Mobile and Online Risk Control May Need To Go Their Separate Ways

May 24, 2017

By Jim Daly
@DTPaymentNews

With e-commerce taking an ever-greater share of total retail sales and mobile commerce accounting for an ever-greater share of e-commerce, merchants need to start treating m-commerce fraud control as more than a subset of online fraud control.

That was the word Tuesday from Susan Pandy, the director of payment strategies at the Federal Reserve Bank of Boston.

“Card-not-present merchants that are doing mobile have to treat mobile as a new channel,” said Pandy, a speaker at the CNP Expo conference in Orlando, Fla. “You can’t just say we’re going to take the tools we use for our e-commerce platform and do that for mobile, because mobile is different.”

While some observers question whether smart phones and tablets are truly secure enough for payments, that hasn’t stopped consumers and merchants from embracing them. Mobile-commerce’s share of e-commerce reached 20% in 2016’s fourth quarter, double its level in 2012, said Pandy, citing figures from the U.S. Census Bureau and Internet research firm comScore Inc. ComScore estimates **m-commerce sales** reached $22.7 billion in the fourth quarter, up 45% from a year earlier. Meanwhile, e-commerce’s share of total retail sales hit 8.5% in 2017’s first quarter.

Such growth justifies separate treatment of mobile devices from desktop and laptop computers for payment-security purposes, according to Pandy. Certainly, mobile devices can be compromised through weak apps, and rooting or “jailbreaking,” she noted. But their attributes, including geo-location and the ability to use biometrics and other authentication technologies, mean they can be configured to provide strong security, she said.

“So the big question is ... is mobile riskier than e-commerce?” she asked, noting that she was speaking for herself and not the Fed. While both channels have their pros and cons, “mobile has the potential to be more secure,” she said. But before mobile devices can come into their own security-wise, merchants, processors and others involved in m-commerce need to beef up authentication, according to Pandy.

“Authentication is still a challenge across the industry,” she said. “There’s a need to move more toward multi-factor authentication. It’s being able to leverage that rich data that’s on the device to enhance your authentication.”

Better authentication also would include wider use of biometrics, which already is being used with several mobile wallets as well as PayPal, and finally moving beyond user names and passwords.

“We all know that user name and password alone isn’t sufficient anymore,” Pandy said. “You have to have multiple layers and multiple factors of authentication, that’s just the nature of the business now.”

In addition, data encryption needs greater adoption, she said. “We’re seeing inconsistent encryption across the industry.”

But even before they can consider better authentication and other security protocols, merchants need to get a better handle on the extent of m-commerce fraud. Only 27% of merchants track mobile fraud, said Pandy, citing data from Visa Inc.’s CyberSource subsidiary. According to CyberSource, the overall fraud loss rate for online stores is 0.8% compared with 0.5% apiece for m-commerce and telephone orders.

The Boston Fed and the Federal Reserve Bank of Atlanta sponsor the **Mobile Payments Industry Workgroup**, a group of 40-plus merchants, processors, tech providers and others that researches risk-control and other issues of concern to the m-commerce industry.

Another speaker at the session, Roberto Cárdenas, digital payments consultant at Columbus, Ga.-based processor Total System Services Inc. (TSYS), cited predictions from United-Kingdom-based Juniper Research that 2 billion mobile-payment transactions will be authenticated this year with biometrics, up from 600 million in 2016.

With growth like that, “security cannot be an afterthought in our business,” said Cárdenas.