NUANCE | WHAT'S NEXT BLOG

Customer engagement, Authentication & fraud prevention

The roaring 20s: How to reach the golden age of fraud prevention

Brett Beranek | Vice President & General Manager, Security & Biometrics

May 6, 2020

A new decade with new beginnings and new opportunities, 2020 was a year heralded as the tipping point for technology and innovation. But 2020 hasn't quite started in a way any of us would have predicted...

The spread of coronavirus has resulted in increased uncertainty for many. Feelings of ambiguity have triggered a variation of consumer behavior. Many are calling their banks to check on payments and seek reassurance. Some are diving into their work to stay productive and keep the feeling of progression going. Others are 'switching off' from the news and current affairs by diving into their Netflix box-set.

Lurking behind the scenes of it all is an unfortunate reality tied to the uncertainty and corresponding behaviors – threat actors, also known as fraudsters. And these fraudsters are deploying increasingly sophisticated attempts to hoax individuals and get access to their sensitive data. From social engineering to email phishing and the creation of bogus websites, fraudsters are taking advantage of any lowered defenses during this time.

Organizations across the globe have witnessed a significant rise in the volume of fraud attacks – ranging from 200% – 400% in the past few weeks, depending on their industry. Some of these relate directly to the pandemic, with recent reports suggesting there have been hundreds of coronavirus-related scams and thousands of phishing attempts so far. And, these figures are expected to increase as time goes by.

The weakness of traditional authentication

During uncertain times like this, it's even more important to offer consumers peace of mind that your organization is doing everything it can to protect them from fraudulent activity – authentication plays a key role in this process. The Oxford English Dictionary defines authentication as *"the act of proving that something is real, true or what somebody claims it is."*

Traditionally, knowledge-based credentials have been relied upon to prove we are who we say we are – the use of names and addresses, passwords or PINs, or your mother's maiden name, for example. However, this means of identification is even more susceptible to social engineering in today's COVID-19 climate.

Vulnerable consumers are being targeted by fraudsters phishing for such information, whether it's by email, phone, text, or in-person – and without sophisticated techniques to identify such fraudulent activity, they can use that information to get access to an individual's funds or accounts.

One Time Passwords (OTPs) via SMS for example, give a false sense of security but do not represent an effective way to stop ID theft and account takeovers. If a fraudster already has enough information on a victim to target their bank account, then they have enough to take over their telephone account and intercept any SMS sent to them.

Last year, even before the impact of coronavirus hit, fraud reportedly cost the global economy $5 (USD) trillion. A global poll conducted by Nuance around the same time found one in four (24%) of consumers had fallen victim to fraud in the previous twelve months, losing an average of $2,000 (USD) due to inefficient passwords. This number is likely to be on the rise, given the volume of fraudulent activity tied to the coronavirus.

That fraud loss doesn't just hit the consumer, or the bank's insurance premiums. It hits the companies unintentionally associated with the fraud. Consumers are quick to disconnect from those associated to fraud when it happens, with two thirds (62%) noting they would change service providers or brands if they fell victim to fraudsters through their services.

Enter biometrics

Biometrics provides an answer for organizations looking to keep fraudsters at bay and can ensure the security of both their contact center customers and employees.

A more powerful and effective alternative to passwords and PINs, voice biometrics, for example, cannot be compromised in the same way as knowledge-based security methods. This is because human voices are as unique as a fingerprint. By using sophisticated algorithms to analyze more than 1,000 voice characteristics, voice biometric technology uses a caller's voice to not only validate their identity but also protect them against hackers. The authentication method through OTP, for instance, can be efficient if paired with biometrics and push notifications.

Another protective layer on top of voice biometrics is behavioral biometrics. This technology measures how an individual interacts with a device – how they type, how they tap, how they swipe, or even how they hold the phone – in order to identify whether they are who they say they are.

When biometrics is used alongside other technologies such as multi-factor authentication, end-to-end encryption, and public key infrastructure, it becomes a powerful tool in an organization's armory against fraudsters.

When prompted that biometrics technology is proven to help catch criminals in the act of trying to commit fraud and preventing it before it happens, a third (36%) of consumers said they would do business with companies that offered biometrics. A similar number (25%) even called for more businesses to be using it.

So, how is the golden age of fraud prevention reached?

Biometrics is playing a critical role, as the demand on contact centers increases, with customers calling for reassurance and critical services. Against this backdrop, agents are being forced to work from home, which can result in changes to service delivery if the provision of tech varies from 'business as usual' in the contact center. So when armed with biometrics to tackle the role of authentication, a contact center agent can focus on the task at hand: customer service.

With today's circumstances forcing businesses to take extraordinary measures to re-mobilize their workforces, alter working styles and – in some cases – entirely reimagine business models, now is the time to consider how your organization authenticates its users, and safeguards them from fraudulent activity. Uncertainty often imposes innovation. If that innovation helps protect consumers from fraudsters, a step forward will have been taken to prevent the growing threat of fraud – now and in the future.

Take the Challenge

Forrester, Javelin Research, Aite Group and Fierce Telecom all recommend replacing PINs and passwords with biometrics for customer authentication and fraud prevention. Now, we've built a system for you to try it for yourself – and see just how secure it is compared to other means of authentication. Take the challenge and try to break into my VB-protected bank account. You won't win millions, but you will see how Nuance customers are providing enhanced security while automating the authentication process to cut Average Handle Time by over 1 minute. This is significant anytime but especially today while contact centers are dealing with increased call volumes, hold times and remote agents.

Tags: World Password Day, Fraud prevention

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 it's 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