Guidelines for Using Venmo

Venmo, a service of PayPal, is intended as a method of non-commercial payment between subscribers. Subscribers generally link Venmo accounts to bank accounts allowing transfer of funds in and out of VENMO accounts. In some cases, fees are charged for transactions, as detailed in <https://venmo.com/about/fees/>.

By default, Venmo operates using principles of social networking in that it ‘shares’ information about transactions with an audience larger than just the payer and payee. The tiers of information sharing are *Public* (visible to everyone on the internet), *Friends* (visible to sender, recipient, and their friends), and *Private* (visible to sender and recipient only).

When using Venmo, it is important to understand the Venmo Privacy Policy and User Agreement:

<https://venmo.com/legal/us-privacy-policy/>

<https://venmo.com/legal/us-user-agreement>

**The following guidelines should be followed for use of Venmo in processing payments to IRB study participants:**

* Create a dedicated Venmo account that will be used for the sole purpose of processing study related payments. If a personal account were used, information about prior transactions would be retained by the account custodian should they leave the organization and would be lost to JHM. Information about payments made to study participants must not be subject to such transfer of custody outside the organization.
* Venmo account transactions are stored in the *Statement* section of the Venmo account portal. Download a monthly record of transactions to protect against possible loss of access to the account.
* Venmo account transactions should be verified and reconciled by a person other than the one who performed the transaction.
* Venmo phone app should be configured with a PIN or Touch ID <https://help.venmo.com/hc/en-us/articles/217532257>
* JHM does not have control over payees configuration or management of their Venmo settings. For example, they may choose to allow popup notifications, which could reveal the name of payer and information typed into the *What’s it for* field of payments received. Therefore,
	+ The account name must not reveal information that should otherwise be protected. For example, if the name of a study reveals information about a possible medical condition, the study name should not be included in the account name. In some cases, even the name of the Center, Department, or School could raise unwanted questions for payees, if seen by others on their phone screen.
	+ Information included in the *What’s it for* field should be similarly protected to protect the source and purpose of the payment.
* Venmo accounts should not be linked to social networks (Facebook is a currently available option).
* Venmo accounts should be configured with a secure, complex password that is a minimum of eight characters and includes a combination of upper case, lower case, numbers, and special characters.
* Venmo passwords should not be saved to the phone, computer, or other device being used to process transactions. Password should be required for each use.
* The default privacy settings for Venmo accounts should be altered from default *Public* to *Private*.
* Upon every transaction, the privacy setting (bottom right corner of payment window) should be verified to be *Private*.
* Following each session of use, Venmo app should be closed to protect against unintended use of open session.
* Payments in Venmo are irrevocable. The identity of intended recipients must be verified prior to processing transactions. Venmo may contain many accounts that have the same name, making it possible to inadvertently send payment to the wrong person. Each Venmo account has a unique username that starts with an @ symbol (although it is unlikely that it is the email address of your payee). Alternatively, each Venmo account has a corresponding QR code that uniquely identifies the account. Either of these may be used to identify an intended payee. Account username should be verified with payee. For large payments or ones that are expected to repeat, it may be appropriate to send a small payment and verify receipt to positively confirm that the correct payee account is being used.

**The following recommendations should be provided in instructions to research participants and possible payees of funds using Venmo:**

* The computer, phone, or other device being used to access Venmo should be protected using a secure password, PIN, touch scan, or other authentication method.
* Device notification settings should be managed so that text, app, and email notifications are suppressed if such notifications are unwanted or might inadvertently reveal information to others in proximity to the device.
* Venmo account settings should be configured as follows:
	+ Secure password.
	+ Default Privacy settings changed to *Private*.
	+ Account password is not remembered by the device.

**Note on limiting exposure to financial resources**

Venmo accounts are generally linked to bank accounts or credit/debit cards. This allows for seamless transfer of funds in and out of Venmo accounts. When using VENMO for JHU institutional purposes PCard use is required. Links to financial accounts expose a risk in that a compromise of a Venmo account might result in loss of assets from the linked account. This risk could be mitigated by linking the Venmo to a PCard, transfer the appropriate funds, and then unlink the PCard.