Rules-Based Payer Authentication

Benefit from liability shift – while streamlining the checkout experience for your genuine customers.

Checkout friction can impact revenue

Checkout abandonment is a major concern for businesses. But so are chargebacks that can damage the bottom line. And here lies the argument about the implementation of 3-D Secure:

Either you enable 3-D Secure – and accept a higher level of checkout abandonment. Or you choose not to use 3-D Secure at all, sacrificing the liability shift.

> On average 30% less orders are reviewed manually by merchants using 3-D Secure.[1]

[1] % of 100 respondents performing manual review, CyberSource UK 2016 Fraud Report

CyberSource®
A Visa Solution

Rules-Based Payer Authentication

The benefits

1. Increase sales through higher order conversion

Tailor rules to suit you. And reduce checkout abandonment caused by implementation of traditional 3-D Secure – while capturing internal transactions that require 3-D Secure.

2. Optimise operations and improve margins

Reduce liability on applicable transactions. Authenticate high-risk transactions that otherwise would have been sent to manual review. Be flexible, and choose to enable 3-D Secure for risk-based authentication banks, while keeping it disabled for issuers that always challenge.

3. Improve the customer experience

Let protected transactions flow through your system unchallenged. And choose when to authenticate payments. Control what your customer sees. Embed authentication in the checkout.

44% of businesses using 3-D Secure cite customer friction as a major concern.[2]

42% are concerned that the solution is not optimised for mobile.[2]

Control your customers' experience

Rules-Based Payer Authentication allows for a truly dynamic implementation of 3-D Secure. Using real-time data to fine-tune its use based on both your own risk scoring and on issuer-level information.

With Rules-Based Payer Authentication you can also make changes at any time. For example, if you see a rise in fraud rates that seems to be down to disabling 3-D Secure, it's simple enough to remove or change the rule to counter the trend, giving you even more flexibility and control over your customers' payment experience.

[2] % of 196 respondents, CyberSource UK 2016 Fraud Report

Rules-Based Payer Authentication – how it works

Rules-Based Payer Authentication provides you with a pre-defined set of options to specify which transactions go through the 3-D Secure process, and which do not. You can also specify custom rules based on a variety of criteria.

Run a traditional 3-D Secure model – and authenticate every transaction – using the pre-defined rules for passive types of authentication. Or leverage the 'custom rules' settings to suppress authentication in situations where it may disrupt the checkout experience.

Pre-defined Rules You can choose from one of CyberSource's pre-defined rule sets to determine which orders are authenticated and which are not. For example, you could choose to turn on 3-D Secure for non-participating banks – but turn it off for traditional banks.

Custom Rules Custom rules can be created and used instead of – or in conjunction with – pre-defined rules. We implement and manage your chosen rule. You can change, add or remove rules, any time, as often as you like.

Canned Rules

Rule Setting Options	Description	Benefits
Traditional 3-D Secure	All enrolled customers are prompted to authenticate, all others prompted to activate during shopping.	Fraud liability shift applies when enrollment is checked/authentication is successful.
Non-participating banks	Card-issuing bank does not participate in 3-D Secure program. Customer is not prompted to enroll or authenticate.	Fraud liability shift applies when enrollment is checked.
Risk-based banks: passive authentification	Card issued by bank using risk-based authentication program, risk identified as low, customer is not prompted to authenticate.	
Risk-based banks: challenge	Card issued by bank using risk-based authentication program, risk identified as high, customer is prompted to authenticate.	Fraud liability shift applies when validation is successful.
Active authentification	Customers enrolled in a 3-D Secure program are prompted to authenticate.	
Activation during shopping	Customer is prompted to enroll in 3-D Secure program during checkout. Issuer may require enrollment. This rule is most often set to 'OFF'.	Fraud liability shift is typically still received on the transaction even if customer does not enroll.

Custom Rules

Amount Enables rule setting based on the transaction value

Currency Enables rule setting based on different accepted currencies

Authentication Path Allows rule setting at a deeper level including customisation of canned rules and the combination of custom rules

Date/Time Enables you to bypass authentication during specific dates or times

Card Type Ability to specify card types to run authentication on

CYBS MID Rules can be customised per MID while each MID can have different rule sets

ACS Provider Enables specific ACS provider to be presented to consumer e.g. Arcot, RSA

Card BIN Ability to bypass enrolled Consumer Authentication when BIN is underperforming

User Agent Enables rules configuration based on browser used by consumer

Why CyberSource?

- Our platform is built on a secure Visa infrastructure with the benefits and insights of a $427 billion global processing network.

- We offer payment acceptance in 190+ countries – and accept 137 currencies.

- We have 100 acquirer processor connections. This is increasing by 20+ each year.

In 2017 we:

- Managed 277 billion payments

- Managed approximately 1 out of every $10 spent online, worldwide

- Served 450,000 customers worldwide

- Provided x200 the visibility into fraud patterns[5]

Supported 3-D Secure programmes include:[6]

- Verified by Visa

- Mastercard

- SecureCode

- American Express SafeKey

- JCB J-Secure

[5] Based on the average number of transactions for a top merchant
[6] All brand names and logos are the property of their respective owners and the above-mentioned reference does not imply product endorsement or affiliation with Visa.

Find out more about our Multi-Phased Fraud Management Platform at
www.cybersource.co.uk/strengthenyournumbers

Contact us

Email. europe@cybersource.com www.cybersource.co.uk

CyberSource®
A Visa Solution