Apple Pay’s pitch: Simpler is better. But some security experts disagree.

By Hayley Tsukayama and Sarah Halzack March 23, 2015, Washington Post

When Apple introduced its pay-by-smartphone feature last fall, the company touted the simplicity of the setup. All shoppers needed to do was wave their iPhones in front of a special scanner at the cash register — no need to fumble through pockets and purses for plastic cards or identification.

But a sharp rise in reports of fraudulent Apple Pay transactions is raising questions about the security of the first mobile payment system to find a measure of popular success. One payments analyst, Cherian Abraham, estimated that as many as 6 percent of Apple Pay purchases are completed with stolen credit cards, or 60 times the rate of the old-fashioned plastic swipe.

The problem is that Apple Pay may be too simple to set up, security analysts said. Fraudsters have been loading stolen cards onto iPhones to buy things at stores. As it turns out, it might have been better if Apple Pay required users to do more to prove their identities when they sign up for the service, these experts said.

The balance between security and ease of use has long bedeviled technologists, especially those pushing for a new payment system to replace the plastic cards that are highly vulnerable to thieves. That need has grown more urgent as credit card hacks — such as those that have afflicted Target and Home Depot in recent years — have risen in scope and frequency.

Mobile payments offer a potential solution. They are considered much harder to hack than traditional payment systems. And they avoid the swipe — a critical advancement since a lot of credit card numbers are stolen by fake card readers. But consumers, banks and retailers have been slow to embrace the technology, partly because of its complexity.

Apple's Kevin Lynch discusses the Apple Pay feature of the new Apple Watch on March 9 in San Francisco. (Eric Risberg/AP)

Launched in October, Apple Pay was billed as simple to use, and the universe of stores and banks accepting the service has been growing steadily over the past few months. Apple boasts that Apple Pay is now accepted at hundreds of thousands of store locations. Bank of America said customers added 1.1 million of its credit and debit cards to Apple devices in the first two months of Apple Pay. JPMorgan Chase cited a similar figure.

But reports of fraud are now giving retailers and banks some pause.

“The issuers were probably so eager to be involved that they kind of forgot best practices and sidestepped some procedures they normally would’ve had [in order] to accept Apple Pay,” said Michelle Evans, senior analyst for consumer finance at market research firm Euromonitor.

The essential problem with Apple Pay is the setup, security analysts said. Users need only to open the app on their smartphones and enter a credit card number, the expiration date, and the three- or four-digit verification code. Apple rates the consumers as safe or risky, based on what it knows about their buying habits at its stores or on iTunes. Apple's rating and the credit card information are sent to the card issuer, which decides whether or not to reject a user.

In most cases, the decisions by Apple and the card issuers occur within a few seconds.

Compared with traditional credit cards, Apple Pay does not do enough to weed out bad consumers from good ones, security analysts said. That has made it easy for the unscrupulous to trick banks and other financial firms into approving stolen cards, they said.

Criminals can buy credit card numbers and their verification codes by the bundle — and cheaply — online, said cybersecurity blogger Brian Krebs. They then plug those numbers into unlocked Apple devices that are hard to trace.

"A lot of the fraud people [at banks] were annoyed that they rushed into it without thinking it through," said Avivah Litan, a security analyst for Gartner. "You can't count on iTunes at all — they should use their own processes and their own records."

Fraudulent purchases at brick-and-mortar stores are covered by the card issuers and banks. And Apple said it is up to them to increase scrutiny of Apple Pay applicants.

"Apple Pay is designed to be extremely secure and protect a user's personal information," Apple said in a statement sent to The Washington Post. "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."

But if card issuers created a much more involved application process for Apple Pay — or instituted a host of different procedures — that would almost certainly slow down sign-ups or discourage consumers altogether.

"It's to the benefit of consumers to have a consistent process," said Jason Malo, CEB TowerGroup's cybersecurity specialist.

Anxiety over Apple Pay could grow as Apple and other companies offering mobile payment services set their sights on online purchases, said Amitabh Saxena, the founder of the digital-payment consulting firm Digital Disruptions. When fraud occurs online, liability defaults to the merchant rather than to the banks.

"I think there is a legitimate concern for online merchants," he said. "They'll want to know how many bad cards are in the system, and that might give them a little more pause."

But others say that this fraud, as it stands, is more an early growing pain than a major problem for Apple Pay or other mobile payment systems down the line.

“This is more of an implementation issue than it is with the technology itself,” said Krebs, the security blogger. No matter how you slice it, he said, Apple’s technical strategy is a “sound one and is a much better approach than relying on these insecure stripes” on plastic cards.

And while Apple may take a hit to its reputation while headlines about fraud fly, other security analysts said the company should be able to weather it.

“Criminals will always follow the money, and payment-card fraud will always be an issue,” said Darren Hayes, an assistant professor at Pace University who studies cybersecurity. “Right now Apple Pay has a very large target on its back.”