LexisNexis®
RISK SOLUTIONS

CASE STUDY

# LexisNexis® Digital Identity Network® Helps *Boost*, a Malaysian Ewallet Provider, Detect Fraudulent Use of Its App

## AT A GLANCE

### CUSTOMER

Boost™

Boost

### REQUIREMENTS

- Protect existing customers from fraudulent account takeovers
- Eliminate registration of fraudulent accounts
- Increase the return on investment of promotions

### SOLUTION

Malaysian ewallet provider Boost started using identity intelligence from our Digital Identity Network® to reliably differentiate between trusted and fraudulent online behavior. Our fraud detection happens automatically in near real time, so there's no delay to Boost's service or the customer experience. It works by identifying the device and location, and running behavior data to help discover high-risk scenarios.

### BOTTOM LINE

- There was a significant reduction in fraudulent account takeovers.
- Fewer accounts were created by malicious users.
- We were able to help prevent, detect and eradicate threats to offer a more secure and safer business transactions environment for merchants.

CASE STUDY

*"LexisNexis® Risk Solutions has helped prevent fraudulent account registrations and protect our existing customer base. We've also managed to devise solutions to reduce first-party fraud."* — Boost

## Overview

One of our channel partners, Level Five Asia, knew first-hand how LexisNexis® Risk Solutions could help Boost with their security and helped lay the foundations for our relationship with them.

Boost is a homegrown, Malaysian, lifestyle ewallet that was created to disrupt the status quo. It aims to combine lifestyle needs with cutting-edge digital technology to make transactions fast, secure and rewarding.

Since they launched the app in 2017, Boost has offered their customers cashback rewards, vouchers and exclusive promotions for using their ewallet, among a suite of other services.

## Business problem

People are switching their everyday lifestyle to digital, including paying for goods and services through an ewallet. This has prompted a dramatic rise in online transactions.

However, ewallet providers are stuck treading a fine line between providing the smoothest possible experience for their customers (new and existing) while protecting themselves from fraudsters taking advantage of the anonymity provided by digital channels.

Fraudsters continue to be masters of impersonation, cloaking themselves with genuine customer data to appear wholly convincing in creating a new ewallet account. There is no shortage of stolen data available on the dark web, and this is constantly updated with fresh pickings from the continual stream of global data breaches.

## To prevent Boost from being used as a financial crime conduit, the software:

- **Uses security protocols to detect and prevent fraud**
- **Identifies fraudulent transactions**

CASE STUDY

## Building a picture of true digital identity at each stage of the online journey

The solution for Boost started with being able to reliably recognize trusted, returning customers and merchants, regardless of when and where they transact. We observed and reviewed transaction patterns to help design rules to block dubious transactions.

LexisNexis® ThreatMetrix® enabled us to collate intelligence relating to the customer's device, location, online behavior and payment credentials, building up a complete digital identity of every transacting user.

The Digital Identity Network solution collects and processes millions of global transactions across thousands of websites every day, helping to piece together the digital footprint of online users across businesses, industries and locations.

This capability meant that any behavior deviating from this trusted profile would be flagged to Boost in near real time. Any unusual logins or transactions from new locations were quickly identified.

## Leveraging trust to identify account takeover in near real time

Regardless of whether a fraudster was in possession of genuine login credentials, LexisNexis ThreatMetrix was able to flag if the transaction was:

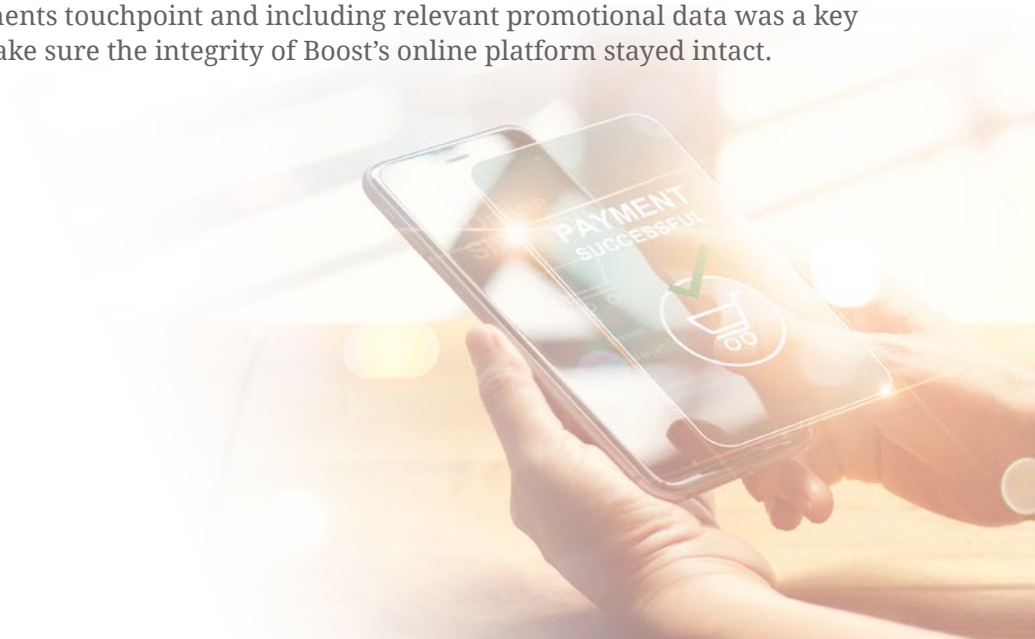
- **coming from a new or high-risk device**
- **in an unusual location we haven't previously associated with the user**
- **being made by manipulated or virtual devices**

In these cases, Boost could block login attempts that were deemed high-risk, protecting good user accounts without imposing unnecessary friction.

## Harnessing global shared intelligence to reliably risk-assess online payments

The ultimate endgame for a fraudster is to "cash-out". That could be by monetizing stolen credit card or banking details or abusing promotions run by Boost.

Securing the payments touchpoint and including relevant promotional data was a key requirement to make sure the integrity of Boost's online platform stayed intact.



## Boost's online platform was underpinned by the following core capabilities from LexisNexis ThreatMetrix:

- **ThreatMetrix SmartID®**: Identifies returning users that wipe cookies, use private browsing and change other parameters to bypass device fingerprinting. This improves returning user detection and reduces false positives. Derived from the analysis of many browsers, plug-in and TCP/IP connection attributes, ThreatMetrix SmartID is based exclusively on device attributes to improve the detection of returning visitors, especially those trying to elude identification.
- **ThreatMetrix Mobile**: A lightweight software development kit (SDK) for Google Android and Apple iOS mobile devices, providing complete fraud protection for Boost's mobile app. This includes advanced persistent device identification, anomaly and device spoofing detection, application integrity evaluation, malware detection, location services, jailbreak and root detection technologies.
- **TrueIP**: Reliably detects the use of location and identity cloaking services, such as hidden proxies and VPNs, allowing Boost to see the true IP address, geolocation and other attributes of each transaction.
- **Champion Challenger**: Helps Boost to determine the effectiveness of policy changes, as well as fine tune policies to keep pace with changes in consumer behavior and to stay ahead of emerging fraud patterns.
- **LexisNexis Risk Solutions Professional Services**: Provides hands-on fraud expertise, tailoring the LexisNexis ThreatMetrix solution to meet the unique and evolving requirements of Boost. The team helps to continually optimize rules and policies to ensure that the full spectrum of fraud attacks are effectively detected, while minimizing false positives and manual reviews.

For more information, visit risk.lexisnexis.com/FIM-EN

LexisNexis® RISK SOLUTIONS

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.