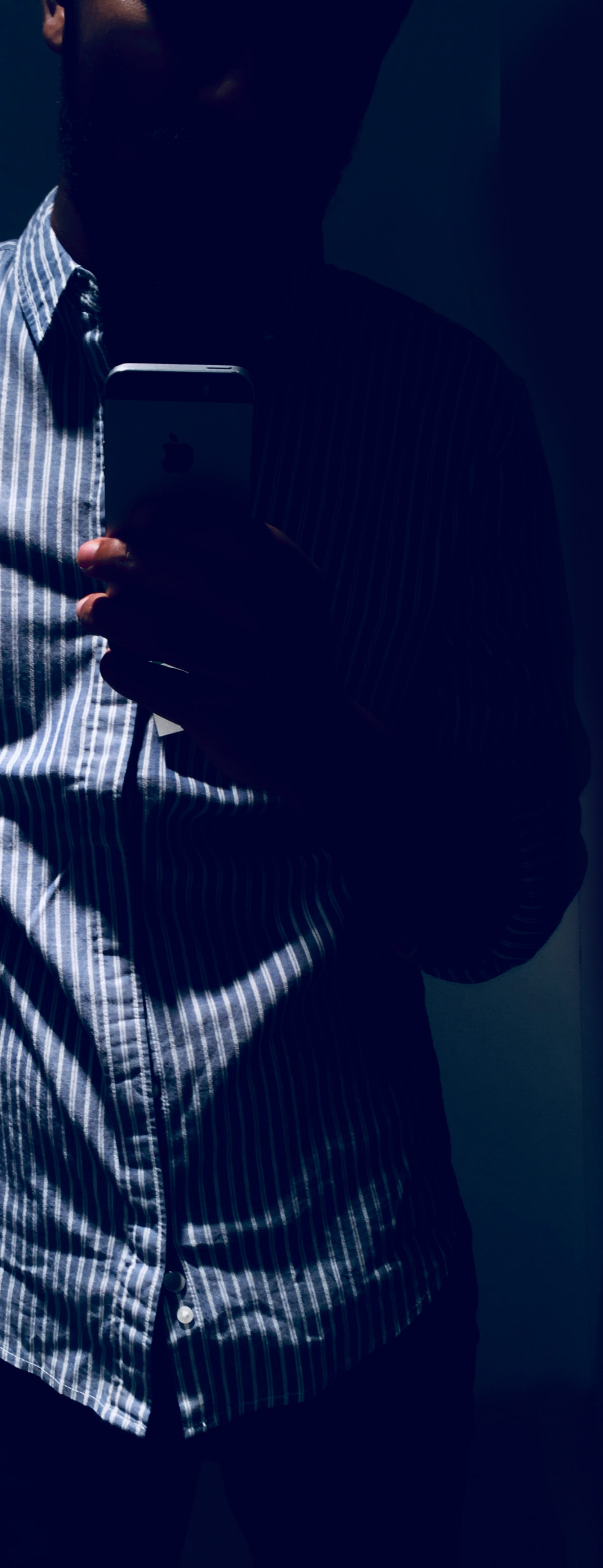

A Boku white paper

Online impersonation is getting too easy.

We need to act.

boku

As our lives move increasingly online, we need to find a better way of verifying user identity. The digital world has enabled so many new products and services, yet that world – and securing our identity in it – is overly dependent on personal data: data about who we are and what we know. With databases being routinely breached, hacked into and stolen, enabling malefactors to impersonate users, we can no longer rely on personal data to confirm our identities online. The longer we continue to rely on personal data alone to establish and verify who we are, the more we risk losing the trust that exists between parties in a relationship – whether that's a commercial transaction, a community of interest, or the many other ways we now engage online.

Adam Lee, Chief Product Officer at Boku, argues that the way we verify our identities online needs to change.

If ID verification is going to work sustainably, we need the capacity to know who we are dealing with remotely, reliably, and in real time. We also need to be innovative to combat the relentless ingenuity of fraudsters and others who seek to compromise or impersonate us online, usually for nefarious purposes.

A brief history of ID verification

Previous concepts of ID centered around someone's name and address, coupled for security purposes with a photograph and/or signature for in-person verification. As the internet took off, interactions moved online. At that point, users supplied data relating to their profile – such as name, address, date of birth, and ideally a government ID number – which could then be matched with authoritative records to confirm the user's identity. The assumption was that only the real individual would have knowledge of this information so a correct match meant the user was indeed who they claimed to be. This technique of verifying knowledge worked until people started getting their information stolen via high-profile data breaches such as Equifax's 2017 US compromise that saw 147.9 million consumer records exposed to potential fraud.

Stolen user data: making online impersonation simple

In a world where users' identities rely too heavily on easily-compromised data sets, crimes and deceptions related to impersonation are rife. From fraudsters to pranksters, individuals and organisations will seek to impersonate innocent users for every kind of illegal activity, ranging from illegitimate access to online communities and marketplaces to carefully orchestrated bank fraud and credit card scams.

User impersonation usually occurs when a new account is falsely created using data stolen or purchased by criminals on the dark web. Fraudsters then substitute their own contact information in place of the victim's, allowing them to hijack any subsequent communication with the business. Armed with this synthetic ID, fraudsters are able to use stolen credit card numbers and apply for bank loans incognito. They are also free to book rideshares and private lodging or access community forums and dating sites, all without ever revealing their real identity. What's worse, businesses believe the fraudsters' identity is authentic, having successfully verified the personal information of the victim whose data was stolen.

> Total bank losses stemming from stolen identities and user impersonation in 2019 came to just under $11 billion.

Information from Javelin Research suggests there were 14.4 million US victims of identity fraud in 2018. Fraud attacks which utilised this stolen user data to impersonate victims accounted for US$14.7 billion in financial losses. In total, the 2018 US Identity Fraud Study estimated that US$107 billion had been stolen from individuals, retailers, banks and other organisations in the previous six years – and the problem continues to grow as fraudsters become more adept at harvesting stolen credentials via the dark web. In the crypto-currency arena alone, a new study from online security specialists CipherTrace claims that stolen identities were employed by criminals to open fake accounts at all of the top ten US retail banks in order to shift criminal proceeds from crypto-currencies to US dollars, accounting for around US$4.5 billion in 2019. Factor in the fines handed out by regulators to the banks executing these trades, and banks' total losses stemming from stolen identities and impersonation in 2019 came to just under US$11 billion.

Putting the financial damage to one side for a moment, the reputational costs of allowing fraudulent accounts to infiltrate a business for illicit purposes can be as bad, or worse, than the dollar losses. For instance, if fraudsters are able to freely access marketplace services for rideshares, home rentals, food deliveries, used goods or personal services, the trust and safety so vital to peer-to-peer commerce would simply be destroyed. These peer-to-peer businesses create value by brokering transactions between buyers and sellers: but if the identity of their participants cannot be trusted, then the entire ecosystem is at risk of breaking down. The same applies when impersonators are allowed to join community forums and dating sites, enabling them to illegally solicit business or victimize individuals.

The Pew Foundation estimated in late 2018 that companies suffer a 7% drop in overall revenue in the months after an ID-related fraud scam, as clients shy away from working with those affected. The FBI also cautions that user impersonation's knock-on reputational effects can cost as much as $1 billion in lost revenues. Indeed, the situation is so acute that a 2018 poll in *Accounting Today* found US accountants considered reputational damage by far the greatest risk (cited by 48% of respondents) stemming from ID fraud.

Secondary ID verification: costing time, causing friction

Given these fast-growing fraud vectors, we need a better approach to user verification. In response to compromised data being used by fraudsters to impersonate users, the industry is moving towards secondary forms of identity verification. User information is still matched with authoritative sources as before – but now it may be linked to other factors, such as biometrics (fingerprints) or points of knowledge like Personal Identification Numbers (PINs) that are delivered to the user's home address before being confirmed online. That said, inherence factors such as biometric verification usually require some form of pre-registration which remains fairly uncommon at this time. PINs that are mailed to a user's home address can be effective, but their physical delivery leads to a confirmation process that can take days if not weeks to complete. While it's possible to deliver a PIN to a mobile number instantly, criminals would simply enter their own number instead.

> What's needed is a solution that verifies mobile phone ownership and possession together.

What's needed is a solution that verifies mobile phone ownership and possession together, thereby preventing the fraudster from substituting their own mobile number. Such a solution could thwart this kind of online impersonation in real time without any special pre-registration and would be of interest to all organisations which rely on verified identity to allow user engagement – which means pretty much every organisation out there at present.

Boku Match: simple and immediate ID verification

Boku has created one of the industry's first ID verification (IDV) solutions that centers on the mobile number - Boku Match. Using Boku Match, a user's mobile phone number becomes a route to two-factor ID verification that can be performed remotely and instantly. Boku Match employs mobile operator records and other authoritative sources not only to verify a match with the user's name and address, but also to match the mobile number to prevent a fraudsters' number from being used. And because possession of a mobile number can be verified immediately, the user's identity can be confirmed on the spot via both a knowledge and possession check. Best of all, Boku Match only requires the addition of a mobile phone number to the user's registration flow – and mobile numbers are usually already

Helb
my name is
Jon Smith
326
knowledge
knowledge + possession

included in the registration process.

The risk of online impersonation is dramatically reduced using Boku Match. Any fraudster attempting to substitute their number for a victim's number would be stopped by Boku Match. And if the fraudster tries to circumvent Boku Match by using the victim's number, a simple possession check easily stops them.

User impersonation risk is dramatically reduced using Boku Match

Conclusion

User impersonation and synthetic ID fraud have become significant fraud vectors encountered by organisations. In response, organisations have moved towards secondary forms of identity verification that utilize biometrics or PINs. Unfortunately, these add time and friction to the user journey. Used in combination with a phone number possession check, Boku Match is the most effective means of providing a reliable, real-time and frictionless response to these threats. Our solution verifies identity along with a phone number, and dramatically reduces the risk of online fraud at a low cost per use.

To find out more about Boku Match and how your organisation can reduce its exposure to user impersonation and synthetic ID fraud, go to www.boku.com or get in touch with us at sales-id@boku.com.

www.boku.com

boku