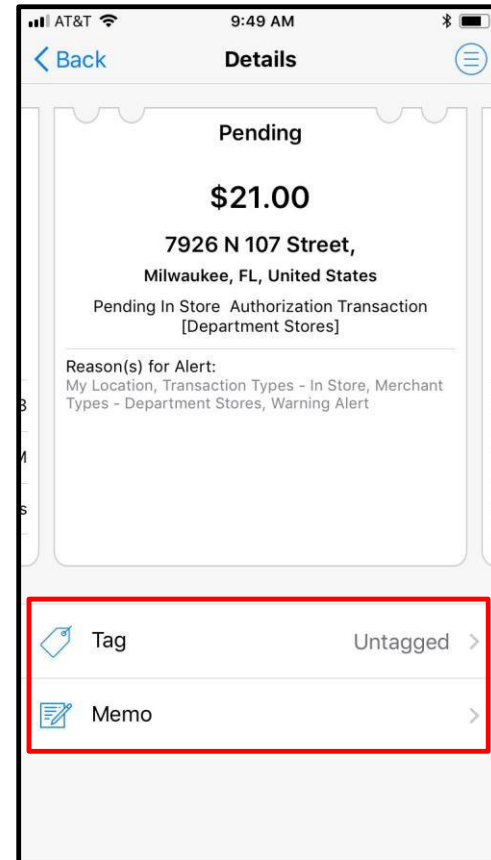
## Transaction Details

Front



Tap

Back

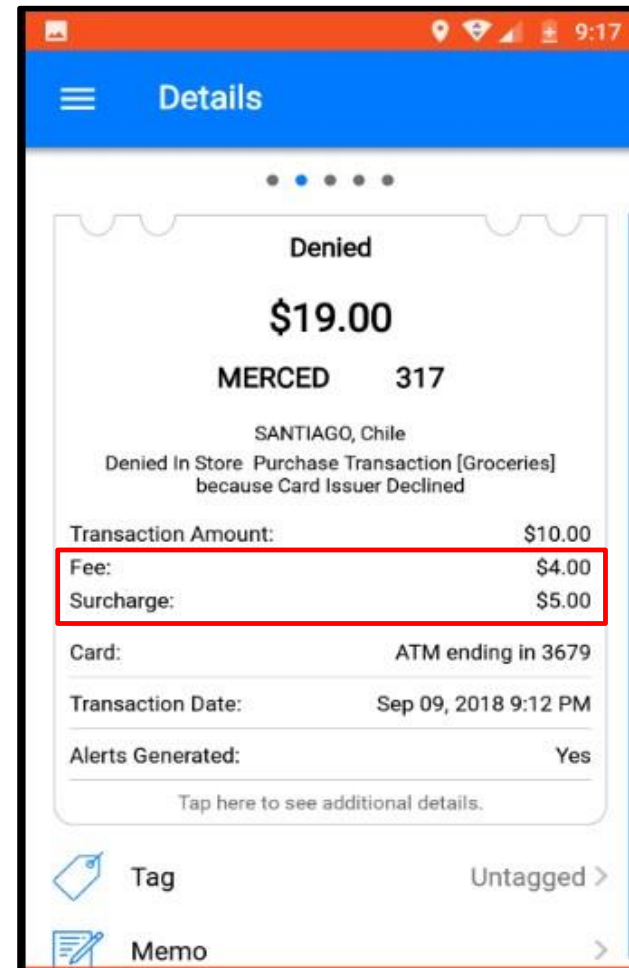


- Tapping to rotate the receipt will display additional details: Transaction amount, Merchant name and address, Transaction status, Reason for the alert and, if the transaction was denied, reason for denial.
- User is provided with the options to Tag or add a Memo to each transaction receipt.

# View Transactions

## Transaction Details – Surcharge and Fees

- For transactions with a fee and/or surcharge, the Transaction Details screen will show the transaction amount, along with the surcharge and/or fee separately, as applicable.
- Transactions without a surcharge or fee will not have these fields shown on the Transaction Details screen.



**View**

# View Transactions

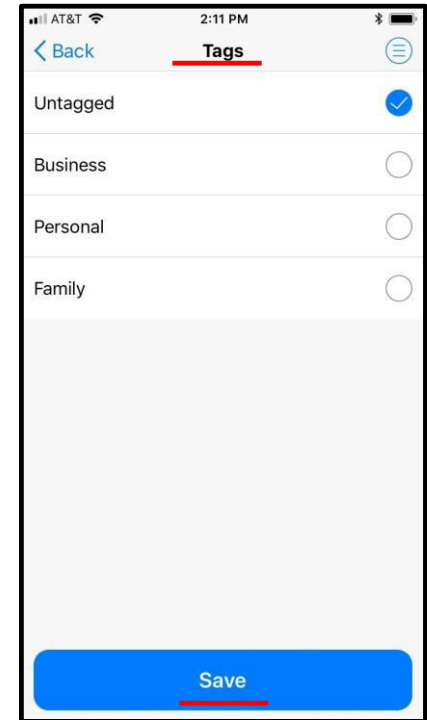
## Transaction Details – Tags and Memos

**Tap**



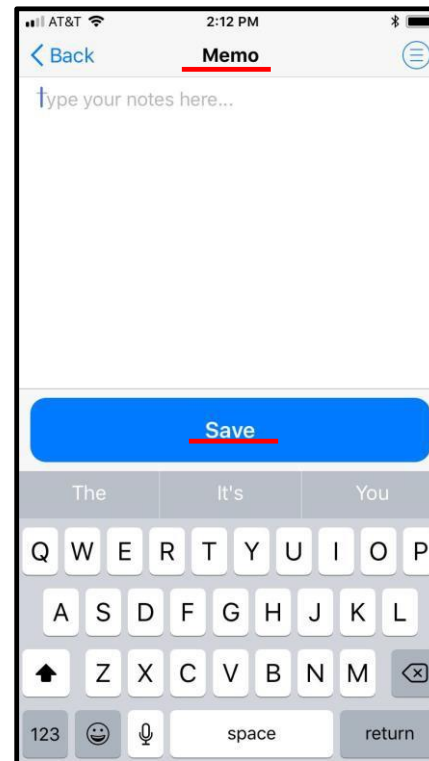
- Tap 'Tag' to assign the transaction receipt to a category:
  - Untagged
  - Business
  - Personal
  - Family
- Tap 'Memo' to open the Notes screen and enter a memo about the transaction.
- Tap 'Save' for the Tag and Memo selections to take effect

**Select**



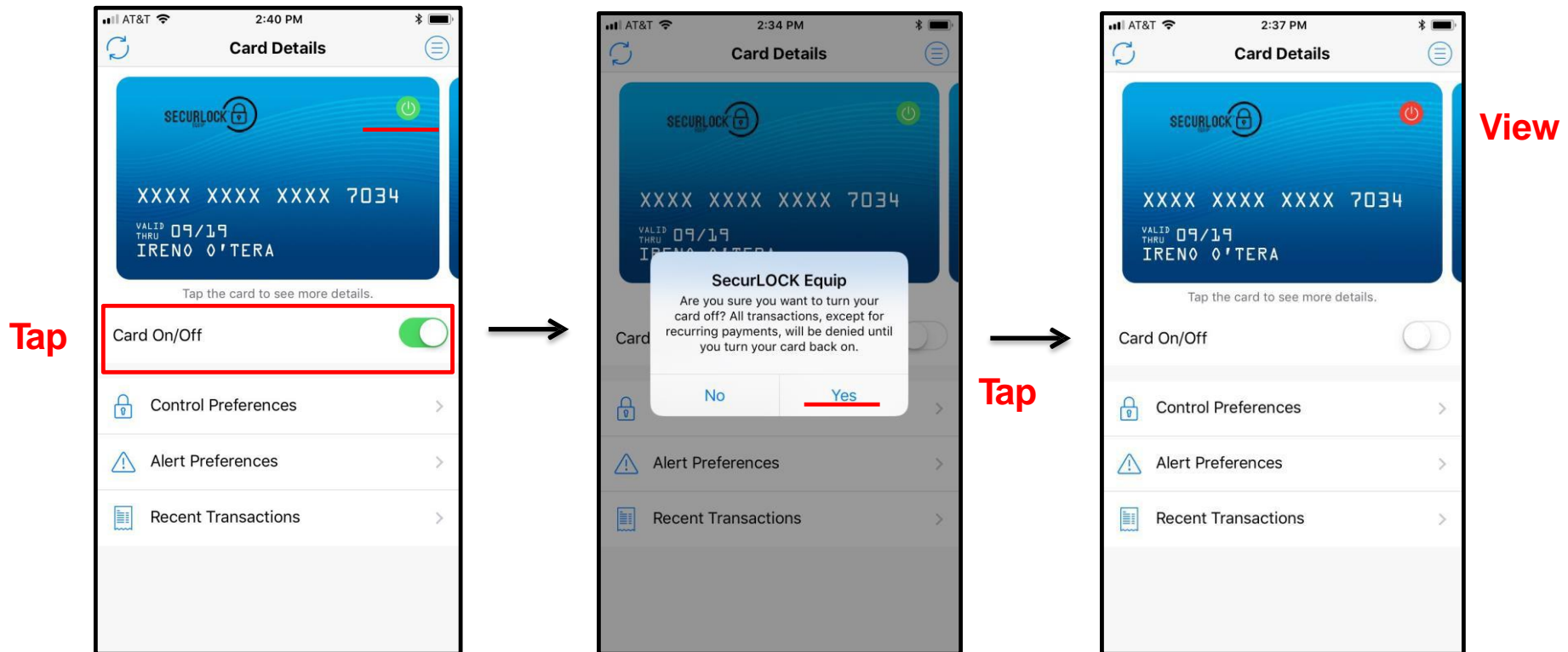
**Tap**

**Tap**



# Set Up Control Preferences

## Turn Card On/Off



- Tap the Card On/Off control to turn a card on or off. An alert message appears for confirmation.
- Once the card is turned off, the Card On/Off icon in the upper-right corner of the card image changes from green (On) to red (Off).

# Set Up Control Preferences

## Turn Card On/Off

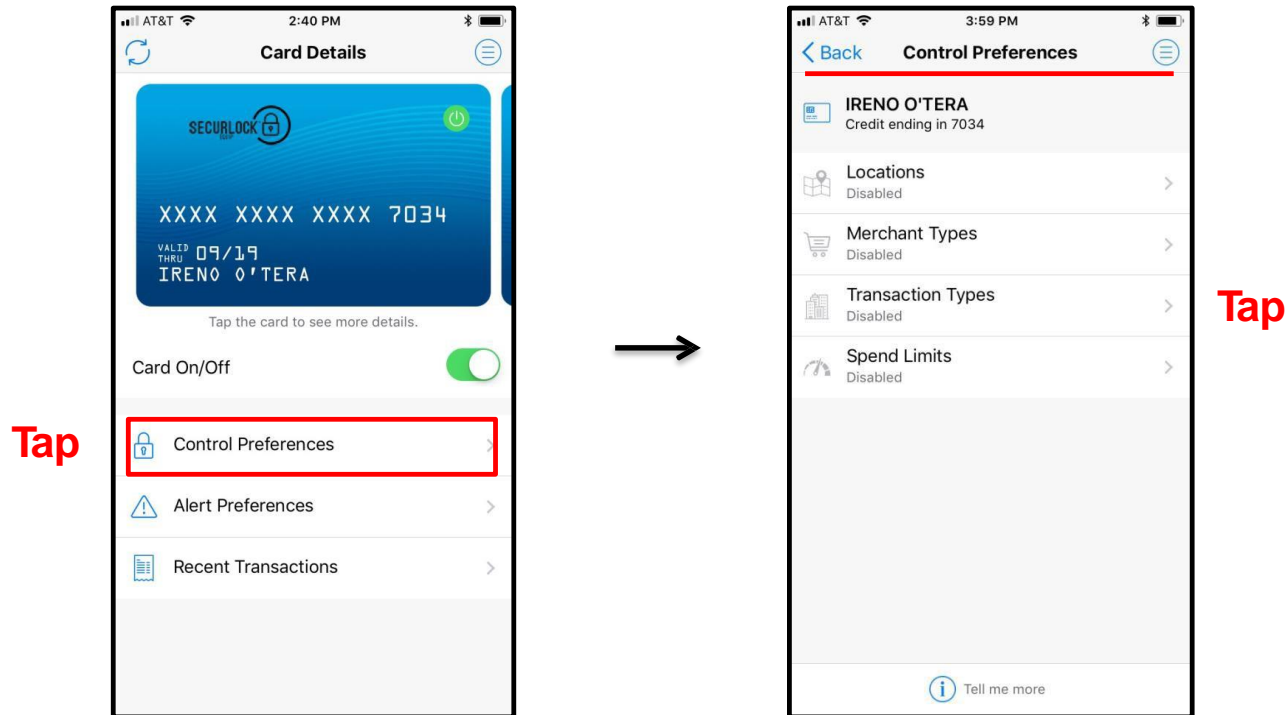


- **Decline alerts will be pushed to the user. No other transaction alerts will be sent.**
- **If the card status is changed (e.g., closed or hot carded or blocked by Falcon) in the system of record, the card status will not be changed to red within the app.**
- **The On/Off feature only impacts the 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



- Use Control Preferences to define how and where a card may be used.
- Tap on 'Control Preferences' on the Card Details screen to access these features.
- On the Control Preferences screen, the user selects the control from the Control Preferences options: Locations, Merchant Types, Transaction Types, Spend Limits.
- Controls are applied immediately.
- SecurLOCK Equip cannot override a parameter or status on the system of record.

# Set Up Control Preferences

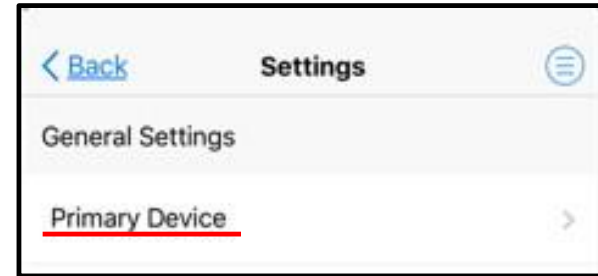
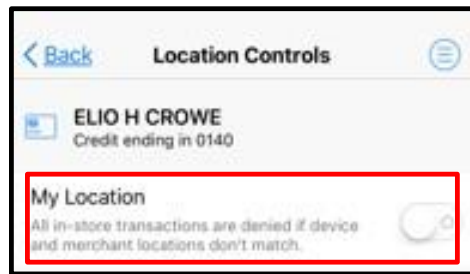
## Location Controls



- On the Control Preferences screen, tap 'Locations' to open the Location Controls screen.
- Use Location controls to specify the geographical areas in which the card may be used. An alert message appears for confirmation.
- In-store transactions attempted outside the specified locations are denied.

# Set Up Control Preferences

## Location Controls – My Location



- When the 'My Location' control preference is set, the app will compare the last known location of the mobile device and the merchant location to decide whether to approve or deny the transaction.
- The 'My Location' control is based on an 8-mile radius around the mobile device.
- Transactions made at merchant locations that differ significantly from the user's location will be denied.
- The service assumes that you are carrying your mobile phone (configured as your primary device) and uses your phone's Location Services to determine your current location.
- For 'My Location' Control and Alert policies to work, the user must turn 'On' the device's Location Settings and enable location tracking for the app.
- If more than one user registers the same card under separate profiles and each user turns on 'My Location', all shared users' locations are considered in the 'My Location' control check.

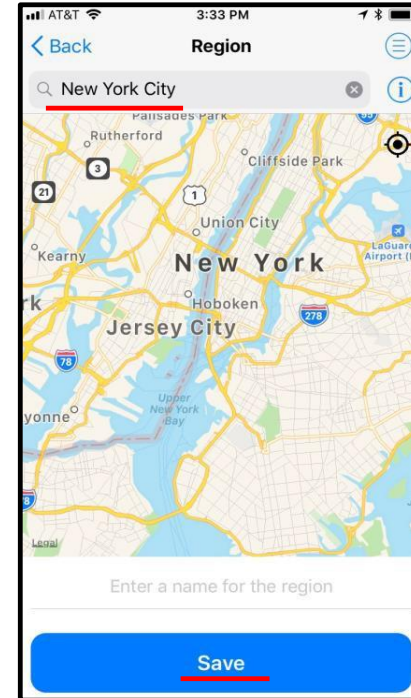
# Set Up Control Preferences

## Location Controls – My Regions

A. Tap



B. Tap



C. Enter

D. Tap

- Use 'My Regions' to define geographical areas in which in-store card transactions are permitted.
- In-store card transactions occurring outside the defined regions are denied.
- Tap the '+' in the 'Add Region' field to display the map on the Region screen.
- Use a zip code, city name, state or country and zoom in or out on the map to define a region.
- A user must enter a name for the region and tap 'Save'.
- A user can specify up to three control regions per card.

# 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 device's 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 device's 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 Dallas, 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.
  - For reference, a document with the full listing of Control Exceptions can be found on the SecurLOCK Equip Toolkit site.

# Set Up Control Preferences

## Location Controls

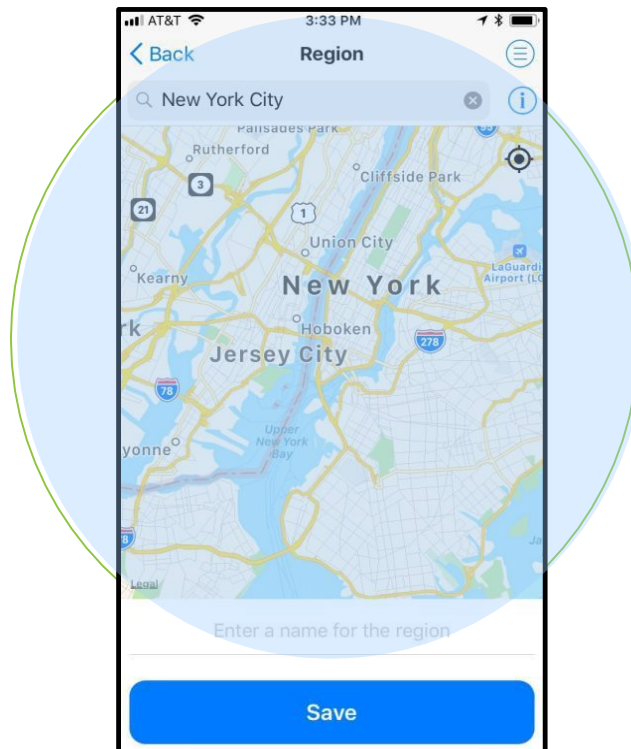
Below is a list of the current MCC Codes that Equip excluded from location controls (My Location AND My Regions).

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

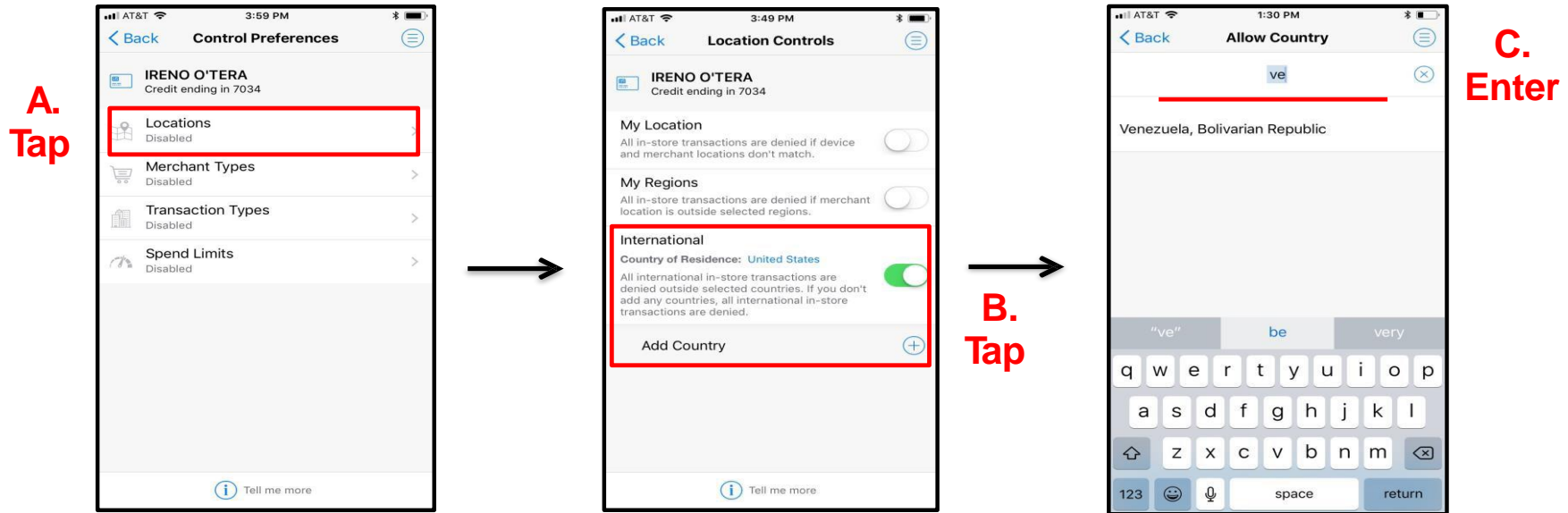
- The coverage area for a location control is a radius. For My Location, the radius is 8-miles and cannot be adjusted.
- For My Regions, each region is set by the user with a minimum 5 mile radius. Note the controlled area displayed on the device does not reflect the total coverage area.





# Set Up Control Preferences

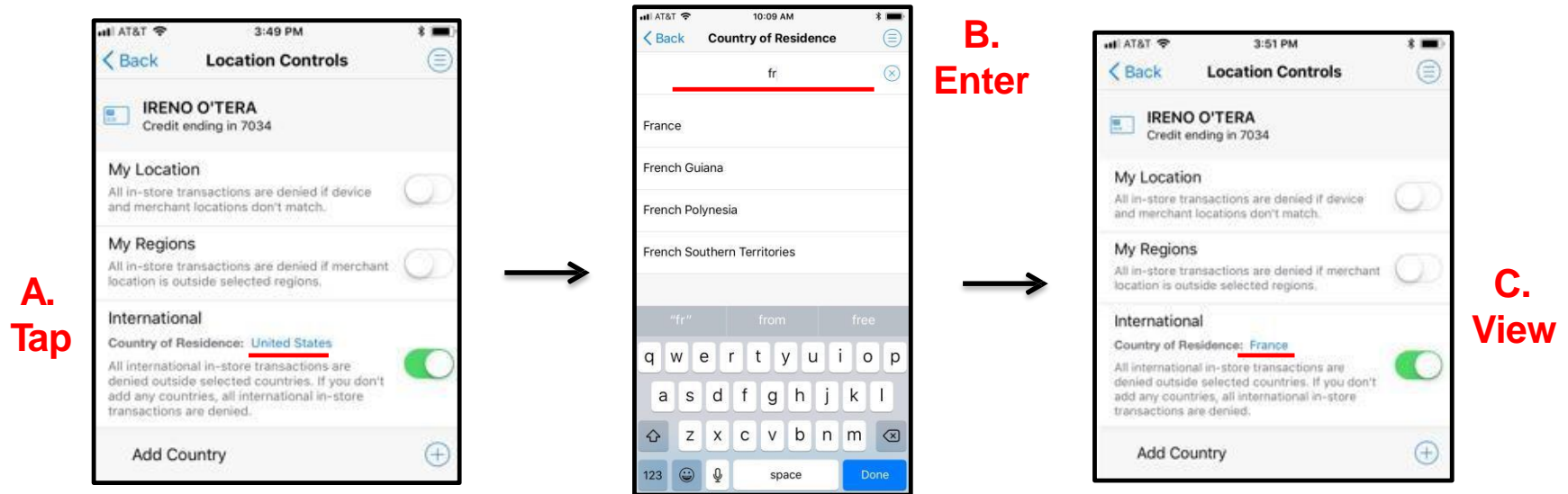
## Location Controls – International



- To block transactions made outside of the user's home country, the user selects the 'International' option by tapping the respective slider to enable the control.
- If enabling the International Control Preference, the user will be presented with the option to add selected allowed countries.
- User can add or remove specific countries by tapping on the '+' next to the 'Add Country' field and in the text box, enter the country name and tap 'Save'.
- Users can add a maximum of 5 countries to the International control.

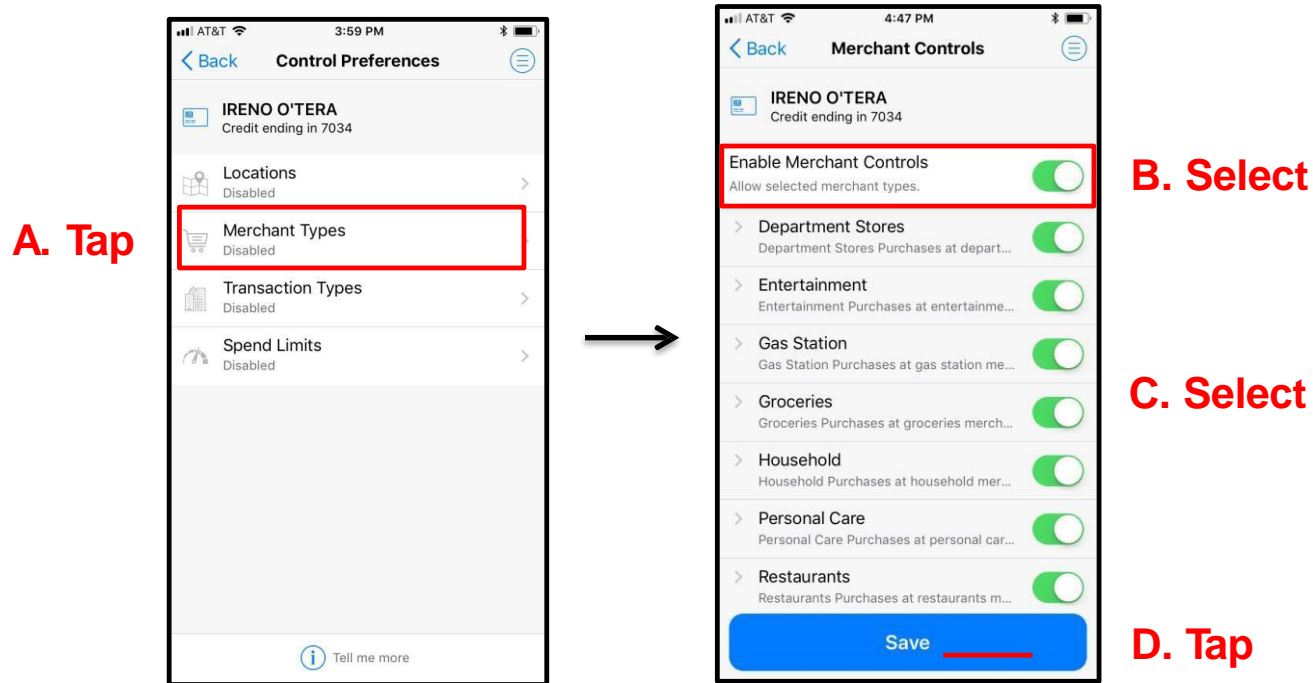
# Set Up Control Preferences

## Location Controls – International



- The user defined Country of Residence feature allows users to set a card's country to a country other than their FI's default setting.
- International must be enabled on the Location Controls screen in order to set Country of Residence.
- To make a change, tap the current Country of Residence name and in the text box, enter the new country name and then tap 'Save'.
- If the cardholder modifies the Country of Residence under Control preference, the same setting will be entered for Alert preference and vice versa.
- When enabled, any card present transaction made outside the country of residence (in addition to those countries the user has set) will be declined.

# Set Up Control Preferences Merchant Types

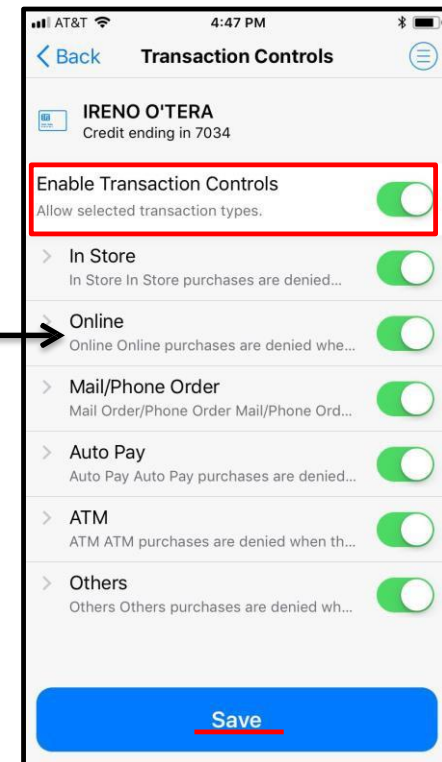
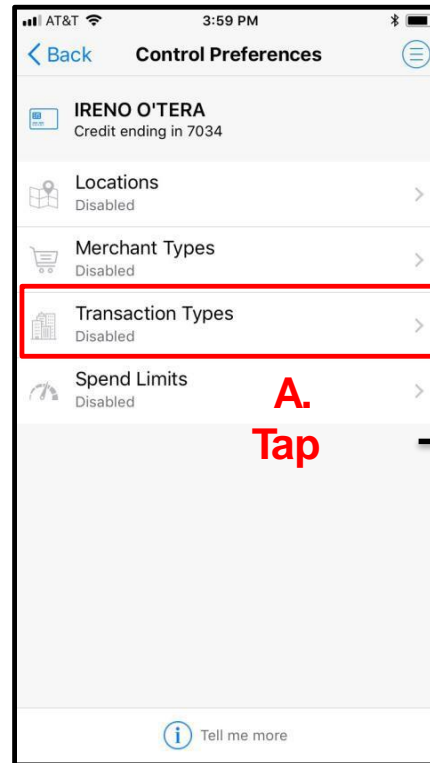


- Use the Merchant Types control to specify the types of businesses at which the card can be used.
- When 'Enable Merchant Controls' is turned 'On', the individual types are shown.
- To prevent in-store transactions at a particular type of store, turn off that Merchant Type. Any attempt to use the card in a store of that type is denied.

# Set Up Control Preferences

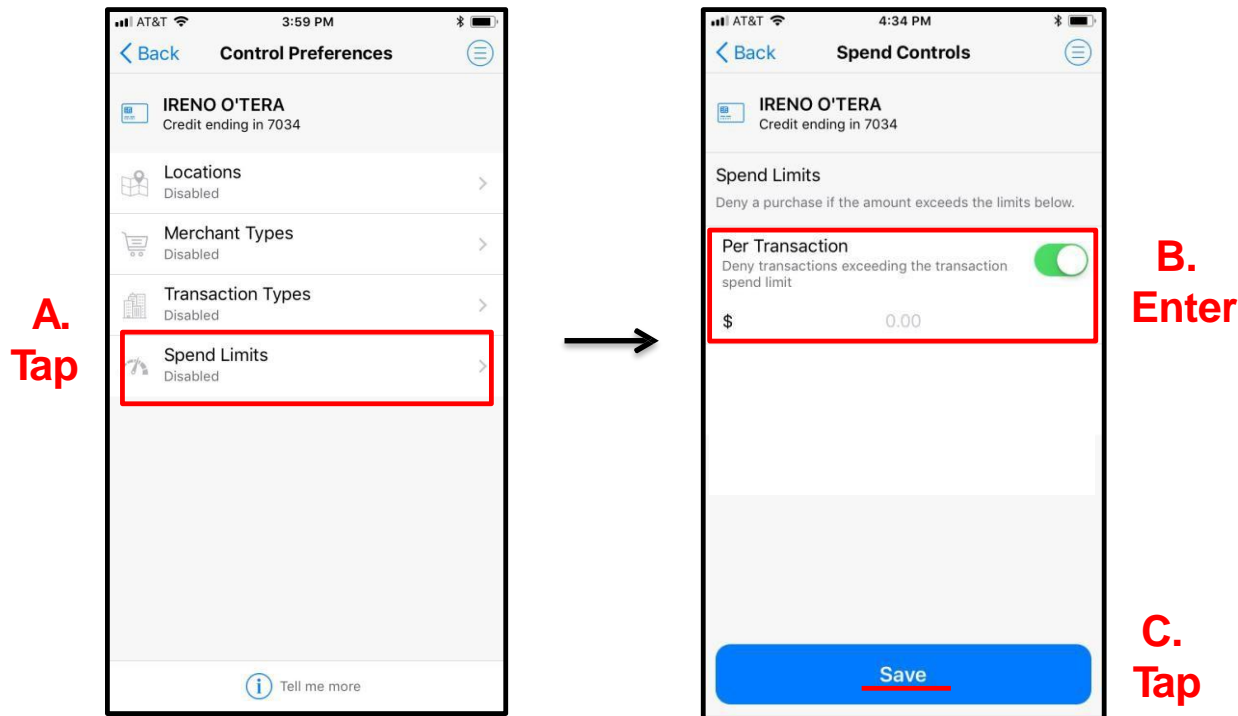
## Transaction Types

- Use the Transaction Types control to specify the types of transactions that may be made with the card.
- When 'Transaction Types' is enabled, the individual types are shown.
- Turn on the 'Enable Transaction Controls' and enable the Transaction Types that should be approved.
- To prevent the card from being used for a type of transaction, turn off that Transaction Type.



# Set Up Control Preferences

## Spend Limits - Per Transaction Spend Control



- Use the Spend Limit control to set a limit on how much can be spent on one transaction.
- A user may set Spend Limits on the Control Preferences screen by tapping 'Spend Limits'.
- On the Spend Control screen, turn on 'Per Transaction' and enter the maximum amount that can be spent on one transaction and then tap 'Save'.
- A purchase is denied if the amount exceeds the specified spend limit.

# SecurLOCK™ Equip – Mobile App Procedures

## One-Time Override - App Not Open

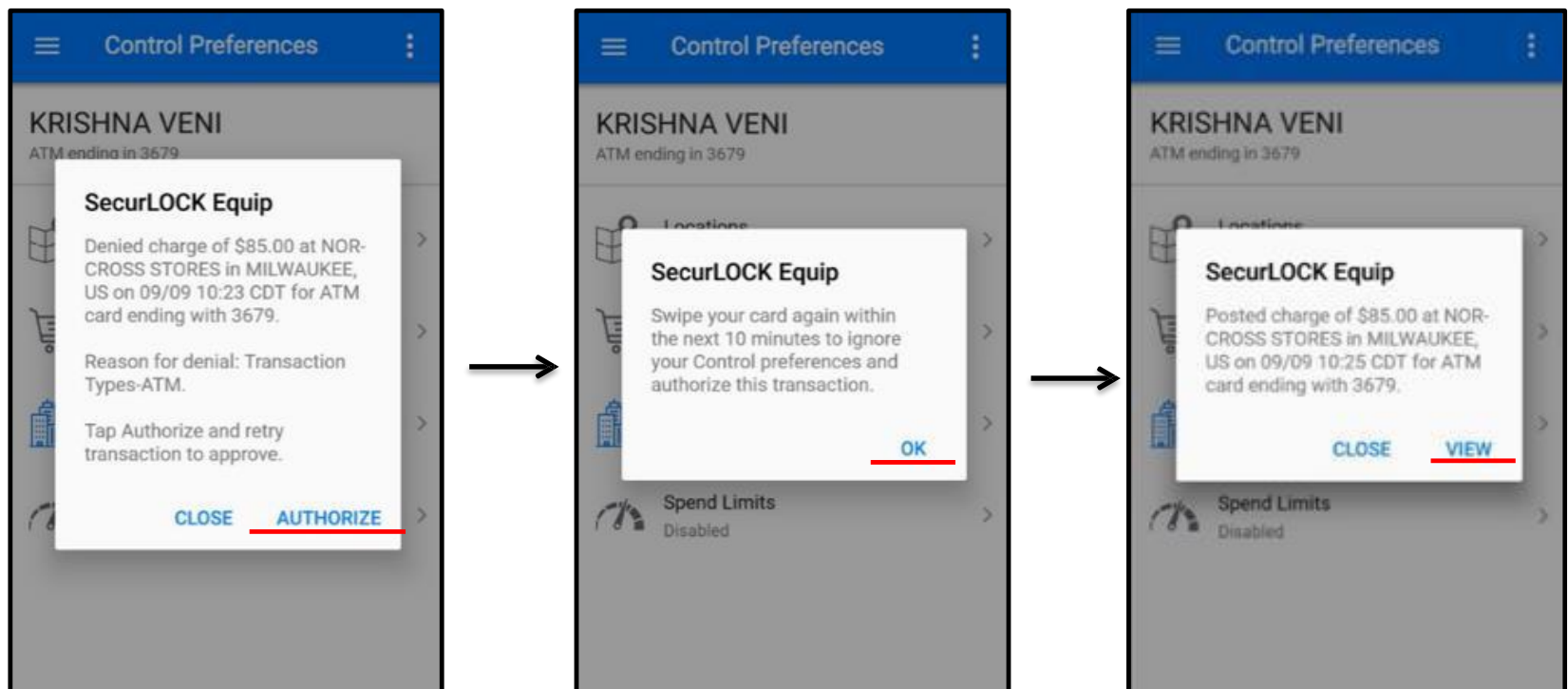
- Transactions can be denied based either on a user's control preferences or on a financial institution's business rules.
- If a transaction is denied based solely on the user's control preferences, users can tap on the standard Declined Transaction notification to be offered the option of a One-Time Override at that merchant.
- This allows automatic approval of the next transaction made on this card within the next 10 minutes, regardless of their control preferences.
- **Note:** After tapping 'Authorize', the user then needs to perform the transaction again for it to be approved.



# SecurLOCK™ Equip – Mobile App Procedures

## One-Time Override - App Open

- If a transaction is declined based solely on the user's control preferences while the app is open, the OTO notification will appear and the user can simply tap 'Authorize' to allow the next transaction on that card.
- A confirmation message will be received and the user then needs to perform the transaction again within 10 minutes to ignore the control preferences and authorize the transaction.
- User will then receive an alert to view the posted transaction.



# **SecurLOCK™ Equip – Mobile App Procedures**

## **One-Time Override - Additional Information**

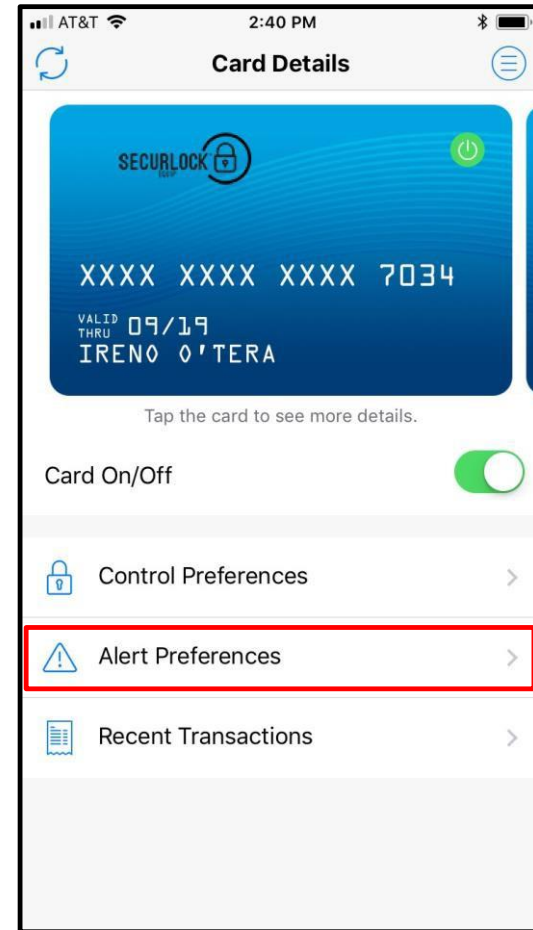
- **If the 10-minute limit for One-Time Override expires before another transaction occurs, a message is displayed notifying the user that the transaction request has expired.**
- **Each Primary Shared Card User receives the One-Time Override notification, regardless of which user has actually made the denied transaction. Anyone who receives the notification can take advantage of the One-Time Override offer as long as the transaction occurs within the 10-minute timeframe.**
- **If a transaction denial is based on something other than the card control app settings, no One-Time Override notification will be generated and therefore that denial cannot be overridden.**



# Set Up Alert Preferences

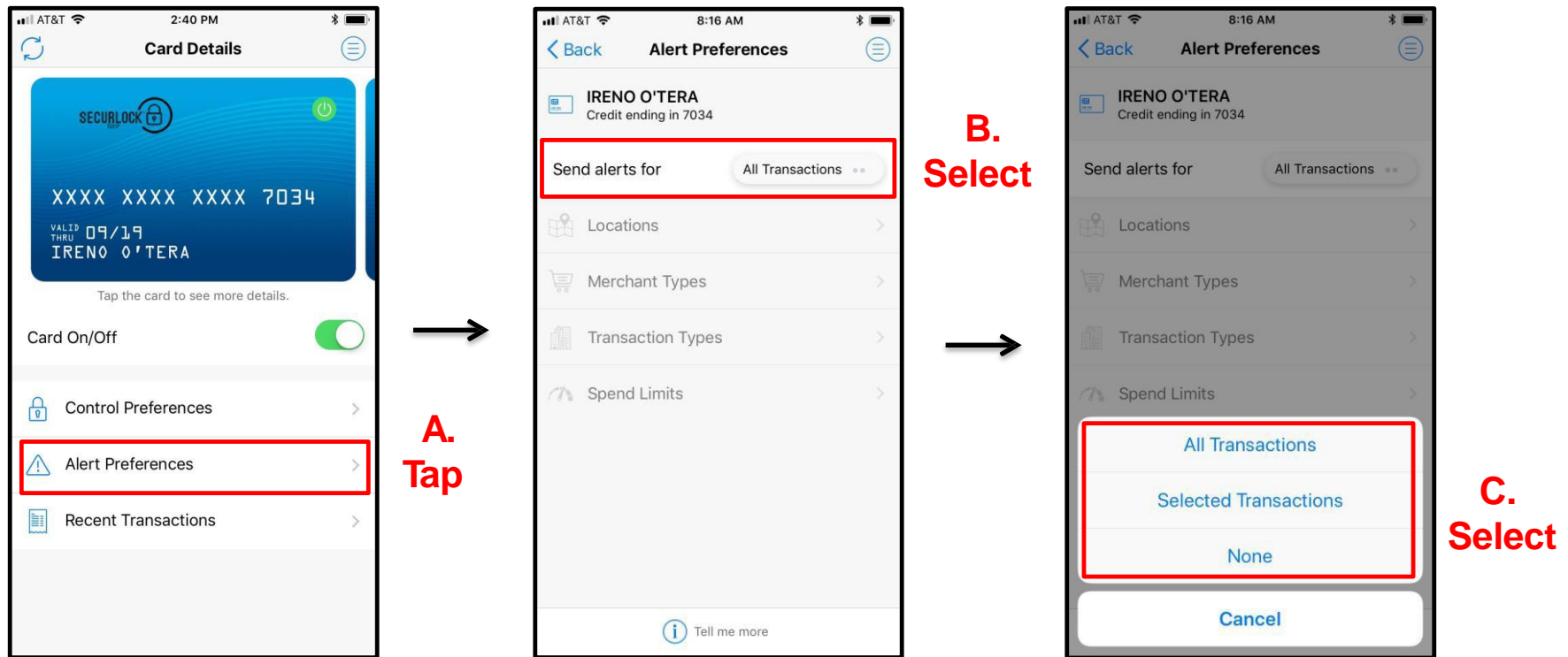
## Alert Preferences Control

- Alert preferences are used to specify the kinds of transactions that should generate an alert.
- Generating an alert does not cause a transaction to be denied; it simply alerts the user that the transaction has occurred, regardless of whether it was approved or denied.
- When a card is shared, each cardholder can set up individual Alert preferences and receive alerts based on those individual Alert preferences.
- All denied transactions will generate an alert, irrespective of the alert setting by the user.



# Set Up Alert Preferences

## Alert Preferences Control

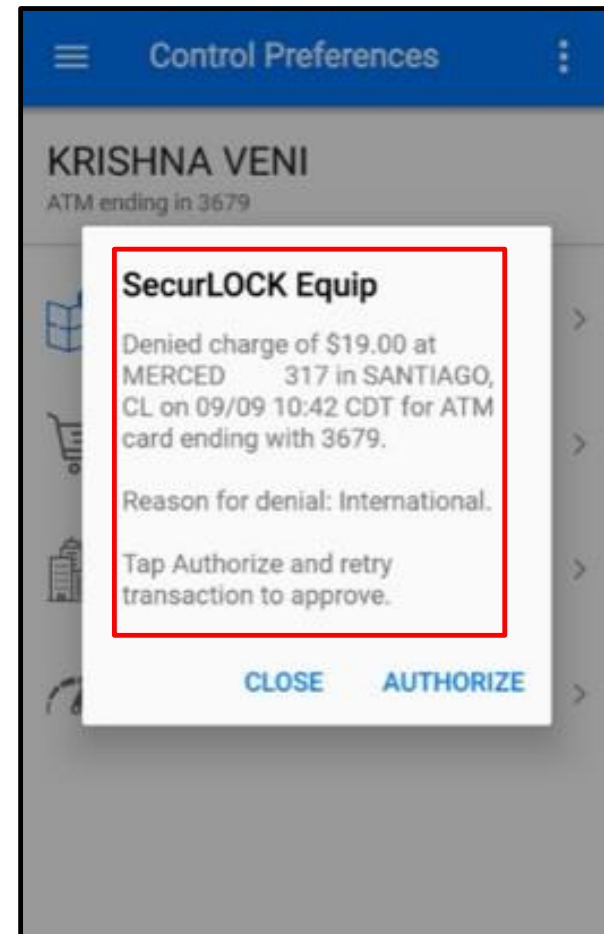


- Use the Alert Preferences control to specify the kinds of transactions that should generate an alert: All Transactions, Selected Transactions, None.
- Choosing 'Selected Transactions' from the drop-down box on the Alert Preferences screen presents the user with the several custom alert options.
- Once an alert preference is enabled, its icon changes from light grey to blue.

# Set Up Alert Preferences

## Push Notification Message

- A push notification is sent to the user's mobile device when alert preferences are enabled.
- A push notification is displayed as a pop-up or a banner on the mobile device and delivered in real-time.
- The push notification alert message includes the card type, last 4 digits of the card number, lists all control policies causing the denial and could potentially include an option for a One-Time Override.

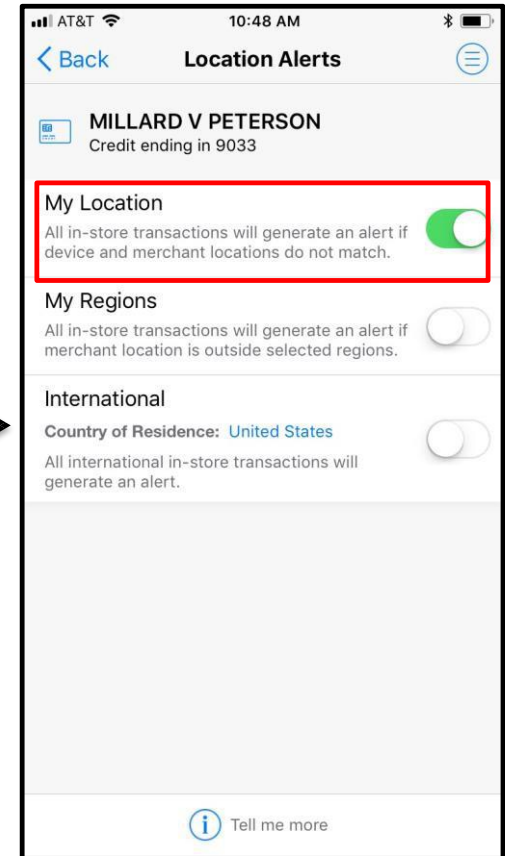
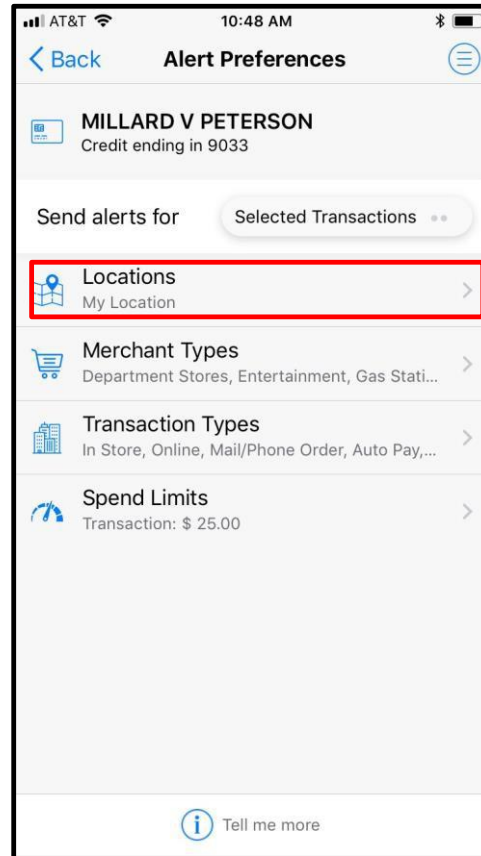


**View**

# Set Up Alert Preferences

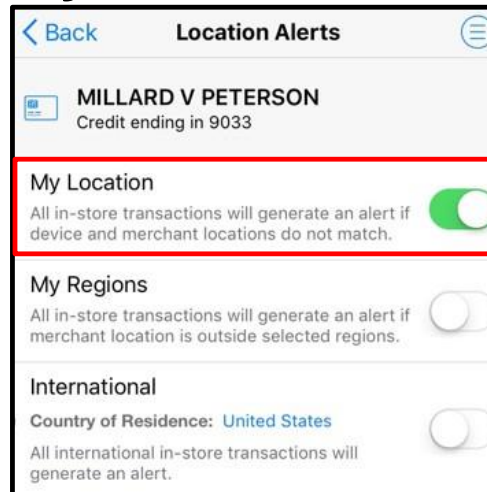
## Location Alerts

- Once Location Alerts are enabled, card transactions occurring outside the specified locations generate an alert.
- Available Locations Alerts are: My Location, My Regions, and International.
- Users can set multiple location alerts for each card.



# Set Up Alert Preferences

## Location Alerts – My Location

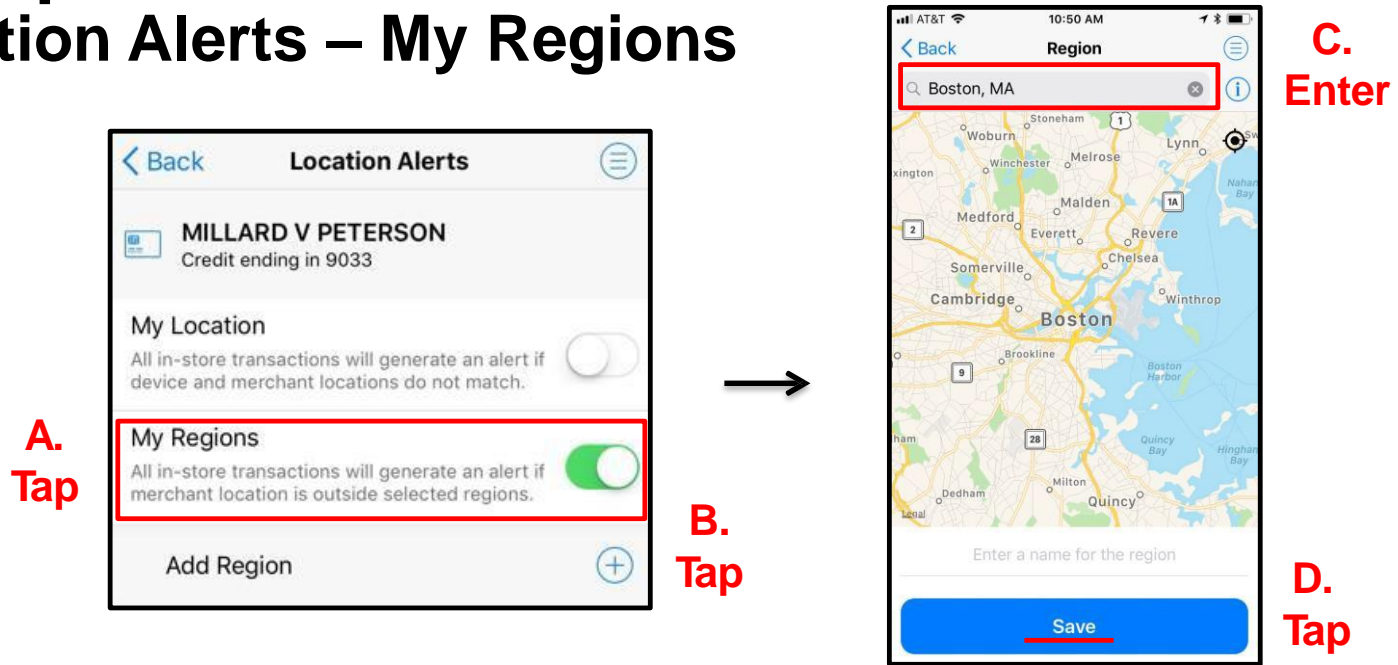


Tap

- When the 'My Location' control preference is enabled, the app will compare the user's mobile device location and the merchant location and decide whether or not to trigger an alert.
- Transactions made at merchant locations that differ significantly from the user's mobile device 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 (8 mile radius).
- For 'My Location' Control and Alert preferences to work, the user must turn 'On' the device's Location Settings and enable location tracking.

# Set Up Alert Preferences

## Location Alerts – My Regions

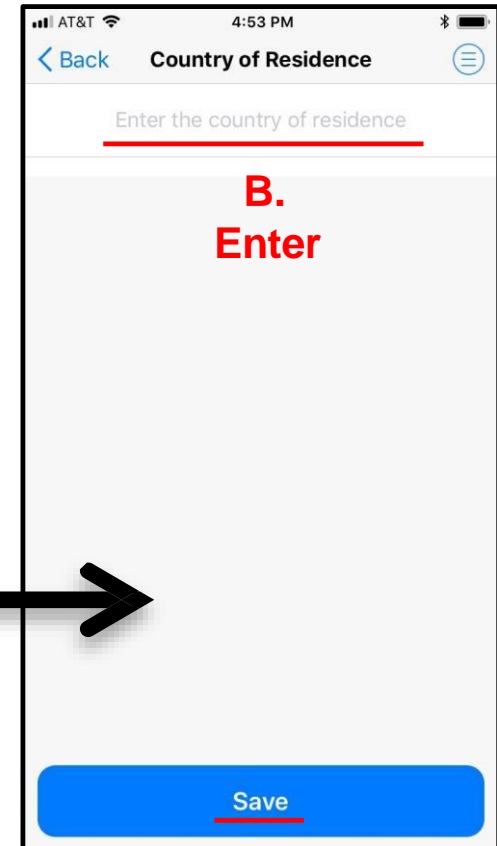
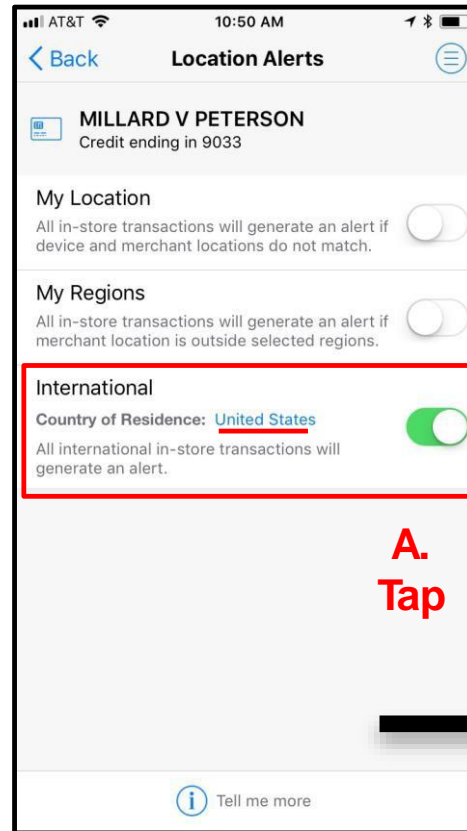


- A user can select 'My Regions' to set one or multiple geographical areas where in-store transactions can be made. When 'My Regions' alert is enabled, any in-store transactions made outside the specified regions will trigger an alert to the user's mobile device.
- A user can specify up to three Alert 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

- Turn on the International alert to generate an alert notification each time an in-store transaction occurs at a location outside of the user's Country of Residence or any countries the user may have set via this control.
- As a reminder, the user defined Country of Residence feature allows users to set a card's country to a country other than their FI's default setting.
- International must be enabled on the Location Controls screen in order to set Country of Residence. To make a change, tap the current Country of Residence name and in the text box, enter the new country name and then tap 'Save'.



# Set Up Alert Preferences

## Location Alerts - International



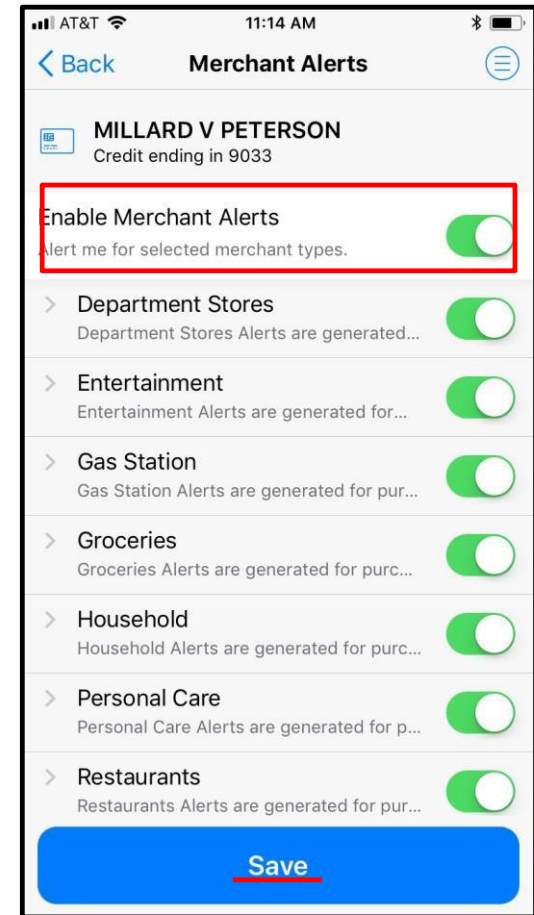
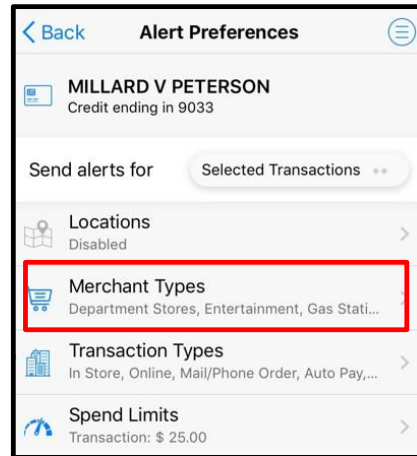
- Users can add/modify the Country of Residence for both Alert and Control preferences. If the user modifies the Country of Residence under Alert preference, the same setting will be entered for Control preference and vice versa.
- Changing the 'Country of Residence' on a Shared Card will generate a notification to other Shared Card Users.
- Travel alerts are not integrated into SecurLOCK Equip; follow your normal procedures.



# Set Up Alert Preferences

## Merchant Alerts

**A.**  
**Tap**



**B.**  
**Tap**

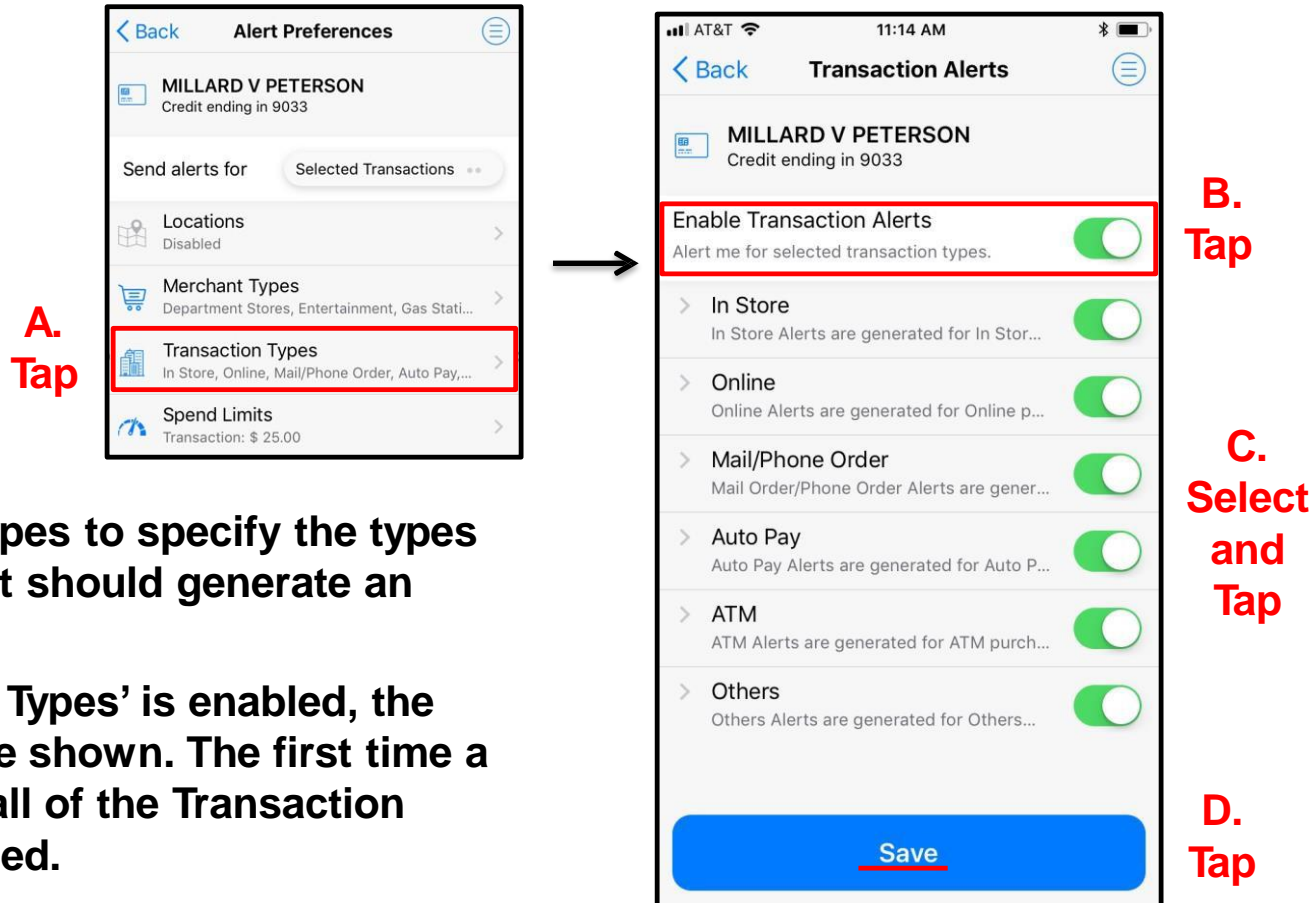
**C.**  
**Select and Tap**

**D.**  
**Tap**

- Use 'Merchant Types' to specify the types of businesses at which in-store card transactions should generate an alert.
- When 'Enable Merchant Alerts' is 'On', the individual merchant types are shown. The first time a user selects 'On', all of the merchant types will be enabled.
- Disable Merchant Types for the types of businesses at which transactions should not generate an alert for the user.

# Set Up Alert Preferences

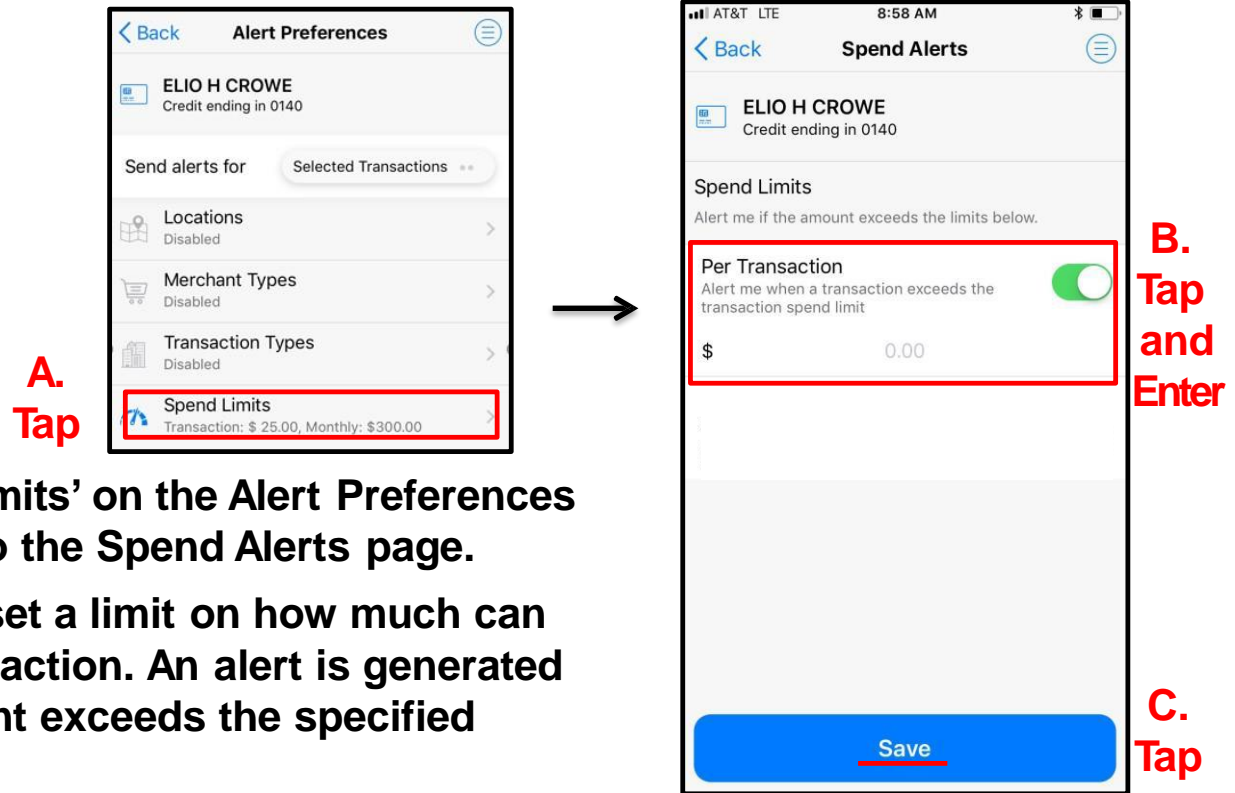
## Transaction Alerts – Transaction Types



- Use Transaction Types to specify the types of transactions that should generate an alert.
- When 'Transaction Types' is enabled, 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 disabled for the kinds of transactions that should not generate an alert for the user.

# Set Up Alert Preferences

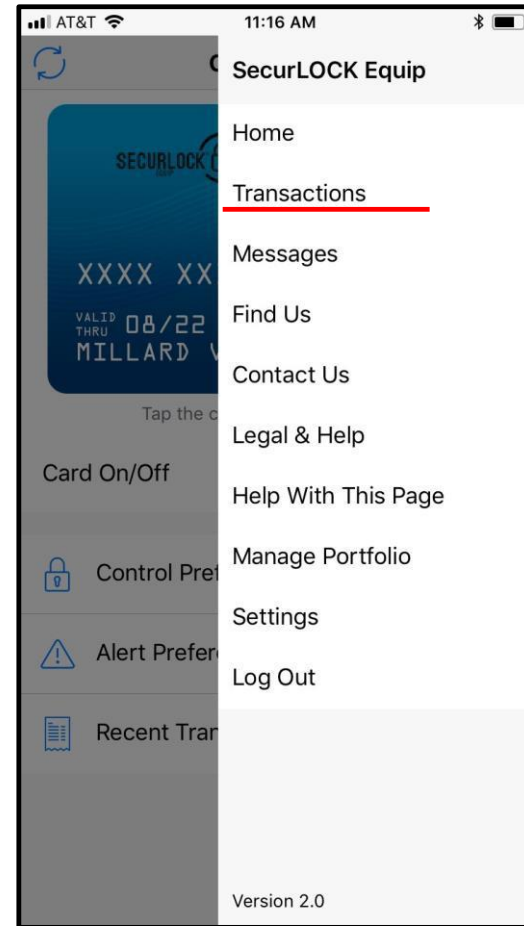
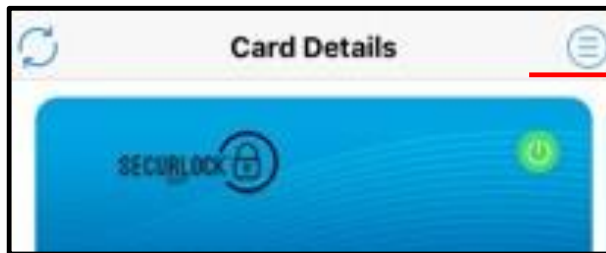
## Spend Alerts – Per Transaction Threshold



- Tapping on 'Spend Limits' on the Alert Preferences page takes the user to the Spend Alerts page.
- Use Spend Limits to set a limit on how much can be spent on one transaction. An alert is generated if a transaction amount exceeds the specified spend limit.
- On the Spend Alerts screen, turn on 'Per Transaction' and enter the maximum amount that can be spent on one transaction before an alert is generated.
- A user must tap on 'Save' for the Spend Limits alert policy to take effect.

# Home Screen – Main Menu Options

## List of Options

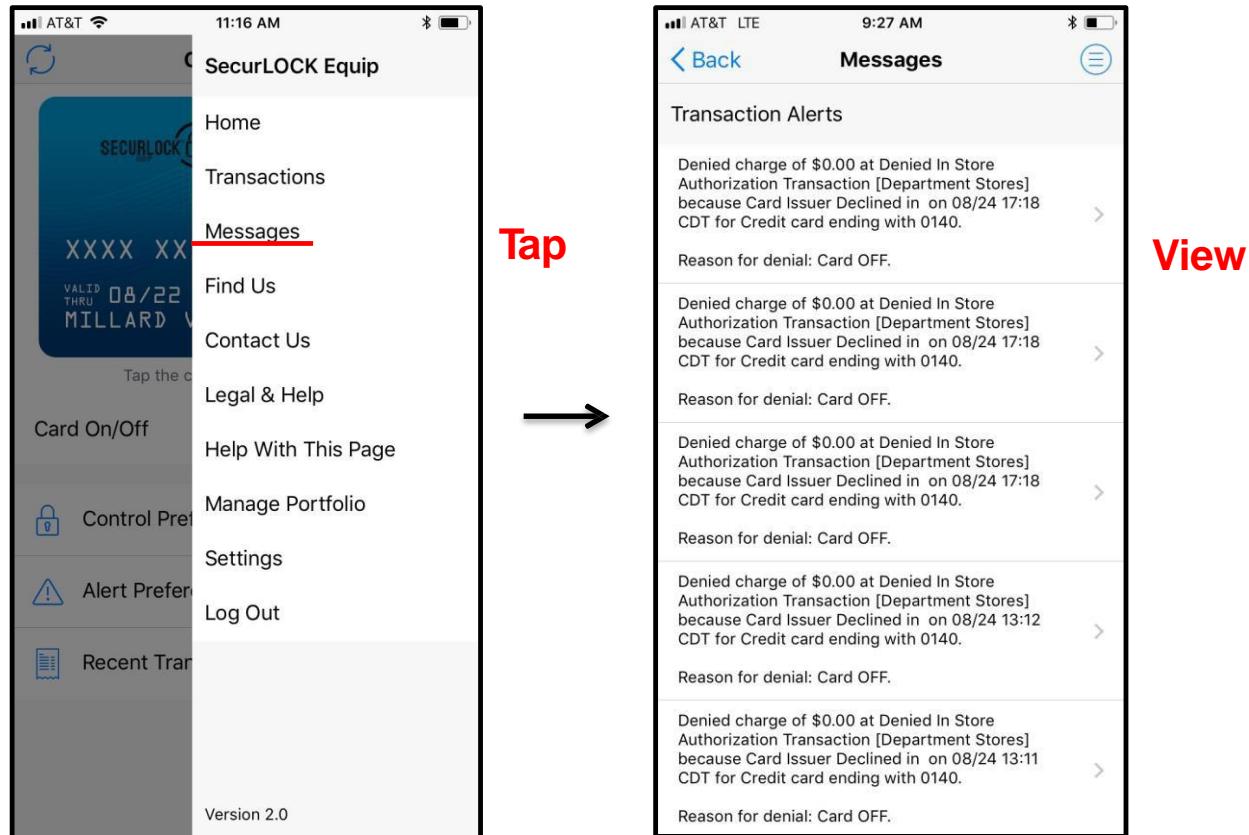


**Select  
an option**

- 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

## Messages

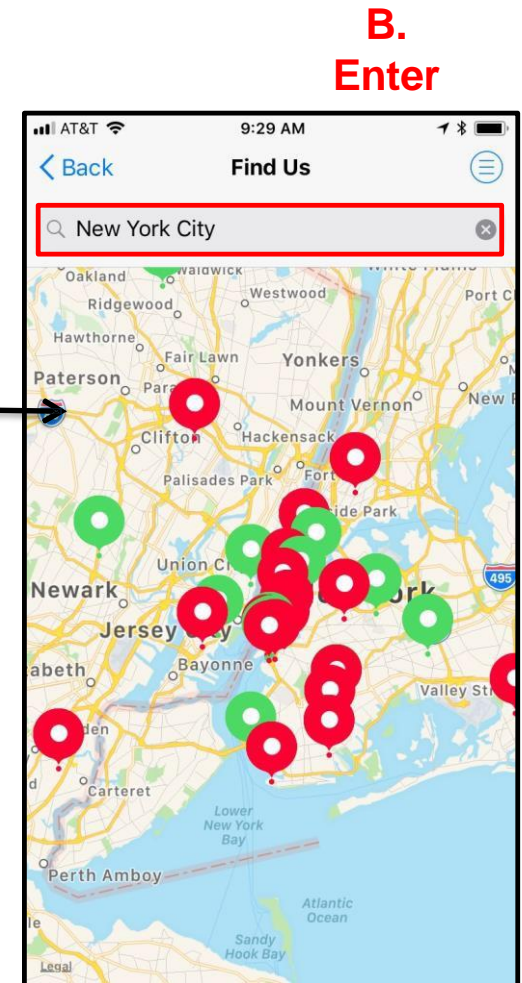
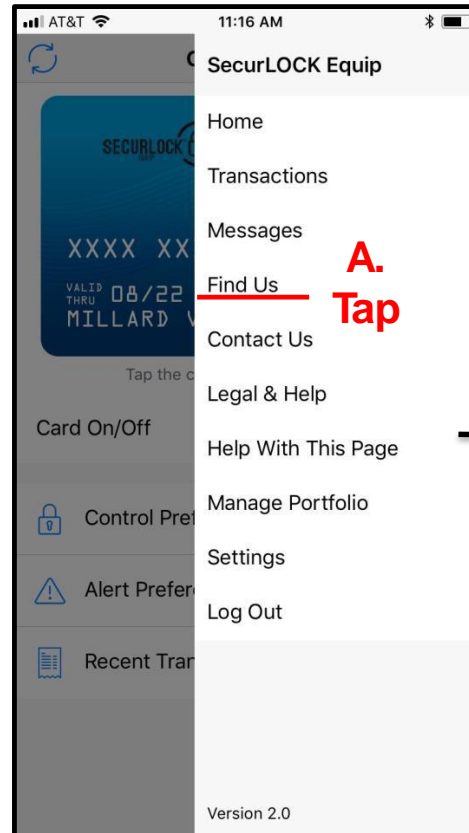


- Tapping 'Messages' on the Home Menu takes user to the Messages screen to see messages that have been sent to the user's device.
- Messages include Transaction Alerts and Card Alerts (Change of Info by Shared Card Users).

# Home Screen – Main Menu Options

## Find Us (ATM Locations)

- Tapping the 'Find Us' icon on the Welcome page or Home Menu takes the user to the 'Find Us' screen.
- The Mobile App displays a map of the user's current location on which local ATM locations are identified with pins.
- To find ATMs at locations other than the user's current location, in the Search field at the top of the map, enter a city or zip code and tap 'Search'.
- This feature is configurable and may be turned off. This feature is also dependent upon the financial institution's Google account.

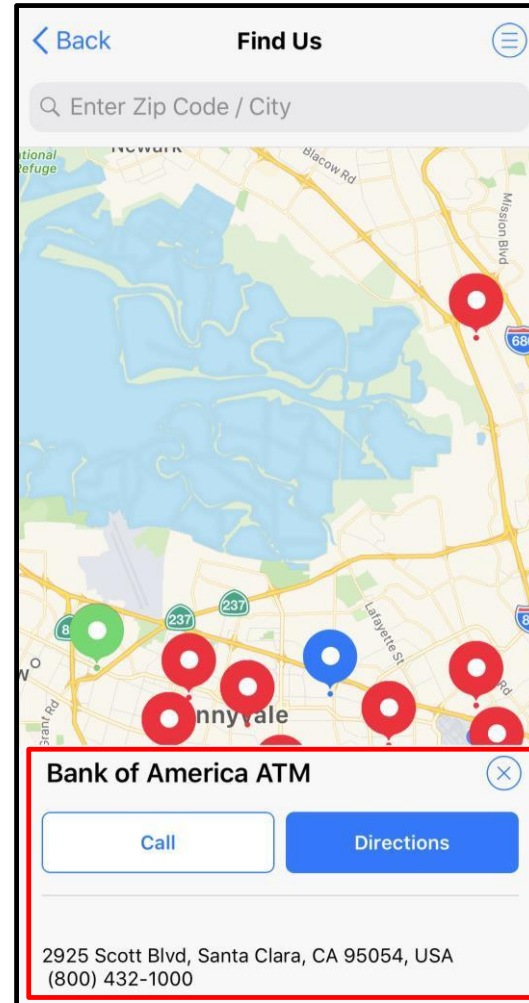




# Home Screen – Main Menu Options

## Find Us (ATM Locations)

- Tap on a pin to display the address of the ATM.
  - ATMs belonging to the user's financial institution are identified with green pins.
  - ATMs belonging to other financial institutions are identified with red pins.
- The user is provided with the option to place a call based on the contact details shown, or view directions from the device's current location.

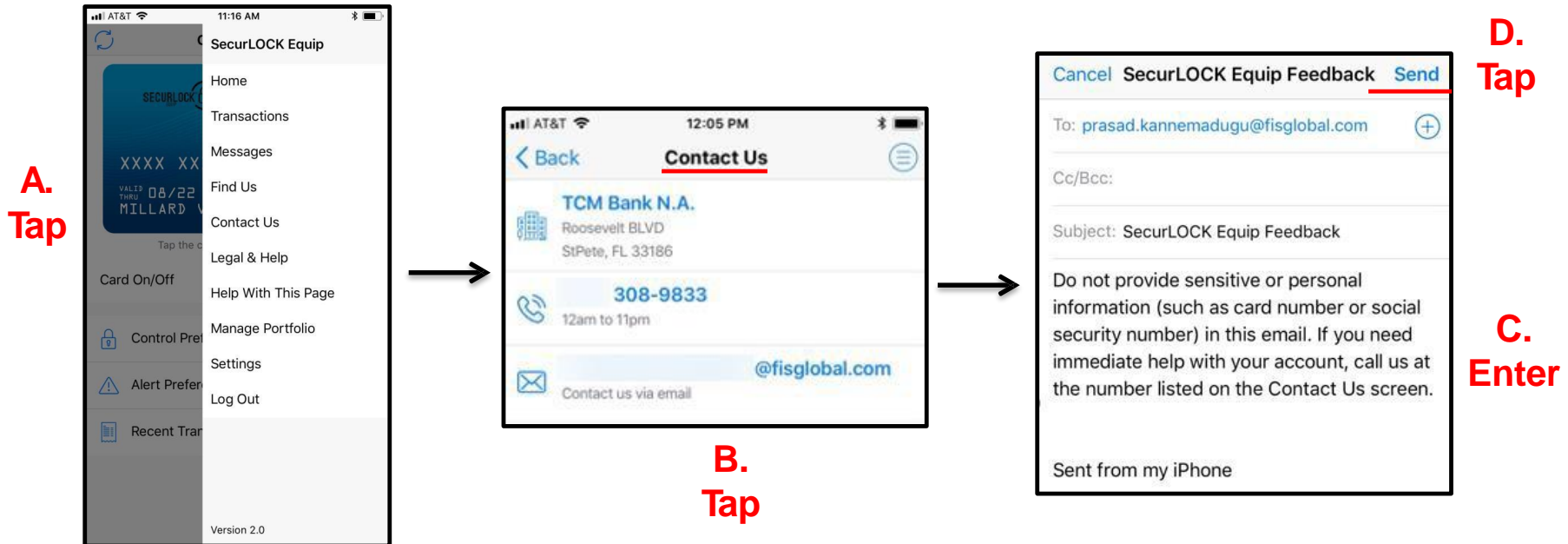


C.  
Tap

D.  
View  
and  
Tap

# Home Screen – Main Menu Options

## Contact Us

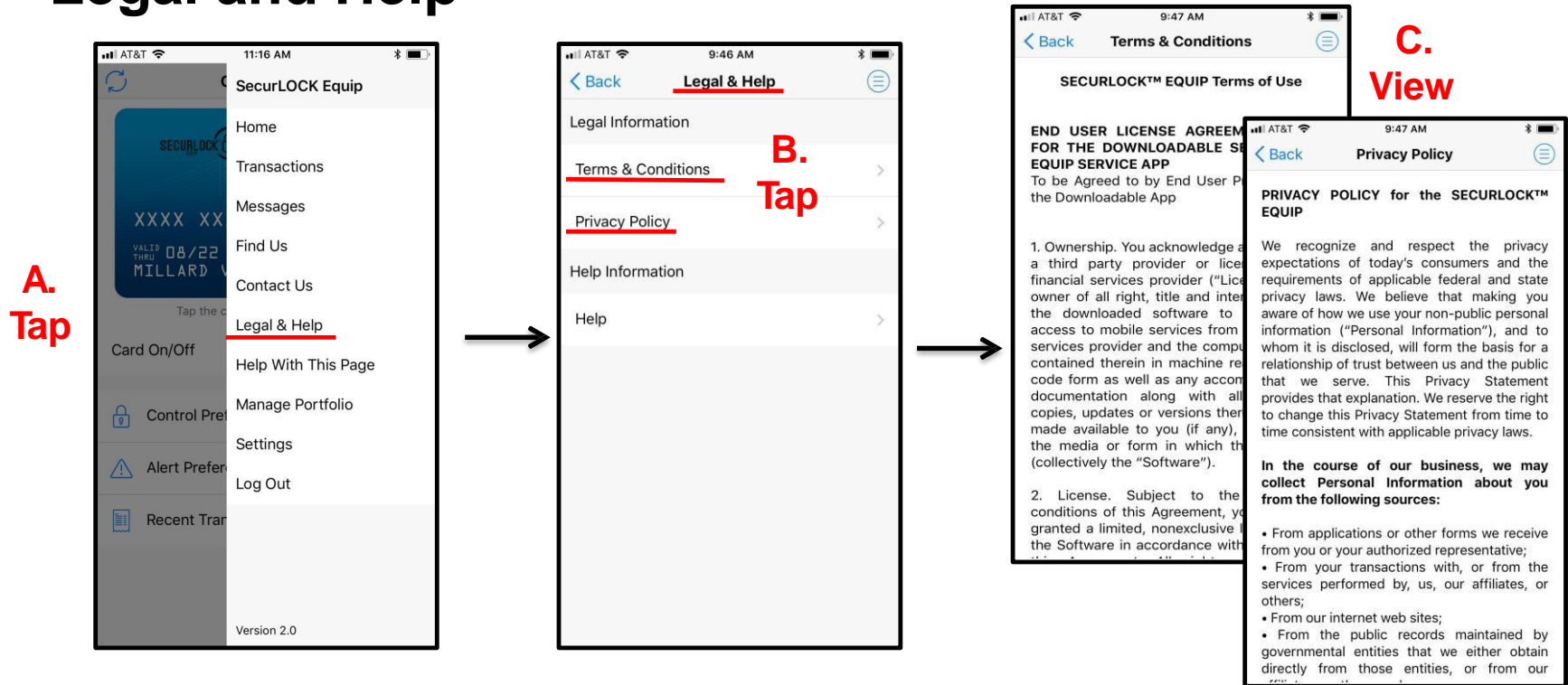


- By tapping the 'Contact Us' icon from the Home Menu or from the Welcome screen, the user can see the contact information of the financial institution.
- Tapping the phone number and then tapping 'Call' enables the user to reach the financial institution for assistance.
- Tapping the email address provides the user with the ability to send an email directly to the FI.
- When the user taps on the email link, the app will activate the mobile device's default email to send a message to the FI.



# Home Screen – Main Menu Options

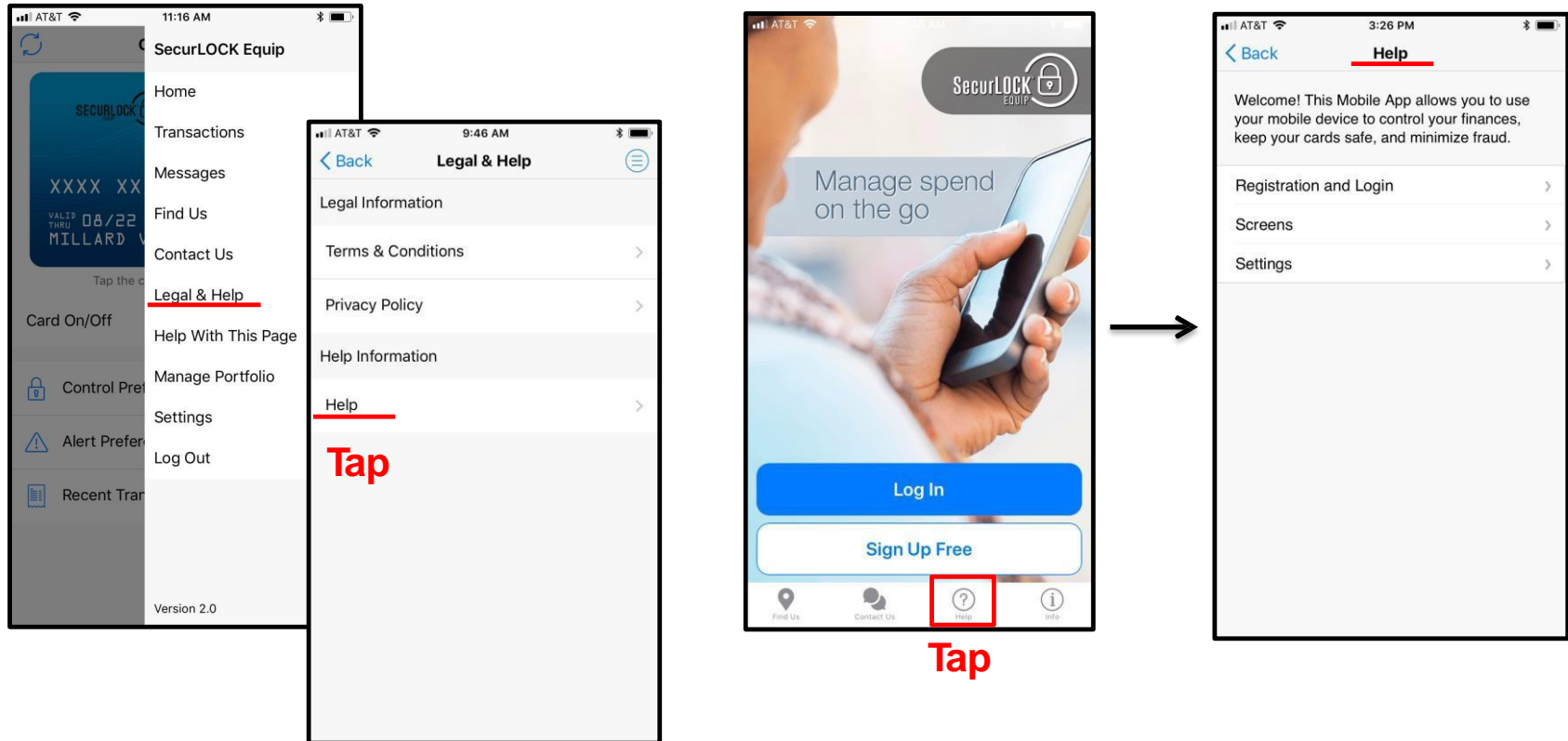
## Legal and Help



- Tapping 'Legal & Help' on the Home Menu takes the user to the Legal & Help screen.
- The Legal & Help screen feature provides the user with access to the 'Terms & Conditions' and 'Privacy Policy' to view the respective legal statement that was accepted during the registration process.

# Home Screen – Main Menu Options

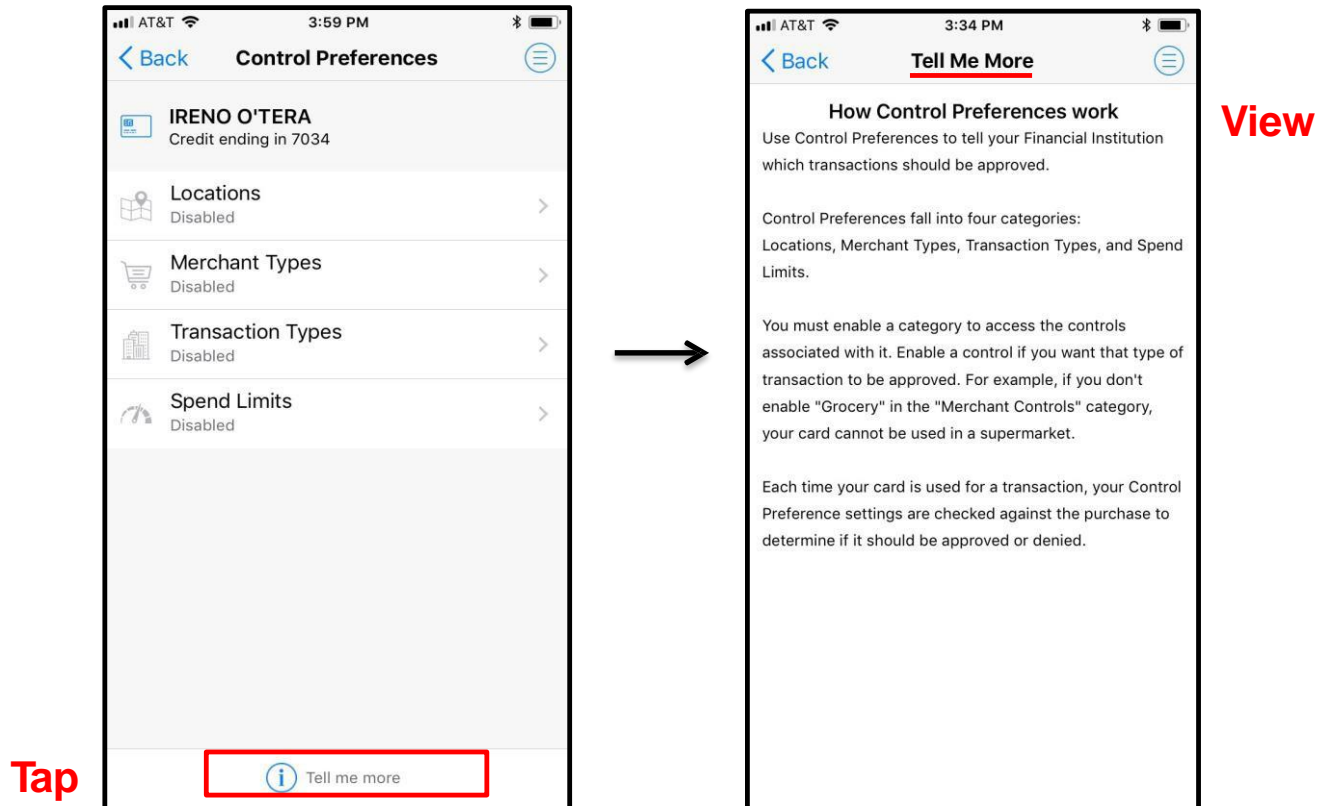
## Legal and Help



- Access the Legal & Help option on the Menu or by using the 'Help' button on the Main Login screen.
- 'Help' is a text document that covers all major functions of the application.
- On this screen, a user can tap different sections to see more detailed information.

# Home Screen – Main Menu Options

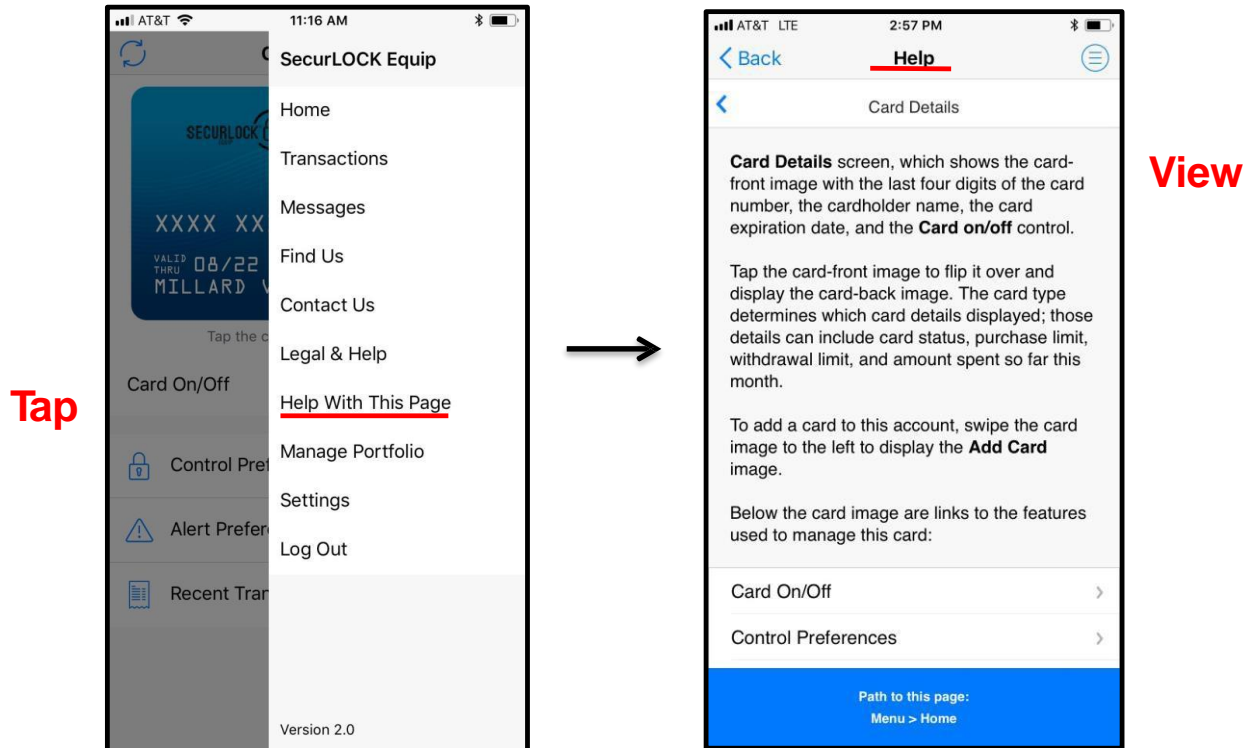
## Tell Me More



- Tap 'Tell Me More' at the bottom of selected screens within the app.
- This will take the user to the 'Tell Me More' screen with additional information about the screen that the user is currently on.

# Home Screen – Main Menu Options

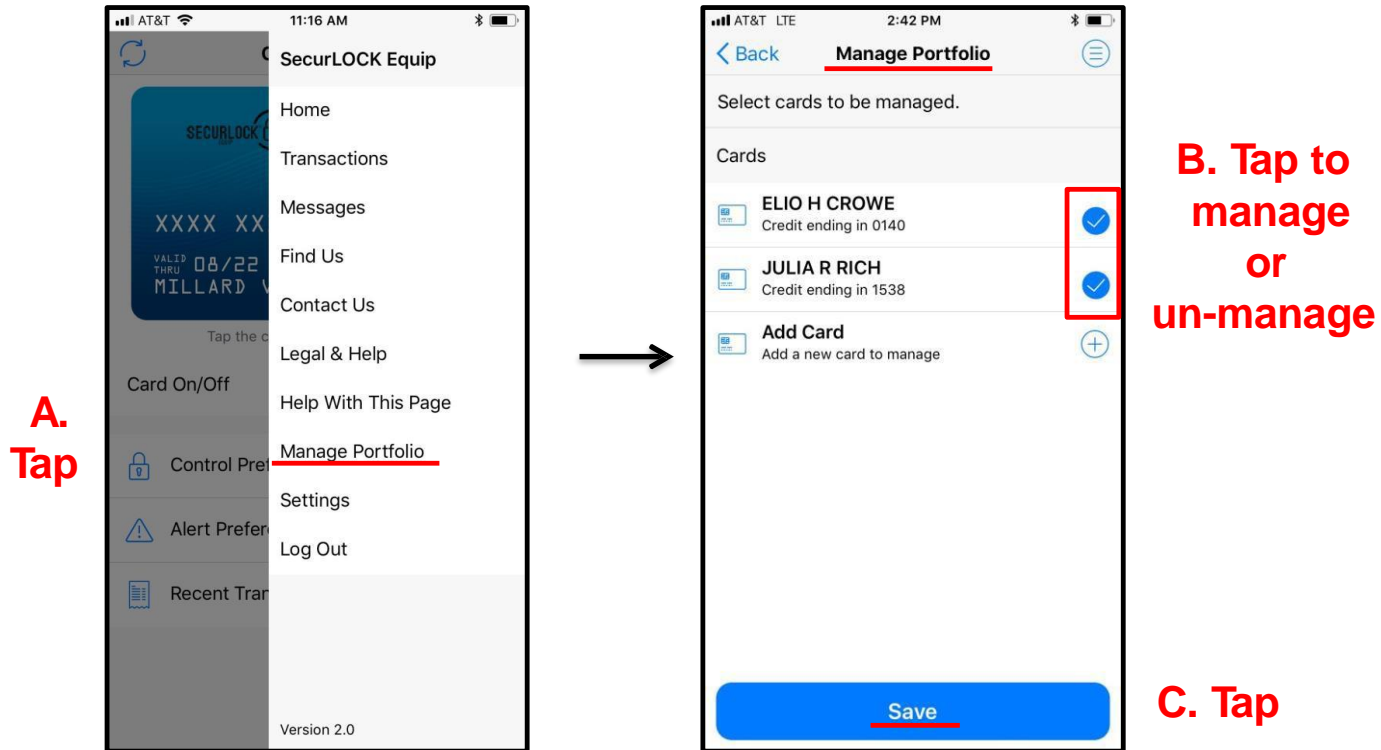
## Help With This Page



- 'Help With This Page' is available to better assist users in quickly accessing the information they need.
- When selected, the specific 'Help' screen will open that directly relates to the screen the user is on.

# Home Screen – Main Menu Options

## Manage Portfolio

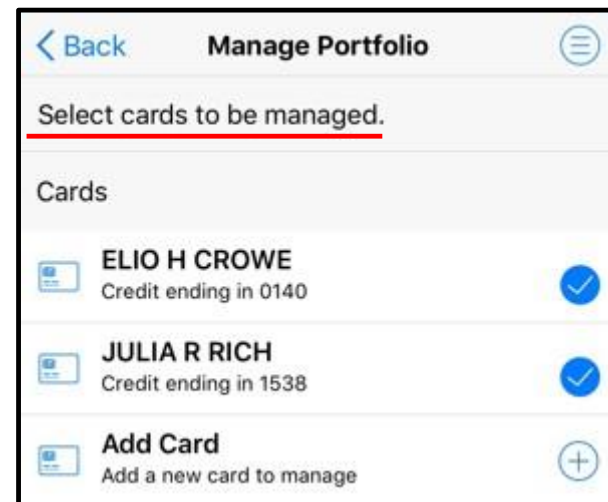


- Tapping 'Manage Portfolio' from the Home Menu takes a user to the 'Manage Portfolio' screen. Here, the user can select cards to be managed or un-managed by the app.
- To un-manage a card, the user unchecks the box next to it, then taps 'Save'.

# Home Screen – Main Menu Options

## Manage Portfolio

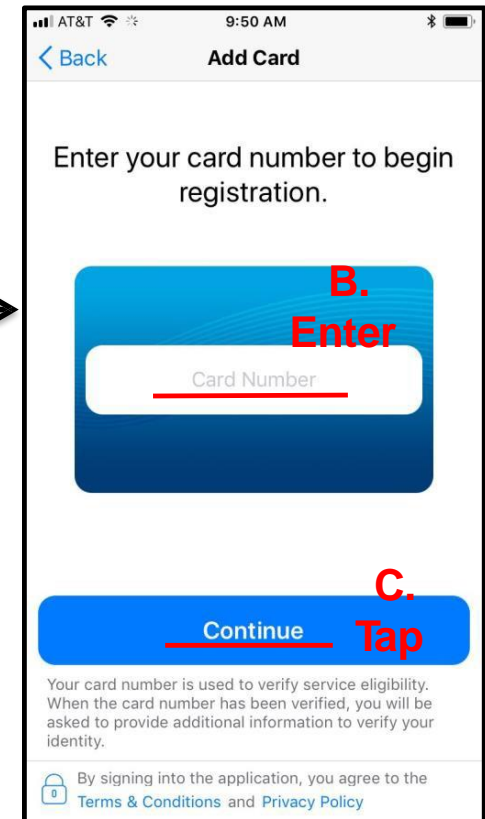
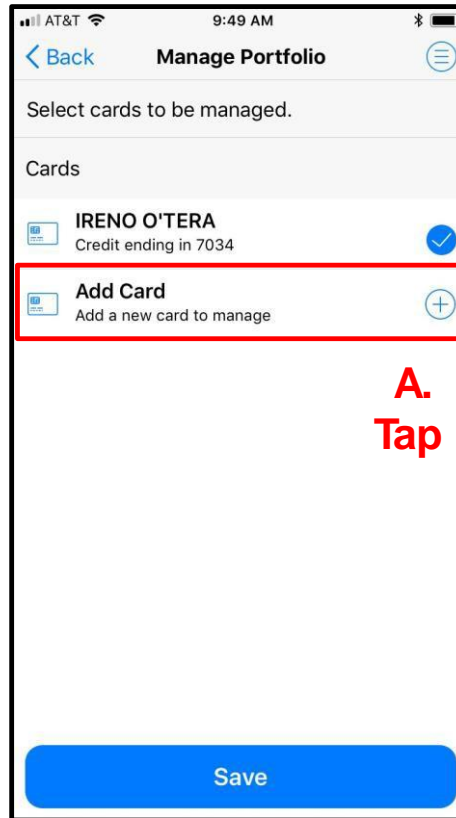
- An unmanaged card will no longer be viewable on the Card Details page.
- If a user chooses to un-manage all cards s/he will be asked if s/he wishes to unsubscribe from the service.
- If the user wants to use the app again after un-subscribing, s/he will have to register as a new user.
- Users are able to reuse a Login Name that was unsubscribed – as long as another user is not currently registered 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

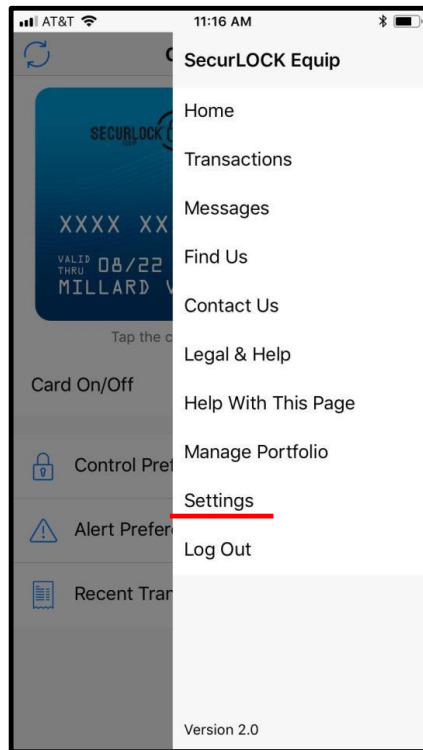
## Manage Portfolio – Add a Card

- On the Manage Portfolio screen, the user can add a new card for management in the app by tapping 'Add Card'.
- The 'Add Card' process is process, with the following exceptions:
  - A user is not asked to accept the Terms & 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'.
- There is no limit to the number of cards that can be added to the app. However, management of more than 20 cards at one time may negatively impact app performance.

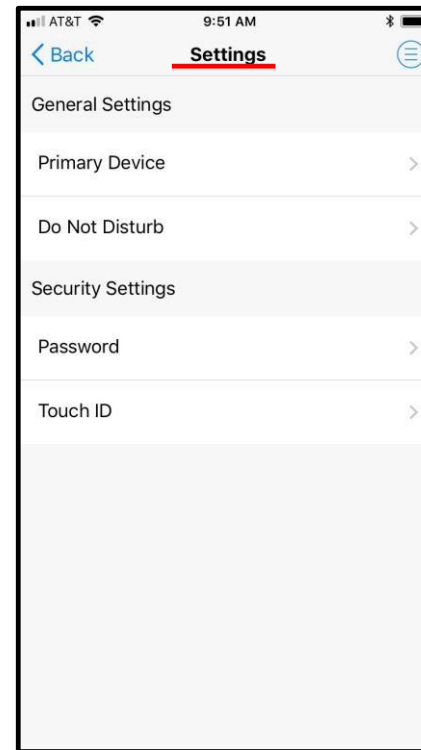


# Home Screen – Main Menu Options

## Settings



Tap



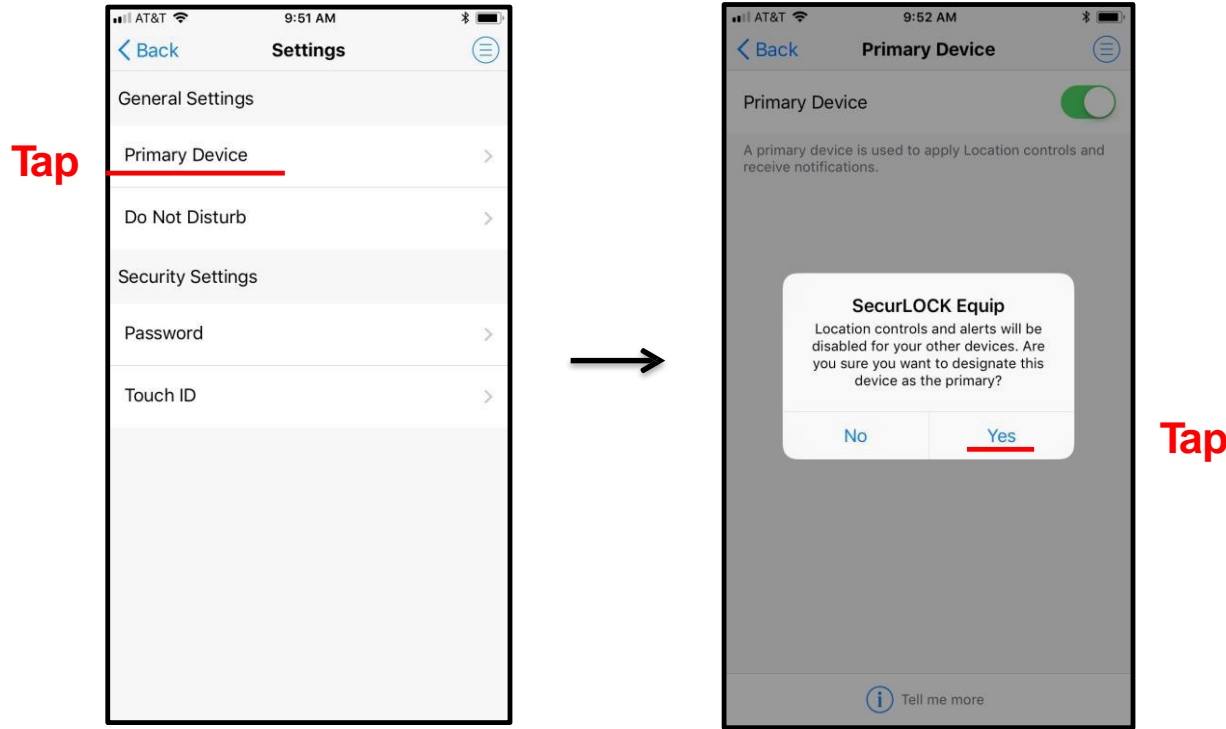
Options

- Tapping 'Settings' on the Home Menu takes a user to the 'Settings' screen.
- This screen provides the user with the following options:
  - Set Primary Device
  - Set Do Not Disturb window
  - Change Password
  - Enable/Disable biometric login (Touch ID/Face ID or Fingerprint)



# Home Screen – Main Menu Options

## Primary Device

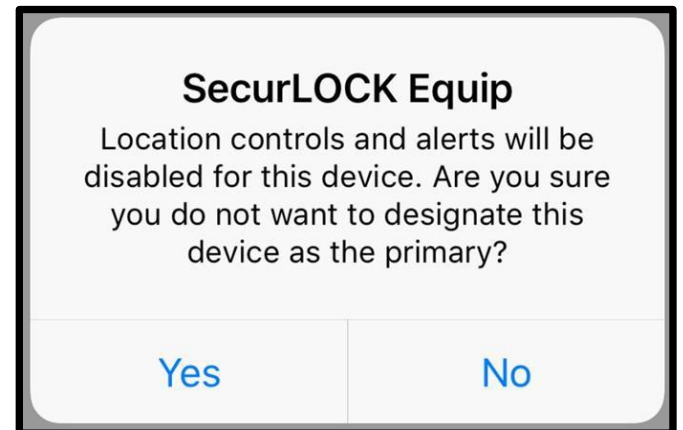
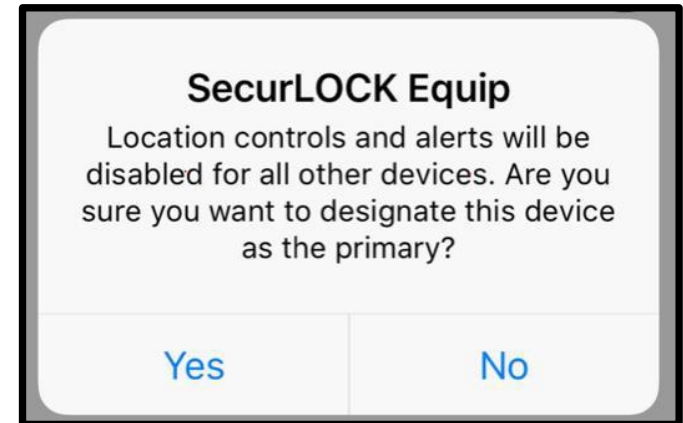


- A user must set their device to the Primary Device in order to receive alerts.
- To set a phone as the primary device, follow these steps:
  - Tap on “Primary Device.”
  - Tap the “Primary Device” slider to the “ON” position.
  - Tap ‘Yes’ when a confirmation message is received asking ‘Are you sure you want to designate this device as the primary?’

# Home Screen – Main Menu Options

## Primary Device

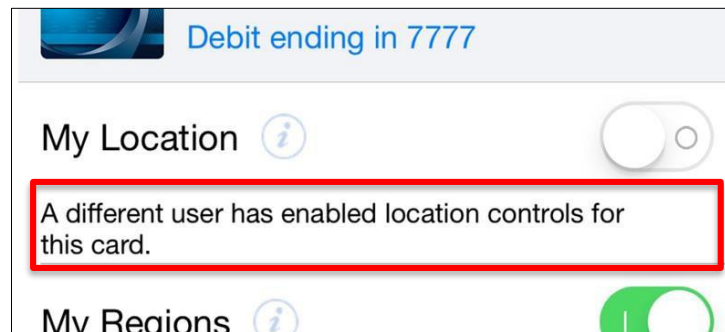
- The message that displays after the device is made primary indicates that if the same Login Name was used to login to another device, *that device* will no longer be primary.
- Only one device can be primary when logging into multiple devices with the same Login Name.
- When Primary Device is disabled, another message will display to ensure the user wants to make the change.
- One Login / Multiple Devices / Shared Card Number:
  - The Primary is based on the DEVICE, not the user.
  - Only the Primary Device will 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.



# Home Screen – Main Menu Options

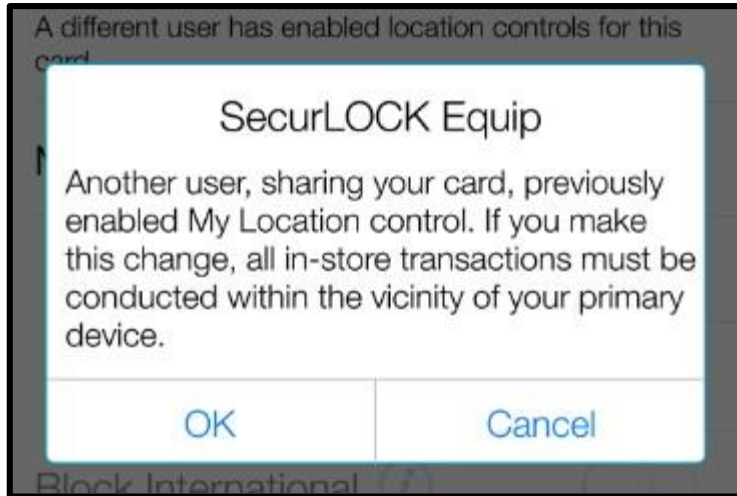
## Primary Device

- **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 last enabled My Location. For other users, the app will display a message under the My Location control.**



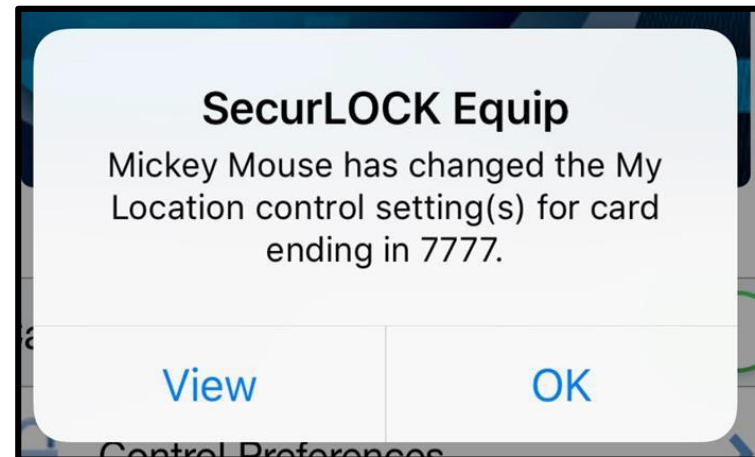
# Home Screen – Main Menu Options

## 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 Mouses' device is now being used for My Location.



# Home Screen – Main Menu Options

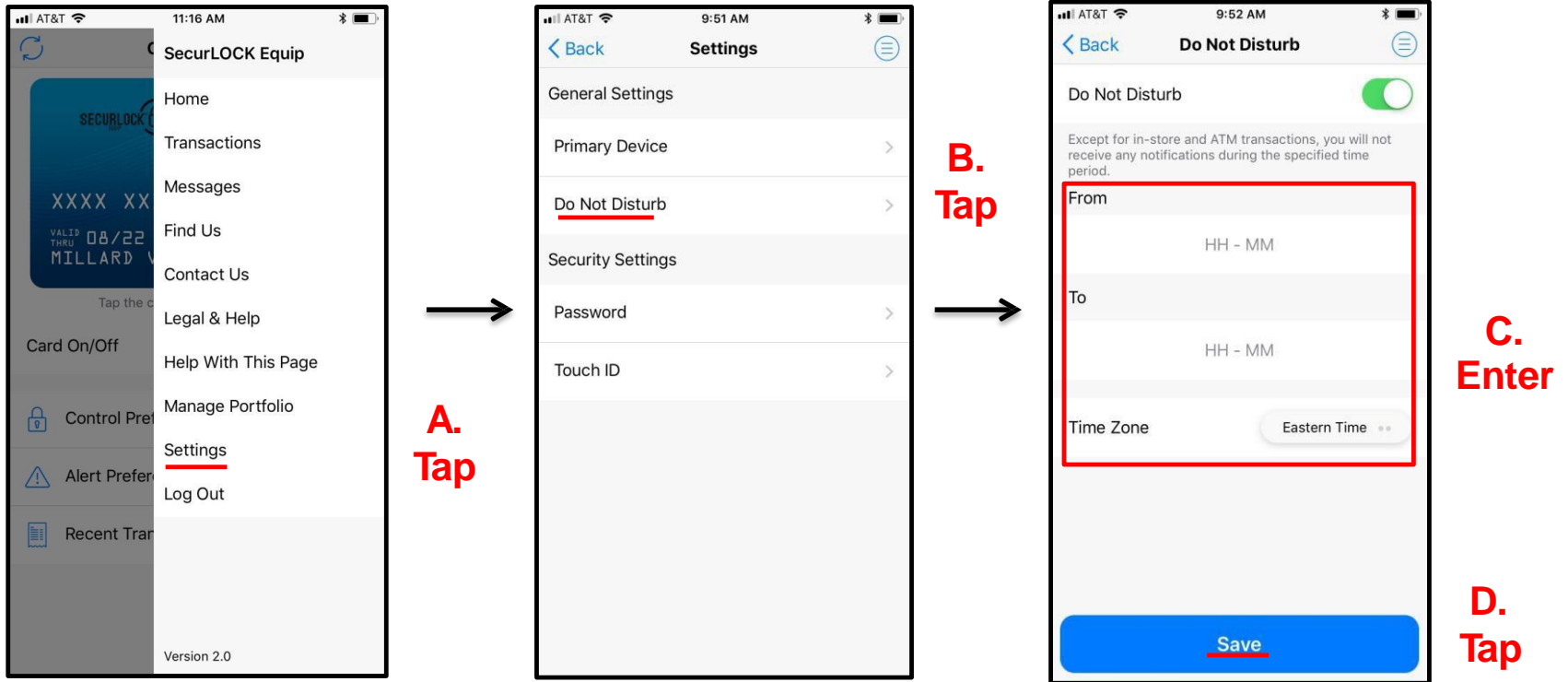
## Shared Cards

### **Additional information regarding 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 a shared card or unsubscribes from the app, no notification of this event is sent to the other card users who have registered or added the same card.

# Home Screen – Main Menu Options

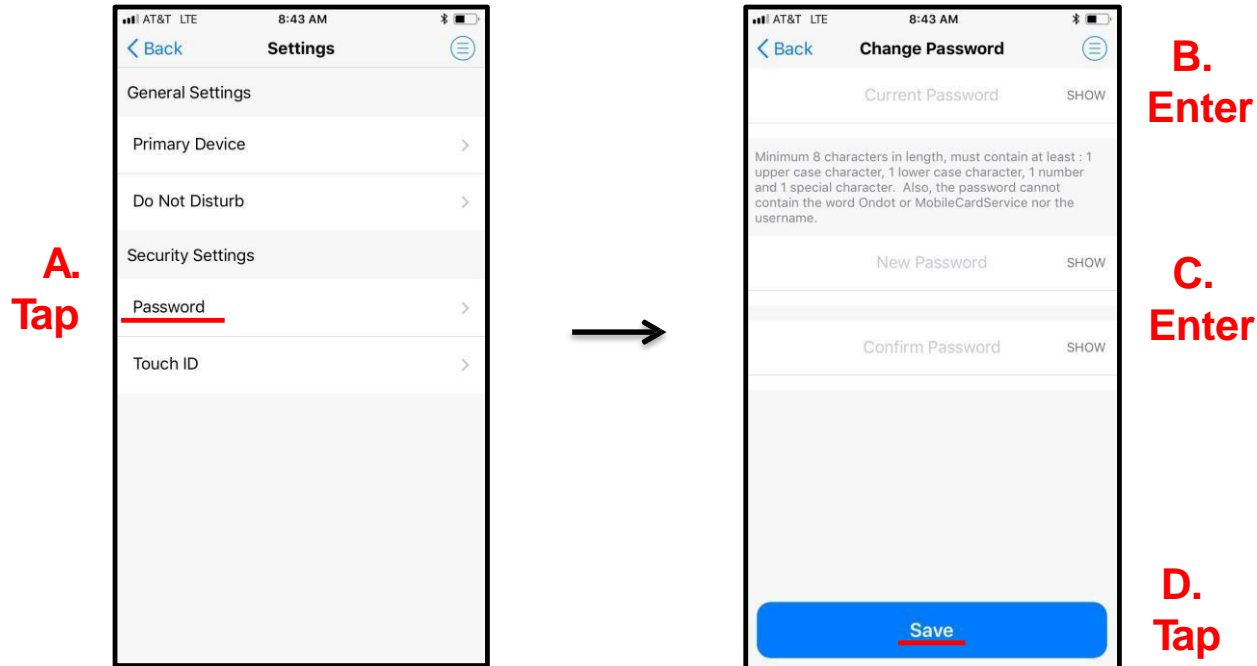
## Do Not Disturb



- Use 'Do Not Disturb' to set quiet hours during which notifications are stored in the Messages section of the app without disturbing the user, except for in-store transactions, ATM transactions and denied transactions.
- In order to set 'Do Not Disturb' within the app: On the menu, tap 'Settings', select 'Do Not Disturb', set 'From' and 'To' times, select the desired time zone and then tap 'Save'.

# Home Screen – Main Menu Options

## Change Password

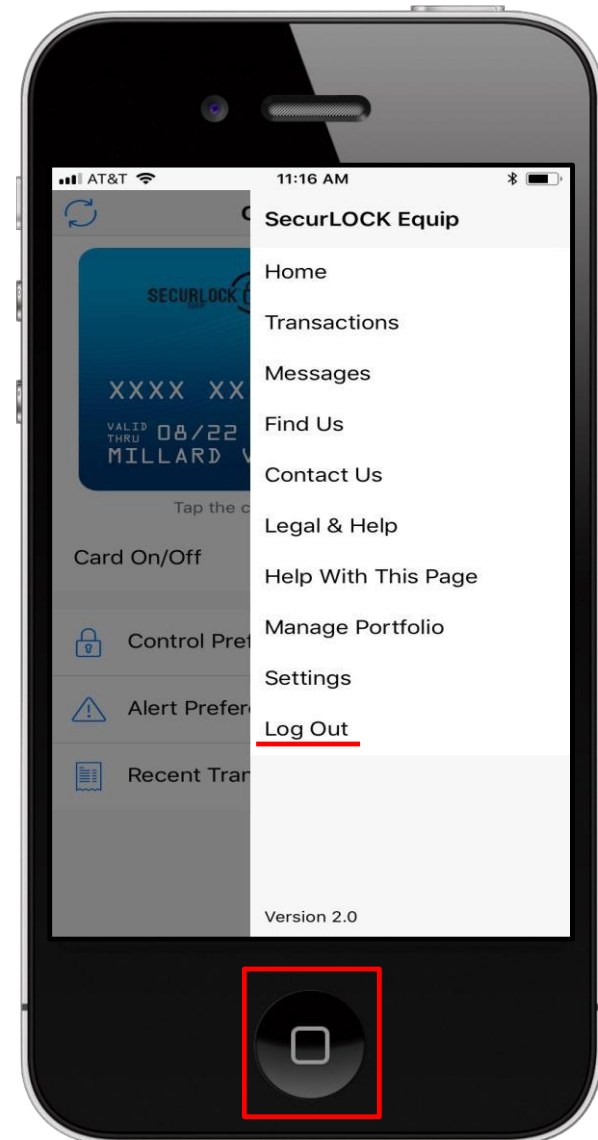


- Tapping 'Password' on the Settings screen takes user to the 'Change Password' screen where the user can change the password used for logging into the app.
- To change the password, the user needs to enter the old password and enter the new password twice to confirm the entry and then tap 'Save'.
- To assist the user with correctly entering the password characters, the user can tap 'SHOW', which will make the password visible.

# Home Screen – Main Menu Options

## Logout

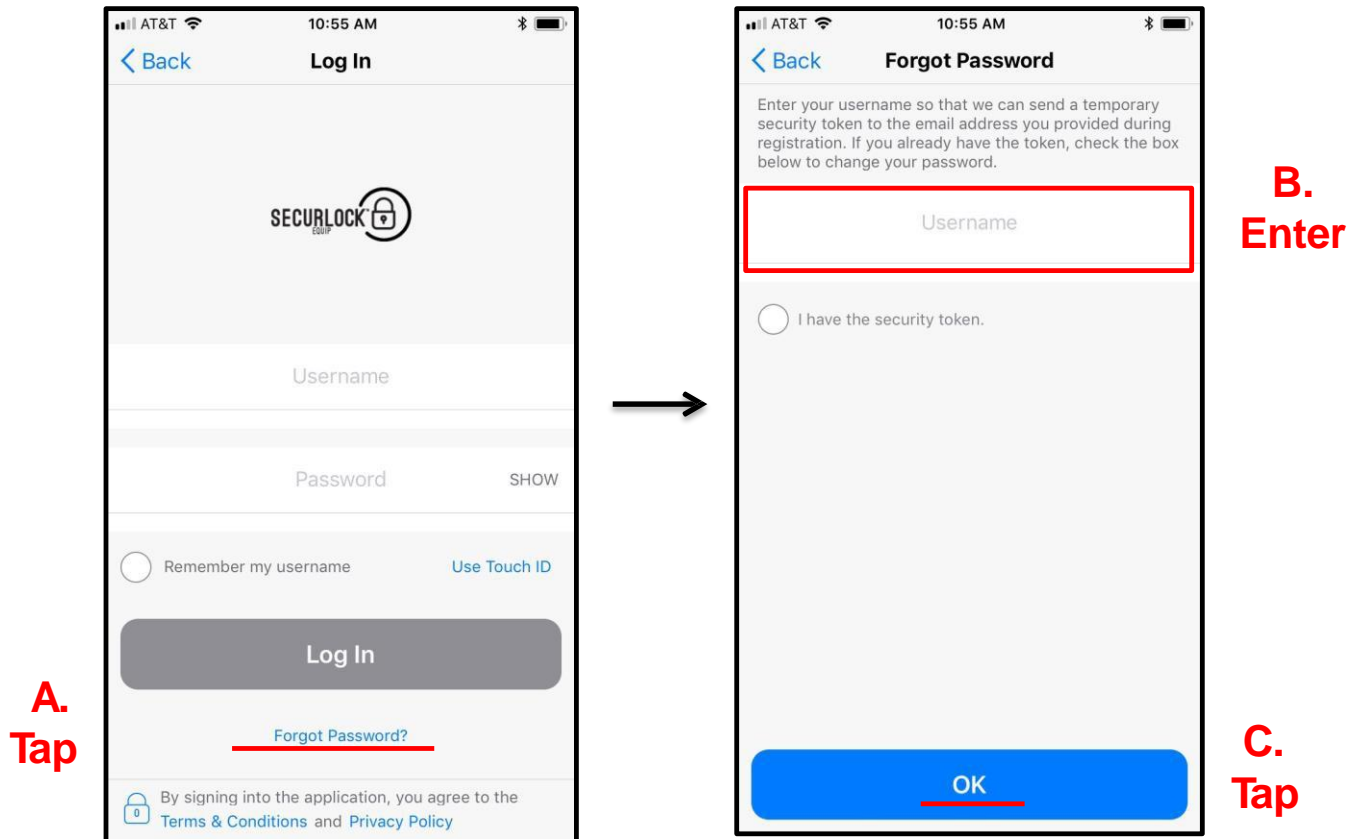
- There are two ways to exit the app:
  - By navigating to the device's home screen
  - By logging out
- By navigating to the device's home screen, the user is brought to the home page and can access the app again by using biometric login or Passcode.
- By selecting 'Log Out' from the Menu, the user will be logged out of the application and brought to the Login page.
- To log back into the application, the user will need to either use biometric login or enter their login credentials.



Tap



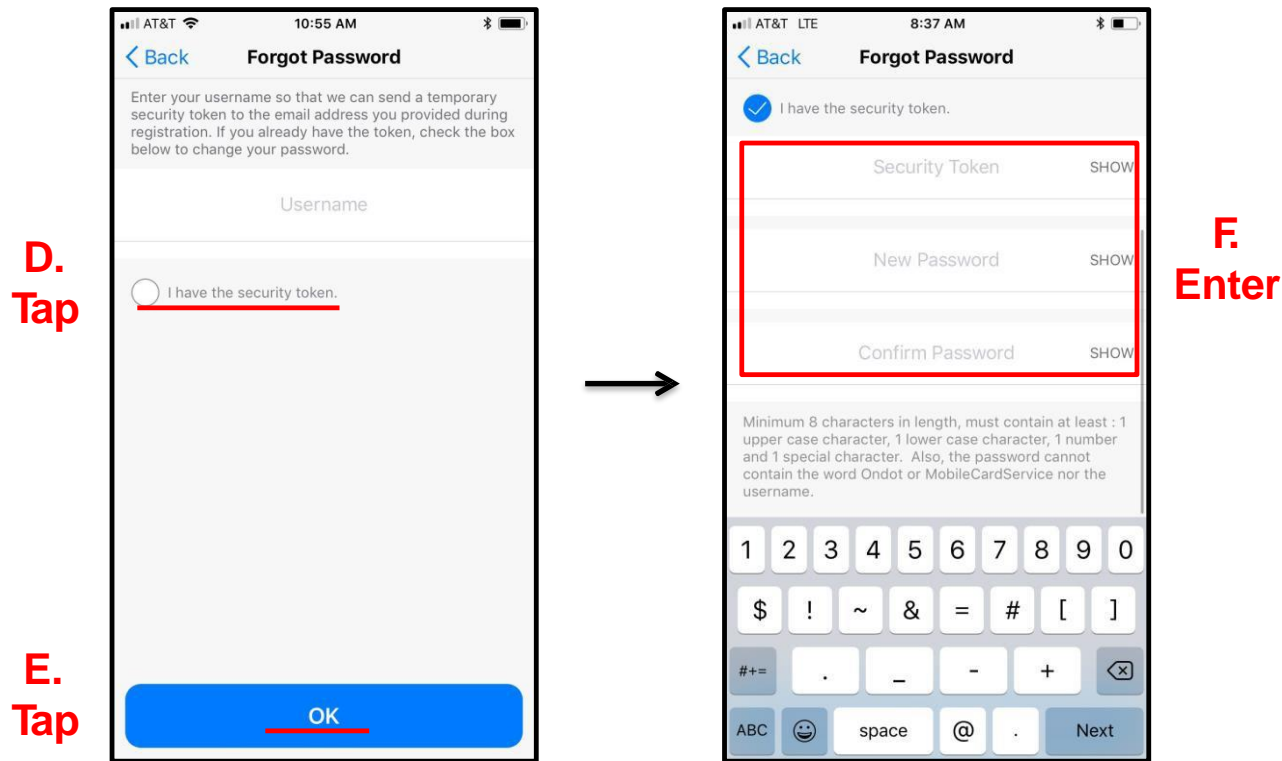
# Reset Password Procedure – Request a New Password



- Tapping on the 'Forgot Password?' link on the Login screen will cause the Forgot Password screen to display.
- The user enters their Username and then taps 'OK' to have a one-time passcode sent to the email address that was entered during registration.

# Reset Password

## Procedure – Select New Password

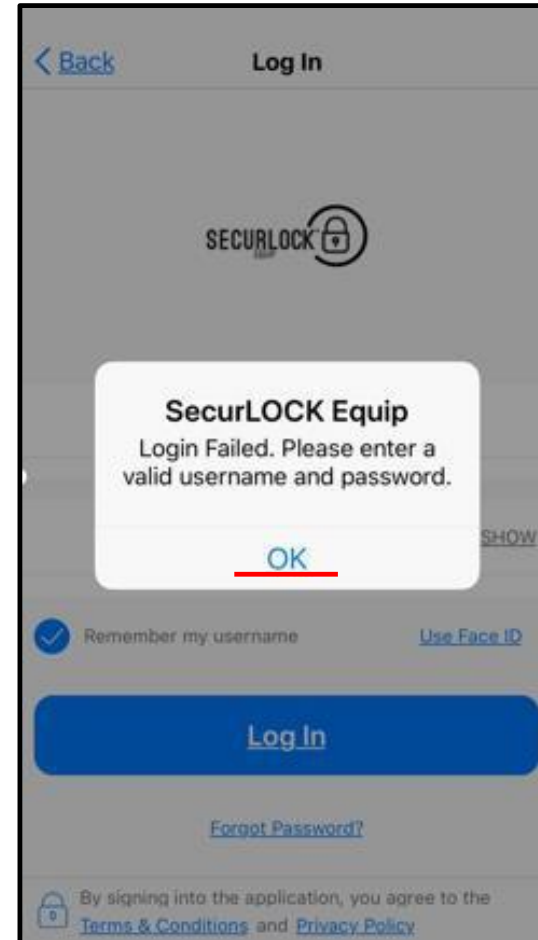


- The user needs to check their email to retrieve the one-time passcode sent, then tap the radio button 'I have the security code' on the Forgot Password screen.
- The user will be prompted to enter the OTP, choose and confirm a new password, then tap 'OK' to proceed.
- The email with the one time passcode will include the OTP expiration time (e.g., token will expire at 10:15am ET).

# Reset Password

## Login Failure Error Message

- Message user receives when login credentials are entered incorrectly.
- Same message will display if login failures continue to occur. After three failed attempts, the user will be locked out from the login process, but the message will not change.
- The only way the user can get passed this is to tap 'Forgot Password' or contact their financial institution to have their profile enabled via mConsole On Behalf Of.

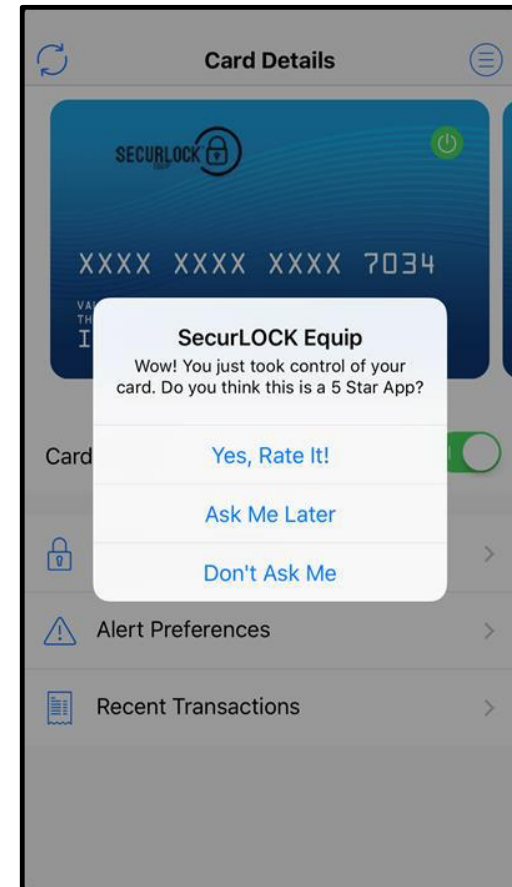


Tap

# SecurLOCK™ Equip – Mobile App Procedures

## App Rating

- **This feature enables users to rate the application after completing one of the below activities:**
  - Successfully turned the card On/Off 10 times
  - Successfully set the My Location Control preferences 10 times
  - Successfully logged into the Mobile App 1,000 times
- **Options to rate the app:**
  - **Yes, Rate It!** takes the user to the respective app store to rate the app.
  - **Ask Me Later** clears the message and resets the trigger.
  - **Don't Ask Me** causes the app to stop displaying this message for as long as the user is still using the same app version.



# SecurLOCK™ Equip – Mobile App Procedures Review

- [Objectives](#)
- [Communicate vs. Equip Quick Comparison](#)
- [Marketing Website Link](#)
- [Install Application](#)
- [Register User](#)
- [Logging In to the Mobile App](#)
- [View Card Details](#)
- [View Transactions](#)
- [Set Up Control Preferences](#)
- [One-time Override](#)
- [Set Up Alert Preferences](#)
- [Home Screen - Main menu options](#)
- [Reset Password](#)
- [App Rating](#)

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.*