

Customer engagement, Authentication & fraud prevention

Consumers get ready to fight fraud with biometrics

[Brett Beranek](#) | Vice President & General Manager, Security & Biometrics

May 2, 2019



1 in 4 people have fallen victim to fraud in the last twelve months, losing an average of \$2,000 due to inefficient passwords – biometrics is on the rise to change that.

[World Password Day](#) is a great opportunity to evaluate the role of PINs and passwords today and consider their limitations when it comes to safeguarding financial and personal information in today's digital society – never mind causing consumers serious headaches. Nuance recently commissioned a survey asking 5,000 citizens, aged 18+ across the US, UK, Germany, Spain and Australia, how they feel about traditional passwords and the potential of new technologies designed to safeguard their data and reduce fraud. Here's what we learned:

Password frustrations are real

Passwords are still creating challenges for consumers. The survey found consumers manage an average of 11 online accounts (for example, emails, banking, bills, shopping, entertainment, etc.) each and have to remember around nine different passwords for use across those accounts for access.

One in four people forget those passwords at least once a month, with nearly a third (28%) calling a contact center every three months to reset login credentials. One in 10 US consumers have to make this call **more than once a week** due to forgetting their login information.

Fraud still hitting consumers hard

More than causing frustration, traditional passwords are not secure. Nearly one in four (24%) citizens across the globe have fallen victim to fraud in the last 12 months, losing an average of \$2,000 as a result of poor account protection. Those in the US were the hardest hit, with nearly two in five (38%) affected in the same time period. To make matters worse, fraud claims took over a month on average to be resolved.

Consumers are quick to act when this happens, with three in five (62%) respondents noting they would likely change service providers if they fell victim to fraudsters through their services – and the loss of bank, online shopping and utility account details were cited as most inconvenient. That said, more than a quarter (27%) of victims did not change their passwords for other accounts following fraudulent activity, leaving them exposed to further criminal activity, as is typical in Account Takeover (ATO) attacks.

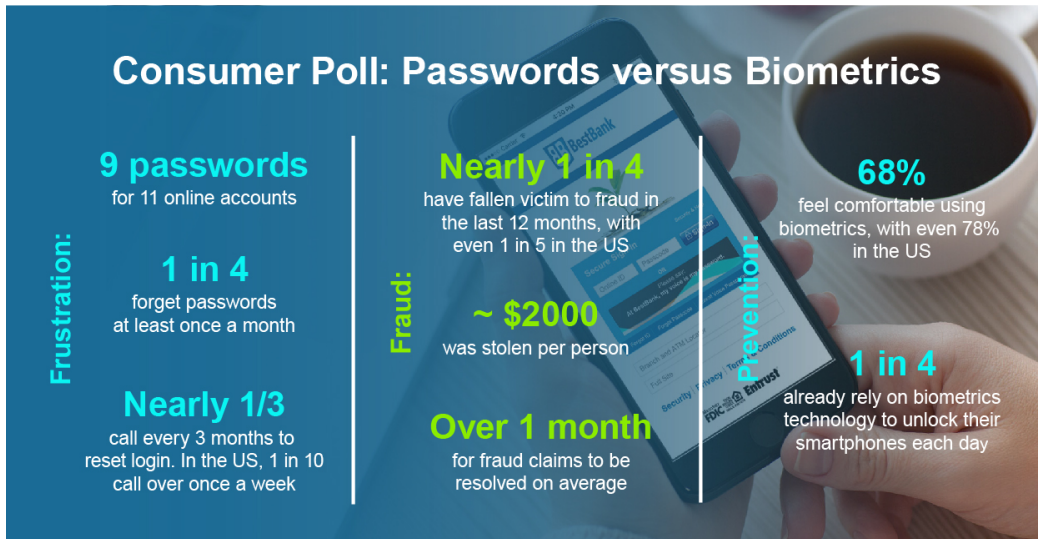
Getting ready to prevent fraud

As PINs and passwords continue to fail – and hacks and breaches climb – more and more organizations are deploying biometrics to enable a simpler and safer way for customers to validate their identities and access services. The adoption is growing at a rapid rate. Over 400 million consumers globally make more than eight billion successful authentications yearly already. Just recently HSBC announced that their innovative voice biometrics system, VoicelD, has stopped over £300 million of customers' money from falling into the hands of telephone fraudsters. HSBC customers have used the technology 15 million times since it launched in 2016. Each month around 50 weeks or 8,400 hours of customers' time is saved due to fewer password resets and less use of manual security.

According to the survey data, consumer comfort level with the use of biometrics – which authenticates individuals by their physical and behavioural characteristics – is growing, with more than two thirds (68%) globally and 78% in the US saying they feel comfortable using the technology.

Nearly one in three (30%) respondents already rely on biometrics technology – via fingerprint or facial biometrics – to unlock their smartphones many times each day. 18-24-year-olds are most prolific in their use of biometrics, with nearly two-thirds (59%) using it for this purpose, compared to around one in five (22%) aged 55+.

This year's World Password Day comes at an interesting time in the world of security, as fraudsters continue to evolve their hacking strategies and consumers demand more streamlined access to their accounts. Biometrics takes the onus away from insecure and tedious PINs and passwords and places the emphasis on our unique characteristics – making authentication not only more secure but a lot easier to do.



Survey methodology: Nuance Communications commissioned OnePoll to conduct an online survey of 1,000 adults (18+) in each of UK, US, Australia, Germany and Spain (5,000 participants in total). The survey was carried out between 9th – 18th April 2019.



Survey methodology: Nuance Communications commissioned OnePoll to conduct an online survey of 1,000 adults (18+) in each of UK, US, Australia, Germany and Spain (5,000 participants in total). The survey was carried out between 9th – 18th April 2019.

All figures in USD are representative of the Google Finance exchange rate between GBP and USD on 23 April 2019.

Tags: [World Password Day](#), [Biometric authentication](#)

More Information

Ditch the password

Get simpler, stronger customer authentication with multi-modal biometrics

[Learn more](#)



About Brett Beranek

Brett Beranek is responsible for overseeing the security and biometric line of business at Nuance, a Microsoft company. In this role for the past 12 years, Beranek has brought Nuance to a leadership position in the biometric authentication and biometric fraud prevention space. A thought leader in the field of biometrics, Beranek is a frequent contributor in industry events and the media on the topic of AI technology and its use by the fraud community, and how society can mitigate against these evolving threats. Prior to Nuance, he held various leadership positions in the biometrics and security industry. He has earned a Bachelor of Commerce, Information Systems Major, from McGill University as well as an Executive Marketing certificate from Massachusetts Institute of Technology's Sloan School of Management. Beranek is also a certified Master Fraud Prevention Black Belt professional.



[View all posts by Brett Beranek](#)