6 STEPS

TO DIGITAL TRANSFORMATION FOR A LEADING ASIAN BANK

How one bank handled a surge in online and mobile banking while improving its fraud security

With more customers switching to online and mobile banking every day, a large commercial bank in Asia knew it was overdue in evaluating its fraud prevention security and regulations compliance. With the help of LexisNexis® ThreatMetrix,® the bank followed a six-step process to a safe, effective digital transformation.

Step 1 Migrate customers from branches and ATMs to digital and mobile banking

The bank offered a hybrid digital integration strategy that made use of its numerous branches and ATMs and its online banking and mobile platforms. By 2021, mobile accounted for 10 times the transactions of the bank's browser-based product. The bank accelerated growth by making customer activation of mobile banking extremely easy. External factors, such as COVID-19, also contributed to the rapid development of its mobile channel.

Step 2 Differentiate trusted customers from fraudsters and bots

The bank needed a 360-degree view of identity risk of its online customers at every point in the customer life cycle to:

- Screen new and existing customers to keep fraudsters out
- Monitor transactions to prevent potential fraud
- Avoid money laundering and illicit finance risks

Step 3 Launch LexisNexis® ThreatMetrix® on its internet banking platform

LexisNexis ThreatMetrix was added to its browser-based internet platform. The platform had fewer users than its mobile counterpart and would serve as a good starting point. What it quickly revealed to the bank was alarming:

- **Unknown sessions:** 40% of events were from unknown sessions, meaning the API call differed from the profiling ID, suggesting fraud.
- **Mule accounts:** Some customers were potentially laundering money.
- **Multiple devices:** Some customers were using a large number of devices, and some devices were connected to multiple accounts, both of which could indicate fraud.
- **Excessive logins:** Some customers were logging on thousands of times a day. The bank learned they were aggregator bots from accounts used as mules for illegal gambling.

Step 4 Investigate areas of concern

With information from ThreatMetrix, the bank was able to resolve any false positives, monitor suspicious accounts and close accounts that were clearly fraudulent. It could also share real-time data intelligence with ThreatMetrix to collectively fight complex fraud with other businesses.

Step 5 Apply biometrics to identification

In the next phase, LexisNexis® Behavioral Biometrics will be added to the bank's workflow as another layer of fraud defense. Behavioral Biometrics provides additional risk signals across account openings, high-risk pages and payments by analyzing the way a user interacts with a device and differentiating between different user profiles.

Step 6 Look toward the future

The bank has implemented ThreatMetrix on its browser-based and mobile platforms. As the bank adds more functionality to mobile like real-time payments and opens the platform to third-party payers, it will be increasing its risk exposure, making fraud security all the more important.

The dynamic threat intelligence from ThreatMetrix will improve the bank's fraud defenses in the following areas:

- **Streamline onboarding:** Optimize screening workflow that meets regulator expectations and keeps fraudsters from entering its eco-system.
- **Screen transactions:** Assess transactions in near real time, minimizing friction for customers while preventing fraud.
- **Increase functionality:** Allow customers to fully manage their financial transactions safely via their phone.
- **Add cardless ATM:** Permit customers to use their phone to get cash in an ATM, making security on mobile even more critical.
- **Welcome third-party payers:** Add more payment services through the mobile banking app.
- **Implement ThreatMetrix on corporate products:** Leverage ThreatMetrix across other lines of business.

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