LexisNexis®
RISK SOLUTIONS

CASE STUDY

Global Market Research Firm Reduces Fraud by Preventing Illegitimate New Accounts

Dynamic shared intelligence accurately differentiates between fraudsters and legitimate survey respondents in near real-time

AT A GLANCE

COMPANY

Global market research firm

REQUIREMENTS

- To detect fraudulent new accounts registering as survey respondents.
- To protect the integrity of survey data.
- To reduce fraud losses.

SOLUTION

Leveraging anonymized global intelligence from the LexisNexis® Digital Identity Network®, a global market research firm can accurately detect fraudulent new account requests in near real-time. Identity and payment information is validated as the transaction is happening, reducing friction and safeguarding long-term revenue.

BOTTOM LINE

- The firm can confidently continue to provide unparalleled survey capabilities to its clients.
- Preserved quality, accuracy, and legitimacy of survey data.
- Reduction in fraud losses through accurate detection of fraudulent registrations.

CASE STUDY

The firm needed a global, holistic response to this growing fraud trend, while maintaining its trusted reputation and reducing friction for legitimate survey respondents.

Overview

The firm is the premier global provider of data solutions and technology for consumer and business-to-business survey research. This firm reaches participants in countries via Internet, telephone, mobile/wireless and mixed-access offerings. It offers sample, data collection, questionnaire design consultation, online custom reporting, and data processing. With the firm's global presence, the risk of fraud is high where isolated fraudsters as well as organized criminal networks seek to monetize fraudulent survey information. The firm needed a global, holistic response to this growing fraud trend, while maintaining its trusted reputation and reducing friction for legitimate survey respondents.

With LexisNexis® Risk Solutions, the firm was able to:

- Leverage global shared intelligence from the LexisNexis® Digital Identity Network® to accurately detect fraudulent survey respondents.
- Reduce fraudulent incentive payouts.
- Ensure that legitimate respondents were not turned away.
- Protect brand reputation and reduce fraud losses by ensuring that only legitimate survey respondents were providing survey data.

Business Problem

The firm observed inconsistent survey data and unusually high incentive payouts. Upon investigation, it was determined that cybercriminals were filling out surveys to capitalize on monetary incentives. Cybercriminals would register new accounts to fill out surveys with fake data, extract payment incentives and then re-login into existing accounts to obtain more rewards. Cybercriminals were also leveraging the firm's multi-mode market research capabilities where they were collecting data from multiple sources such as mobile to web applications.

The firm's flexible platform had also allowed cybercriminals to easily re-engage, to theoretically receive as many incentives as possible by signing back into the websites. Cybercriminals threatened the firm's brand reputation as its clients relied on accurate data to make better business decisions.

Leveraging LexisNexis® ThreatMetrix® to Ensure Accurate Survey Results

One of the key business requirements for the firm was to ensure that any fraud and security solution was not overly aggressive and did not deter legitimate survey respondents. The ThreatMetrix solution created no friction in the sign-up procedure because respondents were passively authenticated in near real-time, yet it could still accurately detect high-risk behavior indicative of fraud.

The Power of Global Shared Intelligence to Detect High-Risk Event in Near Real-Time

The best way to tackle complex, organized 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. Leveraging LexisNexis ThreatMetrix product capabilities and using information from the Digital Identity Network, the company is able to create 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 accurately identified in near real-time, alerting the firm to potential fraud. Suspicious behavior can be detected and flagged for review, step-up authentication or rejection before a transaction is processed, creating a frictionless experience for trusted users.

CASE STUDY

Leveraging anonymized global intelligence from the LexisNexis® Digital Identity Network®, a global market research firm can accurately detect fraudulent new account requests in near real-time.

Using the LexisNexis® ThreatMetrix® Policy Engine to Customize Risk Scores

The firm took advantage of the flexibility of the ThreatMetrix policy engine to customize risk scores to suit its global business requirements. Additional rules were incorporated to target individual, larger-scale fraud attacks in specific geographical locations, without changes to the wider global strategy.

LexisNexis® RISK SOLUTIONS

For more information,
call 866.528.0780 or visit risk.lexisnexis.com/FIM-EN