MARCH 2020

DIGITAL IDENTITY TRACKER®

NATWEST'S BIOMETRIC PAYMENT CARD PUTS AUTHENTICATION AT CUSTOMERS' FINGERTIPS

Page 6 (Feature Story)

PYMNTS.com

Digital ID solutions for banks

Bank of Thailand authorizes biometrics for customer onboarding at Thai banks

Biometrics are becoming more popular in the global banking sector, as well. The Bank of Thailand, the country's central bank, recently authorized facial recognition verification for remote account openings, also called electronic know your customer (eKYC) checks. Customers can now biometrically verify their identities at six banks across the country: Bangkok Bank, Bank of Ayudhya, CIMB Thai Bank, Kasikornbank, Siam Commercial Bank and TMB Bank. These financial institutions (FIs) cross-reference applicants' biometric data through Thailand's national digital identity program, which contains records from several types of government sources.

The Bank of Thailand hopes the new onboarding process will reduce participating FIs' identity theft and fraud experiences, and that it will encourage facial recognition adoption among other businesses nationwide. It also plans to expand authorization to several other banks, pending analysis of the new system's performance.

South Africa's Standard Bank deploys facial recognition security layer

South Africa-based Standard Bank, Africa's largest lender by assets, recently rolled out a new biometric security system called DigiMe. The system leverages facial recognition biometrics to verify mobile banking customers, which Standard Bank said has become significantly more sought-after in recent years. Consumers can use the bank's app to remotely activate the new security feature, proving their identities with selfies and passports or other documents.

The new system is Standard Bank's latest security upgrade initiative. It recently introduced quick-response (QR) codes and multifactor authentication (MFA) to protect its mobile offerings from fraud, and it plans to deploy these features in conjunction with the biometric system.

Bank of Uganda to develop digital ID system for bank customers

Digital identity solutions are also making their way to Uganda. The nation's central bank, the Bank of Uganda (BoU), has partnered with FinTech Laboremus Uganda to develop a digital ID verification system for FIs. BoU's servers will host the solution, which will function as a shared gateway for banks to cross-reference applicants using Uganda's national ID cards. BoU plans to make the system available for all Ugandan banks and financial service providers.

The solution will accelerate authentication protocols by replacing manual processes. BoU also hopes that the new system will boost banking service access to Ugandans in rural areas and that it will fuel additional financial service innovations.

New biometric technologies and solutions

SenseTime develops biometric ID system to identify masked faces

Global developments are pushing firms to improve and adapt their biometric technologies. The recent coronavirus outbreak that originated in China presents a particular challenge to ensuring facial recognition accuracy due to face masks' prevalence, prompting Hong Kong-based developer SenseTime to launch a system that uses a combination of thermal imaging and body and facial image data to identify individuals wearing medical masks. The system's camera can sense individuals' body heat and locate their foreheads to verify their identities.

The Chinese government is reportedly using the technology to monitor individuals who have been exposed to the coronavirus, including those who may fail to follow quarantine restrictions. Widespread mask usage has challenged China's existing facial recognition-based state surveillance protocols, which means mask-compatible biometric technology will be valuable even after the outbreak ends.

GreatHorn to launch typing biometric analytics solution for email ATO protection

Cloud email security provider GreatHorn has created its own biometric solution, recently adding a typing analytics function to its platform. The system leverages analytics, data science and machine learning (ML) to study users' typing patterns, authenticating them through variables such as frequency, pattern anomalies and delays. Administrators can adjust the error margins before the system determines users are fraudulent.

This offering can replace passwords or MFA measures, which can be bypassed via social engineering and phishing attacks. It is currently available in beta and is expected to roll out later this year.