LexisNexis® RISK SOLUTIONS

LexisNexis® ThreatMetrix®
Helps Gaming & Gambling Company Detect Real Time Fraud

Requirements

- **Profile devices to enhance identification of trusted customers**
- **Detect patterns of high-risk behavior**
- **Reduce gaming & gambling bonus abuse**

Results

$195K
saved in fraud for deposits

73%
of attempted bonus abuse registrations flagged to reject in H1 2021

Streamlined
user experience while preventing fraudsters in near real time based on digital identity intelligence

> We chose LexisNexis® ThreatMetrix® before it became a part of LexisNexis® based on the **crowd sharing power of the network, the Digital ID aspect, and the device profiling capabilities of the system.** The fact that ThreatMetrix is now part of LexisNexis Risk Solutions only bolsters our confidence in the system and the network."
>
> *– The Gaming and Gambling business*

Overview

The Gaming and Gambling platform, operating out of the Caribbean and Europe, offers its customers a wide range of online activities from sports betting to online casino games and poker. To the industry two things are of importance; a fast, streamlined customer journey and identifying fraudster from their trusted customers. Allowing their customers to feel secure whilst placing online bets or playing games is at the core of the Gaming and Gambling business.

Constantly acquiring new customers while keeping up with the latest fraud trends is the balancing act all gaming and gambling platforms perform. For this, a robust fraud prevention system is required which can profile device and behavior and reliably predict risk across the customer journey. For an online gaming and gambling merchant it is incredibly important to have a view of risk and enable fraud detection capabilities across Logins, New Account Openings, Deposits and Withdrawals.

Business Problem

Online gaming and gambling has seen an increase as regulations loosen around the world. As more and more players are moving online, fraudsters are quick to react. Companies in this sector offer promotional schemes such as bonuses or better odds for quick registration and to encourage customers to play, this is a hotbed for bonus abuse. As genuine customers often leave funds in their account for quick bets, fraudsters understand this and take advantage via account takeovers or withdrawals.

The Gaming and Gambling business faces a range of attacks from fraudsters looking to fraudulently access schemes or accounts, these include:

Account Takeover: Fraudsters know customers have money sat in their accounts, so they access the account and either withdraw the victim's money to their preferred bank account or make unauthorized bets.

Bonus Abuse: Online Gaming and Gambling companies offer promotional schemes to acquire customers, these schemes can give risk free gambling and free tokens to game with. Fraudsters know this and can create multiple fraudulent accounts to take advantage of promotional schemes that gaming and gambling businesses offer.

Payment Fraud: Fraudsters can also monetize stolen cards or payment credentials. They make unauthorized payments to place bets or top up money to play online games from stolen payment details. Another recent problem in the payment space is the use of cryptocurrency by fraudsters is increasing.

A recent trend in the gambling industry is the use of cryptocurrency by fraudsters is increasing in the payments and deposit space. As we learn and anticipate fraudsters behavior and preferred methods it is important to be checking for fraud across the customer journey, from New Account Openings, to Logins, to Payments and Withdrawals.

A method of fraud which has been ongoing since the inception of online gambling is friendly fraud or chargeback fraud, where a genuine customer claims a chargeback under false pretence after losing their money on a bet. This can be solved by correctly identifying their digital identity to determine if it was actually a fraudster or just a rogue customer claiming friendly fraud.

To solve for all the above use cases, the Gaming and Gambling organization was looking for a single solution which would give them a better understanding of patterns of behavior of their trusted customers and which would detect and prevent fraud in near real time across the customer journey.

Harnessing Global Shared Intelligence to Protect Against Real Time Fraud On Desktop

Deployed in-app and on browser, ThreatMetrix® enhances fraud detection and protection of customer accounts using a number of key capabilities including:

Digital Identity Intelligence: Helped the Gaming and Gambling business 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 the Gaming and Gambling company 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: More players and gamblers are using VPNs and proxies. To reliably detect the use of location and identity cloaking services, such as hidden proxies and VPNs, TrueIP allows The Gaming and Gambling business to see the true IP address, geolocation, and other attributes of each transaction.

Smart Rules: help to better understand genuine customer behaviour, while accurately detecting genuine fraud. ThreatMetrix uses key data attributes, such as behaviour, age and location to examine the historical data and context related to a given customer or transaction. This helps to more reliably differentiate between true fraud and legitimate behavior change, reducing the step-up frequency without increasing overall risk.

LexisNexis®
RISK SOLUTIONS

For more information, visit risk.lexisnexis.com