LexisNexis® Behavioral Biometrics

Customer Success Stories

Behavioral Biometrics is the term used to describe the way an online user interacts with a desktop, mobile or laptop device via their keyboard, mouse and/or touchscreen. LexisNexis® Behavioral Biometrics was built as an enhancement to the existing LexisNexis® ThreatMetrix® product in order to:

- Add an additional layer of defense for fraud and risk decisioning by combining the way a user interacts with their device, with existing digital identity intelligence.
- Better profile high-risk behavior associated with fraudsters, automated bots, social engineering and remote access attacks.
- Build a clearer view of trusted user behavior over time, reliably identifying deviations from an established behavioral pattern.
- Identify trusted and high-risk behavioral profiles to better predict fraudulent behavior in near real time.

Key Benefits Include:

Tight Integration: LexisNexis Behavioral Biometrics is fully integrated within the current LexisNexis ThreatMetrix® portal, streamlining alignment with existing digital identity intelligence capabilities and promoting straightforward implementation.

White-Box Approach:

- Behavioral Biometrics data relating to mouse, keyboard and mobile device interactions is available to use within policies and rules.
- Machine-learning models and scores for different risk categories are provided with associated reason codes to expose the logic behind the scores. Behavioral Biometrics attributes can be used standalone or in combination with digital identity attributes.

Privacy-by-Design: Alphanumeric keys are not logged so no password or Personally Identifiable Information (PII) data is captured.

Low-Friction: Implemented as part of the existing LexisNexis ThreatMetrix JavaScript payload. No performance degradation or impact on latency when Behavioral Biometrics is activated.

The Business Case for Behavioral Biometrics:

Making reliable risk decisions increasingly involves layering multiple pieces of intelligence in a way that imposes little restriction on good, trusted users. The challenge for digital businesses is that fraudsters often mimic good user behavior, either by impersonating legitimate customers, training automated bots to behave like humans, or persuading humans to initiate transactions on their behalf.

Behavioral Biometrics data gives organizations another dimension of intelligence, capturing how an end user behaves on their device. Layering this knowledge with digital identity intelligence relating to device reputation, location intelligence, transaction behavioral patterns and known threats, helps businesses better differentiate between trusted users and potential threats.

Behavioral Biometrics in Action: Success Story 1

Two Tier 1 Banks in EMEA Saw Immediate Results After Integrating Behavioral Biometrics on New Account Creation and New Channel Registration Pages

BUSINESS PROBLEM

New account creations and new channel registrations present a significant risk point in the customer journey, as fraudsters attempt to monetize stolen credentials or intercept a mobile/online banking registration to gain access to good customer accounts.

BEHAVIORAL BIOMETRICS ADVANTAGE

Fraudsters obtain lists of stolen or intercepted identity credentials and use this data to fraudulently register for new products or services. Capturing digital identity data (e.g. device integrity and location), as well as the way a user inputs application data, helps differentiate between genuine user behavior and fraudsters leveraging stolen identities.

RESULTS

BANK A:

70%
fraud rate on a rule that has identified recurring, high-risk behavioral patterns on specific fields in the credit card application process.

92%
of all fraud stopped by this rule.

BANK B:

66%
fraud rate on new mobile app registrations that used particular patterns of high-risk behavior.

75%
fraud rate on the password reset page when specific keyboard functions were used.

Behavioral Biometrics in Action: Success Story 2

U.S. Financial Services Organization Models High-Risk Behavior for New Credit Card Applications

BUSINESS PROBLEM

Detecting fraudulent credit card application attempts helps this financial services organization reduce fraud losses and minimize operational demands associated with managing merchant chargebacks.

BEHAVIORAL BIOMETRICS ADVANTAGE

A fraudster was found to behave in a markedly different way to a trusted user when filling out an application form. Mouse usage, keyboard cadence, and time spent populating fields helped identify high-risk applications before they were processed.

Using this intelligence, the LexisNexis ThreatMetrix professional services team created a bespoke Behavioral Biometrics Fraud Model by combining Behavioral Biometrics raw data with LexisNexis ThreatMetrix behavioral analytics.

RESULTS

Between

10-20% Uplift

This custom fraud model helped achieve an uplift in fraud detection of **between 10-20%** on top of existing digital identity capabilities.

OR

1/3

A reduction in false positives by **one third**.

Behavioral Biometrics in Action: Success Story 3

Global Travel Company Differentiates Between Trusted and Fraudulent Reviews Using Behavioral Biometrics Attributes

BUSINESS PROBLEM

Fraudulent reviews can pose a real challenge for travel service companies. Fraudsters write and post phony reviews to add credibility to fake travel listings or to give unfair advantages.

BEHAVIORAL BIOMETRICS ADVANTAGE

Legitimate travelers tend to write generally well thought through reviews whereas fraudsters often mass-produce fake reviews, sporadically changing key details. This difference in behavior helped the travel company identify which behaviors were most indicative of a fake review.

RESULTS

4x

Timing analysis helped reveal patterns of review behavior that were found to be **four times** more likely to be fraudulent.

2x

Keyboard data analysis revealed reviews that had not been written from scratch were nearly **two times** more likely to be rejected.

Behavioral Biometrics in Action: Success Story 4

Cryptocurrency Exchange Can Reliably Differentiate Between Human and Non-Human Traffic

BUSINESS PROBLEM

A cryptocurrency exchange became a key target for automated bot attacks attempting to take over good user accounts to access digital currency.

BEHAVIORAL BIOMETRICS ADVANTAGE

By its very nature, bot traffic has an often uniform pattern of interaction with digital businesses, with traits that can be identified as machine-like rather than human-like. Isolating these behavioral traits gave the crypto-exchange a reliable indication as to whether the user accessing the account was a human or bot.

RESULTS

Bot traffic had a **more homogeneous** login speed for every interaction.

Humans displayed **small variations** in login speeds over time.

Behavioral Biometrics in Action: Success Story 5

Online Gaming Company Secures Payments by Detecting High-Risk Behavior in Near Real Time

BUSINESS PROBLEM

Gaming companies are a key target for cybercriminals looking to cash out fraudulent funds, launder money, and monetize stolen credit cards.

BEHAVIORAL BIOMETRICS ADVANTAGE

Keyboard data analysis revealed that fraudsters in possession of stolen credit card data displayed consistent behavioral patterns that were unique and distinct from how typical consumers input data.

RESULTS

32%

fraud rate achieved by the gaming company for payments displaying behavior linked to the use of stolen credit card data.

Behavioral Biometrics Key Features

- Mouse and keyboard data collection
- Sensor and touchscreen data collection
- A dedicated mobile Software Development Kit (SDK) module
- Attributes including paste detection, mouse off page, page elements and field timings
- An overall behavioral biometrics score, fraudster score, anomaly score, bot score, remote access score, social engineering score and associated reason codes
- Historical anomaly detection
- Fraud clustering capabilities
- An intuitive user interface accessed via the LexisNexis ThreatMetrix portal

For more information, please call 866.528.0780 or visit risk.lexisnexis.com/FraudandIdentity

LexisNexis® RISK SOLUTIONS

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.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis products identified. LexisNexis does not warrant this document is complete or error-free.