Intelligence from LexisNexis® ThreatMetrix® Helps Spanish Wallapop better Detect Fraudulent Activity Across the Customer Journey

AT A GLANCE

CUSTOMER

Wallapop

REQUIREMENTS

• Provide a more secure user environment for customers, establishing trust between buyers and sellers
• Detect new account opening fraud and returning fraudsters
• Improve reputation and brand while protecting customers from fraud

SOLUTION

Wallapop, the leading platform for a more human, sustainable and responsible method of consumption, leverages digital identity intelligence from the LexisNexis® Digital Identity Network® to reliably differentiate between trusted and fraudulent online behavior in near real time. Device, location and behavior data help the retailer identify high-risk scenarios.

BOTTOM LINE

• Improved capability to detect fraud and returning fraudsters with high accuracy
• Significant uplift in fraud detection rates
• Provided trusted customer insight and customer protection from fraud
• Aided a secure user environment and trust in transactions
• Enabled operational efficiency
Overview
Wallapop’s geo-localized technology connects a community of 15 million users by offering an easy and convenient way to buy and sell items that are no longer used. The platform, which has found a second home for more than 180 million items, provides people with access to unique goods at great prices, while extending the life of fully functional products. Since its inception, Wallapop has been committed to FROWLQXRVLQQRQYDLRQLQWKRQQLQHQFDVVL4HGVLQGXVWUIDGVPXRBJQCDGQPDUN aspires to use technology to contribute to sustainability.

Business Problem
Today, more than ever, customers are turning to e-commerce, prompting a dramatic and steady rise in online transactions. +RZHYUROQLQHUWLOHCLUDLOUVDFUXFNEHWFHHOSRLGLQWKHVPRWRKHWWSRVLQWEOH experience for customers (new and existing) and protecting themselves from IUDXGVWHUVZKRDNDQYDQWDJHRIWQHDQRQPLWSURLYGHEGLJLWDOFDQDOHOV Wallapop brings together buyers and sellers by offering them an easy and convenient way to buy and sell items that are no longer used. Fraudsters, however, have RFFDVLRQDOOWULHGWRH[SORLWVKHSOWIRUPDOOSSZDVOORNLOJIRUDVROXWLRQWKDVLQWU could maintain the integrity of the platform for the enjoyment and success of good XVHUVZKLOONLQLQWKHIUDXGVWHUVRXW

Key Pressure Points for Wallapop Included:
• Working on maintaining a secure environment for trusted users and interactions
• Detecting fraudsters establishing new accounts
• Identify returning fraudsters using new identities

“LexisNexis ThreatMetrix® helped us detect fraudsters before they could create any friction or harm to our users. This was vital to provide the best experience to our users.” — Wallapop
Building a Picture of True Digital Identity at Each Stage in the Online Journey

The design of an effective solution for Wallapop started with being able to reliably recognize trusted, returning customers, regardless of when and where they transact. LexisNexis ThreatMetrix® helps Wallapop collate intelligence relating to the customer’s device, location, online behavior and credentials, building up a complete digital identity of every transacting user. Not only was this intelligence harnessed from Wallapop transactions, but it was also collated across all transactions relating to the LexisNexis Digital Identity Network® transactions across thousands of websites every day, helping to piece together the digital footprint of online users across businesses, industries and locations.

Using this information, the Digital Identity Network 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 Wallapop to new users who may be using stolen identity data, obfuscating their location or attempting to sign up for multiple accounts from the same device and other such scenarios.

Leveraging Trust to Identify Returning Fraudsters in Near Real Time

Regardless of whether a fraudster is in possession of genuine identity information, LexisNexis ThreatMetrix could flag the fact that the transaction was coming from a returning digital persona that was associated with previous fraud, an unusual location not previously associated with the trusted user, or at a velocity that was anomalous as returning fraudsters. This protected good customers and improved Wallapop’s reputation for providing a trusted online user marketplace and safe interactions.

“LexisNexis ThreatMetrix is key for having a better understanding of the potential risk of each new user.”
— Wallapop
The Wallapop solution 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, 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 the Wallapop 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 Wallapop to see the true IP address, geolocation and other attributes of each transaction.

- **LexisNexis Risk Solutions Professional Services**: The LexisNexis Risk Solutions Professional Services team provides hands-on fraud expertise, tailoring the LexisNexis ThreatMetrix solution to meet the unique and evolving requirements of Wallapop. The team helps to continually optimize rules and policies to ensure that the full spectrum of fraud attacks is effectively detected, while minimizing false positives and manual reviews.