Risk Based Authentication

Risk Based Authentication (RBA) is an innovative method of authentication that can significantly improve the cardholder's online shopping experience while still providing the Card Issuer and the Merchant with a robust mechanism for managing fraud.

Card Issuers are currently piloting or considering a rollout of RBA during the next 12 months.

Since 2002 Verified by Visa and MasterCard SecureCode have been commonly deployed as a static password solution that requires the cardholder to register for the service and authenticate themselves for every transaction. When implemented properly, this approach has proved effective in combating fraud.

WorldPay want to ensure that our staff and our customers are kept at the forefront of these industry developments and this short resume of Risk Based Authentication explains how it works and how if affects our customers.

Risk Based Authentication now allows an Issuer to examine every authentication request presented to them as part of the authentication process and pass these transactions through a decision matrix before deciding whether further authentication is required.

Liability Shift

There are no changes to the current Card Scheme rules on the liability shift providing merchants with protection for transactions denied by the cardholder as today.

Merchant benefits

- Reduced cardholder abandonment rates
- Faster checkout times
- Decreased cardholder authentication interaction at checkout

Cardholder benefits

- Enhanced cardholder experience
- Potential elimination of cardholder registration in some applications

Issuer benefits

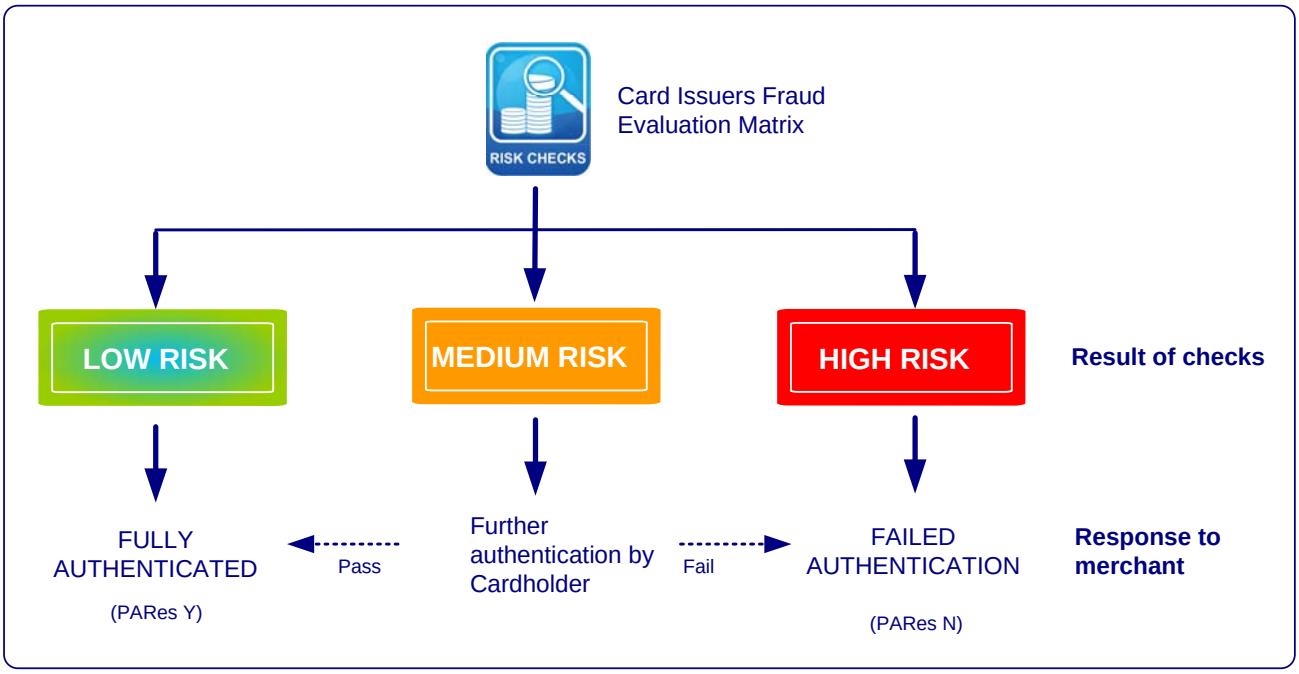
- Reduced incidences of "fully authenticated" fraud
- Improved fraud detection
- Reduced customer service enquiries

A new approach to Verified by Visa and MasterCard SecureCode

How does it work?

The Card Issuer using RBA creates an internal risk score for a particular transaction. Risk scores fall into one of the following categories: Low, Medium or High Risk.

Results then determine the actions taken by the Card Issuer to authenticate the cardholder. See Table 1 below.



Risk Score	Resulting action	Card Issuer Response
Low (80% of transactions)*	Cardholder proceeds with the transaction uninterrupted with no further request for authentication.	Fully Authenticated
Medium (15-18% of transactions)*	Card Issuer requests the cardholder to authenticate themselves using Verified by Visa or MasterCard SecureCode.	Fully Authenticated (if the cardholder successfully completes authentication) If the cardholder fails authentication then our advice to merchants would be not to proceed with the transaction.
High (less than 2% of transactions)*	Transactions automatically fail the Card Issuers authentication request. The cardholder is not prompted for authentication due to the high risk nature of the transaction.	In this instance our advice to merchants is not to proceed with the transaction.

Table 1. Risk Based Authentication

*Typical deployment statistics sourced from MasterCard Worldwide June 2011

Frequently Asked Questions

Do I need to retain my existing fraud prevention tools?

Yes, cardholder authentication is an important fraud prevention tool however, when combined with merchant or 3rd party fraud screening tools it becomes very powerful indeed.

Cardholder Authentication relies on the card data supplied as part of the payment transaction. Proprietary fraud screening tools will assess additional parameters which are not supplied to the Card Issuer as part of the payment transaction i.e. IP address, email address, phone numbers etc.

When are the UK Issuers looking to implement RBA?

The card schemes have advised that a majority of the UK Issuers are currently piloting or considering a rollout of RBA during the next 12 months.

Are there any additional costs?

There are no additional costs to merchants.

Do I still need to keep my 3D secure implementation in place?

Absolutely, RBA is a product enhancement to your current 3D-Secure implementation.

How does RBA affect the requirement for me to authenticate all Maestro transactions?

You should continue to attempt to authenticate all Maestro transactions and act upon the response provided by the Card Issuer.

Will a static password continue to be used as the authentication method for Medium Risk transactions?

Issuers can use a number of dynamic methods of authentication including: Static password, One Time Password delivered by SMS, Smart Phone applications and Two Factor authentication using Chip and PIN card readers. This will be driven by the Card Issuers own authentication strategy which will vary from Issuer to Issuer.

Revision History

Version no.	Date	Author
1.0	07-07-2011	Keith Payne