ARCOT OPINION: SEPTEMBER 2025

Boosting Authorization Rates with 3-D Secure Data-Only: Practical Guidance for Merchants and Issuers

Introduction

Arcot believes that 3-D Secure (3DS) Data-Only is an important mechanism to improve e-commerce authorization rates. False declines, legitimate transactions wrongly declined by issuers, are a real problem, particularly here in the U.S. They reduce revenue for both merchants and issuers, add operational costs, and impact genuine customers.

3DS Data-Only solves this problem by using the 3DS rails to share data without the friction associated with traditional 3DS. In fact, 3DS Data-Only transactions cannot be challenged. Merchants can send these low-risk transactions with complete confidence that the issuer will not step in. Friction is even reduced with Data-Only as the additional data provides issuers with a better view and the ability to allow more genuine transactions through.

3DS Data-Only is rapidly gaining momentum in the U.S. It appears to have the full backing of the card networks and is already in use by major merchants in the U.S., including Square. Broader adoption is expected.

This document introduces to 3DS Data-Only and guides merchants and issuers on implementation, key considerations, and partnering with Arcot to maximize percentage improvement in Authorization without increasing chargebacks.

The Problem: False Declines

Fraud prevention remains a concern but, for many merchants, the larger issue is false declines. With limited data available in a standard authorization message, issuers often take a conservative stance and decline transactions that are genuine. This creates lost sales, higher servicing costs, and dissatisfied cardholders.

More Data in Authorization Leads to Better Results

In a Data-Only flow, the merchant submits a full 3DS request without requiring a cardholder challenge. The transaction passes through the Directory Server and Access Control Server (ACS), and the resulting dataset is carried into the issuer's authorization stream (for example, through Visa IDX or Mastercard AAV/UCAF).

The additional data includes:

- Cryptogram (CAVV / AVV)
- ECI
- Transaction Identifiers (XID, DS Txn ID)
- Auth Result: Visa = I only; Mastercard = I or N (issuer denial)
- Device and browser fingerprint
- Merchant risk information (account age, shipping match, login history)
- Transaction context (recurring, subscription, stored credential)
- Delivery method

This allows issuers to incorporate richer context into authorization rules and fraud scoring.

Arcot
by Broadcom

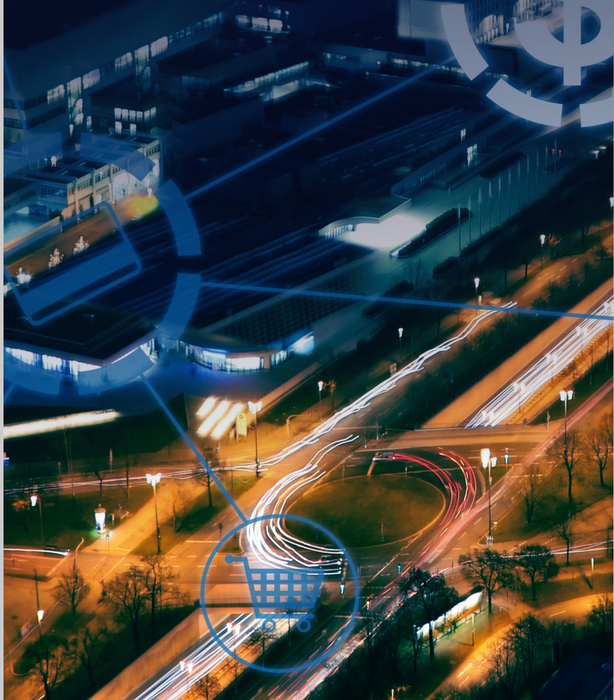
Smarter Collaboration via 3DS Data-Only for Higher Approvals Without Friction

Merchant Data-Only
– Richer inputs for issuers

Issuer Optimization
– Smarter risk decisioning

Better Outcomes for Merchants & Issuers

Better merchant data and smarter issuer decisioning come together to deliver higher approval rates, stronger fraud protection, and an improved customer experience.



The Role of RCI Codes

The **Requestor Challenge Indicator (RCI)** guides how the ACS should treat the transaction. For Data-Only, merchants should send an RCI06 for low-risk transactions (as determined by the merchant or Payment Service Provider (PSP)):

- RCI06 (Data-Only): The ACS does not challenge and passes information into the authorization stream.
- Higher-risk transactions can be sent with RCIs that allow for challenge and liability shift; e.g., RCI04 (Challenge Mandated).

Visa and Mastercard

Arcot understands the following differences in approach to Data-Only. In both cases, RCI06 cannot be challenged. Please speak with your network representative to confirm. Arcot's team of Customer Success Managers (CSMs) can support with Arcot rule and Smart Rule optimization.

Visa Data Only Authentication Rules: Data Only cannot be challenged or denied. Issuers must use the IDX data in authorization rules.

Mastercard Data Only Authentication Rules: Data Only cannot be challenged but may be denied. Issuer ACS rules must be tuned carefully to avoid unnecessary refusals.

Comparison: Authorization Messages

By leveraging Data-Only, merchants can be confident that additional transaction data will be sent to the issuer's Authorization platform, increasing its intelligence and allowing more genuine transactions to be approved. The table below compares Standard Authorization with Data-Only where additional data is provided via Arcot in the CAVV, Visa via IDX, and Mastercard via AAV.

CATEGORY	STANDARD AUTHORIZATION (NO 3DS)	AUTHORIZATION WITH ADDITIONAL DATA (DATA-ONLY + IDX / AAV)
Core Fields	PAN, Expiry, Amount, MCC, CVV2, / AVS	Same
Cryptogram	None	CAVV (Visa)(/ AAV (MC)
ECI	None	Auth status codes
Transaction IDs	None	XID, DS Txn ID
Auth Result	None	Visa = I; Mastercard = I or N
Device Data	Limited (maybe IP)	Fingerprint (IP, OS, browser)
Merchant Data	MCC only	Account age, shipping match, txn history
Transaction Context	Basic CNP flag	Recurring, subscription, stored credential
Delivery Method	Not present	Digital, shipping, pickup

Arcot Data-Only Guidance / Recommendations

For Merchants:

1. Use RCI06 for low-risk transactions.
2. Send high-risk flows with RCIs that allow challenge when needed.
3. Populate optional 3DS fields; e.g., Merchant Risk Indicator, IP address, use Methodcall.
4. Track results versus non-3DS flows (A/B testing at typically 50:50 ratios for ~3 to 6 months).
5. Engage with Arcot to optimize upstream merchant data, ensure acquirer/gateway support, and measure outcomes via the Arcot Scorecards.

For Issuers:

1. Update authorization logic to incorporate IDX / AAV and RCI06 data.
2. Treat Visa “I” and Mastercard “I” as informational signals; interpret Mastercard “N” as issuer denial.
3. Validate cryptograms as part of standard risk checks.
4. Adjust ACS rules to minimize unnecessary denials.
5. Engage with Arcot to align ACS and authorization models and track progress with the Arcot Scorecard.

Conclusion

Arcot considers 3DS Data-Only (RCI06) a practical way for merchants and issuers to reduce false declines and improve approval performance. The Square case study shows it can operate at scale. Working with Arcot, merchants can improve upstream data quality, issuers can leverage richer inputs in their rules, and both can monitor outcomes with the Arcot Scorecard and their own Authorization data.

SEE DATA-ONLY IN PRACTICE: READ THE ARCOT | SQUARE CASE STUDY RESULTS ON THE NEXT PAGE

Merchants that share consistent, meaningful data with issuers via 3DS Data-Only can expect real improvements in both authentication and authorization rates—without increasing fraud exposure.

CASE STUDY: ARCOT AND SQUARE

EMV 3-D Secure Drives Higher Approval Rates

Introduction

Square provides business technology solutions to over 4 million sellers and processes more than $200 billion in annual payments. Square's technology platform enables businesses to sell anywhere, manage inventory, book appointments, order online, and more.

The Challenge

Square was experiencing more false declines than expected for card-not-present transactions in the U.S. market. These declines led to negative experiences across many Square sellers.

Goals of the Pilot

Square and Arcot wanted to determine if sending additional data to issuers via frictionless EMV® 3-D Secure (3DS) could deliver higher approval rates for card-not-present payments.

Strategy and Implementation

Square:

- Sent a larger volume of transactions to 3DS using Data-Only, covering all risk profiles—not just high-risk cases.
- Used the 3DS Requestor Challenge Indicator RCI06, ensuring processing without challenge by the ACS.
- Maintained fraud liability on transactions.
- Submitted authorizations with ECI 06 and the Account Authentication Value (AAV) cryptogram.

Arcot:

- Update authorization logic to incorporate IDX/AVV and RCI06 data.
- Treat Visa "I" and Mastercard "I" as informational signals; interpret Mastercard "N" as issuer denial.
- Adjust ACT rules to minimize unnecessary denials.
- Engage with Arcot to align ACS and authorization models and track progress with the Arcot Scorecard.

LEARN **MORE**

To learn more about implementing Data-Only or to enquire about the Arcot Merchant Initiative, please contact **Erin Nichols** at **erin.nichols@broadcom.com**

About Broadcom Inc.

Broadcom Inc. (NASDAQ: AVGO) is a global technology leader that designs, develops, and supplies a broad range of semiconductor and infrastructure software solutions. Broadcom's category-leading product portfolio serves critical markets including data center, networking, enterprise software, broadband, wireless, storage, and industrial. Our solutions include data center networking and storage, enterprise, mainframe, and cybersecurity software focused on automation, monitoring and security, smartphone components, telecoms, and factory automation.

For more information, visit our website at: www.broadcom.com

Arcot
by Broadcom

Results Over 9 Months and 6 Million Transactions

- Chargeback rates improved by 6%
- 3DS authentication success increased by 19%

Better Data, Better Approvals

Sharing consistent, meaningful data via 3DS Data-Only improves both authentication and authorization—without increasing fraud.

Customer Feedback

"Arcot's implementation of 3DS Data-Only has been effective in reducing declines and improving the customer experience, without adding friction."

— Square

View the Full Case Study

You can view or download the full case study from the Arcot website under Resources: **arcot.broadcom.com**