OUTSEER
An RSA Company

Outseer Risk Engine™

More Fraud Detection, Less Intervention

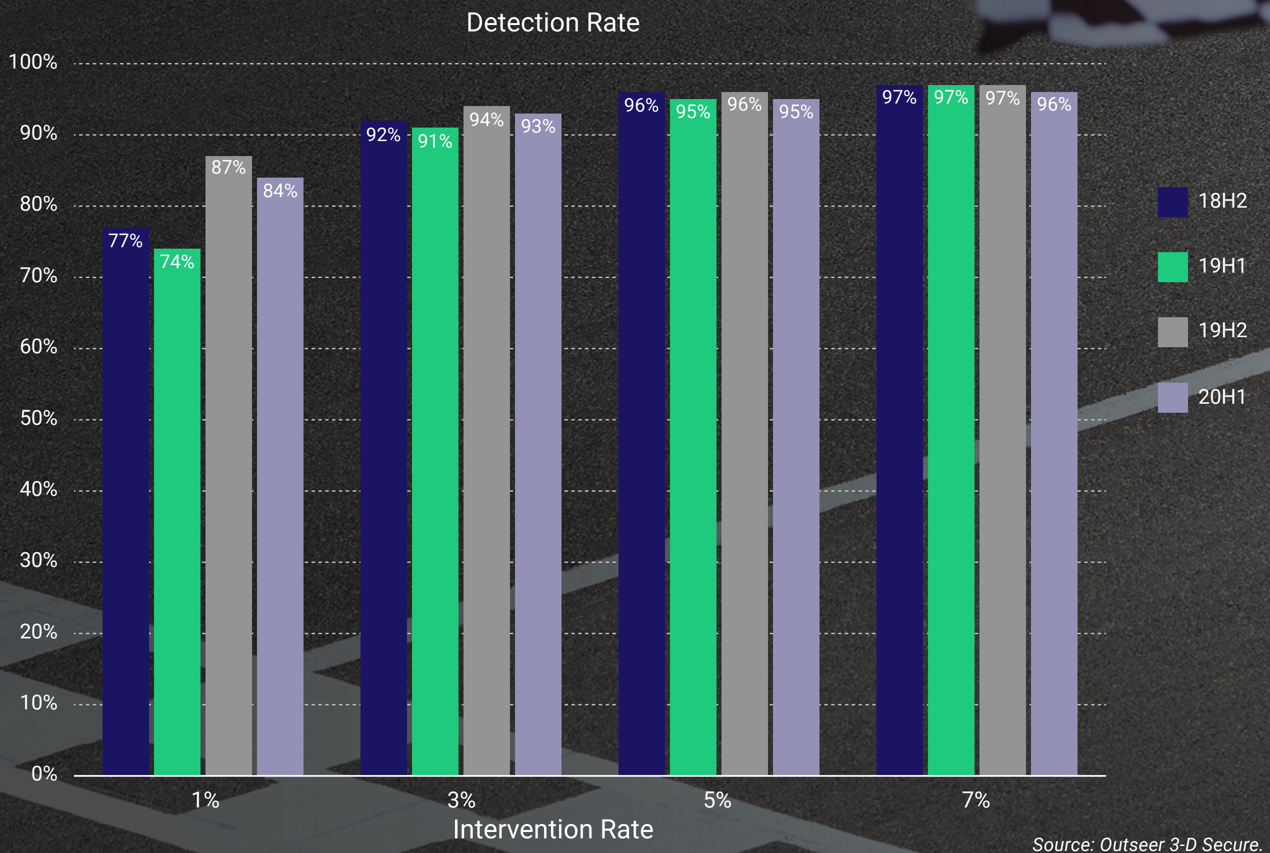
Contents

Powering the Decisions That Protect Your Business

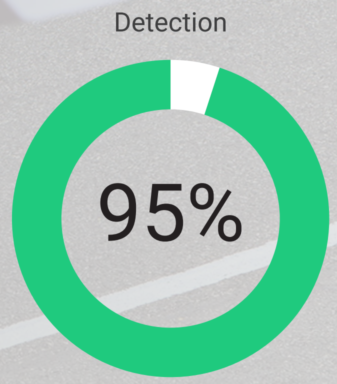
While others debate the merits of different technology models for fraud detection, we're busy proving the value of ours. Outseer products, powered by the Outseer Risk Engine, achieve fraud detection rates as high as 95%, with transaction intervention rates of 5%.

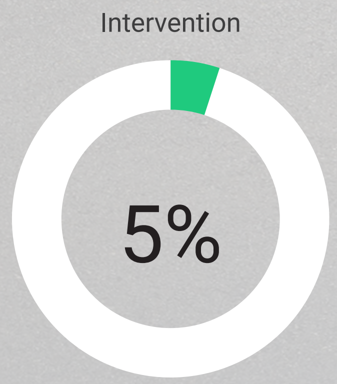
More Fraud Detection, Less Intervention

Modern identity science meets predictive analytics. Outseer Risk Engine predicts what others can't to deliver the best fraud detection and lowest intervention rates in the industry.



Source: Outseer 3-D Secure.



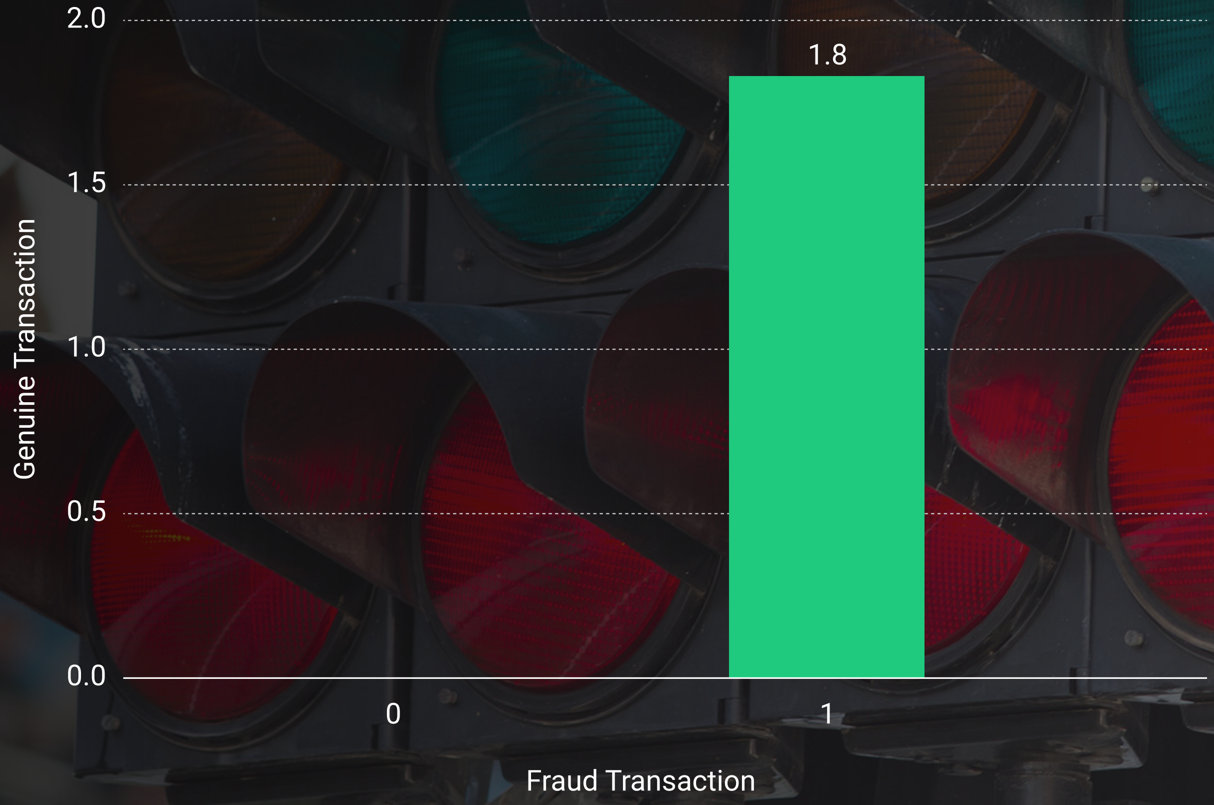


Stop Fraud, Not Customers

The fewer genuine transactions are challenged in the process of blocking fraudulent ones, the better for everyone. A low genuine:fraud ratio means increased convenience for customers, higher approval rates and ultimately, higher revenue for you.

Genuine:Fraud Ratio 20H1

Only 1.8 genuine transactions are falsely stopped to block 1 fraud.



Source: Outseer 3-D Secure.

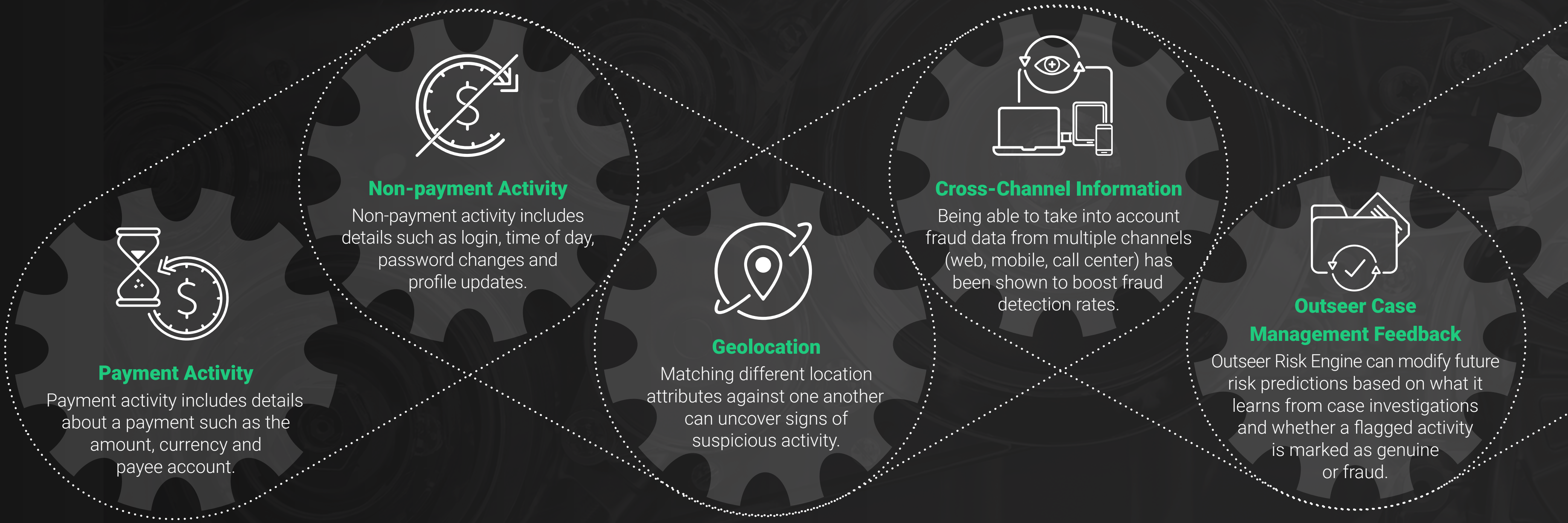
The Road to Results: Outseer Risk Engine

The Outseer Risk Engine drives outstanding fraud detection performance through a powerful combination of diverse data inputs and data science expertise for continual improvement.

Analysis Across a Wide Array of Data Inputs

Using a variety of sources of information, Outseer Risk Engine assigns a unique risk score to every digital transaction. The risk score and the risk policy set by an organization together determine whether a user is challenged with step-up authentication. But a risk score is only as good as the data that goes into it.

Here's what Outseer Risk Engine takes into account.



Payment Activity

Payment activity includes details about a payment such as the amount, currency and payee account.

Non-payment Activity

Non-payment activity includes details such as login, time of day, password changes and profile updates.

Geolocation

Matching different location attributes against one another can uncover signs of suspicious activity.

Cross-Channel Information

Being able to take into account fraud data from multiple channels (web, mobile, call center) has been shown to boost fraud detection rates.

Outseer Case Management Feedback

Outseer Risk Engine can modify future risk predictions based on what it learns from case investigations and whether a flagged activity is marked as genuine or fraud.

Here's what the Outseer Risk Engine takes into account.

To assign the most accurate risk score to detect fraudulent activity, the Outseer Risk Engine takes as many factors as possible into consideration.

Device Profile

Outseer Risk Engine analyzes the characteristics of the device such as IP address, browser characteristics, screen resolution characteristics and indicators of malware infections.

Mobile Activity

Mobile activity includes mobile device details such as mobile geolocation and Wi-Fi MAC address. Outseer Risk Engine can detect whether a device has been jailbroken and whether a mobile app is running in an emulator as opposed to on an actual mobile device.

Third-Party Risk Indicators

Data from third-party sources such as other anti-fraud tools and your organization's own internal intelligence can be imported into Outseer Risk Engine to be considered for additional indicators of risk.

IP Information

Data about a device's IP address can be used to flag suspicious transaction traffic.

Outseer Global Data Network™

Our consortium of globally-shared, cross-industry fraud and transaction data creates a valuable source of data for risk scoring.

Performance Enhancements

Outseer Global Data Network: Sharing Data to Prevent Fraud

The Outseer Global Data Network receives data from Outseer customers around the world. As a source of data for the Outseer Risk Engine, the network provides direct feeds on fraud threats.

5 million/month

Transactions flagged as fraudulent by the Outseer Global Data Network

$350 million/year

Fraud savings attributed to Outseer Global Data Network

Source: Outseer

$44,000

Savings per month a major U.S.-based financial institution realized by using cross-channel data from their call center to increase fraud detection on web and mobile banking channels

Source: Outseer

Outseer's Ecosystem Approach: Our Expertise, Applied to Your Data Elements

The Outseer ecosystem approach enriches the Outseer Risk Engine risk score calculations by enabling you to include your organization's own data inputs from internal and third-party channels. The Outseer Risk Engine consumes this additional data, learns from it, and incorporates it into the risk model to enhance risk scoring. This helps you gain more value from your investment in other fraud prevention tools while centralizing fraud management.

The Risk Scoring Process

Risk scoring with the Outseer Risk Engine begins with gathering facts from the data inputs and continues through the steps below. The risk engine learns from case markings feedback, charge-backs and authentication results and applies that learning to the next risk scoring event.

1. Data Gathering

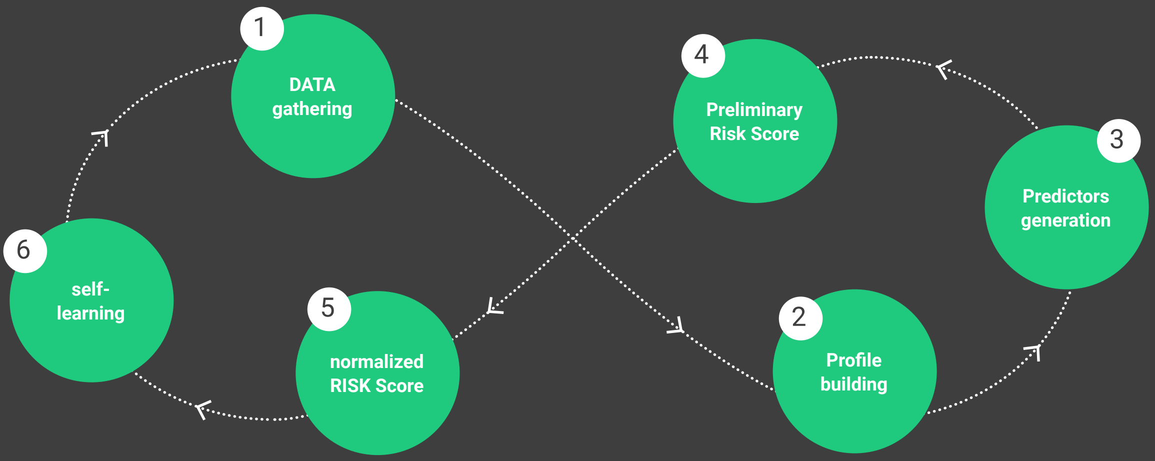
The Outseer Risk Engine collects data from diverse inputs, enriches it and applies a uniform data format to it, and then uses the data to analyze the risk presented by a transaction.

2. Profile Building

Profiles are sets of accumulated historical data and statistics about the user, IP address, device and other relevant entities. Using these profiles, the Outseer Risk Engine can distinguish between normal transaction behavior and abnormal behavior that may suggest fraud.

3. Predictors Generation

Predictors are data variables in the risk model assumed to correlate with fraud. They're generated from facts about the current transaction as well as from historical data from profiles. The better the predictors, the more accurate the prediction of fraud.



4. Preliminary Risk Score

The Outseer Risk Engine generates a preliminary risk score based on the probability of fraud given the predictors that are present. All data variables are taken into account in this preliminary score, with each one weighted based on its relevance.

5. Normalized Risk Score

Risk scores are normalized to a logarithmic scale from 0-1000, using linear interpolation to convert the risk score to a common scale. Normalization gives you more predictability and control (see sidebar).

6. Self-Learning

The Outseer Risk Engine learns automatically and in real time, and then develops new patterns based on what it learns. Its self-learning is based on anomaly patterns detected and real-world feedback received about step-up authentication results and case management feedback.

Normalization of Risk Scores Puts Control Where It Belongs: With You

Risk scores generated by the Outseer Risk Engine gives you more control over the percentage of transactions requiring intervention. In turn, this gives you the ability to modulate staffing (both call center and anti-fraud center). It also brings predictability to the impact on score-based policies on the end user experience (intervention/ challenge rates and false positives).

Final Score represents fraud likelihood and controls the percentage of events within score bands:

- 0.25% of events will get a score of 900-1000
- 1% of events will get a score of 700-1000

Normalized Risk Score

Lower Bound	Upper Bound	Percentile	Cumulative Percentile
900	1000	0.25%	0.25%
800	900	0.25%	0.50%
700	800	0.50%	1.00%
600	700	2.00%	3.00%
500	600	2.00%	5.00%
400	500	5.00%	10.00%
300	400	10.00%	20.00%
200	300	10.00%	30.00%
100	200	20.00%	50.00%
0	100	50.00%	100.00%

See How It Runs

You've seen the results. You've seen the data that goes into the risk scores. Now let's take a look under the hood at the technology and science that enable accurate scoring and constant improvements—and lead to outstanding results.

A Modern Machine Learning Approach

You may have seen fraud detection products that swear by combining three, four, or even more machine learning algorithms.

Just remember: It's about quality, not quantity. Outseer fraud detection products rely on one unique machine learning algorithm with multiple patents. Our algorithm has served our customers extremely well in recent years.

Why Our Algorithm Works So Well for Outseer Fraud Detection Products

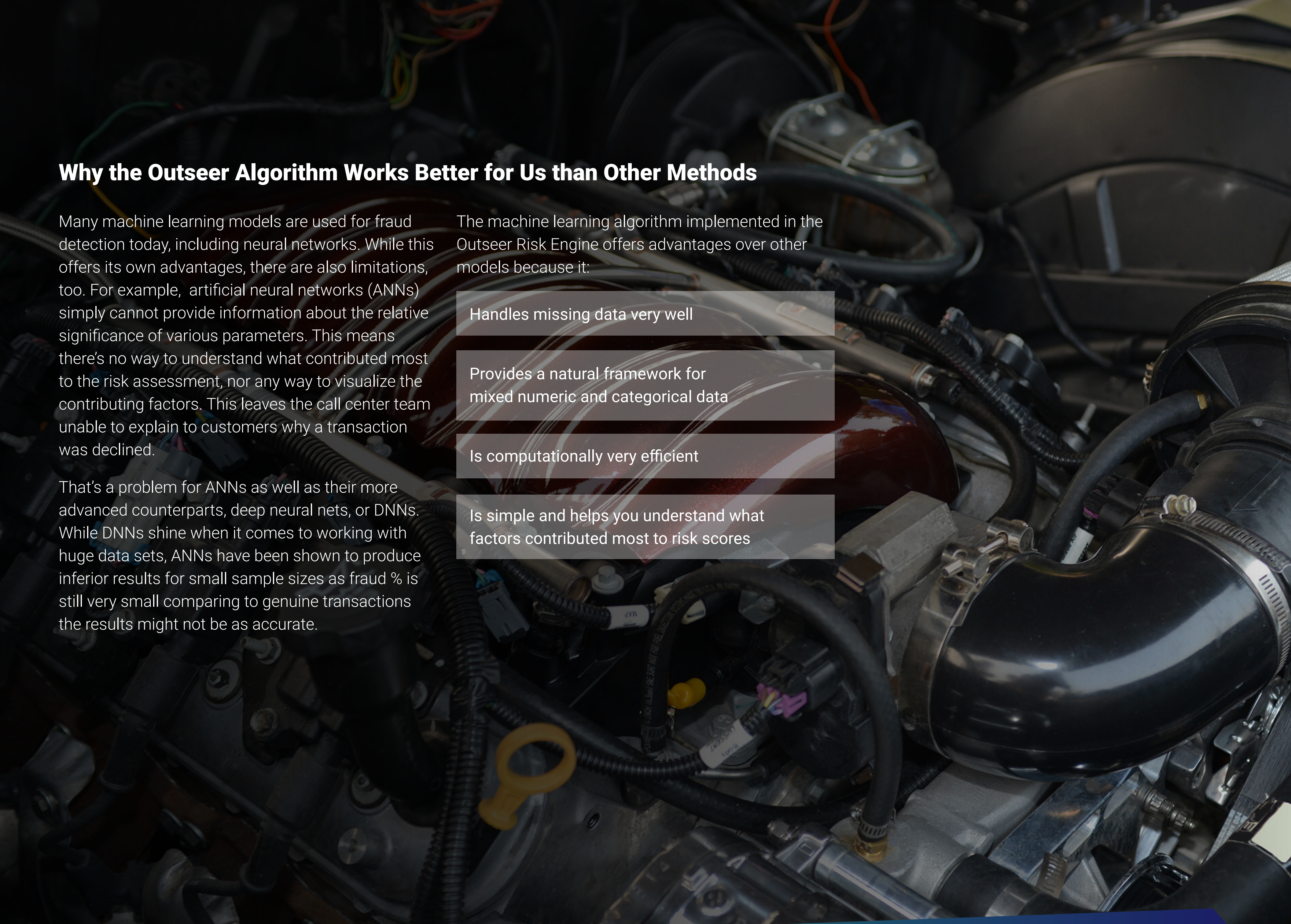
Our proprietary machine learning algorithms and risk models can[1,2,3]:

Easily accommodate the addition of new predictors, which is crucial given the rapidly changing nature of fraud today

Quickly learn new fraud patterns on smaller data sets (e.g., when there's less feedback available about fraudulent vs. genuine transactions)

Provide visibility into the parameters that contribute to the final result

Just remember:
It's about QUALITY, not quantity.



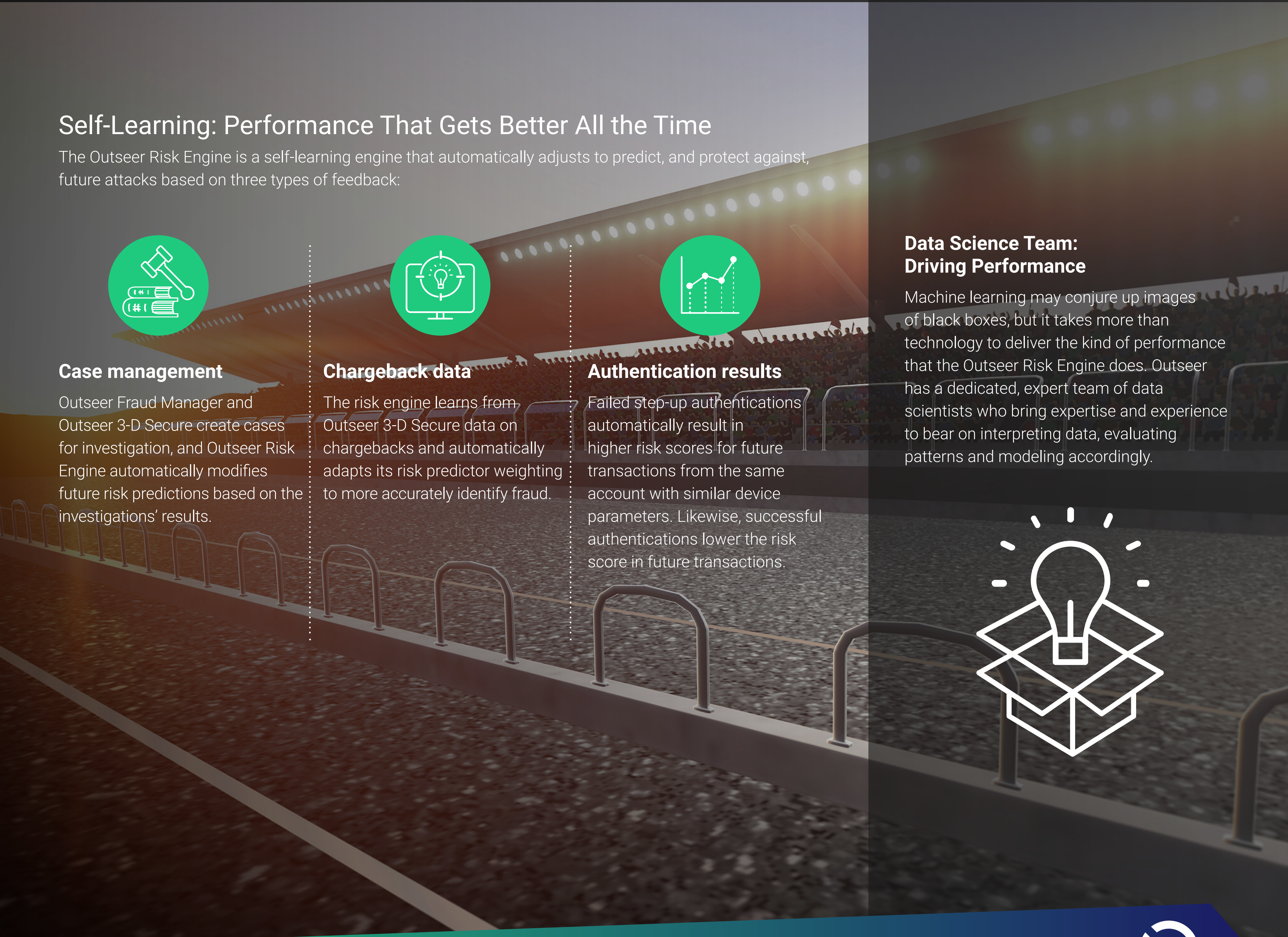
Why the Outseer Algorithm Works Better for Us than Other Methods

Many machine learning models are used for fraud detection today, including neural networks. While this offers its own advantages, there are also limitations, too. For example, artificial neural networks (ANNs) simply cannot provide information about the relative significance of various parameters. This means there's no way to understand what contributed most to the risk assessment, nor any way to visualize the contributing factors. This leaves the call center team unable to explain to customers why a transaction was declined.

That's a problem for ANNs as well as their more advanced counterparts, deep neural nets, or DNNs. While DNNs shine when it comes to working with huge data sets, ANNs have been shown to produce inferior results for small sample sizes as fraud % is still very small comparing to genuine transactions the results might not be as accurate.

The machine learning algorithm implemented in the Outseer Risk Engine offers advantages over other models because it:

- Handles missing data very well
- Provides a natural framework for mixed numeric and categorical data
- Is computationally very efficient
- Is simple and helps you understand what factors contributed most to risk scores



Self-Learning: Performance That Gets Better All the Time

The Outseer Risk Engine is a self-learning engine that automatically adjusts to predict, and protect against, future attacks based on three types of feedback:

Case management

Outseer Fraud Manager and Outseer 3-D Secure create cases for investigation, and Outseer Risk Engine automatically modifies future risk predictions based on the investigations' results.

Chargeback data

The risk engine learns from Outseer 3-D Secure data on chargebacks and automatically adapts its risk predictor weighting to more accurately identify fraud.

Authentication results

Failed step-up authentications automatically result in higher risk scores for future transactions from the same account with similar device parameters. Likewise, successful authentications lower the risk score in future transactions.

Data Science Team: Driving Performance

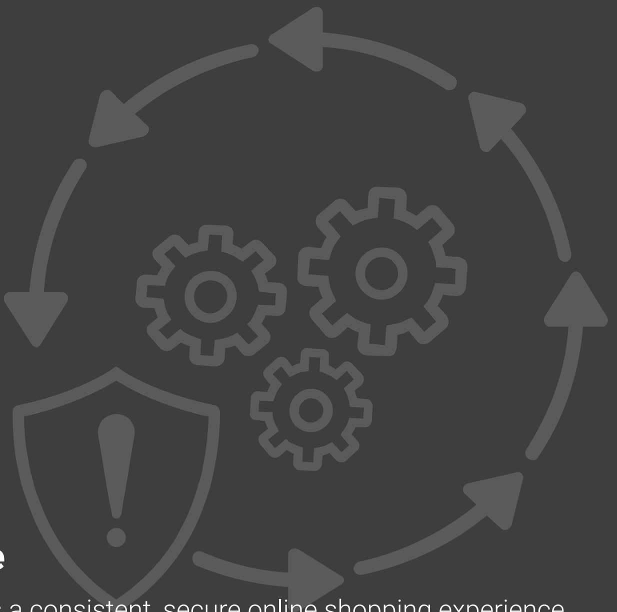
Machine learning may conjure up images of black boxes, but it takes more than technology to deliver the kind of performance that the Outseer Risk Engine does. Outseer has a dedicated, expert team of data scientists who bring expertise and experience to bear on interpreting data, evaluating patterns and modeling accordingly.

Six Questions to Ask When You're Considering a Fraud Prevention Solution

Now it's time to cut through the machine learning hype and get down to business. As you start to evaluate fraud prevention products and the advantages of the machine learning models they offer, here are some key questions to ask potential vendors:

1. What is your fraud detection rate today, and what is your goal?
2. What is your average customer intervention rate today, and what is your goal?
3. What is your average false positive rate today, and what is the impact on your business?
4. What data sources and details does your solution consider in calculating transaction risk scores?
5. How does your solution learn over time to identify emerging fraud patterns and provide better risk assessments?
6. Does your solution learn over time using case resolution feedback?

Outseer Risk Engine, the Foundation Technology and Science of Our Fraud Prevention Solutions



Outseer Risk Engine is foundational to our offerings thanks to its unrivalled accuracy. By seeing what others can't, the risk engine powers the solutions that protect your business—including:

Outseer Fraud Manager

Outseer Fraud Manager relies on the Outseer Risk Engine to assign an accurate risk score to every transaction, and intervenes only when the risk score warrants it. The result: fraud detection rates as high as 95%, and intervention rates of 5%. All while delivering a frictionless user experience.

- Increases fraud detection rates across all digital channels without adding friction
- Optimizes existing investments in anti-fraud tools
- Unlocks internal business intelligence to enhance risk assessment
- Centralizes fraud management like never before possible

Outseer 3-D Secure

Outseer 3-D Secure provides a consistent, secure online shopping experience while reducing fraud loss and chargebacks. By leveraging the Outseer Risk Engine, Outseer 3-D Secure is able to help credit and debit card issuers and payment processors dramatically reduce chargeback losses from CNP fraud.

- Gain your customers trust and loyalty ("top-of-wallet") so they choose your card to transact with—every time!
- Grow profitability by reducing fraud losses, reducing chargebacks and lowering operational costs associated with fraud investigation
- Increase transaction approval rates that drive up revenue and help you grow your business

1. Theodoridis and Koutroumbas, Pattern Recognition, 4th Edition (2009), Chapter 2, "Classifiers Based on Bayes Decision Theory," (in particular section 2.5.7, "The Naive-Bayes Classifier"
2. Duda, Hart and Stork, Pattern Classification, 2nd Edition (2001), Chapter 2, "Bayesian decision theory" and Chapter 3, "Maximum likelihood and Bayesian estimation"
3. Han, Kamber, Data Mining: Concepts and Techniques, 3rd Edition (2005), section 6.4 Bayesian Classification 310

About Outseer

Outseer empowers the digital economy to grow by authenticating billions of transactions annually. Our payment and account monitoring solutions increase revenue and reduce customer friction for card issuing banks, payment processors, and merchants worldwide.

Leveraging 20 billion annual transactions from 6,000 global institutions contributing to the Outseer Data Network, our identity-based science delivers the highest fraud detection rates and lowest customer intervention in the industry. See what others can't at outseer.com