BEHAVIOURAL BIOMETRIC AUTHENTICATION IS KEY TO SEAMLESS AND SECURE ECOMMERCE

AMIR NOORIALA
CHIEF COMMERCIAL OFFICER
CALLSIGN

WITH ONLINE FRAUD SURGING DURING THE PANDEMIC, RETAILERS MUST IMPROVE THEIR AUTHENTICATION TO COMBAT THE ISSUE AND BUILD CUSTOMER TRUST

COVID-19 has driven a phenomenal spike in e-commerce, with the recent surge in online shopping expected to add an additional £5.3bn to UK e-commerce sales this year to make a total of £78.9bn, according to *Edge Retail Insights*. Even though retailers are re-opening their doors, people continue to shop online, causing two main issues for retailers:

1. With consumers forced to do their shopping online, retailers that offer a sub-standard shopping experience, such as unwieldy account opening or checkout processes, are shooting themselves in the foot. Having an inferior e-commerce platform has been shown to have a seriously negative impact on sales, with an *Akamai* study showing that every 100-millisecond delay in website load time can hurt conversion rates by 7%. Furthermore, *Callsign research* revealed that, in April alone, 20% of consumers switched to other brands due to a bad online shopping experience (e.g. failed payments, complicated log-in, etc.).

2. With the shift of physical traffic from store to online, fraudsters are also focusing their efforts toward online channels. We have found that fraudsters have realised that retailers with dedicated mobile apps generally have more up-to-date security technology and that fraudsters are focusing more on web channels, which have been identified as the legacy weak spots in a retailer's technology infrastructure. You only have to look at figures from *Action Fraud*, which show that 16,352 people have already fallen victim to online shopping and auction fraud during lockdown, to realise the extent of the problem.

So, in this context, how does a retailer ensure that shoppers have secure and frictionless experiences online, when that very friction is normally there to keep customers safe from criminals?

BUILDING TRUST POST-COVID

In a crisis where chaos and confusion are rife, consumers want to engage with reliable brands, so, to achieve that perception, retailers must cultivate trust online. But with this massive uptick in fraud, businesses face an uphill struggle. To create an ecommerce experience fit for this new environment, companies must strike the right balance of security, user experience, privacy and accessibility. As these organisations strive for superior service, they cannot neglect their security around customer authentication – instead, using it as an opportunity to improve the relationship with their customers and drive growth.

So how can retailers eliminate the pain points associated with digital authentication and behaviour analysis technologies, while at the same time build online trust and prevent reputational damage?

ELIMINATING DIGITAL AUTHENTICATION PAIN POINTS

In a landscape focused on seamless omni-channel experiences and growing fraud complexities, the traditional tools that are designed to spot threats are likely to hinder rather than help business growth. Retailers should consider moving away from the commonly used one-factor authentication mechanisms such as passwords and SMS OTPs, as they don't offer robust enough security, or positive experiences for customers.

With the advent of AI and Machine Learning, businesses can now benefit from tools that positively identify users, significantly reducing the risk of frauds such as account takeover and even account borrowing. Passive behavioural biometrics which analyses data such as how someone holds theirs phone, their location, muscle memory and even how they swipe the screen provides more certainty that the customer is who they claim to be.Combining this with additional checks such as device fingerprinting and location offers multifactor authentication whilst simultaneously reducing friction during the transaction.

Using this information, retailers can analyse individual behavioural patterns to securely authenticate the consumer. It's this capability to deliver real-time passive identification that enhances the customer experience, giving retailers the ability to meet changing consumer requirements whilst adding greater levels of security and accessibility. This level of protection offers greater business assurance against the potential risks, such as customer data being exposed in data breaches due to reused passwords.

With this level of information at their disposal, retailers can then flag to the customer when a fraudulent transaction might be about to take place. For example, push messaging in mobile channels can be used in real-time – when anomalous indicators appear – and notify the user to think twice about the possibility of fraud.

BOOSTING LOYALTY

This winning combination of reduced friction in the customer journey and improved security will help to considerably boost customer loyalty in the long run. Using passive behavioural biometric authentication should also help alleviate the number of complaints to retailers' call centres from dissatisfied customers experiencing issues around broken password resets or lost SMS OTPs, meaning their customer service staff will be able to dedicate more time to the individuals who need their help most – again, solidifying that all important trust element.

Consumers have enough to worry about regarding the pandemic; struggling to access essential goods online and their security shouldn't add to their concerns. As more and more people shift their lives online, retailers need to take advantage of behavioural authentication while encouraging customers and employees to prioritise personal security – to maintain the level of trust they require to survive.

AMIR NOORIALA
// amir.nooriala@callsign.com

callsign®