How digital behaviours can identify consumers

MARK ELLIOT: BIOCATCH

As financial institutions grow their digital business, distinguishing good customers from bad actors is possible by examining the applicant's digital behaviour patterns

During the peak of the Covid-19 pandemic, financial institutions observed a 250 per cent increase in digital channel usage. This rise has driven them to accelerate transformation plans as digital shifts from one of many customer-acquisition channels to a primary one. Fraud was an inevitable fallout as cybercriminals capitalised on fear and confusion.

Consequently, when reimagining customer acquisition, financial institutions must consider potential fraud losses as well as potential gains from maximising the customer onboarding experience. Traditional security measures are limited in addressing these two considerations. For example, knowledge of personal information is no longer considered a valid form of identity proofing as phishing attacks and massive data breaches have created an abundance of stolen personal information. In addition, device ID-based controls are extremely limited in protecting the account-opening process as a new customer is likely coming from an unknown device. To overcome these challenges, behavioural biometrics have proven to be an effective method of control to reduce fraud risk in the new account-opening process while minimising false declines.

> "As digital interactions become the new normal, unique approaches are required to build trust and safety"

Behavioural biometrics identify clear differentiations in digital behaviour patterns in the account-opening process. For example, cybercriminals input data differently as they don't have the same level of familiarity with personal information as a genuine user. However, they will usually be more familiar with the new account application form than a genuine user since they fill out multiple applications.

Once something only seen in science fiction, enterprise-grade advanced behavioural biometrics are now proven science providing financial institutions with immediate value and more effectively detecting fraud in the account-opening process. For example, a digital bank undergoing a new account-opening fraud attack instantly observed a 70 per cent increase in detection when behavioural biometrics were introduced to their existing security controls and allowed them to continue accepting new customers with confidence. A more recent implementation by a large bank in Asia showed significant value within weeks of leveraging machine learning-powered risk models.

As digital interactions become the new normal, unique approaches are required to build trust and safety in a highly impersonal online world. Behavioural biometrics are a proven solution to identify good customers and for financial institutions to reward them in return. ■

Mark Elliot is the chief marketing officer at BioCatch