Mobile Wallet Fraud: This is Just the Beginning

21 June 2016 By: Al Pascual

Even though the early rush of Apple Pay fraud has been stemmed, mobile wallets remain a valuable target for fraudsters. In 2015, approximately 112,000 consumers reported being victims of mobile wallet-related account takeover and this is likely to get worse before it gets better, largely due to three major factors: EMV, the growing adoption of mobile wallets, and the technical skill of cybercriminals.

The presence of mobile wallets represents a unique aspect of the post-EMV experience in the U.S. As the U.S. continues to transition to EMV, point-of-sale fraud rings will see their supply of easily counterfeited cards and vulnerable merchants constrict. With a business model based around local knowledge of vulnerable (and lucrative) merchants supported by a geographically concentrated network of runners and fences, point-of-sale fraud rings will be slow to move to card-not-present fraud. The opportunity to enroll compromised card-not-present credentials onto a mobile wallet under their control and subsequently use that account in transactions at brick-and-mortar merchants is an opportunity for POS fraudsters to continue their operations unabated as the EMV transition progressively diminishes their opportunity to commit counterfeit card fraud.

Besides the use of compromised payment information, there will be a growing base of mobile wallet users for fraudsters to abuse (increasing from 53 million individuals in 2015 to just less than 90 million in 2019). As mobile wallets become more prevalent, one approach to account takeover that will become more prevalent is malware targeting mobile wallet users. Even wallets with robust application security to prevent direct data compromise should be considered vulnerable. Existing malware has already shown capabilities specifically tailored to attack mobile wallet users and largely manifests in three forms: overlay attacks, rogue apps, and message interception capabilities.

Ultimately, the goal of mobile wallet safeguards is not to provide a secure financial environment simply for security’s sake, but rather to provide a streamlined transaction experience backed by several imperceptible layers of security. FIs and issuers must act to manage the risk of mobile wallet fraud so as to encourage adoption, maintain accountholder loyalty, and prevent fraud loss. For more information on these and other threats facing mobile wallet providers and users, along with remediation steps see Javelin’s newest white paper sponsored by Early Warning, Securing the Mobile Wallet Experience. Mobile wallets are a target fraudsters haven’t been able to ignore, but their success is well within our collective power to deny.

*Photo courtesy of hystrygirlteacher.wordpress.com