Online Platforms and Market Power Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google

Questions for the Record from the Honorable Kelly Armstrong
Questions for Tim Cook, CEO, Apple, Inc.

1. Does Apple allow third-party digital wallet providers to transmit information via iPhone to Near Field Communication chips?

Apple designed Apple Pay to enable a wide array of third parties to offer services to their consumers on Apple devices. Apple currently works with banks, car manufacturers, transit operators, loyalty providers, sporting/entertainment venues, universities, building access providers, electric vehicle charging providers, and more to enable them to provide their customers with innovative uses of Near Field Communication ("NFC") technology.

Banks and payment card issuers (including third-party digital wallets that issue payment credentials like Square Cash and Affirm) can store payment credentials on the Secure Element of Apple devices and transmit information through the NFC chip. Apple developed the Wallet app as a user-interface to enable consumers to easily manage the different cards that have access to NFC on an Apple device. Apple currently has over 8,400 issuers participating in Apple Pay, with most of these issuers having multiple card portfolios. This means that there are tens of thousands of card portfolios that Apple Pay supports.

Apple does provide access to the NFC; however, such access is not unfettered. Apple does not provide uncontrolled access by third parties to the NFC chip in its devices because Apple seeks to ensure the highest level of security and provide the simplest, most consistent customer experience for making payments on its devices. Apple developed hardware and software components that are seamlessly integrated to achieve what it considers the highest security for payments. These include the Secure Element, the Secure Enclave, Wallet, the NFC chip, and Apple servers. Card issuers (including a digital wallet provider with its own payment credential) can store their payment credentials in the Secure Element, and these are transmitted from the Secure Element to the NFC terminal by the NFC chip. This architecture uses EMVCo specifications, allowing any card issuer to store its payment credentials on the Secure Element and use the NFC chip to transmit information to an NFC terminal.

Granting third parties uncontrolled access to the NFC chip for payments would undermine the security offered by this tightly integrated architecture, providing avenues and incentives for third parties to hack into Apple devices and the Secure Element. Indeed, Android devices, which provide open access to their NFC chip to third-party applications for payments, have been shown to be susceptible to third-party attacks that can compromise the customer's card information.[1]

The user experience would also be severely undermined by granting unrestricted access to third parties for payments would undermine the simplicity and ease of use of NFC by card issuers and other providers (such as car manufacturers, transit operators, loyalty providers, sporting/entertainment venues, universities, building access providers, electric vehicle charging providers, and more). NFC technology is designed such that the NFC chip is paired on a one-to-one basis with a particular application. In the case of Apple Pay, because the Apple Wallet app enables multiple payment cards from multiple issuers to be

[1] *See* Cammy Harbison, *New Android NFC Attack Could Steal Money From Credit Cards Anytime Your Phone Is Near*, Player.One (June 29, 2016), http://www.player.one/new-android-nfc-attack-could-steal-money-credit-cards-anytime-your-phone-near-445497; Larry Seltzer, *NFC Phone Hacking and Other Mobile Attacks*, Information Week (July 25, 2012), https://www.informationweek.com/wireless/nfc-phone-hacking-and-other-mobile-attacks/d/d-id/1105508.

stored within Wallet, consumers can easily choose between any of the cards (as well as cards from other non-payment providers such as loyalty/rewards cards) within Wallet at the point of sale, without needing to change any settings on the device or opening a particular app prior to making the NFC transaction. In cases where NFC is paired with a single app from one bank, the consumer would have to manually change the one-to-one NFC chip setting each time she wanted to use a different payment app. Apple believes that these unnecessary steps would significantly impact consumer adoption of mobile payments, undermine the growth of non-payment use cases for NFC, and undermine Apple's reputation for providing a seamless customer experience.

2. Does Apple allow third-party digital wallet providers to store information on iPhone Secure Elements?

The Secure Element and the NFC chip are deeply integrated in order to maximize the security and simplicity of the payment experience. As with Apple's response to Question 1, Apple does provide access to the Secure Element; however, such access is not unfettered. Apple does not provide third parties uncontrolled access to the Secure Element because granting third-party access to the Secure Element for payments would break this tightly integrated framework.

As also noted in our response to Question 1, the Apple Pay architecture uses the same tokenization framework (i.e, EMVCo) available to card issuers (including third-party digital wallet providers that issue a payment credential), allowing them to store their payment credentials on the Secure Element. The Secure Element is a tamper-resistant hardened module in which all payment credentials for Apple Pay are stored. The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes payment applets certified by the payment networks. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these payment applets using keys that are known only to the payment network and the payment applets' security domain. This data is stored within these payment applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the NFC chip over a dedicated hardware bus.

3. Does Apple allow third-party digital wallet providers to launch directly from iPhone "lock" screens? If not, please explain why.

Yes, a third-party digital wallet provider with its own payment credential can launch its payment credential directly from an iPhone lock screen using Apple technology and APIs that are provided by Apple to developers. The capability to present a payment credential directly from an iPhone lock screen requires the use of the NFC chip. As further set forth in our response to Question 1, Apple does not provide third parties with unfettered access to the NFC chip because doing so would undermine the security and simplicity of Apple Pay. The NFC can only be paired with one app. Apple pairs the NFC chip with the Wallet app.

The Wallet app can store myriad credentials such as credit cards, debit cards, merchant loyalty/rewards cards, public transit cards, university ID cards, and building access cards. The Wallet app gives users the ability to seamlessly use a variety of credentials without unlocking the iPhone. An Apple Pay user may purchase a cup of coffee, collect merchant reward points, get on the subway, and then enter her place of work without unlocking her iPhone. Giving third parties the ability to launch their payment credentials outside of Wallet and directly from the iPhone lock screen would compromise this seamless functionality.

4. If an Apple iPhone user sets up an iPhone, what prompts does the user receive to set up Apple Pay?

When a user initially sets up an iPhone using the Set Up Assistant, the user is given the option to set up Apple Pay if Apple Pay is enabled for the particular region. Users may elect to skip setting up Apple Pay at this stage.

5. If the iPhone user "skips" past Apple Pay enrollment during the initial setup of an iPhone, what other notifications or prompts would the user receive to set up Apple Pay?

If the user skips adding a card in an Apple Pay supported region, the iPhone will follow up at a later time by placing a "badge" in Settings. In Settings a "Finish Setting Up Your iPhone" option will be shown to the user, in which Apple Pay will be listed as an option for set-up completion.

6. Are there features the Apple Wallet enables for Apple Card or Apple Cash that are not enabled for other banks products on that platform?

The Wallet app is the only way users can interact with their Apple Card and Apple Cash accounts (as opposed to other credit and debit cards, for which users can go to the bank's mobile app, website, or physical branch to interact with the account). Thus, Wallet does provide the following features to Apple Card and Apple Cash that are not available to other cards:

- Apple Card and Apple Cash include historical transactions, organized by month, category, or merchant, and include a category or brand icon (other Apple Pay credentials show the last ten transactions);
- users can load funds from a debit card or bank account to their Apple Cash account;
- users can transfer funds from their Apple Cash account to their bank account;
- when possible, we present a location match in Maps for Apple Card transactions; and
- users can apply for Apple Card from the Wallet app (other Apple Pay credentials can be provisioned through Wallet, or through a Bank app).

7. Are there payment cards that Apple does not allow on Apple Wallet? If so, what are the reasons that a certain payment card would not be approved for Apple Wallet?

Apple's incentive is to have as many cards in Apple Pay as possible, as this enhances the overall consumer experience when using our products. Apple currently has over 8,400 issuers participating in Apple Pay, with each of these issuers having multiple card portfolios. This means that there are tens of thousands of card portfolios that Apple Pay supports.

Participation in Apple Pay requires that payment credential issuers agree to Apple's bi-lateral agreement for Apple Pay. Some issuers have chosen not to enter into our agreement, meaning that their cards are not eligible to participate in Apple Pay. There are also emerging types of payment products that differ from traditional credit or debit cards (e.g., cryptocurrency-backed cards, staged wallets, and short-term installments). Because our users expect Apple Pay to be secure, easy to use, and private, Apple may not approve these emerging payment products until Apple is comfortable with the safety, security, privacy, and ease of use of these new products.