A Boku white paper

Preventing Account Takeover: is there a better way?

boku

Account takeover, in which customer credentials are stolen or faked by criminals to gain access to customer accounts, is becoming a significant and complex challenge for digitally-enabled businesses everywhere.

From financial services and e-wallets to airlines, lodging and healthcare, account takeover is one of the fastest-growing forms of commercial fraud on the planet.

Adam Lee, Chief Product Officer at Boku, reviews current efforts to combat account takeover, including One-Time Passcodes (OTP) via SMS – and suggests a better way to fight account takeover fraud.

Account Takeover: An Escalating Issue

A recent study from Javelin Research estimates that account takeovers cost U.S. businesses around the world at least $5.1 billion in 2017 – a figure equivalent to the education budget of a small European country. Now factor in estimates from NuData Security and Javelin that account takeover grew by 164% in 2018 and 65% in the first three quarters of 2019, and both the scale – and speed of growth – of this kind of fraud becomes clear. Account takeover is a major issue for any business that is looking to protect its customers' data in the digital environment. And these days, that means pretty much everyone.

Account takeover can occur when criminals purchase stolen account information over the dark net, or through faked extensions to customers' web browsers, which harvest log-in credentials and store them for criminal use. By far the largest growth area for account takeover by criminals is in the mobile internet environment, where this form of fraud is estimated to have risen by 80 percent in 2019 alone. According to data compiled by RSA Security, 70 percent of fraudulent transactions in 2019 originated on mobile devices.

Digital Living: An Opportunity for Fraud

This "growth opportunity" for fraudsters comes at a time of transformation in the way we live. Fraud is migrating to the online environment in lock-step with growth in our use of digital devices to access and pay for services. For instance, more than half of Europeans under the age of 35 prefer to shop online using their mobile device, a figure that drops only slightly to 43 percent of those aged 36-55. Worldwide, FIS Global predicts that m-commerce will grow at 19 percent on average over the next five years, to reach US$2.29tn by 2022, with online commerce overall predicted to grow at 7 percent a year globally, reaching US$4.6 trillion. By contrast, physical sales are set to grow at less than 5 percent a year over the same period. The takeaway here is that business is moving online – and fraud is following, with account takeover at the forefront of this growth in fraud.

In healthcare, providers are increasingly using cell phones to go beyond customer communication and into improved diagnostics using biometric factors stored on devices, as well as transmitting medical imagery and providing customers with access to sensitive medical test information. Compromise in these areas could have serious and upsetting consequences for patients that go deeper than financial losses and cause customer confidence to diminish rapidly.

In addition to customers losing confidence, the financial impact for companies can also be dramatic: in Canada, some 29,000 individuals reported identity theft incidents relating to online and mobile accounts with retailers such as Costco and Target. These incidents are estimated to have cost more than C$12 million – and now account for 75 percent of reported financial fraud in Canada.

The Response to Date

So far, solutions proposed to counter account takeover have varied from sector to sector. Some sectors, such as financial services, have attempted to strengthen fraud detection in transaction processing through the use of Artificial Intelligence and Machine Learning techniques. Though promising, such techniques remain in their infancy. As a result, a lot of companies have relied on mandating changes to consumer behaviour through multi-factor authentication to help them fight account takeover and other fraud types.

While multi-factor authentication may be more effective than a single factor, not all two-factor authentication systems are created equal. Many recent solutions have evolved from a desktop computer environment and involve the introduction of various elements of user friction, such as the entry of one-time passcodes (OTPs). These passcodes are typically delivered via SMS for input on the merchant website or app. However, as more websites and apps come to depend on SMS OTP to secure their operations, there are growing concerns about the vulnerability of this form of authentication to compromise and fraud. The proliferation of SMS OTP as a confirmatory factor risks creating a false sense of security in consumers, as we explain below.

One-Time Passcodes via SMS: less security, more friction

OTPs can be stolen, either directly from the victim via social engineering or malware or indirectly through a mobile account takeover attack, in which the victim's mobile network operator (MNO) is tricked into porting the victim's mobile number to the fraudster's device thereby allowing criminals to intercept all communications intended for the victim.

Boku is one of the only firms in the world to have direct experience of linking SMS OTP with account activities such as identity verification and payments. Based on our experiences at Boku, over 70 percent of SMS OTP compromises can be attributed to the theft of OTPs through social engineering. As SMS OTP continues to be linked to a wider array of account activities worldwide, we anticipate dramatic increases in account takeover fraud using hacked SMS OTPs to gain entry to accounts. Furthermore, we believe that the use of AI by fraudsters will see the velocity of OTP hacking increase in the next few years.

It seems some regulators may share user concerns with the use of OTPs, though more from the perspective of security than convenience. At the time of writing, local regulators in France and Germany are discussing the status of OTP use over SMS as a means of user authentication. The regulators' concerns appear to be well-founded, and relate to the rapid rise in fraud attacks linked specifically to SMS OTP as a confirmatory factor in the authentication process. Despite these regulatory concerns, new regulations mandating secondary authentication are about to drive a material increase in the use of SMS OTP to validate possession as the secondary factor.

Another problem with SMS OTPs is that consumers don't like them, believing they create unwanted friction. While users may put up with one form of authentication friction (such as a traditional login password), it seems two forms might be too much. A mid-2019 study from Gocardless based on 4,000 interviews with consumers from major European markets found that 44 percent of UK online shoppers had abandoned an order because of complex or lengthy security processes, while 48 percent had done so in Germany.

Nearly half (45 percent) of UK digital consumers said they would be frustrated with new security processes during online checkout and a fifth (23 percent) would shop less if new security measures were introduced. Given such levels of consumer negativity around SMS OTP and other friction-generating methods, some companies have sought to limit their use of OTPs delivered by SMS for fear of spoiling the user experience. However, unless those companies can find a viable alternative, they will be forced to accept a higher level of fraud – along with the higher costs associated with that fraud.

If not SMS OTP, then what?

Many companies have begun evaluating in-app push notifications as an alternative to SMS OTP. These push notifications allow users to confirm possession by accepting an in-app request delivered to their device. However, push notifications require each and every consumer to download,

PNV improves the consumer experience and reduces fraud risk.

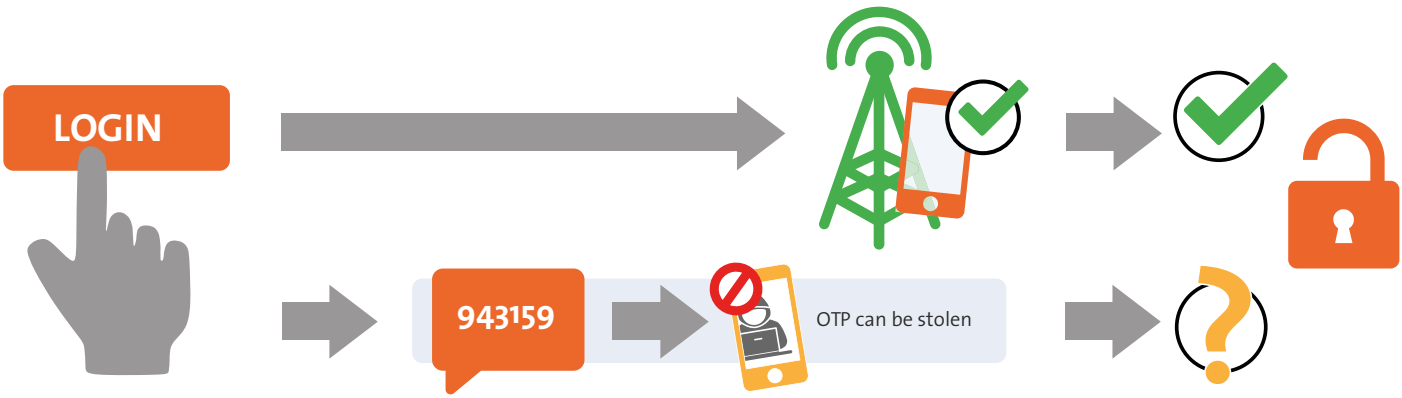
install, and properly set up their mobile app for this kind of authentication which inevitably complicates the user experience. Furthermore, mobile apps are notoriously susceptible to compromise: Positive Technologies, Inc., estimates that between one third and a half of Android and iOS apps include high-risk security vulnerabilities.

Instead of looking to apps, we believe the most promising alternative to OTPs is a next-generation service developed by MNOs that validates a user's mobile phone number and SIM card through a real-time query of the mobile network. We call this silent phone number verification, or PNV for short. Because this service does not utilise an OTP, the risk of passcode theft is eliminated.

The low friction experience on the mobile device makes it much easier to add PNV as a secondary authentication because the user hardly notices the service as it happens silently in the background. Even better, PNV works in both mobile app and web environments. This service does not require a separate app installation.

Conclusion

As long as businesses rely on SMS OTP, account takeovers will continue to terrorize victims of social engineering. In response, Boku has partnered with MNOs globally to integrate their PNV technology into an SMS OTP alternative: Boku Authenticate. With a single connection, Boku Authenticate gives businesses the ability to silently verify a mobile number across a network of mobile operators, resulting in zero friction to the consumer while eliminating OTP hijacking risks. These advantages make Boku Authenticate the single best alternative to SMS OTP.



To find out more about how Boku's solutions reduce friction in user authentication and help lower fraud risk, get in touch with us at www.boku.com

www.boku.com

boku