Cardless ATM Experiment New Territory for Crooks

Robert Capps, vice president of Business Development for NuData Security

One thing about the security industry, there is always something new to worry about. This January Brian Krebs reported on a new vector in ATM fraud whereby, thanks to a new app, customers can withdraw funds from an ATM armed only with valid banking credentials, and a smartphone. What could go wrong with that?

It appears that some banks have been experimenting with cardless ATM pilot programs whereby the mobile application generates a 7-digit code, or in some cases a QR code, that is read by the ATM that will then dispense the amount requested. In what seems, from a security perspective, to be a step backward, access to the original ATM card or knowledge of the ATM card PIN has been omitted from these systems. Unsurprisingly, there have been claims against the banks for account takeover attacks and several fraud schemes stemming from the program.

ATMs have long been the poster child for how multi-factor authentication can be adopted by a mass market consumer audience, reliably performing the identity verification task by requiring something you have (i.e., the ATM card) and pairing it with something you know – the 4-digit card PIN. ATM fraud was mostly kept in check by this constraint because the physical card was a necessary part of the process. To steal from the ATM, you'd either have to obtain the legitimate card from the consumer, convince the bank to send a new card to the fraudster, or capture the information from the magnetic strip of an authentic bank card and re-encode this data onto a counterfeit card.

Yet, with the advent of cardless ATMs we've entered a brave new world of ATM security where the mere knowledge of the consumer's username and password enables a fraudster to withdraw large sums of money from any cardless-enabled ATM via the mobile app. By offering this capability, banks have significantly increased the risk exposure to banking customers, while making theft of deposited funds extremely convenient for the fraudster. Introducing technologies to assist consumers in accessing their accounts is a positive step for customer satisfaction. Banks are heavily dependent on customer loyalty and are always looking for new ways to improve the customer experience without adding friction, but doing so at the expense of account security is mostly counterproductive and dangerous. It's incumbent on all financial institutions to balance convenience with appropriate security measures that protect customers appropriately.

Devices can be stolen, or compromised via rooting or malware that access banking apps in ways that would make it very easy for fraudsters cash-out associated bank accounts without requiring access to a legitimate payment card. Customers are largely blameless in these attacks. The usernames and passwords are often compromised from previous breaches and used without their knowledge to access their account. Unfortunately, because consumers can be held responsible for losses stemming from third-party theft (unlike credit-card theft) account takeover attacks are very impactful for customers.

Technologies are available in the marketplace that can be deployed to protect customers and the bank because these systems differentiate between the legitimate consumer and an illegitimate fraudster, even when the bad guys come armed with stolen valid credentials. And, these solutions can do this without burdening the real user with more hurdles or storing any PII data. With the application of behavioral analytics and passive biometrics to this problem, these risks can be largely mitigated and safety returned to the ATM channel by ensuring that the good user is accessing the account.

About the author:
Robert Capps is the vice president of Business Development for NuData Security. He is a recognized technologist, thought leader and advisor with more than 20 years of experience in the design, management and protection of complex information systems – leveraging people, process and technology to counter cyber risks.