INSIDER INTELLIGENCE | eMarketer

JUN 08
Jenna McNamee

Tisa pilots digital ID program that provides interoperability and data security

Article

The news: The Investing and Savings Alliance (Tisa) will pilot its interoperable digital ID program for financial services this summer, per FinExtra.

Here's how it works: The program lets users set up and reuse digital IDs to interact with multiple financial institutions.

- It will simplify interactions like setting up new accounts, applying for mortgages, and transferring pensions.
- It streamlines **know your customer** (KYC) processes and improves connectivity for customers, productivity for institutions, and data security.

The pilot boasts participants such as **Lloyds**, **NatWest**, and **Barclays**. It's the product of a successful proof of concept (PoC) period with users from firms like **Fidelity** and **Ardent**. **Eighty-four percent of PoC participants** successfully used the digital ID to improve onboarding rates, reduce AML costs, and streamline the customer experience.

The scheme will use a single API and will meet all **Financial Conduct Authority** (FCA), KYC, and anti-money laundering (AML) standards. In the future, the program will increase its use of biometrics, machine learning and artificial intelligence (AI), and blockchain technologies before expanding to nonfinancial sectors.

Authentication in banking: Digital bank users value data privacy and their security. But they also want seamless access to their financial lives and are willing to use new technologies to merge the two.

- **73% of consumers** who access financial accounts via multiple devices are willing to log in with alternative authentication methods like biometric or multi-factor authentication, per a report from PYMNTS and Entersekt.
- Globally, **35% of banking customers** said what irritates them most is that the authentication factors keep changing.

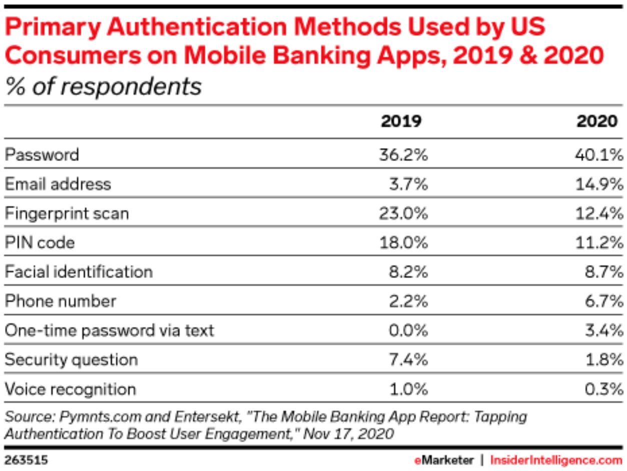
AI is still new: Customers' financial data is increasingly falling victim to theft as financial institutions digitize.

One way banks protect customer data is with AI. This technology can identify activity that doesn't match typical customer behavior and prompt further identification methods. But AI can be susceptible to unintended biases, and machine learning models can be trained with flawed data.

- Regulators in the US and UK haven't issued standards for using AI in banking but have highlighted the risks that can arise from it.

- But they have promoted the use of AI on the grounds that the benefits outweigh the risks.
- Given the lack of clear standards, banking agencies like the **Federal Reserve** and the **Office of the Comptroller of the Currency** (OCC) indicated that traditional banking rules apply to AI.

The big takeaway: If the pilot is successful, it could bridge the gap between the demand for frictionless banking and strong data security. The program could also play an instrumental role in shaping regulation and standards around the use of AI.



Primary Authentication Methods Used by US Consumers on Mobile Banking Apps, 2019 & 2020

% of respondents

	2019	2020
Password	36.2%	40.1%
Email address	3.7%	14.9%
Fingerprint scan	23.0%	12.4%
PIN code	18.0%	11.2%
Facial identification	8.2%	8.7%
Phone number	2.2%	6.7%
One-time password via text	0.0%	3.4%
Security question	7.4%	1.8%
Voice recognition	1.0%	0.3%

Source: Pymnts.com and Entersekt, "The Mobile Banking App Report: Tapping Authentication To Boost User Engagement," Nov 17, 2020

263515 eMarketer | InsiderIntelligence.com