One Payment App Uses Often-Called Friends To Authenticate. (Privacy? What’s That?)

Written by Evan Schuman
February 16th, 2012

A Seattle mobile payment firm is pushing for phone purchases to be done with no PIN, arguing that with this young a market, consumer convenience needs to trump security. Given its focus on authenticating the phone instead of the customer, it’s had to get creative and might be pushing the privacy envelope. It examines the five most frequently called friends, for example, along with a list of installed applications.

Whether or not its methods go too far, it’s in good company in the mobile early-stage convenience versus security argument, with both PayPal—and its phone-less and card-less purchases at Home Depot—and Visa, which is pushing PIN-less EMV transactions while MasterCard is taking the more secure and less convenient pro-PIN EMV position.

The efforts of the Seattle firm—which had been known as Billing Revolution but is now called Buck—are different based on the mobile platform involved. That’s true for several reasons, but one of them is that Apple on Wednesday (Feb. 15) banned Apple apps from engaging in exactly that type of conduct.

"Apps that collect or transmit a user's contact data without their prior permission are in violation of our guidelines. We’re working to make this even better for our customers. And as we have done with location services, any app wishing to access contact data will require explicit user approval in a future software release," said the statement, which was issued after requests from a U.S. congressional committee.

The question of explicit user approval, though, crops up in the Buck efforts, because the firm has received that approval from its customers. That said, it wasn't an opt-in where customers could choose to allow that data exchange via a choice in an Options area. The opt-in was part of the mandatory terms and conditions of the app. In other words, if users don't agree, they are prevented from downloading the app and certainly from using the app. Either way, Buck will not be using that personal information for Apple phones and will instead use it solely for Android phones, said Buck CEO Andy Kleitsch.

The company is relying on more than device attributes for phone authentication, including operating system version, an app cookie, the SD card, the nature of a Wi-Fi connection, carrier, CPU performance and other items, said Buck CTO Randy de los Reyes. When a customer changes elements of those attributes—perhaps by upgrading the OS or deleting no longer needed applications—the system guesses whether those changes make sense. A customer upgrading the mobile OS, for example, would not be a fraud trigger nearly as much as that customer downgrading the mobile OS, Kleitsch said. "It’s all about weighing the attributes," de los Reyes said.
If the Buck system suspects that the phone trying to make the purchase is not the phone that signed up for the service, it can prompt for secondary authentication, such as by asking for a CVV or a ZIP Code, de los Reyes said. Each retailer can also set its own security triggers—such as a number of purchases or a dollar amount, within a set timeframe—and Buck has its own fraud triggers on top of those. "It watches for an excessive number of transactions. If all of a sudden we see 10 transactions all within 30 minutes," the system will either ask for more information, shut down the use of the payment card on file or even shut down the entire application, de los Reyes said.

With all of those mechanisms in place, Kleitsch argues, the single-click payment from the Buck app is reasonably secure. Indeed, it's optimally secure given the nascent nature of the mobile payment market and the need to make the transactions as effortless as possible for consumers. Slow down the process too much—such as by insisting on a PIN—and risk consumers avoiding the mobile transactions entirely. Once consumers are used to and comfortable with mobile transactions, additional security can be added.

The only problem: Who will pay the cost of fraudulent transactions during the initial phase? The most likely hole is when consumers using this app misplace their phones or have those phones stolen. Given that the phone will be authenticated, some bad transactions will proceed before the various excessive-use fraud triggers (or the user disables the phone and cancels the associated payment cards) kick in and end the thefts.

As those decisions are debated among the brands, issuers and processors, apps such as those from Buck are going to look attractive from a market growth perspective but less so from a risk perspective. And yes, the chances are that retailers will end up footing the bill for the experimentation—and pocketing the profits if it all works.