Jasmine Singh and Mary Touma

Apple Pay. Here to Slay?

Does Apple Pay provide users with privacy and security?

Apple Pay. Here to Slay

Jasmine Singh & Mary Touma

Digital payment service, Apple Pay was officially introduced in October 2014. This service is available for any user possessing an iPhone 6 or later model. The service can also be used on the Apple Watch, Mac, and iPad. Replacing traditional wallets, Apple Pay allows users to digitally pay for goods and services in-store or online.

In order to use the service, the user must add an eligible card to the Apple Wallet app, a pre-installed app on the iPhone. This application not only accepts credit, debit, or prepaid cards but also rewards cards, tickets to events and travel passes, effectively replacing a traditional wallet.

The digital payment service grew to have many users within a short period of time. It is suggested that Apple Pay's quick growth relates to the psychological benefits offered by the service. According to a study, Apple Pay offers the user a sense of "coolness" with a successful transaction.

However, success is only guaranteed if the user has enough funds on their card. If not, the user could face some embarrassment from using the service — it's like a double-edged sword.

Speaking of double-edged swords, according to Julien, R., Jr. (2016), Apple Pay can not only provide psychological benefits to its users but could also present a new, secure way for cybercriminals to commit their crimes.

Whilst traditional bank cards rely on magnetic strips and signals as a means of verification, this security feature does little to prevent hackers from accessing, forging, and copying the sensitive data stored on credit, debit, or prepaid cards. Apple Pay does not rely on these magnetic strips and signals to verify a transaction, dodging the bank card features hackers continue to exploit. Although Apple Pay may have corrected a security flaw within traditional bank cards, the digital payment service has possibly

opened a potential safe haven for hackers and cybercriminals to commit fraud. Due to the effortlessness of creating a new Apple Pay account, it is possible that it compromises the security of the service. With Apple Inc.'s dedication to the protection of user privacy, cybercriminals could become more difficult to track and identify.

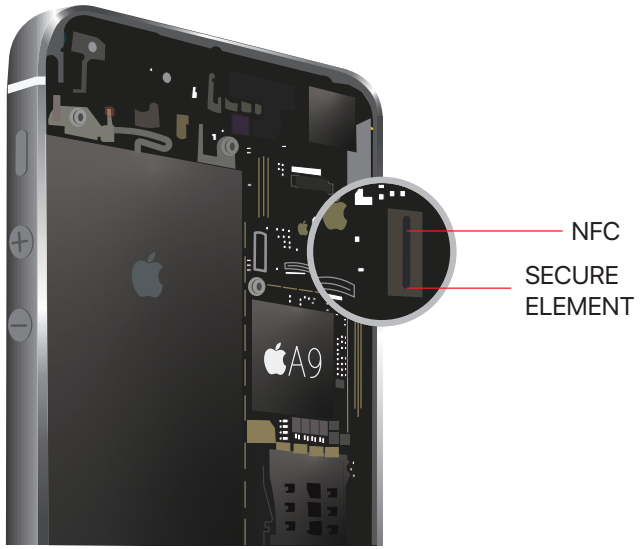
In order to combat the risk of cybercriminals using the service to their advantage, Apple has implemented a number of security measures aimed at preventing cybercriminals from accessing sensitive data and committing fraud. Apple Inc. has implemented security measures such as Rate Limiting, Tokenization, and Secure Element Chip to protect user data throughout the payment process.

Rate Limiting: This policy implemented by Apple strives to stop fraudsters from making forceful login attempts. This security feature includes login delays and blocking of suspicious attempts, discouraging hackers from making the effort. The user is notified of such attempts via email and/or text message.

Tokenization: Apple uses tokenization, a system that replaces a physical card with a coded token. This feature stops hackers in their tracks as these tokens make it harder to access or replicate original data. Although this system works to secure this information, it does not mean that Apple Wallet and Apple Pay are invincible and the apps are impossible to hack.

Secure Element Chip: This chip encrypts credit card numbers and other important data to ensure total privacy from the company itself as well as merchants and stores. Device account numbers and unique transaction codes are used to secure each payment from the service. These unique account numbers and transaction codes ensure your card CCV and other data are not shared with the merchant. The device account number is the only thing shared with the merchant, and also acts as a means of verification ensuring the payment is coming from the device with the unique account number.

With the information that has been presented, it is up to the user to decide if Apple Pay offers enough privacy and security for them.



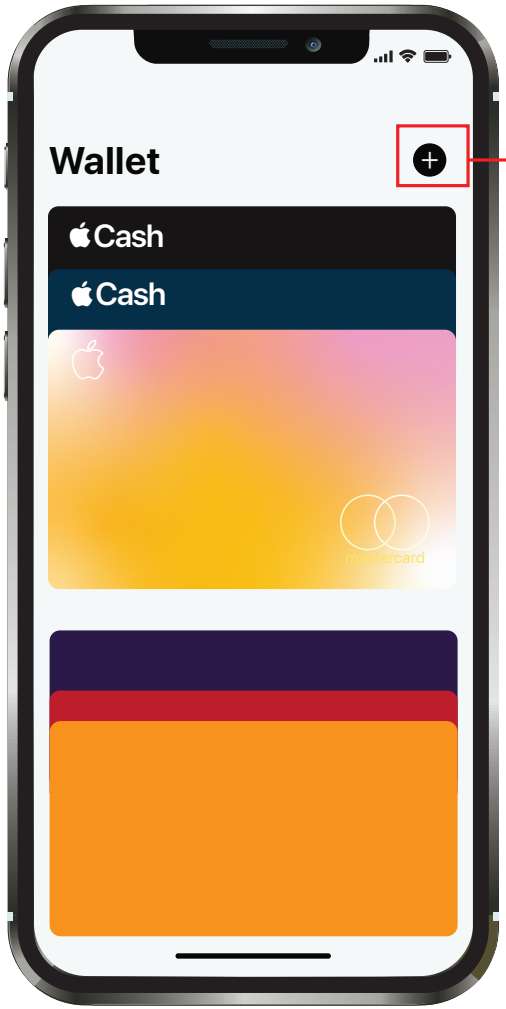
References:
Apple Pay. (2022). Apple (Australia). https://www.apple.com/au/apple-pay/

Liu, S. Q., & Mattila, A. S. (2019). Apple Pay: Coolness and embarrassment in the service encounter. International Journal of Hospitality Management, 78, 268–275. https://doi.org/10.1016/j.ijhm.2018.09.009

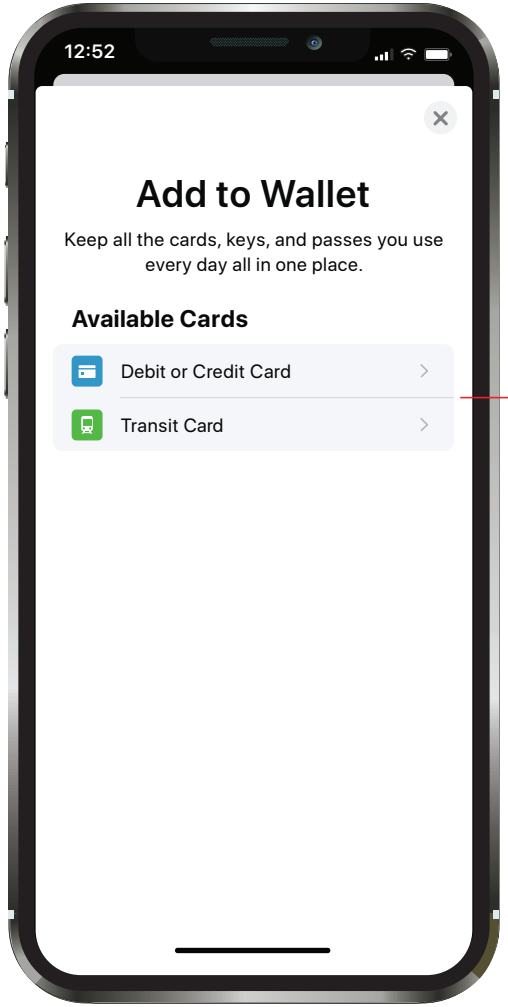
Julien, R., Jr. (2016). The cybersecurity aspects of Apple Pay (Order No. 10252123). Available from ProQuest Dissertations & Theses A&I; SciTech Premium Collection. (1867004335). http://ezproxy.uws.edu.au/login?url=https://www.proquest.com/dissertations-theses/cybersecurity-aspects-apple-pay/docview/1867004335/se-2

How Apple Pay keeps users' purchases protected. (2021). Apple Support. https://support.apple.com/en-au/guide/security/seccb53a35f0/web

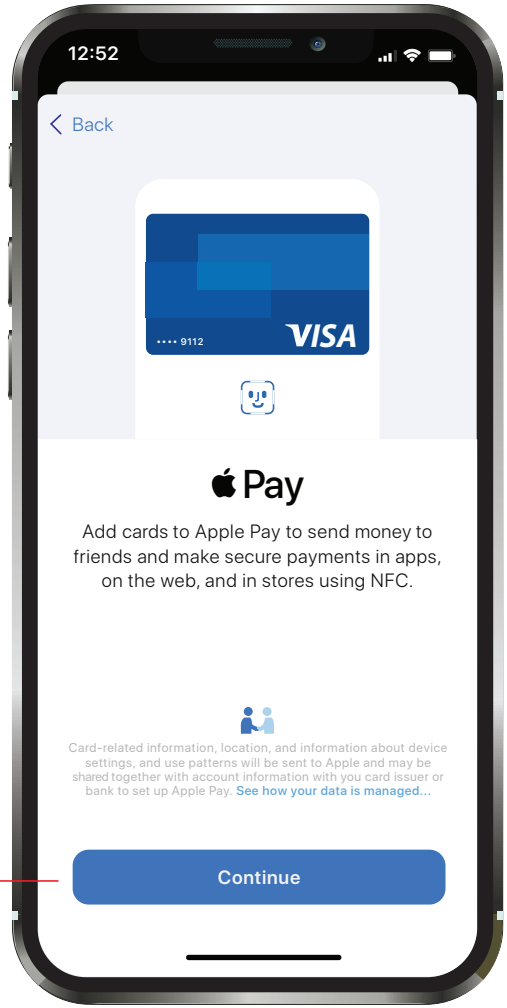
How to add a card to Apple Pay



Tap the '+' icon to add a card.



Select a card type.



Tap continue to add your card to Apple Pay.