A smarter way to authenticate customers

Reshaping the banking experience

Bank fraud is on the rise. In fact, according to a recent KPMG survey of 43 major banks around the world,[1] it's not just the number of fraud cases that is going up; so, too, is the value of fraud overall.

In large part, this increase in fraud is the result of identity theft scams. Indeed, rather than attempting some sort of high-stakes virtual bank heist for all the gold in the vault, most online thieves seem content simply stealing money from every-day customer's accounts when they aren't looking. To do that, they employ a wide range of social engineering scams, from phishing and spear phishing emails through to pretexting and baiting scams.

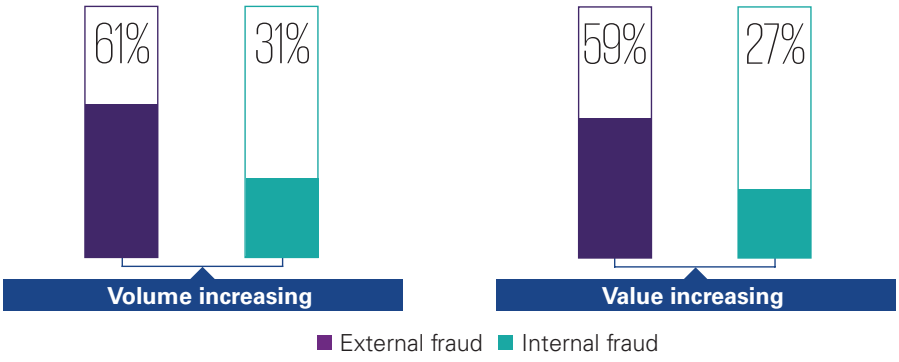
In response, most banks have doubled-down on security, stepping up their controls in an effort to improve their customer authentication processes. Two-factor authentication (2FA) and multi-factor authentication technologies have been deployed. Real-time fraud prevention and detection tools are being adopted. New limits and step up authentication protocols for higher risk transactions have been implemented.

The problem is that — in an era increasingly characterized by competition around customer convenience and experience — adding more layers of security only introduces more friction into the customer journey. And experience suggests that, while bank customers want to be confident their money is being held securely, they do not seem to want to invest a lot of time or effort into jumping through hoops to authenticate themselves.

A better way

Imagine a world where users are only peripherally involved in the customer authentication process: no sign-ins; no passwords; no text verification codes — customers simply open the app or login to the website and conduct their daily banking.

Volume and value of fraud detection



Source: Global Banking Fraud Survey, KPMG International 2019

1. *Global banking fraud survey*, KPMG International, May 2019

> “Fintechs and challenger banks recognize there is no use replicating the traditional authentication processes they are about to make obsolete.”

Yet, in the background, complex algorithms are working away, continuously ensuring that the person using the device is who they claim to be.

The algorithms check keystroke patterns on keyboards and examine the way the user swipes their screen when using apps. It measures the pace at which the user is walking, the height at which they are holding their phone, the rate at which they speak. It looks at the last few places the user has been and where they are right now. It conjures up dozens of other data points about the device user and decides if anything is out of the ordinary.

If a number of data points seem fishy compared to ‘normal’, the algorithm steps up the authentication process. Perhaps the user is asked to take a selfie to allow the facial recognition software to verify their identity. Maybe they are asked to provide their thumbprint. And two-factor authentication could always be used at this point to add an extra layer of security.

In this world, the user experience is frictionless and fluid. Security and confidence in customer authentication is high and continuous. Incidence of fraud and theft are reduced. And resources are used more efficiently (think of how many work hours could be saved just by eliminating password resets).

Competition heats up

Our work and research suggest that some financial institutions and tech firms are already well on their way towards stitching together the technologies and tools required to make this type of intelligent authentication a reality.

Absent legacy authentication technologies or processes, many fintechs and so-called challenger banks are taking the opportunity to embed intelligent authentication into their operating models from the start. It’s not just that intelligent authentication is generally cheaper, more user friendly and more secure than traditional approaches; it’s also that it is clearly the direction that technology and customer demand is going. Fintechs and challenger banks recognize there is no use replicating the traditional authentication processes they are about to make obsolete.

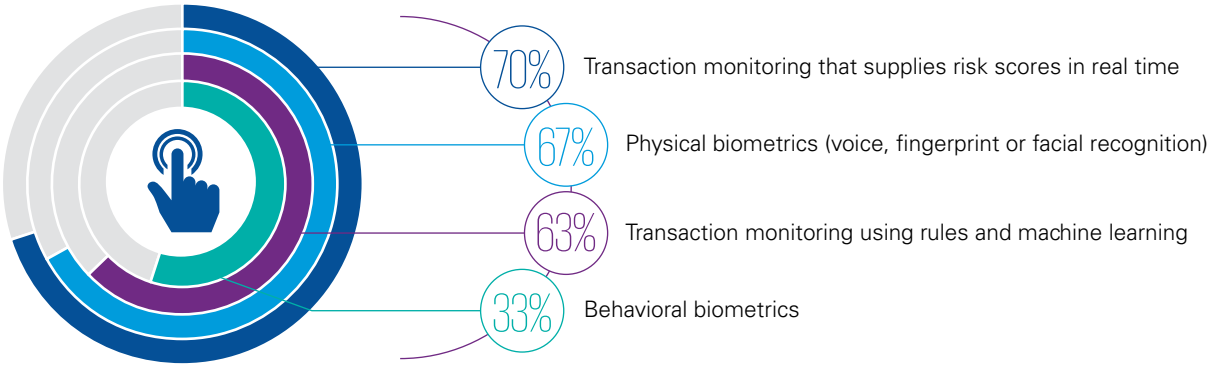
Not to be left behind, many traditional banks are now starting to invest. In fact, two thirds of the respondents to our survey of banking leaders reported that their organization is already investing into physical biometrics technologies such as voice, fingerprint and facial recognition. More interesting still, a third say they are already investing into more sophisticated behavioral biometrics as well.

More than just tech

While cool new gadgets and tech will certainly play a role in enabling a more intelligent approach to authentication, our experience implementing leading-edge systems at fintechs and traditional banks suggests there are five key elements to developing a strong and customer-friendly approach to intelligent authentication.

1. **An exceptional understanding of your customers.** More than just achieving a ‘single view’ of customers, intelligent authentication requires banks to collect and overlay thousands of different data points about individual customers. This will require a smart data strategy built around open data models (see our recent article by our colleagues on open banking)[2] and cloud enablement.

Proportion of banking leaders who have invested in the following technology



Source: Global banking fraud survey, KPMG International 2019

2. https://home.kpmg/xx/en/home/insights/2019/05/open-banking-for-greater-customer-value-fs.html

2. **A sophisticated approach to analytics.** While much of the analytics heavy lifting is conducted by technology, banks will still need to develop a clear understanding of how the analytics work, how they interact with other parts of the business and how they enable or influence existing fraud and risk controls.
3. **A modernized technology infrastructure.** You don't need to be running a fully cloud-enabled and automated digital bank to get value from intelligent authentication, but you do need a technology estate that is capable of flexing with new technology. Again, a focus on open data models to enhance cooperation with third-party tech providers and to improve data flow across the organization will be key.
4. **A new mindset on risk and fraud.** Understanding how more intelligent forms of authentication influence your existing risk appetite and fraud controls will also be important. To be truly competitive, start with a clean slate and build your authentication model to align to the customer journey, incorporating risk and fraud controls along the way.
5. **An understanding with customers.** Based on existing regulations and recognizing that most intelligent authentication processes do not collect personally identifiable information, many suggest that privacy is of little concern here. However, given that cultural and social expectations around data privacy are only now forming, banks would be wise to come to an understanding with customers about their use of intelligent authentication.

Given the direction technology innovation is taking towards smarter, more adaptive and more user-friendly experiences — it seems clear that customers will soon come to expect more intelligent forms of authentication from their banks. Those that move quickly will be able to turn their leadership into a security and innovation advantage. Those that wait will only be playing catchup within the next few years.

> "Based on existing regulations and recognizing that most intelligent authentication processes do not collect personally identifiable information, many suggest that privacy is of little concern here."

For more trends that are reshaping the banking experience, visit kpmg.com/reshapebanking

About the authors

Bia Bedria
KPMG in the UK
T: + 44 20 7311 5278
E: bedria.bedri@kpmg.co.uk

Bia is a Partner and the Global Head of Cyber Security for KPMG's Financial Services practice. With over 18 years of industry knowledge, Bia leads large-scale complex transformation and change programs to enable financial institutions to effectively manage emerging cyber threats, risk and regulatory expectations while delivering business objectives, innovation and growth.

Charles Jacco
KPMG in the US
T: +1 212 954 1949
E: cjacco@kpmg.com

Charlie is a Principal and the Information Protection and Cyber Security Financial Services industry lead for KPMG in the US. He has extensive experience in multiple disciplines of the information security field including security strategy and governance, security transformation, digital identity, and cyber defense. Charlie brings a broad background in technology and infrastructure planning and transformation.

kpmg.com/socialmedia

Designed by Evalueserve.
Publication name: A smarter way to authenticate customers
Publication number: 136276-G
Publication date: June 2019