LexisNexis

RISK SOLUTIONS

LexisNexis® ThreatMetrix® Helps Safeguard Emirates Skywards Customer Loyalty Program

AT A GLANCE

CUSTOMER

Emirates Airline – Skywards

REQUIREMENTS

- Protect Emirates Skywards members' accounts from account takeover.

- Protect Emirates Skywards miles against unauthorized redemptions.

- Protect Emirates Skywards members' data from data breach.

SOLUTION

With LexisNexis® ThreatMetrix®, Emirates Skywards can detect and block unauthorized account takeover by reliably distinguishing between trusted and high-risk behavior; analyzing attributes relating to devices and location information. Leveraging global digital identity intelligence, Emirates Skywards is able to detect anomalies in good customer behavior and shift to a more proactive approach when detecting and blocking suspicious behavior and activities.

BOTTOM LINE

The solution helps Emirates Skywards in:

- Near real-time monitoring of member activities and differentiating between genuine versus suspicious activities.

- Minimizing friction for trusted members.

- Improving operational efficiencies by reducing the volume of manual reviews.

Overview (Pre-COVID-19)

Emirates is the largest airline in the Middle East, with 56 million passengers flown in 2019-20. Based in Dubai, United Arab Emirates, the airline operates over 3,600 flights per week serving 155 countries in 81 countries from its hub at Dubai International Airport and is the fourth largest airline in the world in terms of international passengers carried.

In a competitive industry driven by passengers seeking low cost fares, Emirates rewards frequent flyers with its Skywards loyalty program. Passengers accrue Emirates Skywards miles by flying with the airline and through many of Emirates Skywards partners and can then redeem miles earned for a myriad of flight and non-flight benefits, including flight upgrades, reward tickets and redemption options from a diverse portfolio of Lifestyle, Leisure and Retail partners.

Business Challenge

Emirates Skywards wanted to protect the value of its loyalty program miles, with a solution that could:

- **Protect Emirates Skywards member accounts from unauthorized access, while minimizing friction for good, returning customers**

  Loyalty programs are seen as a lucrative opportunity by fraudsters who aim to redeem miles accrued by genuine customers. Having taken over a member account, fraudsters look to profit from the monetary value of free flights, upgrades and other rewards on offer and in some instances from members' data.

  Emirates Skywards wanted a solution that not only protects customer accounts from unauthorized access, but also preserves a frictionless member experience across key touchpoints throughout the member's journey.

- **Promote proactive fraud monitoring**

  Fraud monitoring was carried out based on exception reporting which was a reactive approach in nature. Emirates Skywards was therefore looking for a solution which would enhance its fraud monitoring from a reactive to a proactive approach.

Harnessing Global Shared Intelligence to Protect Against Fraudulent Member Account Activities

Deployed across various member activities, LexisNexis ThreatMetrix helped to protect customer accounts, data and miles across digital and offline channels using a number of key capabilities, including:

Digital Identity Intelligence: Helped Emirates Skywards detect high-risk events in near real time. The LexisNexis® Digital Identity Network® collects and processes global shared intelligence from millions of daily consumer interactions including logins, payments, and new account applications. Using this information, the ThreatMetrix solution creates a unique digital identity for each user by analyzing the myriad connections between devices, locations, and anonymized personal information. Behavior that deviates from this trusted digital identity can be reliably identified in near real time, alerting Emirates Skywards to potential fraud.

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, SmartID is based exclusively on device attributes to improve the detection of returning visitors, especially those trying to elude identification.

TrueIP: Reliably detects the use of location and identity cloaking services, such as hidden proxies and VPNs, allowing the airline to see the true IP address, geolocation and other attributes of each transaction.

Persona ID: Links current transactions to related transactions in near real time. The rules-based mechanism links transactions via a matrix of attributes associated to the customer's device and connection. It uncovers anomalous behavior in near real time through the association of related historical activity.

LexisNexis®
RISK SOLUTIONS

For more information, visit risk.lexisnexis.com