NUANCE | WHAT'S NEXT BLOG

Authentication & fraud prevention, Customer engagement

How biometrics can keep fraudsters at bay

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

21 April 2020

With a massive shift to work-at-home, enterprises need to be aware of evolving threats and fraudsters looking to take advantage of this societal change. With biometric solutions, enterprises can keep bad actors at bay, ensure the connections they need to make with customers are safe and secure and allow their organisations to adapt rapidly to emerging threats.

Fraudsters don't stop their crimes because of a pandemic. They often seize the immense change that comes with an event like this to ramp up activity. With the recent shift to a stay-at-home world, there is a significant increase in fraudster attacks against call centers – testing for vulnerabilities by directly attacking work-at-home agents, or alternatively, pretending to be remote agents to test for weaknesses that may allow them to perpetrate fraud.

To keep bad actors at bay and ensure the security of their operations and customers, both government and private sector organizations must arm themselves with tools that will keep disruptions caused by fraud to a minimum. Organisations who have deployed biometrics are finding the technology to be incredibly useful in this effort because it can identify fraudsters, instead of relying on more traditional methods focusing on established suspicious transactional patterns.

There are applications for biometrics to help solve some of the new and more complex challenges organisations are facing today:

Safeguarding customer and agent experiences: As contact centres struggle to cope with the influx of inquiries generated by the pandemic, it's all too easy for a slow, stressful service interaction to send everyone's day from bad to worse. Biometric authentication can play a crucial role in not only speeding resolutions and freeing up agent time but ensuring frustration levels are kept to a minimum by not creating unnecessary friction between the customer and agent. Biometrics can eliminate the need for any overt identification and verification process and remove pressure from frontline agents, reducing the chances they will make mistakes during a call.

Fighting new influx of fraud attempts: Many organisations, including financial institutions, insurance companies, telecom providers, and citizen-facing government agencies, are seeing a massive surge in call

volumes as brick-and-mortar locations shut down. And, in some cases, they are seeing an enormous increase in inquiries and transactions across digital channels. With this surge, it's a big ask to expect customer care agents to separate fraudsters from real customers while trying to address customers' needs. Afterall, it's a customer care agents' role to focus on helping customers. Biometrics proves to be an invaluable tool to automatically identify when fraudulent calls are being placed – removing pressure from frontline customer care agents and protecting them from social engineering.

Letting agents safely work from home without comprising security: Empowering agents to work remotely comes with a set of challenges, especially in the case agents are using their personal laptops, desktops, and mobile phones on the job. This rapid shift to work-at-home agents has created countless opportunities for fraudsters, as the usual systems protecting contact centre facilities are no longer present. There is vast potential for biometrics to improve internal security checks in these situations by verifying the identity of agents and preventing fraudsters from taking over agent accounts. Biometrics authentication also allows organisations to display less personal information on their customers to agents, which consequently reduces the risks of occupational fraud in a remote-work context where the lack of direct supervision represents an opportunity to bad actors within organisations.

Now more than ever, secure contact centres are a necessity for organisations to interact with customers.

Tags:

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