mobile payments today
technology, trends & insights

The role of mobile smartphones in identity verification

By Mike Lemanski, principal technical writer - security, Samsung Research America

The vast majority of consumers own a mobile device of some kind. The share of Americans that own smartphones is 77%, up from just 35% in Pew Research Center’s first survey of smartphone ownership conducted in 2011. Consumers today expect the "anywhere, anytime" convenience of using those devices for everything from shopping to paying bills and opening new accounts. Yet, while consumers have gravitated to mobile, so has fraud.

Mobile devices are direct pathways to the type of personal information that fraudsters want to compromise. As mobile fraud continues to rise, businesses must consider the risks presented by mobile malware that can steal personal information and intercept text messages right off a consumer’s smartphone. And with consumer preference for friction-less experiences, businesses must also look at fraud detection and identity verification in a different light, taking into consideration ways to protect consumer data while also delivering a positive customer experience.

Mobile Fraud Tactics

The list of ways that fraudsters target mobile devices is long and always evolving, but some of the more common include:

- Recycling phone numbers: activating phones with new numbers with the aim of receiving a recycled number that is currently attached to a tenured victim's account.
- Intercepting SMS: intercepting inbound SMS communication, such as two-factor authentication messages relaying one-time passcodes (OTP).
- SIM cloning: copying SIM values from a victim so fraudsters can impersonate a subscriber on the network and obtain all incoming communication.
- SIM swapping: social engineering the mobile network operator call center with stolen personally identifiable information (PII) in order to deactivate an existing user's SIM and activate a device in the fraudster's possession to hijack mobile communication.

Mobile Change Events

Within the last 12 months, 47% of consumers (or an estimated 100.6 million mobile phone owners) experienced at least one of type of mobile change event. These mobile change events, which include porting a number or changing carriers, make it easier for fraudsters to compromise consumer data and more challenging for businesses to identify and authenticate digital device identities. This is evidenced by the increase in mobile phone account takeovers — which help criminals gain access to financial accounts when consumers utilize two-factor authentication involving a text message or token app — which doubled in 2017 according to an Identity Fraud Study published by Javelin.

Multi-layered Approach

The opportunity that comes with mobile far outweighs the risk. Mobile identity verification can elevate customer trust, facilitate onboarding and engagement, increase business identity assurance and deter fraud — if done properly. But how?

While there are multiple ways to authenticate identity via a mobile device, no one method is a silver bullet. However, there is a starting point from which other methods can be layered on — mobile network operators (MNOs). Sourcing real-time device and user information directly from MNOs can help businesses create a unique mobile identifier that persists through mobile change events. This means that a customer's device, and by default that customer, is automatically authenticated behind the scenes and granted immediate access. This persistent mobile identifier is effective across devices and networks, so it neutralizes password burdens and instantly builds trust in the business-customer relationship.

When other methods are layered on, such as the ability of a smartphone to take pictures or scan an ID, the mobile device becomes the ultimate identity verification mechanism. By starting with MNO data to verify a mobile identity and building on other methods as needed, legitimate customers are quickly given the green light and additional steps and friction can be applied only when needed.

The ever-increasing number of consumers with a preference for mobile, along with growth of customer-not-present fraud, have created a perfect storm and are paving the way for a new, dynamic approach to authenticating mobile identities. At the end of the day, we have to look at mobile in a different light. The layers of identity verification businesses use should make it difficult for fraudsters to get in, but simple for customers to do business with them. The companies that have been successful at lowering the effort required by customers to access services and solve problems are enjoying a distinct competitive advantage with the ability to attract new customers and retain existing ones.

Cover photo: iStock

Topics: Handsets / Devices, **Security**