5 STEPS

TO DIGITAL TRANSFORMATION FOR A LEADING INDIAN BANK

How one bank is capitalizing on shifts in consumer behavior to grow its business, prevent fraud and provide customers with a positive experience

One of India's leading banks, which caters to retail and corporate customers across urban and rural India, has embarked on a five-step process to a safe, effective digital transformation.

Step 1

Launch a digital alternative to branches and ATMs

When demonetization happened in India in 2016—taking 92% of the currency out of circulation—the bank saw an opportunity to be a part of India's journey to go cash-free. It launched one of India's first digital bank accounts. Customers could open an account and complete all Know Your Customer (KYC) formalities on their smartphone in under 10 minutes.

Step 2

Introduce Video KYC for customer onboarding

As part of its start-to-end, fully-integrated, zero-contact, completely digital and paperless account opening process, the bank initiated a Video KYC facility for customer onboarding. Customers could use it to open savings accounts in its digital portfolio of products.

Video KYC eliminated the need for an individual to visit a branch or have an in-person interaction, biometric verification or sharing of physical documents. Instead, through a video call, KYC documents could be verified, the customer's signature noted, and the entire video process recorded and stored by the bank.

Step 3

Implement ThreatMetrix® to prevent fraud

As the bank launched its digital platform, it wanted to ensure protection from fraud for its customers and its enterprise. It chose LexisNexis® ThreatMetrix® to help differentiate between genuine customers and people or bots attempting to commit fraud across the digital journey.

LexisNexis® Risk Solutions did a "health check" on the bank to assess its accounts and uncovered some surprising facts that could then be used to create rules bolstering the bank's fraud defense:

- Fraudsters often fired **IP velocity** rules (using the same IP frequently in a short time frame)—fraud rate of **68%**
- Fraudsters often **connected from airports**—fraud rate of **18%**
- Fraudsters often **used private browsing**—fraud rate of **13%**
- Fraudsters often **used a proxy**—fraud rate of **2.2%**
- The **anomaly score** could help predict risky behavior—high scores have a fraud rate of **3%**
- The **overall behavioral biometrics score** could help predict risky behavior—high scores have a fraud rate of **2.2%**
- Low scores for **overall behavioral biometrics score** and **fraud score** could help predict trusted behavior and reduce the False Positive Rate (FPR)
- **The bank's base fraud rate was 0.8%**

Step 4

Apply biometrics and smart learning

To optimize the bank's fraud defenses further, the bank may choose to implement LexisNexis® Behavioral Biometrics and Smart Learning functionality on top of ThreatMetrix. Modeling on the bank's historical data showed that if the optimized model were in place during the historical evaluation window, the bank's fraud capture would have increased from 0% to 52% with a 3.5% impact to FPR. The bank can expect to see this performance in the live production environment if they implement the recommended changes.

Step 5

Continually improve the digital and mobile experience for customers

- Provide customers with digital banking experiences on par with the seamless, personalized, brand-building experiences they have with online retailers and other businesses.
- Offer mobile access to more products and services such as phone-based lending. The mobile channel is critical. In India, the ongoing shift to 4G roaming and cheaper smartphones has created many customers who are not just mobile-first; they're mobile-only.
- Reach the under-banked and un-banked as connectivity and broadband infrastructure come to semi-urban and rural India.
- Explore offering banking across other non-proprietary channels such as Siri, Alexa and Google Assistant.
- Expand intelligent automation like machine learning or artificial intelligence to better serve customers.

LexisNexis ThreatMetrix combines digital insights, analytic technology and embedded machine learning to detect and prevent more fraud, reduce false positives and ensure a positive customer experience.

To request a free demo

visit risk.lexisnexis.com/ThreatMetrix

LexisNexis® RISK SOLUTIONS