CASE STUDY

LexisNexis® ThreatMetrix® Helps Ride-Hailing Pioneer Careem Detect and Block Fraudulent New Passenger Applications in Near Real Time

AT A GLANCE

CUSTOMER

Careem

REQUIREMENTS

- Prevent fraudsters registering new passenger accounts.
- Detect patterns of high-risk behavior.
- Enhance the identification of trusted customers, streamlining the user experience.

SOLUTION

Leveraging global digital identity intelligence, LexisNexis® Risk Solutions helped Careem enhance fraud detection on new passenger applications submitted to its ride-hailing platform. The ThreatMetrix® solution helped Careem build a more reliable profile of trusted customer behavior; improving the detection of genuine fraud, while maintaining a frictionless experience for good customers.

BOTTOM LINE

- Reliably detected fraudulent new passenger applications in near real time.
- In Q1 2020, the ThreatMetrix solution helped identify 30% of all fraudulent new passenger applications.

> “Fraudsters are masters of disguise, and we needed to ensure that we could find them amongst all of our good customers. With LexisNexis ThreatMetrix we were able to differentiate good applications from bad, without impacting the user experience for our customers.”
>
> — CAREEM

Overview

Careem is a pioneer of the ride-hailing economy, offering mass transportation, delivery and payments across the Middle-East region. Founded in 2012 and acquired by Uber in 2020, Careem operates in over 100 cities across 14 countries, with over one million drivers, or ‘Captains’, providing transportation to more than 30 million customers.

Careem’s mission is to simplify and improve the lives of people, while building an organization that inspires the community it serves. Having created more than one million employment opportunities in the region, Careem is expanding services in order to become the region’s everyday ‘SuperApp’.

Business Problem

Ride-hailing apps and services are central to the Sharing Economy. Fueled by mobile technology, the Sharing Economy has disrupted businesses across the world, with the peer-to-peer model revolutionizing how people interact in the growing digital economy. Fraudsters have been quick to see the opportunity amidst the disruption caused by this new way of doing business, evolving attacks to exploit weaknesses in apps and online platforms.

Careem was seeing a range of attacks targeting new passenger applications from fraudsters trying to abuse the ride-hailing platform. These included:

- **Bonus Abuse:** Fraudsters create fraudulent passenger accounts in order to target the increased commission or bonus drivers receive for making a certain number of journeys, or picking up passengers at locations such as airports.
- **App Cloning:** Fraudsters create fake passenger accounts and then use an app to clone and run those multiple accounts from the same app simultaneously. This enables a fraudster to be both the passenger and driver on the same device. As passenger and driver, the fraudster can clock up multiple journeys which did not occur.
- **Monetizing Stolen Credentials:** Fraudsters use stolen credentials to create accounts, monetizing these through loyalty vouchers or rides.

In order to protect the platform from fraudsters seeking to exploit free bonuses or stolen credentials, Careem was looking for a solution that can help detect high-risk applications before accounts are created.

CASE STUDY

> “Simplicity is a key aspect of our mission as an organization. We required a solution which would detect increasingly complex mobile attacks and fraud, while maintaining our simple, friction free user experience. The ThreatMetrix solution delivered just that.”
>
> — CAREEM

The Power of Global Shared Intelligence to Streamline and Protect the User Experience

The best way to tackle complex, global cybercrime is using the power of a global shared network. 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, Careem is able to better distinguish between trusted customer behavior and potential fraud.

Harnessing Global Shared Intelligence to Protect Against Fraudulent Passenger Applications

Deployed on new passenger applications, LexisNexis ThreatMetrix enhances fraud detection and the protection of customer accounts using a number of key capabilities, including:

Digital Identity Intelligence: Helped Careem 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 Careem to potential fraud.

ThreatMetrix Mobile: A lightweight software development kit (SDK) for Google Android and Apple iOS mobile devices, providing complete fraud protection for the mobile channel. This includes advanced persistent device identification, anomaly and device spoofing detection, application integrity evaluation, malware detection, location services, jailbreak and root detection technologies.

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 Careem 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 device and connection. It uncovers anomalous behavior in near real time through the association of related historical activity.

CASE STUDY

> “With the ThreatMetrix solution we gain innumerable insights about those who use our services and platform — both the good and the bad. For example, we can now see if a passenger is faking or hiding their current location, or if multiple applications are coming from the same device — these insights allow us to protect our customers, which is key.”
>
> — CAREEM

LexisNexis® RISK SOLUTIONS

For more information, visit risk.lexisnexis.com

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.