

Prioritizing convenience and safety across the customer journey with passive authentication

DIGITAL INTERACTIONS ARE NOW INGRAINED CONSUMER NORMS

Online and mobile banking have been embraced at speed by consumers worldwide.

2B+



More than 2 billion customers globally were estimated to be using online banking in 2021 and this number is expected to exceed 2.5 billion by 2024¹

+29%



Digital transaction volumes across financial services grew by 29% globally in 2022²

78%



78% of new accounts are created via mobile channels, higher than all other use cases³

GLOBALLY NETWORKED FRAUDSTERS FAVOR THESE EASY AND LUCRATIVE DIGITAL TARGETS

The fraud attack rate in financial services increased by 31% in 2022, entirely driven by the mobile channel⁴

Automated bot attack volumes, high velocity automated attacks designed to mass-test stolen credentials, reached 1.9 billion in 2022, a 23% YOY increase⁶

Attack rates on digital payments also saw significant growth in 2022, up 27% year-over-year (YOY), with broad increases across all desktop and mobile channels⁵

There has also been a sharp rise in the number of login attacks through mobile apps — the attack rate increased by 104% in 2022, more than doubling YOY⁷

ADDING INCREASED RISK CONTROLS ON DIGITAL CHANNELS HELPS PROTECT CONSUMERS

Strong Customer Authentication (SCA): PSD2 mandates multi-factor authentication to verify the identity of consumers accessing their account online, initiating an electronic transaction or executing other transactions through a remote channel that might carry a risk of fraud. Multi-factor authentication is confirmed on the basis of two out of three elements:

Something they know (knowledge)
A PIN or password

Something they have (possession)
Their phone or device

Something they are (inherence)
A facial scan or fingerprint

3D Secure: 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.

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.

EXTRA CONTROLS AND STEP-UPS CAN CREATE OPERATIONAL ROADBLOCKS AND NEGATIVELY IMPACT REVENUE

-€25B



It is estimated that merchants in Europe lost €25B in revenue in 2021 due to implementing SCA⁸

30%



30% was the average rate of failed or abandoned payments challenged through 3DS in 2021⁹

- High transaction volumes make multi-factor authentication costly and time consuming to execute
- Increasing friction during low-risk interactions equals greater inconvenience for trusted customers
- Sophisticated fraud networks are beating strong customer authentication checks by leveraging social engineering and scams. Identity theft and scams were among the top types of fraud detected in high-growth markets globally in 2022.¹⁰

PASSIVE AUTHENTICATION BALANCES SEAMLESS CUSTOMER EXPERIENCES WITH DIGITAL SAFETY CONTROLS

Passive authentication supports convenient digital interactions by utilizing multi-dimensional digital, physical and behavioral identity context to help businesses recognize trusted users and spot suspicious anomalies in real time.

Device Binding: Strong ID creates a cryptographic bind between a customer's web/mobile browser/app and LexisNexis® ThreatMetrix® for persistent and secure device recognition, meeting SCA possession-based compliance for PSD2.

Mobile App Authentication: LexisNexis® Push Authentication streamlines step-up authentication for known/trusted devices by using a secure mobile banking app to authorize a desktop or mobile browser transaction.

Behavioral Biometrics: LexisNexis® BehavioSec® promotes passive authentication by analyzing the user from a trust and experience framework. BehavioSec® evaluates how a user interacts with a device, webpage or application in real time to dynamically differentiate between a legitimate customer, a bot or a fraudster.

CONTROL RISK ACROSS THE CUSTOMER JOURNEY AND REALIZE COMPETITIVE ADVANTAGE

Combining multi-factor and passive authentication tools in a layered approach helps optimize risk-appropriate verification for specific journey touchpoints to enable businesses to:

- Deliver highly-personalized customer experiences
- Enable risk-appropriate PSD2 and 3DS processing
- Achieve differentiation in crowded digital marketplaces
- Reduce costs and improve operational productivity

90%



90% of one large UK bank's customers can log in without being stepped-up via SMS, phone or email thanks to transparent device binding techniques¹¹

99.7%



Another large bank is using behavioral biometrics to authenticate 99.7% of their challenged 3DS transactions, significantly reducing the requirements on passwords or OTPs while creating considerable cost savings¹²

Read our [Global State of Fraud and Identity Report](#) for the latest insights into the identity trends, threat vectors and technologies impacting your business.



¹ Statista, Online banking users worldwide by region, 2020

^{2,3} LexisNexis® Risk Solutions Cybercrime Report 2022

⁴ CMSPI, Strong Customer Authentication: What UK Merchants Need to Know from the EU Experience, 2022

⁵ CMSPI, Article: PSD2: The European Payments Revolution, 2021

⁶ LexisNexis® Risk Solutions Digital Payments and Fraud in High-Growth Markets, 2022

^{11,12} LexisNexis® Risk Solutions Data Analysis, 2022