CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

Behavioral Biometrics and Customer Identity Authentication

Zeynep Salman

Zeynep Salman
Principal Consultant,
FICO Advisors Digital
Practice, FICO

Biography

Zeynep Salman is a credit risk professional with direct experience managing originations, customer management, credit risk and collections strategies for consumer and small business portfolios. She joined FICO (https://www.fico.com) in 2014 and is currently Principal Consultant in the FICO Advisors Digital Practice.

The FICO Advisors Digital Practice is a business consulting group staffed with seasoned digital practitioners focused on the mobile and digital transformation of financial services providers.

Zeynep is passionate about driving automation, seamless onboarding experiences, convergence of credit and fraud evaluations across the lifecycle, AI driven customer engagement, and working with clients to set near and long-term roadmaps to drive value.

Before joining FICO, Zeynep held many key roles at financial institutions such as Citibank, HSBC, Toyota Finance and Yapi Kredi (UniCredit).

Zeynep blogs at https://www.fico.com/blog

Keywords Synthetic fraud, Behavioural biometrics, Customer authentication
Paper type Research

Abstract

With synthetic identity fraud on the rise, behavioural biometrics enable banks to balance customer experience and fraud prevention. Combined with machine learning and risk assessment techniques, behavioural biometrics provide a much more innovative approach to on-line user authentication, by analyzing the unique ways users interact with their device via keystrokes, swipe patterns, scroll speed, etc. As the author of this article explains, the technology is able to deliver a seamless experience for customers while ensuring a high level of security.

Introduction

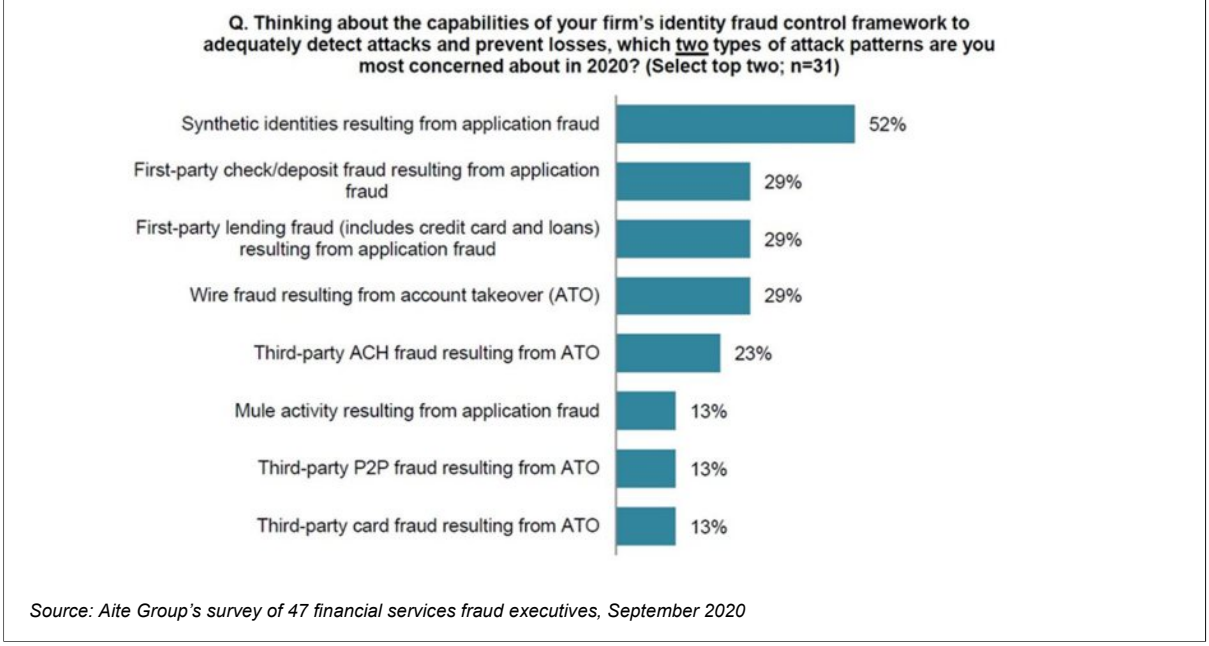
As COVID-19 has spread, concerns about fraud have increased. According to an Aite Group survey of U.S. fraud managers[1], their biggest concern in 2020 was synthetic identity fraud – 52% reported that this was their biggest issue in identity fraud control.

This presents a challenge to banks, as to be competitive in digital lending they need to provide a superior customer experience. Customers that perceive that they will get a better service elsewhere are likely to leave, particularly in countries such as the UK and the Netherlands that offer simple account switching services.

CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

Figure 1: 2020 attack patterns that concern fraud executives the most



Source: Aite Group's survey of 47 financial services fraud executives, September 2020

The key to resolving the tension between customer experience and fraud prevention is to ensure that the bank is using an integrated platform.

Why is being integrated so important? At every stage of the customer lifecycle, banks get more and more data from their customers and fraud managers want to use that data to make better fraud decisions. They can't do this if the data only exists in a silo, and they have no access to that source.

What are the key elements for securing digital accounts?

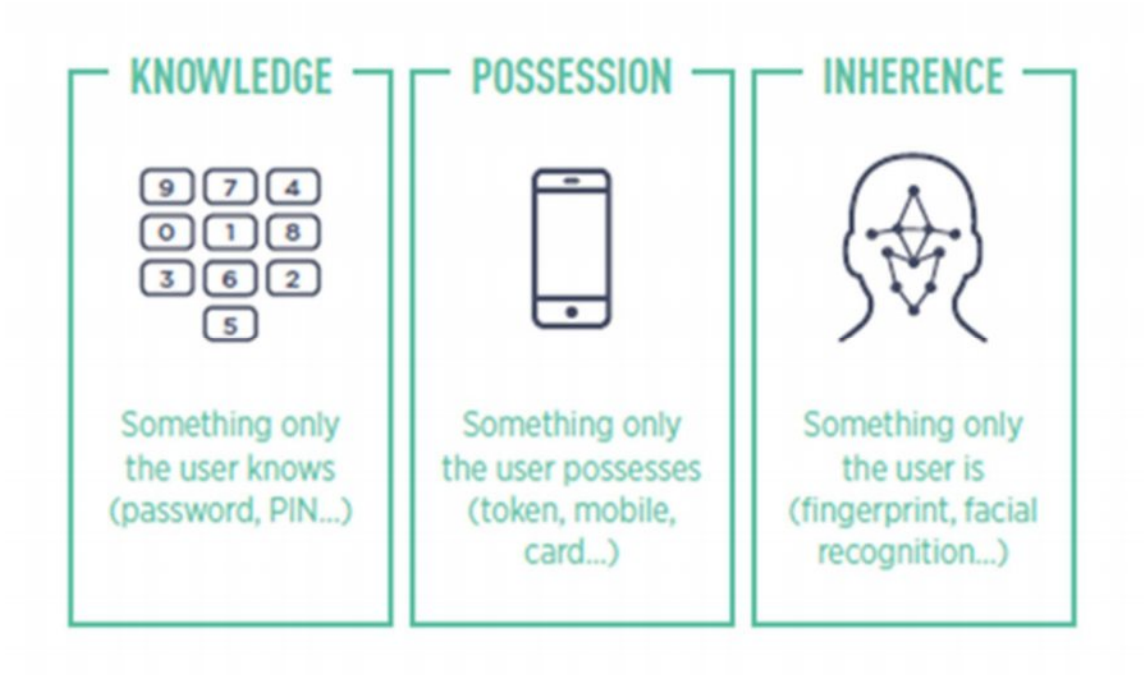
Best-in-class customer experience is achievable when the levels of security do not unacceptably increase friction, as my colleague Liz Lasher noted in a recent post[2]. When the balance is right customers gain easy access to their accounts when and where they want it. Seamless identity verification when accounts are opened, coupled with ongoing, smart authentication as accounts are used, is the right strategy for success. Authentication needs to create a balance between security and convenience. Customers look for this convenience, but if banks fail in protecting their accounts, customers easily switch to a competitor.

Behavioural biometrics empower banks to achieve balance

Customer authentication has evolved: in the past, it was mainly reliant on knowledge factors or something only the customer knows, such as a password. Given data breaches and poor password practices, this had to evolve and banks now routinely send one-time passcodes to confirm the identity of their customers by checking they are in possession of their mobile device.

Today people are becoming used to the authentication factor of inherence, or something they are – in other words, a biometric. This trend is being rapidly adopted as people find it convenient to use voice, face or fingerprint recognition. Even though these biometric methods are convenient, they still require the customer to do something. Now there is an alternative that is both reliable and to the customer invisible – behavioural biometric authentication.

Figure 2: Knowledge, Possession, Inherence



Source: FICO

CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

How do behavioural biometrics work?

Behavioural biometrics identify a customer by recognizing the way they do something. Given that this is typically through an activity they were already engaged in, it is a security method that does not add friction to a customer's journey.

Behavioural biometrics monitor user behaviour during the duration of a session and detect any suspicious activity. These behaviours can include keystroke dynamics, mouse dynamics or handwriting dynamics. It's possible to generate several parameters from a user's unique way of doing these actions. These range from monitoring human motion gestures and patterns to keystroke dynamics, and factors such as speed, flow, touch, sensitivity pressure and even signature formats.

By leveraging behavioural biometrics to analyze physical and cognitive attributes, it's possible to detect if an account is being accessed fraudulently, regardless of the customer's location or device. By incorporating those behavioural insights into the risk analysis process, it's possible to realize immediate ROI from reduced fraud losses, decreased operational costs, and improved customer satisfaction.

Reference

1 Fooshee, F. (November 17, 2020), *Application Fraud: Accelerating Attacks and Compelling Investment Opportunities*, Aite Group. Available at: https://aitegroup.com/report/application-fraud-accelerating-attacks-and-compelling-investment-opportunities

2 Lasher, L. (11 January 2021), "5 Steps to Stop Identity Fraud and Improve the Digital Experience', FICO. Available at: https://www.fico.com/blogs/5-steps-stop-identity-fraud-and-improve-digital-experience