Source: October 8-October 14, 2012 Bloomberg Businessweek
Article by Olga Kharif

Cyber Security
A New Frontier For Criminals

• The nascent mobile-payments industry is vulnerable to fraud
• "Potentially, it could be billions of dollars a year in losses"

Eddie Lee has created an app that lets him steal a credit card by simply waving his Samsung Nexus S phone over a leather wallet tucked into the back pocket of a stranger's jeans. He can then walk into a nearby store and tap his phone at a cash register to charge a sandwich, a coffee—or even a flat-screen TV—to the card.

Fortunately, Lee's not a thief but a security expert paid to find vulnerabilities in wireless payment technologies. By 2015, consumers worldwide will buy $1.3 trillion worth of goods with their phones and tablets—four times the amount today, forecasts Juniper Research. The expectation is that fraud will account for 1.5 percent of all mobile payment transactions in four to five years, says Avivah Litan, an analyst at tech researcher Gartner. "There's huge concern," says Mike Urban, director of financial crime solutions at Fiserv, a Brookfield (Wis.)-based technology company that caters to banks and mortgage lenders. "Potentially, it could be billions of dollars a year in losses."

Only 12 percent of Americans have tried mobile payments, according to a March report from the Federal Reserve. To rev up adoption of their own platforms, companies such as PayPal, Google, and Square are under "pressure to remove the controls, "thereby improving ease of use, Litan says. For criminals, that means easier access.

Nearly 70 percent of mobile phones aren't password protected, according to Sophos, a mobile security vendor. Parents allow children to play with their phones without considering that they may download some bit of malware, says Shirley Inscoe, a senior analyst at Aite Group: "They don't realize the risk they may entail given the data stored on their mobile device."

Criminals can access a mobile wallet by stealing the handset or by tricking its owner into downloading a piece of malicious code. Malware attacks on U.S. smartphones have risen 18 percent since 2011 and now add up to 15.3 percent of the world total, says mobile security vendor NQ Mobile.

Sometimes the weak link is not the phone but accessories designed for it. Using an earlier generation of attachments sold by Square, which allow iPhones to accept credit- and debit-card payments, security experts were able to show how criminals could set up merchant accounts and accept payments using stolen credit-card numbers. "The technology is so vulnerable and so easy to defeat," says Adam Laurie, a director at security researcher Aperture Labs. Square is phasing out the older attachments and has added encryption to

ward against this type of fraud. The company would not comment for this story.

Banks and mobile-payment providers are scrambling to build—or buy—better defenses. "There's lots of investment into solving this problem," says Fiserv's Urban. Guardian Analytics, a Silicon Valley startup, has developed software for banks that analyzes a consumer's past transaction behavior—whether she made small or large purchases and how often—to determine if her phone has been hijacked. There are also security tools that can triangulate a mobile user's location and verify that she is using her usual wireless device. PayPal has identified more than 1,000 variables that can help the company determine the authenticity of a transaction, says Michael Barrett, its chief information security officer. "We tend to use a lot of contextual security," he says. "And we are always evolving those controls."

Nitesh Saxena, an assistant professor of computer Science at the University of Alabama at Birmingham, has taken the notion of contextual security a step further. In a research paper, he proposes having a user's phone and a store's scanner each record the audio of background noises during a mobile-payment transaction. The two recordings would then be matched up on some distant server. "The good thing about the phones is, they have all the computing power, the sensors, and you can use them," Saxena says. The goal is to prevent so-called relay attacks, in which a criminal scans a credit card with a phone and then passes the card number wirelessly to an accomplice overseas, who uses it to make purchases with his mobile device.

Getting the technology right is simpler than figuring out how to divide responsibility for fraud detection and apportion losses when fraud has taken place. A typical transaction involves a wireless carrier, a payment service, and a bank. "Depending on how you paid for the thing, it might not be clear who's holding the responsibility," says Suzanne Martindale, staff attorney at Consumers Union, which publishes *Consumer Reports.* "In many cases, unfortunately, it's the consumer left holding the bag, because they get frustrated with the runaround."

Once the wrinkles are ironed out, though, mobile payments could become more secure than checks or card-based payments. "If your phone is lost or stolen, with a single call, you can remotely disable the wallet," says Jaymee Johnson, head of marketing at Isis, a mobile-payment venture of AT&T, Verizon Wireless, and T-Mobile USA that is expected to launch service this fall. For anyone who has had to spend an afternoon canceling credit cards after being pickpocketed, that sounds appealing.

The bottom line

With mobile transactions set to hit $1.3 trillion worldwide by 2015, banks and payment services are scrambling to plug security gaps.