ARCOT ISSUER FRAUD SCORE

Stop more fraud with less friction and fewer rules

The Arcot Issuer Fraud Score is designed to predict the likelihood a transaction is fraudulent. The score ranges from 1 to 999. The higher the score is, the higher the risk of fraud. We score each transaction within milliseconds and make that real-time score available within the Arcot Rules Engine. Data from each transaction is immediately loaded to our global fraud consortium where it informs all subsequent transactions on the network.

THE CHALLENGE

Criminals are sophisticated and constantly innovating new ways to steal payment card data and commit fraud. Even with additional data provided through 3-D Secure (3DS), identifying and blocking fraud attacks can require writing new rules constantly—like a high stakes game of whack-a-mole. This causes a number of challenges:

- Constant monitoring is required to spot new fraud attacks
- Operational costs increase to manage and maintain many rules
- Old and poor performing rules may cause unnecessary declines unless purged
- Blocking complex fraud behaviors is difficult or impossible using rules alone

THE SOLUTION

The Arcot Issuer Fraud Score solves this challenge by providing a simple way to identify most fraudulent transactions. Our predictive score identifies many fraud attacks in real time, so you don't have to write a new rule to block or challenge those transactions.

Our scoring model was developed by our world class team of data scientists and engineers leveraging the largest collection of 3DS data in the world—the Arcot Global Data Consortium. Decades of experience in payment fraud detection and machine learning enable us to engineer sophisticated and robust nonlinear features. Our strong team and focused investment in technology gives us stronger scoring and analytics capabilities than our competitors.

Key Benefits

- Identifies emerging fraud patterns and threats
- Empowers issuers to customize their risk thresholds
- Learns within milliseconds from all transactions on the Arcot Network
- Sees across all Arcot Network clients to identify risky devices
- Reduces time spent identifying fraud and writing fraud rules
- Simplifies rule management and maintenance
- Outperforms scheme/association models
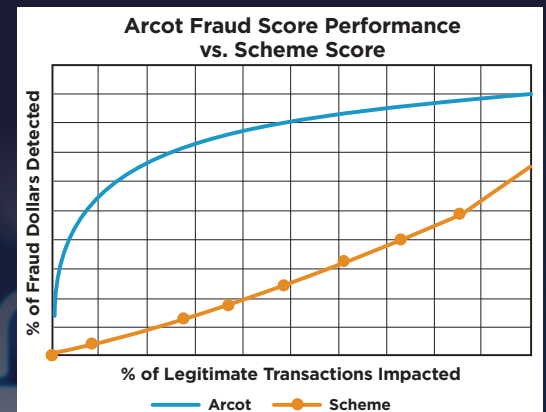
Arcot
by Broadcom

HOW DOES IT WORK?

During a 3DS authentication transaction, Arcot:

1. Receives 3DS protocol card, transaction, and merchant data

2. Collects and synthesizes device metadata via Arcot's proprietary algorithm

3. Transforms protocol and device data to match Arcot's proprietary feature engineering framework

4. Computes thousands of algorithms in real time against historical data from Arcot's global consortium which stores more than 1 trillion data points

5. Calculates the Arcot Issuer Fraud Score and sends to the Arcot Rules Engine

6. Evaluates transactions according to client rules and policies

7. Provides authentication response to the card scheme and merchant (Approve, Deny, or Challenge)
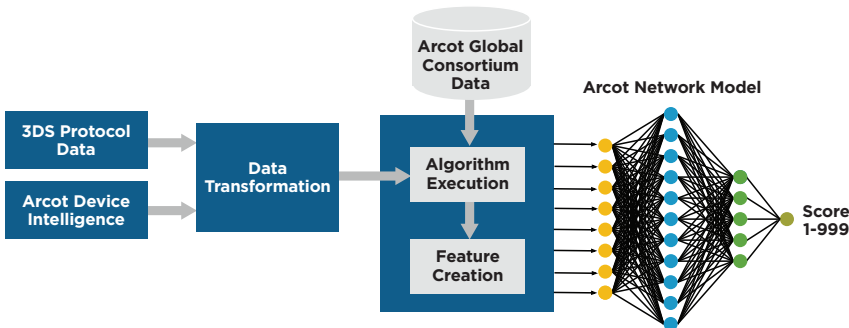
STRONG PERFORMANCE

To measure performance, we analyzed transaction and fraud reporting data over a 3-month period. For many of our clients we receive a scheme fraud score in the 3DS message in addition to generating our own fraud score. As outlined in the graph below, the Arcot Issuer Fraud Score outperformed the scheme 3DS model significantly and enabled our clients to detect more fraud while challenging fewer cardholders. In addition, we observed that in over 50% of the transactions the scheme did not provide a score. While useful to supplement other criteria, issuers cannot consistently rely on the scheme score to make decisions.

Arcot Fraud Score Performance vs. Scheme Score

LEARN **MORE**

→ Contact your Arcot Manager to learn more about the Arcot Issuer Fraud Score.