APPLE PAIN

Apple shirks responsibility for fraud happening on Apple Pay

Watch your back. (Jordan Strauss/Invision for Disney Store/AP Images)

SHARE

WRITTEN BY

Alice Truong

To convince consumers to make purchases with their phones, Apple has touted the state-of-the-art security features of its mobile payment system Apple Pay. Those include tokenization (which provides merchants with one-time use tokens instead of credit card numbers), storage of sensitive information on the device's secure element, fingerprint verification, and encrypted data transfer.

But it appears Apple didn't account for one major vulnerability: social engineering, a term for the tactics hackers use to gain access to personal accounts by posing as the people whose identities they've stolen. This was the very weakness that led to last fall's high-profile iCloud breach, when hackers leaked nude photos of celebrities online. The company insisted then there wasn't "any breach in any of Apple's systems." While technically that may have been true—hackers gained access to accounts not through Apple's infrastructure but likely by using widely known details about celebrities to answer security questions—customers felt stung from the experience. (Apple turned on two-factor authentication, an additional security measure, for iCloud after the attack.)

As for Apple Pay, Cherian Abraham—a mobile payments advisor to banking and retail clients as well as Apple Pay competitor SimplyTapp—wrote in a blog post that he has noticed fraud happening at the earliest stages of getting set up on Apple Pay, when users add credit cards to the app.

The process to verify new credit cards varies from bank to bank and sometimes requires customers to phone call centers to answer additional security questions, which a hacker armed with stolen information can likely answer.

"Fraud rings are sophisticated and organized," Abraham tells Quartz. "On the flip side, [call centers] are expensive, labor intensive, hard to scale, and staffed by individuals that need to be incentivized and trained continually as fraud patterns shift. So it's no surprise that Apple, among other Silicon Valley firms has this as a blind spot."

In a statement provided to Quartz, the Cupertino, California-based company emphasized that Apple Pay is "extremely secure," and that the responsibility of verification lies with the banks themselves. "During setup Apple Pay requires banks to verify each and every card and the bank then determines and approves whether a card can be added to Apple Pay. Banks are always reviewing and improving their approval process, which varies by bank."

David Robertson, publisher of the research publication the Nilson Report, says these instances of Apple Pay fraud are indistinguishable from traditional credit card fraud. Criminals are putting stolen credit card data on Apple phones, and it's banks—not Apple—that are alerted to potential red flags. "It has nothing to do with the breach of the Apple system," he insists.

Abraham has said in a previous blog post that such issues aren't unique to Apple Pay and that "much of it translates to any other competitor—irrespective of origin, scale, intent, or patron saint." That said, he clearly thinks Apple can do more to protect consumers.

“Why do we think it’s acceptable for Apple to display disparity in the care it designs its products from the lack of such care displayed in securing the provisioning process?” Abraham asks. “If Apple can mandate [that] banks pay 15 basis points to Apple for every transaction, couldn’t they mandate a better provisioning process by banks?”

http://qz.com/355

KNOWN UNKNOWNS

The Apple Watch: What we don’t know