never underestimate the power of identity

hackers in an increasingly vulnerable digital world

Without question, the power of the digital economy permeates nearly everything we do. Evolving well beyond eCommerce and mBanking, the connected society includes social media, video subscriptions, file sharing, ride hailing, and homestay, all of which have quickly become a regular part of our lives every day. While the convenience is alluring, the risk can be alarming. These applications often contain payment and other confidential information that need to be secure in order to ensure that only the right people are properly entitled to access the information or assets involved. To complicate matters further, applications are constantly trying to improve the user experience by reducing the friction in the authentication process. Unfortunately, making access easier for the customer is also making it easier for fraudsters. According to a 2016 article in Forbes, hackers compromised a victim's email account once they had control of the victim's mobile phone number and then proceeded to compromise 30 other accounts within seven minutes. Hackers can have access to your bank accounts, bitcoin, payment services and many other aspects of your digital life before anyone is the wiser. That is a powerful proposition for fraudsters.

> "Hackers can have access to your bank accounts, bitcoin, payment services and many other aspects of your digital life before anyone is the wiser."

Clearly, the digital world is increasingly vulnerable. Fraud is getting progressively sophisticated and more difficult to prevent resulting in billions of dollars in financial losses annually. Victims are not only unsuspecting senior citizens and always-connected millennials, but also bitcoin entrepreneurs and everyday consumers. Even the chief technologist of the very organization vested with the responsibility to protect consumers by stopping unfair, deceptive or fraudulent practices in the marketplace has been a victim of fraud. Interestingly, the telephone number, which is the entryway for much of this fraud, is being exploited by adept criminals in novel ways. Fortunately, the victims no longer need to be victimized because much can be done to protect consumers from this type of identity theft and related harms.

never underestimate the power of identity

the importance of identity verification to prevent fraud

protecting the integrity of the phone number

The power of that protection begins with putting the integrity back in the telephone number, which is essentially our digital identity, tethered to a mobile device. Consumers expect that identity to simply, seamlessly and securely facilitate all of our digital experiences and transactions. We expect that it is safeguarded such that it always be used legitimately. If it is compromised we expect that our service provider and the digital businesses we transact with are performing the requisite authentication checks to protect us from fraud, early and quickly. Today, however, the phone number is under attack. We can get texts intended for the previous owner of our number, we often receive spoofed calls that are not from who they claim to be and, worst of all, we might not get the messages we need for authentication, for example one-time passwords being sent to the fraudster instead.

Online banks, payment processors, corporate servicers, and other providers of secure, personally authorized online services rely on our mobile identity to securely conduct a wide range of digital transactions. This technology uses the consumer's phone to authenticate an identity using something that you and the rest of us also have. Authentication through your mobile identity presents a powerfully simple version of multi-factor authentication, which otherwise impedes a website or app's ease of use.

"Authentication through your mobile identity presents a powerfully simple version of multi-factor authentication, which otherwise impedes a website or app's ease of use."

account takeover

Account takeover is the second most common fraudulent activity reported in the mobile environment.[1] Fraudsters have been able to use porting, SIM swapping, and other sophisticated means to compromise consumers' mobile identities, take over their accounts, and instigate fraudulent transactions. Once the account takeover compromise has occurred, the fraudster will attempt to access consumer services (e.g. financial institution information) immediately, usually in less than two hours. Put another way, account takeover is pretexting on steroids: not only do fraudsters pretend to be a consumer in order to gain access to sensitive information; these cybercriminals fuel the underground fraud-as-a-service economy with the compromised accounts, which are sold or exchanged for a variety of downstream attacks involving retailers, financial services, reward programs, mobile games and other consumer-facing services. Worse, once a fraudster hacks one account, the next account often is easier to crack because consumers frequently use the same username and password combination on many different web properties including email accounts. As

never underestimate the power of identity

noted earlier, roughly 30 online accounts, including 2 banks, 1 payment processor and 2 cryptocurrency accounts, were compromised recently within 7 minutes of the mobile account takeover.

There are many ways fraudsters can accomplish account takeover. For example, they can "age" burner SIMs and phones so that the device appears to have network tenure before they imitate a victim's mobile identity. They can effect SIM swaps, using the last four digits of the social security number (SSN), for example, in order to intercept one-time SMS passcodes. They can use multiple SIM cards across multiple mobile network operators ("MNOs") to create fake accounts in the name of legitimate subscribers. They can obtain victims' personal information through social engineering or buy it from illicit sources and then use that information to transfer the victim's telephone number to a new SIM card on the fraudster's device. A thief can also use a victim's personal information to impersonate him or her, and have the victim's wireless service provider port the number to a new provider. A criminal can often accomplish account take over through porting fraud with only a consumer's name, telephone number the last four digits of his or her social security number, and a compelling story.

Fraudsters easily procure typical authentication data involving "something you know", like passwords and knowledge challenges. "Something you have", such as hard tokens or "something you are", such as biometrics are much more secure from fraudsters. These, however, are not ubiquitous enough to protect the majority of consumers. These credentials often reside in the device itself, so if the hacker moves the phone number to their device, those credentials are not available and the application will often revert to a one-time passcode sent to that phone number via text message service. So, we are back to square one. The mobile phone remains the primary authenticator representing "something you have" that can reach the vast majority of the consumer base to provide multi-factor authentication

in the digital economy. It goes without saying that the phone number must be safeguarded from account takeover so it cannot be used to perpetrate fraud and other consumer harms.

Access to cross-network information in a timely manner is the key to combating the fraud. Individual service provider data is unable to efficiently detect account take over fraud because there is a lack of knowledge of what is happening on other networks with a different device and the same phone number. Analytics-based contextual risk calculations can leverage historical customer traffic and geographic patterns as well as account tenure to mitigate the vulnerabilities of the mobile phone and the public network for authentication. By establishing a mobile baseline in advance of a security incident, threat indicators can be detected and transmitted quickly to alert businesses that consumer transactions are being done using a suspicious mobile device. Thus, transaction requests can be given more scrutiny and the authentication process can be enhanced so that calls and texts are sent to the mobile device only when it is safe to do so. This can even be done in a frictionless manner, while safeguarding sensitive competitive and confidential information. Consistent with an enterprises' evolving authentication strategy, legitimate customer actions can proceed smoothly while fraudulent ones are promptly flagged.

how do we keep the power of the mobile identity in the hands of the individual?

A circle of trust is needed that is supported by a set of fraud prevention partners that can aggregate and analyze cross-network information quickly and then reliably transmit threat indicators to relevant parties. By never underestimating the power of the mobile identity, we can help consumers trust their phone numbers as assets, not liabilities, while they increase their reliance on the connected society.

[1] IDology 2015 Fraud Report

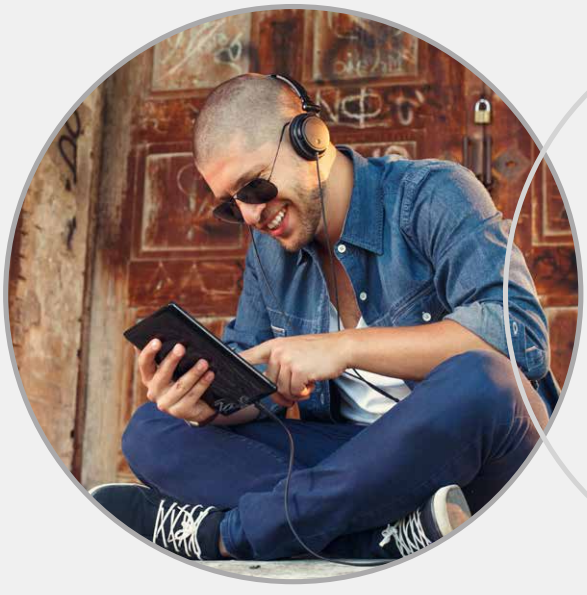
about iconectiv

As the authoritative partner of the communications industry for more than 30 years, iconectiv's market-leading solutions enable the interconnection of networks, devices, and applications for more than two billion people every day. Working closely with private, government and non-governmental organizations, iconectiv continues to protect and secure telecommunication infrastructures for service providers, governments and enterprises, while providing network and operations management, numbering, registry, messaging and fraud and identity solutions to more than 1,200 organizations globally. A US-based company, Telcordia Technologies, doing business as iconectiv, is a wholly owned subsidiary of Ericsson.

make the connection.

For more information about iconectiv, contact your local account executive, or you can reach us at:

+1 732.699.6800
info@iconectiv.com
www.iconectiv.com



© 2017 Telcordia Technologies, Inc. All rights reserved. Telcordia is a registered trademark, and iconectiv is a trademark, of Telcordia Technologies, Inc. dba iconectiv ("iconectiv").

iCOL-WP-IY-E-LT-001, Mar2017