Prioritizing convenience and safety across the customer journey with passive authentication

Digital interactions are now ingrained consumer norms.

- More than 1 billion consumers globally are estimated to be using online banking and mobile payments over the next 10 years.
- Digital humankind consists of financial services generally IoT globally in 2022.
- 82% of new accounts are created via mobile channels, higher than all other use cases.

Globally networked fraudsters favor these easy and lucrative digital targets.

- 30% of the average value of failed and abandoned payments carried through are 
- 3% of the average value of failed and abandoned payments carried through is confirmed on the basis of two out of three elements:

- Passive authentication supports convenient digital interactions by utilizing multi-dimensional digital, cognitive and behavioral understanding.

- 3D Secure:

- Two out of three elements:

- The review process mandated by PSD2 has led to the development of the PSD3 draft proposal which will evolve requirements for prioritizing consumers’ interests, security and trust.

- The 3DS protocol (such as Verified by Visa and Mastercard’s SecureCode) provides an additional security layer for online credit and debit card payments and complies with PSD2.

- Strong Customer Authentication: What UK Merchants Need to Know from the EU Experience, 2022

- PSD2 mandates multi-factor authentication to verify the risk-appropriate verification for specific journey touchpoints to enable businesses to:

- Achieve differentiation in crowded digital marketplaces
- Control risk across the customer journey and realize competitive advantage

- Extra controls and step-ups can create operational roadblocks and negatively impact revenue

- Total fraud losses in 2021 were €25B.

- 99.7% of one large UK bank’s customers can log in without being stepped-up through 3DS in 2021.

- It is estimated that merchants in Europe lost €25B in revenue in 2021 due to implementing SCA.

- One in four of all financial institutions noted an increase in fraud.

- Cybercrime Report 2022

- Digital transactions are exposed not because they are more vulnerable, but because they are more engaging.

- High transaction volumes make multi-factor authentication costly and time consuming.

- In 2022, entirely driven by the mobile channel, the fraud attack rate in financial transactions increased by 31% in mobile and desktop channels.

- Digital transaction volumes across financial services grew by 29% globally in 2022.

- More than 2 billion customers globally were estimated to be using online banking and mobile payments in 2021.

- 78% of new accounts are created via mobile channels, higher than all other use cases.

- 30% of the average value of failed and abandoned payments carried through is confirmed on the basis of two out of three elements:

- High transaction volumes make multi-factor authentication costly and time consuming.

- In 2022, entirely driven by the mobile channel, the fraud attack rate in financial transactions increased by 31% in mobile and desktop channels.

- Digital transaction volumes across financial services grew by 29% globally in 2022.

- More than 2 billion customers globally were estimated to be using online banking and mobile payments in 2021.