



Mobile Wallet - Do's and Dont's

- Utilize all available PIN, password, and fingerprint protection options.
- Turn on notifications and regularly monitor transaction history for unauthorized payments.
- Only transfer money to people or merchants you know and trust.
- Do not link your mobile wallet application to a social networking service (e.g. Facebook, Twitter.)
- Link a bank account only to cash out; delete bank account information once the cash out process has completed.

What are Mobile Wallets?

Mobile wallets allow you to link credit cards, debit cards, and bank accounts to complete one or both of the following transaction types:

- **User to friend:** Allows you to transfer money to friends using their email address or phone number. Money is stored in a balance within the mobile application. You can use this balance for further transfers or deposit it into your bank account.
- **User to merchant:** Allows you to pay for goods and services at the point-of-sale using a QR code or NFC chip (near field communication). You can pay selecting a specific card, account, or existing balance, if available.

Mobile wallets from different companies do not interact with each other; for example, you cannot transfer money from Google Wallet to a friend with Venmo. Given that different mobile wallets perform distinct functions, you may maintain multiple wallets.

Benefits of Mobile Wallets

Mobile wallets are primarily designed to provide convenience. They allow you to quickly settle debts with friends wherever you are, without cash or checks. Mobile wallets can also consolidate many credit cards, debit cards, bank accounts, loyalty cards, and gift cards into a single app on your mobile device.

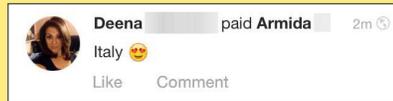


On iPhones, fingerprints can be used as a purchase authentication method, enhancing your security over a physical credit or debit card.

Threats from Mobile Wallets

Consolidating multiple cards into a single app exposes you to an increased risk. Physically losing possession of your phone may allow an unauthorized user to make payments with any linked card or account. Unauthorized users will also have access to consolidated transaction logs, exposing a wide range of your habits, activity, and finances.

Most wallets are also accessible through a web browser. Although cards may physically be in your possession, unauthorized access to your online wallet account will expose your personal information and activity and also put your money at risk for theft.



Some mobile wallets offer social features, such as an activity feed of friends' transactions or the option to post transactions to Facebook. Without strict privacy settings, social features expose your activity and potentially even your whereabouts, as shown to the left.

Choosing the Right Mobile Wallet

You should consider the following questions when choosing a mobile wallet:

- What operating system do you have?
- Are you transacting with your friends or paying merchants?
- What security features do you require?
- Do you want social options? Do you want the ability to limit social options?



Six of the most popular mobile wallet services are outlined below.

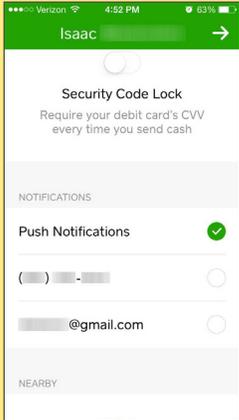
Service	Operating System	Transaction Type	Identity Data	Available Security	Social Network Links	Default Transaction Visibility
Square Cash	iOS, Android	User to friend	Photo, phone number, email, debit card number	CVV requirement before transfer	None	None
Apple Pay	iOS	User to merchant	Full name, billing address, shipping address, email, phone number	Fingerprint required for transaction	None	None
Google wallet	iOS, Android, browser	User to friend, User to merchant	Photo, full name, email, bank account and card numbers	PIN required to open app	None	None
venmo	iOS, Android, browser	User to friend	Photo, full name, email, about (optional), phone number, bank account and card numbers	PIN or fingerprint required to open app	Facebook (optional), Internal social features	In-app friends
LevelUp	iOS, Android, browser (limited)	User to merchant	Full name, email, birthday, gender, card numbers	PIN or fingerprint	Facebook (optional)	None
PayPal	iOS, Android, browser	User to friend, User to merchant	Photo, full name, email, phone number, bank account and card numbers	Password required to open app	None	None



Mobile Wallets Smart Card

Last Updated: 11/05/2014

Square Cash



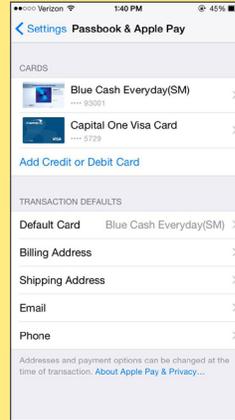
Navigate to *Settings* in the upper left portion of the home screen:

- Add your *Email Address* to verify your account
- Require CVV *Security Code Lock*.
- Enable *Push Notifications*.

Utilizing Cash's Bluetooth-based Nearby option allows you to be seen by nearby users. This feature is not recommended.

An activity log is located in the upper right portion of the home screen. Monitor this section for unauthorized transactions.

Apple Pay



In the iPhone **Settings > Passbook & Apple Pay** menu, add credit or debit cards you wish to use with the service.

Note that an unauthorized user of your iPhone can view the last 4 digits of your cards, your billing address, shipping address, email address, and phone number.

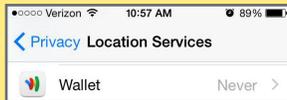
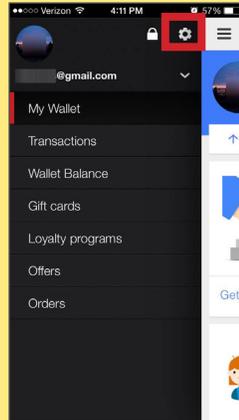
To mitigate the risk of exposing personal information, enable PIN, password, or fingerprint protection for your iPhone's lock screen.

Google Wallet

In the *Settings* menu:

- Turn on *Notifications* for Wallet Card purchases.
- Set *PIN Timeout* to '15 minutes.'
- Check *Monthly statements* for unauthorized transactions.
- Monitor the *Transactions* section of the sidebar for unusual activity.

Navigate to your iPhone's **Settings > Privacy > Location Services** and set Wallet location access to 'never.'

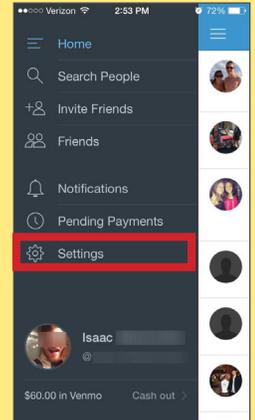


Note to Android users: It is recommended you disable all location services by navigating to **Settings > Personal / Location Access**

Venmo

Navigate the dropdown menu to *Settings*:

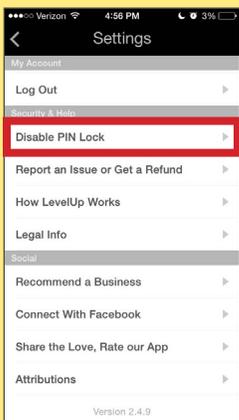
- Under *Notifications*, enable push notifications for payment sent, trust charge received, and bank transfers to Venmo completed.
- Enable *Touch ID & Passcode* and turn on 'Use Touch ID.'
- To limit social visibility, under *Privacy*, set audience for future transactions to 'Private.' Set "Who can share transactions involving you?" to 'Only Me.' Make all past transactions 'Private.'
- Venmo provides an option to 'trust' friends and automatically pay their requests. Utilizing this feature is not recommended.



Monitor your transaction activity by clicking on the logo of a single person at the top of the home screen. Navigate to your iPhone's **Settings > Privacy > Location Services** and set Venmo location access to 'never.'



LevelUp

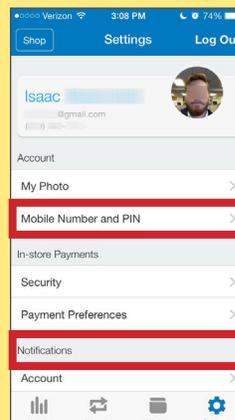


Navigate to the *Settings* menu, found in the top left corner of the home screen:

- Monitor your transaction history under *Transaction History*.
- Enable PIN lock.
- iPhone users should utilize the Touch ID lock option
- Do not connect your Facebook account to LevelUp.

Navigate to your iPhone's **Settings > Privacy > Location Services** and set LevelUp location access to 'never.'

PayPal



Navigate to *Settings*:

- Upload an up-to-date *My Photo* to protect against fraud.
- Set a PIN under *Mobile Number and PIN*.
- Verify your phone number *Mobile Number and PIN*.
- Turn on all options under *Notifications*. Your account activity can also be monitored on the *Activity* home screen.
- Only enable Bluetooth when engaging in an in-store transaction.

Navigate to your iPhone's **Settings > Privacy > Location Services** and set PayPal location access to 'never.'

Useful Links - For more information or questions regarding this card email smartcards@novetta.com

A Parent's Guide to Internet Safety
 Privacy Rights Clearinghouse
 Microsoft Safety and Security
 OnGuard Online

www.fbi.gov/stats-services/publications/parent-guide
www.privacyrights.org/fs/fs18-cyb.htm
www.microsoft.com/security/online-privacy/social-network
www.onguardonline.gov/topics/social-networking-sites.aspx

