Quick Q&A

ON MOBILE PHONE TAKEOVER RISK

with DON SMITH

Product manager of global fraud solutions at Neustar, a TransUnion company

Knowledge-based authentication, such as the name of a customer's third-grade teacher, is not the best way for financial services organizations to thwart a cybercriminal from defrauding their customers.

But striking a delicate balance between security measures and a frictionless digital customer experience can be done, says Don Smith, product manager of global fraud solutions at Neustar, a market leader in marketing, fraud and communications solutions. This can be accomplished leveraging identity, device, mobile network operator data as well as biometric data.

Smith says the key to mitigating phone fraud risk is to get consumers engaged in the use of best-in-class authentication technologies like possession of a device, such as a phone, or biometrics that help can distinguish a legitimate customer from someone who's not. For device-based authentication, we have to ensure that the individual interacting with us is the actual owner of the phone, that the phone is legitimate and that the actual customer is in possession of the phone before we can trust it enough to send a one-time passcode (OTP) to the phone.

---

1 What is the basic case for banks hardening their defenses against phone takeover?

With fraudsters becoming more adept at taking possession of customers' phones, it behooves the banks to use technology to protect customers and themselves. This can save banks money while protecting against account takeover through automation, by doing it earlier and by making it more difficult for fraudsters. If the technologies are invisible and easy to adopt, they can take a lot of friction out of the experience. It's a win-win when banks improve security and lower their costs.

---

2 What are some of the inherent risks to multifactor authentication (MFA)?

MFA is an authentication system that requires more than one distinct authentication factor for successful authentication. Possession of a phone with a number tied to an account, plus a username and password, is the most common way to achieve MFA. A fraudster gaining access or controlling the phone is probably the biggest risk factor. It can be by taking over ownership of a phone and leveraging that as their own to bypass MFA. Or it could be taking over other attributes, such as an email of a customer to obtain information that can be used to answer knowledge-based authentication questions.

---

3 Authentication is increasingly being done through a bank's mobile app. How is that impacting fraudsters?

Generally, we think customers using a bank's mobile app poses less fraud risk. That's because the bank has access to more granular data than it would have if the user was coming from a website. From a behavioral perspective, the bank has more customer attributes it can look at via their mobile app such as attributes of the device itself.

4 Are regulators addressing this risk?

Not from what we can see. By and large, regulations are being left up to the individual organizations—there are regulations within the banks and within the carriers. The Federal Financial Institutions Examination Council (FFIEC) has guidelines encouraging multifactor authentication as a general rule, but it's only a guideline. The Federal Communications Commission has established call authentication standard called STIR/SHAKEN, which are acronyms for the Secure Telephone Identity Revisited and Signature-based Handling of Asserted Information Using Tokens standards. They provide a secure way to validate caller identity and stop illegal caller ID spoofing. The National Institute of Standards and Technology (NIST) is expected to release new identity guidelines soon and this should include more emphasis on MFA approaches.

"If the technologies are invisible and easy to adopt, they can take a lot of friction out of the experience. It's a win-win when banks improve security and lower their costs."

5 How can banks apply these same concepts in a call center?

These same methods can be used to erect barriers for risky callers while they're still in the interactive voice response (IVR) and have yet to reach an agent. As soon as we identify the number that a customer is calling from, we can apply the same concept of verifying the identity of the caller, that the phone actually belongs to the account that is associated with that device and that the customer is in possession of the phone by inspecting the live phone call end-to-end. This makes it more difficult for a risky caller to get to an agent in the first place. A combination of proper routing and stronger barriers to risky callers, as well as giving agents indications of risk, provides a much safer level of authentication.

---

*Content sponsored by Neustar, a TransUnion company. Don Smith can be reached at **Don.Smith@transunion.com**.*

BAI® POWERING SMART DECISIONS.