The new bank vs the old bank

CHANGING THE MINDSET TOWARDS OPEN BANKING

Private banks face significant security challenges with the advancement and growth of digital and mobile channels.

Frans Labuschagne

ATTRACTING AND RETAINING HIGH NET-WORTH INDIVIDUALS – FROM tech-savvy 35-year-old entrepreneurs to a more conservative 55-plus demographic – is placing strain on private banks. These institutions have to ensure that they protect the financial assets and information of customers who place a premium on privacy and security, but they also need to deliver a user experience that is both elegant and simple. User authentication lies at the core of that challenge.

Juggling act on tightrope

It is a balancing act complicated by a number of important factors. Many private banking clients are wary of adopting digital banking channels, especially for high-risk transactions involving large sums of money.

Others, particularly a younger cohort, are at home with the increasing seamless integration of digital platforms for social media, payments and banking. To them, one-click checkouts and on-the-go banking are welcome improvements in speed and convenience, and they expect their banks to continue streamlining digital interactions without exposing them to fraud.

In Europe, the Revised Payment Services Directive (PSD2) heralds an era of open banking, forcing financial institutions operating in SEPA countries to allow a host of third parties access to their customers' accounts if these customers consent to it. The aim is to foster competition and customer-centric innovation.

Some banks have underscored the importance of opening access to new entrants, saying that older and larger banks do not have to compete hard enough for consumers' business. In general, many are simply more hesitant about sharing banking data, for reasons such as fear of overloading data servers, but their reluctance to cooperate with the banking community can also be seen as a strategic move.

Open banking will necessarily require stronger user and transaction authentication. But the perceived friction inherent in two-factor authentication has been high on the agenda of private banking security groups, which are understandably reluctant to institute additional steps in their user authentication process.

Biometrics not the Holy Grail

There are those in the financial world that would favor a biometric login for online banking services. Their desire for a simpler login process is shared by their banks, but biometrics is not a cure for all ills.

Biometrics represents a leap forward in usability, but the approach is not, on its own, much more secure than the old-fashioned password. These irreplaceable identifiers represent a highly attractive target for hackers. To avoid their theft and ensure the sustainability of mass-market biometric-based security systems, industry bodies and mobile manufacturers require that these identifiers never leave the mobile device on which they were scanned.

A biometrics-protected mobile app never transmits the record for server-side matching; it simply attests that the fingerprint or voice pattern has been matched on the device. The concern is that fraudsters can very easily attest the same thing – without matching anything at all.

Risk-based authentication comes with own challenges

As with mass market biometrics, there have been significant advancements in machine learning technologies. These promise improved risk analysis based on past and present user behaviour and the state of the user's device as they access digital services

This approach is attractive to banks, because the data it requires to make a risk assessment is collected without the user's direct involvement. This allows access to at least some digital services with low to no friction.

Over-reliance on risk-based authentication may not translate into the desired outcome. A false positive could result in an account breach, and a false negative in a declined transaction – a key cause of the current prevalence of abandoned e-commerce carts. Card issuers are finding their top-of-wallet status threatened as consumers resort to competing institutions in frustration over risk-based declines.

What you really need to know

Biometrics and transactional risk analysis can play valuable roles in a layered security regime, but step-up (strong) authentication must be in place to secure high-risk transactions. Globally, regulators are demanding or advising that multi-factor, out-of-band authentication be used for sensitive transactions.

Meanwhile, banking and security companies are pointing to the 'digitalisation' of security as a trend that tracks very closely the rapid rise of mobile banking and payments. Dave Birch from Consult Hyperion predicted a year and half ago that the mobile phone would be the mass-market solution to the problems of recognition, relationships and reputation. He mentioned repeatedly that a model based on strong authentication against a local, revocable token held in tamper-resistant memory delivers the right platform.

So, no – SMS one-time passwords will not be making a comeback. Mobile's cryptographic capabilities and rich user interfaces offer so much more in security and ease of use. Many financial institutions are fast realising this as they respond to changes in consumer preferences, fraud vectors and government regulations. Gartner predicts that phone-as-a-token and out-of-band push modes will account for 80 per cent of the global authentication market in three years' time – up from just 15 per cent today.

International institutions are making strong statements in the direction in which regulators are moving on strong authentication. Consumers, on the other hand, are more demanding than ever of hassle-free, on-the-go access.

Selecting an authentication solution that combines the best security with low user friction will go a long way to meeting the requirements of these distinct groups, and help prepare private banks for years of swift change. The answer lies in deploying digital certificate technology to the mobile phone for out-of-band, multi-factor authentication, encrypted communication and advanced app security. •

Frans Labuschagne is country manager UK and Ireland at Entersekt, a Stellenbosch, South Africa-based company offering online push-based authentication and application security solutions for banks and enterprises. Founded in 2008, it provides online and mobile banking, mobile application, and card not present authentication services.