Environ
Commitment To Growth and Development

Strengthening of telephone call centre and mobile money with Envrion-Lumenvox active Voice authentication

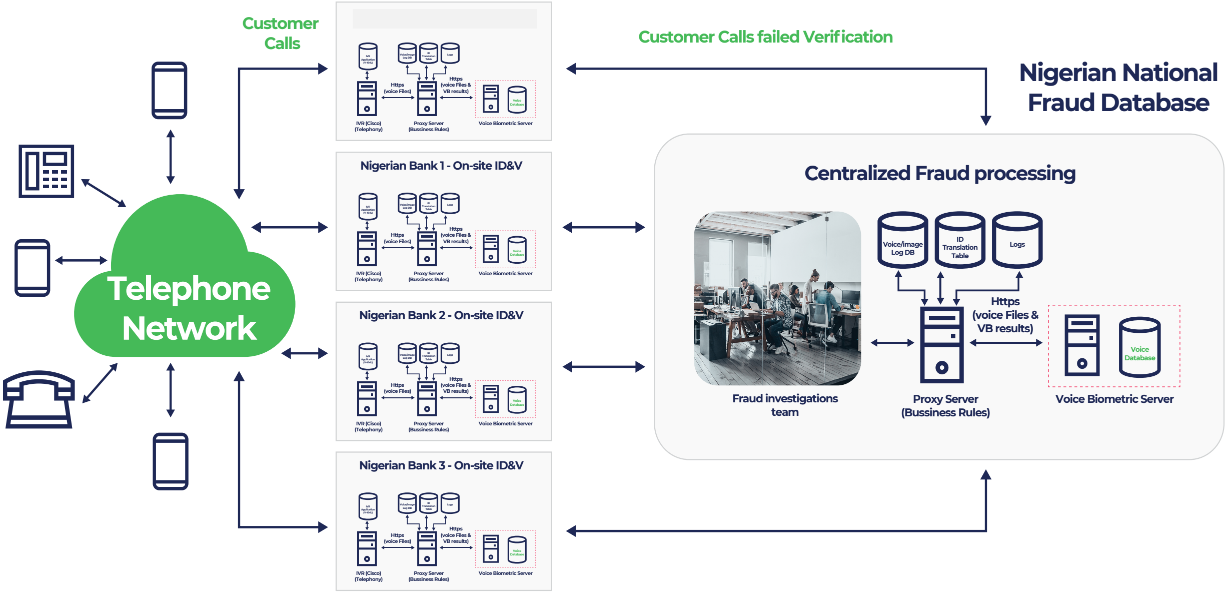
DATASHEET

Helping to defend against financial crime whilst revolutionising the customer phone experience

Streamlined calls and mobile transactions with a centralised database of known fraudsters

The Client: A bank, retailer or etailer, mobile phone operator, or a government digital operation center located in Nigeria Africa, launch their new customer experience to meet a critical need of processing mobile application authentication replacing pins, tokens and passwords: Within emerging markets, many customers are 'unbanked', however, mobile phones usage is prolific and a rapid-growing niche. In response, the recent demand is to allow customers to easily set up a bank account and make financial transactions digitally. The platform finally offers these customers a financial services solution which enables their active participation in the economy in a safe and secure manner.

A social inclusive non-discriminative system is required to process high volume low value transactions and where voice biometrics can address channels of phone authentication. As part of a wider holistic solution this function could work in conjunction with a Finger Vein biometric system that would cover physical authentications in the office for staff digital signatures, retail electronic PoS and ATM transactions. The end user customer will recognise the benefits of using biometrics – both vein and


Customer Calls
Telephone Network
Customer Calls failed Verification
Nigerian National Fraud Database
IVR Application (V-XML)
Voice/Image Log DB
ID Translation Table
Logs
Https (voice Files)
Https (voice Files & VB results)
Voice Database
IVR (Cisco) (Telephony)
Proxy Server (Bussiness Rules)
Voice Biometric Server
Nigerian Bank 1 - On-site ID&V
Nigerian Bank 2 - On-site ID&V
Nigerian Bank 3 - On-site ID&V
Centralized Fraud processing
Fraud investigations team

voice. At the same time, they envision a more seamless, remote and digital process, one that will not require engagement with a live agent or a physical location.

To fulfil the voice biometric component of the process, the client will require an authentication solution provider to implement Environ-LumenVox Active Voice Biometrics within a digital identity platform. Users will be able to register their voice password with a simple statement: “At [NAME of COMPANY] my voice is my password.” On subsequent calls these registered users can then use this same phrase to quickly validate their identity and secure transactions.

The Client’s Mobile Money solution now features self- service PIN reset using active Voice Biometrics, with fall-back options to facilitate the resetting of PINs in-store or via a mobile app. The next phase of security integration will introduce Facial Recognition.

By including biometrics, the Client will be able to design a complete digital customer journey that ticks all boxes: greater security, improved customer experience and strict compliance.

Fingerprint, facial and Iris systems both have the credibility of long-time use by national and governmental organisations in many countries. However, these modalities have been proven to be far more disproportionate in application performance failure for black and people of colour population citizens.

Biometric considerations for African users and countries with black and people of colour citizen populations

In 2005 the UK government scrapped the use of Iris recognition for the UK immigration services as the False Rejection rate (FRR) was too high within identifying black and ethnic citizens representing 13% of the UK population. The official FRR of Iris recognition is at 10%, although this number is considered to be significantly higher amongst black and ethnic individuals hence the decision taken by the UK Home Office to remove the use of Iris recognition. In 2018, MIT computer scientist, Joy Buolamwini, conducted an exercise to test the application of Facial Recognition biometrics for black female individuals. Her results concluded figures as high as 35% FRR amongst this segment of individuals. This is a worrying development given this form of biometric facial recognition system is used in the United States (US) by the FBI. The US Government Accountability Office (GAO) analysed the FBI biometric results recording an FRR of 15% for overall results. However, this number is considered to be significantly higher and possibly closer to an FRR of 50% amongst US black population citizens. The late Elijah Cummings, a US congressman for Maryland, called for the FBI to test its technology for racial bias given this category of individuals are subjected to this type of technology more than any other group of US citizen.

The National Fraud centralised biometric database

The use of both Voice and Finger Vein biometrics can be allied to work side-by-side, at the point where Finger Vein carries out authentications where there is less environmental noise pollution (critical for voice speech recognition), secondly Vein biometrics are seen to score the highest optimum security performance levels and practicality scoring False Acceptance rate of 1/1m (0.0001%) for 1:1 and a 0% False Rejection Rate (FRR) biometric matches requiring less than 2 seconds for a correct accurate match. Therefore, for lower value transactions (NIP) or call centre support calls, Voice biometrics is a perfect fit to complete the customer digital journey. Like Vein biometrics, voice is a 1:1 match in order to process the authentication match to the voice print database in 2 seconds. However, there is a 1:N capability in making the match of a known fraudster imposter to a centralised database of known attempted flagged imposters. Once a known fraudster or individual that has not been able to authenticate using the automated voice print is flagged, this caller can now be diverted to a live call centre agent for further verification or to be rejected from the system and forwarded to the law enforcement agencies. This type of capability would be a first in the country and a game changer in protecting against cybercrime.