E-commerce Security

MasterCard Worldwide

ADVANTAGES OF A RISK BASED AUTHENTICATION STRATEGY FOR MASTERCARD SECURECODE

Purpose

This document explains the benefits of using Risk Based Authentication (RBA)—a dynamic method of cardholder authentication in the e-commerce environment—in conjunction with the MasterCard® SecureCode™ infrastructure and the Three Domain (3-D) Secure protocol.

The primary audience for this document is MasterCard issuers, although acquirers and merchants may benefit from understanding the RBA approach presented here.

RISK BASED AUTHENTICATION IS AN INNOVATIVE METHOD OF AUTHENTICATION THAT CAN SIGNIFICANTLY IMPROVE THE CARDHOLDER'S ONLINE SHOPPING EXPERIENCE WHILE PROVIDING ISSUERS WITH A ROBUST MECHANISM FOR MANAGING FRAUD.

MASTERCARD SECURECODE OVERVIEW

Since its launch in 2002, MasterCard SecureCode has provided issuing financial institutions with a method for securing e-commerce transactions worldwide. MasterCard SecureCode uses the 3-D Secure protocol as the framework to deliver cardholder authentication capabilities at the e-commerce point of interaction (POI).

MasterCard SecureCode has been commonly deployed as a static password solution that requires each cardholder to register for the service and authenticate himself or herself for every transaction. When implemented properly, this approach has proved effective in combating fraud. However when implemented improperly, weak static password deployment may lead to:

- Increased cardholder abandonment at the POI, potentially resulting in lost revenue for the merchant in addition to an alternative form of payment being selected by the cardholder
- High volumes of customer service inquiries which impact the issuer's bottom line
- Incidences of "fully authenticated" fraud that may occur when criminals leverage weak issuer Identification and Verification (ID&V) to successfully register as a cardholder and commit fraud at a SecureCode-enabled merchant

Through recent advancements in technology and vendor solutions, various innovative approaches are now available to issuers that deliver improvements and flexibility to the MasterCard SecureCode proposition. For example, issuers can use dynamic methods of authentication including:

- One-Time-Passwords (OTP) delivered by Short Message Service (SMS) text messaging to a cardholder's registered mobile phone
- Chip Authentication Program (CAP) for chip-capable markets
- Smart-phone OTP applications
- Risk Based Authentication

By implementing these dynamic methods of authentication, issuers can more effectively manage fraud and address the concerns presented by the traditional static password and cardholder registration approach. These new methodologies also lay the groundwork for future MasterCard SecureCode implementations in other card-not-present (CNP) channels.

By implementing these dynamic methods of authentication, issuers can more effectively manage fraud and address the concerns presented by the traditional static password and cardholder registration approach.

Using the RBA methodology, issuers and cardholders may experience the following benefits compared to the traditional static password authentication approach:

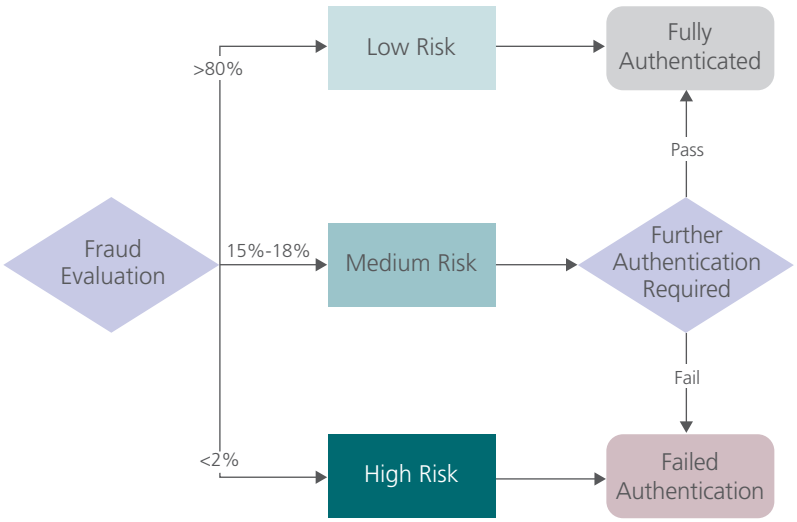
- Improved fraud detection and reduced fraud losses for issuers
- Reduced cardholder abandonment rates at the POI
- Quicker checkout times
- Decreased cardholder authentication interaction at the POI
- Fewer call center inquiries
- Potential elimination of the need for cardholder registration in some applications

RISK BASED AUTHENTICATION APPROACH WITH MASTERCARD SECURECODE

This section highlights how a strong RBA approach can work well in conjunction with MasterCard SecureCode and the 3-D Secure framework.

RBA allows an issuer to examine every MasterCard SecureCode authentication request presented to its Access Control Server (ACS) and pass these requests through a decision matrix. An issuer ACS either has a risk module integrated into the ACS or, more commonly, passes transaction data through a risk engine to determine a risk score for a particular transaction. Risk scores fall into one of the following three categories:

FIGURE 1: ACTIONS TYPICALLY TAKEN BY ISSUERS BASED ON THE RISK SCORE RESULT



Low Risk

In a typical deployment of RBA, approximately 80 percent of transactions would be categorized as low risk. As a result, the cardholder would proceed with the transaction uninterrupted—with no authentication request from the issuer. This process is also referred to as "transparent authentication".

One possible reason for a transaction being categorized as low risk is that the issuer has a transaction history for the cardholder at this particular online merchant. Therefore, the issuer can determine whether to authenticate the transaction on behalf of their cardholder without requiring the cardholder to participate in the authentication. Consequently, the issuer would flag such a transaction as fully authenticated.

Medium Risk

In a typical deployment, 15-18 percent of transactions would be categorized as medium risk. For a medium risk transaction, the issuer typically would request the cardholder to authenticate himself or herself using the issuer's preferred method, such as a series of challenge questions or SMS OTP passwords. If the cardholder successfully completed authentication, the result would be a fully authenticated transaction. If the cardholder failed authentication, the issuer would indicate that in its response to the merchant. The merchant would then decide whether to proceed with the transaction as a non-SecureCode transaction (See High Risk).

High Risk

In a typical deployment, less than 2 percent of transactions would be categorized as high risk. For a high risk transaction, the cardholder would automatically fail the issuer's authentication request. Therefore, the cardholder would not be prompted for authentication due to the high risk nature of the transaction, and the issuer would respond to the online merchant within the 3-D Secure protocol with a failed authentication. **Typically when receiving this response, the merchant would not proceed with the transaction.**

Issuers should note that MasterCard Standards permit the online merchant to proceed with the transaction without MasterCard SecureCode authentication; however, the merchant is required to flag the authorization message as a non-SecureCode transaction.

The MasterCard SecureCode Merchant Implementation Guide requires merchants to review and assess their risk tolerance levels to determine if they should terminate this type of transaction or request a different payment option from the consumer.

Issuers can use the risk score categories highlighted in Figure 1 to determine the appropriate level of authentication for each authentication request. These scores allow issuers to focus their fraud prevention efforts on the transactions that present the most risk.

CONSIDERATIONS FOR RBA IMPLEMENTATION

- If an issuer chooses to authenticate a cardholder using ID&V, careful consideration should be given to the strength of the identification criteria requested. Weak ID&V may result in a fraudster being able to compromise cardholder credentials and commit fraud.

  If an issuer decides to use a more robust authentication mechanism, such as a mobile application (e.g., SMS of dynamic passcodes), the issuer can consequently avoid possible concerns regarding weak ID&V.

- Issuers should ensure that their cardholder authentication method can be successfully completed within an acceptable time frame to avoid consumer frustration and potential lost revenue by both the issuer and online merchant.

- RBA is globally supported by MasterCard SecureCode and can be deployed in any region, including Canada, where this authentication strategy aligns with the existing mandate for usage of the "Activation During Shopping" (ADS) method of cardholder enrollment in MasterCard SecureCode by Canada-based MasterCard consumer card issuers for e-commerce transactions.

Careful consideration should be given to the strength of the identification criteria requested. Weak ID&V may result in a fraudster being able to compromise cardholder credentials and commit fraud.

CHIP-CAPABLE MARKETS

In examining options for dynamic authentication, MasterCard developed solutions that leveraged existing investment in EMV chip and PIN to create the Chip Authentication Program (CAP).

The CAP provides a similar shopping experience to that of face-to-face transactions wherever chip and PIN have been deployed. The cardholder inserts his or her card into a CAP device, enters his or her PIN, and an eight-digit one-time number is generated by the device.

This solution has already been implemented by various issuers to protect card payment transactions in addition to Internet banking and call center access. MasterCard SecureCode has been predominantly deployed as a security measure for e-commerce transactions. However, with the development of the CAP and further one-time pass code solutions, the other CNP channels can benefit from cardholder authentication using the existing MasterCard SecureCode infrastructure.

MasterCard has also expanded the CAP service to allow the generation of numbers to be sent to a mobile phone via SMS as an application. This application can be uploaded to a smart phone and even embedded into a card, so that no additional device needs to be carried—the display and keypad are built into the card.

RBA is a viable option for MasterCard issuers across the globe, and the following case studies by RSA Security and Arcot (CA Technologies) demonstrate the benefits of this approach.

RSA SECURITY

Enrollment-Based versus Risk-Based 3-D Secure

A fundamental requirement of the 3-D Secure protocol has been the enrollment of a card in the service prior to the successful completion of an authenticated transaction.

This enrollment can be a stand-alone process or performed in alignment with the shopping experience. However, in both cases the intent is the same—to validate the identity of the cardholder prior to use and to assign a means of authentication to that card. In some situations, particularly when specific guidance or regulation deems explicit authentication necessary for every transaction, this enrollment process is a viable and effective means for deploying MasterCard SecureCode. However, with any kind of enrollment process, the cardholder is presented with no fewer than two additional screens before the enrollment process is complete and a transaction can be completed. In countries where 3-D Secure enrollment is not mandatory for cardholders (e.g., the United States), as many as 52 percent of users will opt out of 3-D Secure participation at this point. Another 18 percent may close the activation window altogether. Even in environments where mandatory participation in 3-D Secure is required (e.g., the United Kingdom, Canada), 20 percent of cardholders have been observed to opt out of the ADS experience and choose to enroll at a later time. Each cardholder opting out of 3-D Secure when prompted to enroll is an example of a cardholder being inconvenienced by the enrollment-based system, eventually leading to dissatisfaction and abandonment of purchases by legitimate consumers.

By contrast, applying an RBA approach to 3-D Secure can eliminate the need for enrollment prior to completing an authenticated transaction. Rather than relying on a cardholder to provide enrollment data, careful evaluation of transactional, behavioral, and cross-institutional data can replace the traditional enrollment process and allow an issuer to challenge only those transactions that are determined to be high risk, letting most transactions pass completely untouched. A risk-based 3-D Secure authentication scheme can allow up to 95 percent of users to be **transparently** authenticated, thereby limiting interruption of the shopping experience to just 5 percent of cardholders. Figure 2 (using data taken from a pilot at a top U.K. issuer) and Figure 3 (page 7) show concrete evidence of the effectiveness of applying an RBA approach to MasterCard SecureCode implemented in the proper environment.

RSA SECURITY®

FIGURE 2: THE EFFECTIVENESS OF THE RBA APPROACH

85	Percent reduction in check-out time when compared to previous 3DS solution
70	Percent reduction in abandonment when compared to previous 3DS solution
5	Percent of customers who had an interrupted shopping experience via 3DS with RBA approach
0	Percent increase in fraud when compared to previous 3DS solution

FIGURE 3: EFFECTIVENESS OF RBA APPROACH FOR A U.S. ISSUER

	MONTH 1	MONTH 2	MONTH 3	MONTH 4	MONTH 5	MONTH 6	MONTH 7	MONTH 8	TOTAL FOR PERIOD
Total Transaction Challenged by %	0.06	2.11	8.57	7.79	7.70	8.08	7.51	7.42	5.98
Total Blocked Transaction by %	0.05	0.77	3.29	2.98	3.08	3.12	3.79	4.12	2.53
% of Blocked Transactions Investigated by Issuer	90.43	82.33	79.49	77.80	71.57	69.47	23.55	20.23	58.29
% of Investigated Transactions Confirmed as Genuine	19.22	6.92	7.35	7.13	6.81	7.76	24.39	24.36	9.38
% of Investigated Transactions Confirmed as Fraud	77.65	23.41	13.40	11.92	17.01	18.61	60.37	68.90	21.70
% of Transactions Flagged by Issuer as Suspicious	3.14	69.28	78.56	80.10	75.29	72.66	11.88	3.70	67.81
Genuine Fraud Ratio (X:1)	0.25:1	0.30:1	0.55:1	0.59:1	0.40:1	0.42:1	0.40:1	0.35:1	0.43:1

Accurate Risk Assessment in Transparent Authentication

When comparing an applied RBA approach with MasterCard SecureCode to a more traditional enrollment-based approach, the priorities and goals of the stakeholders in the environment must be considered before choosing a solution. Where strict control of transactions and cardholders for the sake of fraud reduction is the top priority, a traditional approach to deploying MasterCard SecureCode can allow for rigorous evaluation of cardholders prior to transactions taking place. Although this approach may result in slightly higher abandonment rates as the authentication process becomes more selective, the intended result is for fraud to be reduced by a corresponding amount. When opting for the traditional authentication method, consideration should be given to the method or methods used and the anticipated effectiveness weighed against cardholder impact.

Therefore, serious consideration should be given when prioritizing MasterCard SecureCode's ease of use over transaction control, which could result in slightly higher fraud rates for a given population. However, many issuers consider RBA for the evaluation of cardholders and transactions on many more elements than traditional MasterCard SecureCode enrollment typically requires.

A risk-based MasterCard SecureCode implementation begins with an assessment of transactional data intended to identify **where** a transaction is being initiated. This assessment is similar to identifying the POI. Internet Protocol (IP) data (both specific device IP and IP geolocation data) of the device

on which the transaction is being conducted gives insight into the history of the user and the location where the transaction is originating. Along with the use of device fingerprinting via cookies, flash objects, and various other methods of unique identification, the following questions can be answered: "Where is this transaction coming from, and has it been seen before?" Of particular benefit at this point is the ability to compare a current transaction against a historical database of confirmed or suspected elements of fraud across a broad population. This comparison answers the question: "Has this device or user been seen before, **anywhere**, even outside this organization?"

This data can then be filtered with behavioral analysis of common questions such as:

- "In what currency is this transaction?"
- "Has this cardholder transacted recently?"
- "Does this fit the kind of transaction that is expected from this merchant?"

All of this data can be entered into a risk engine to determine the relative risk associated with a particular transaction.

The risk assessment should be performed using a self-learning, non-rules-based risk engine. Therefore, the more volume that the system is exposed to, the more accurate the system will be. Even in a high-risk, high-fraud environment, an RBA approach to MasterCard SecureCode can provide results equal to or greater than a traditional enrollment-based approach, given proper modeling. At one top Latin American issuer, where fraud rates were well into the double-digit percentage points of overall transaction value, RSA has identified fraudulent transactions with a 0.57:1 goods-to-fraud ratio. This identification resulted in more than a 90 percent reduction in fraud on the protected portfolios with fewer than 10 percent of total users currently impacted by the risk-based approach (or 90 percent of users being transparently authenticated).

When working with issuers that are evaluating an RBA strategy for MasterCard SecureCode, RSA finds there are common success criteria:

- Does it detect fraud?
- Is it minimally impactful for cardholders?
- Does it reduce MasterCard SecureCode management expenses?

To determine the effectiveness of an RBA approach to 3-D Secure, RSA examined the results of a top U.S. issuer during an eight-month time frame. When analyzing the data against the success criteria, the following conclusions can be drawn regarding an RBA approach:

- **Low volumes of cardholders were impacted, and the majority were authenticated successfully and continued the transaction.** Out of the total transaction volume (on average), only 7 to 8 percent received an authentication prompt (Total Transactions Challenged). Also (on average) more than half of those transactions challenged passed the authentication and continued with the purchase (the inverse of Total Blocked Transactions).

- **Out of the blocked transactions, significantly more than half were either confirmed or believed to be fraudulent.** The false positive ratio (Genuine:Fraud Ratio) was better than 1:1, meaning the majority of transactions blocked were transactions that were undesirable in the first place.
- **Banks using a risk-based approach to 3-D Secure averaged more than 58 percent fewer call center inquiries related to 3-D Secure than banks that chose to use the enrollment-based system (see Figure 4).** Analysis of data from eight U.K. issuers (in bold, Figure 4) and five U.S. issuers clearly showed that customer service calls related to 3-D Secure dropped dramatically as a percentage of overall transactions when a risk-based approach was implemented. This conclusion aligns with the typical pattern of customer service calls, as most customer calls are in reference to account lockouts and password resets, which are both issues that can be eliminated by using risk-based MasterCard SecureCode authentication. In fact, in looking at one top 10 global issuer that moved from enrollment to risk-based 3-D Secure, customer service activity dropped nearly 97 percent after eliminating enrollment from the environment. This drop represented substantial cost savings to the bank as fewer resources were needed to be dedicated to 3-D Secure customer service.

FIGURE 4: 3-D SECURE CUSTOMER SERVICE CALLS DROPPED AS A PERCENTAGE OF OVERALL TRANSACTIONS

	ISSUER	CS ACTIVITY AS % OF TRX
3-D SECURE "CLASSIC™"	**U.K. Bank 1**	**6.70%**
	U.K. Bank 2	**5.20%**
	U.K. Bank 3	**2.54%**
	U.K. Bank 4	**3.06%**
	U.K. Bank 5	**2.06%**
	U.K. Bank 6	**3.13%**
	U.S. Bank 1	1.91%
	U.S. Bank 2	5.47%
	Weighted Average (3DS™)	3.99%

	ISSUER	CS ACTIVITY AS % OF TRX
RISK-BASED 3-D SECURE	**U.K. Bank 1**	**0.80%**
	U.K. Bank 2	**0.92%**
	U.S. Bank 1	3.91%
	U.S. Bank 2	0.86%
	U.S. Bank 3	2.76%
	Weighted Average RBA 3-D Secure	1.66%

Summary

As noted previously, the purpose of a risk-based approach to MasterCard SecureCode is to reduce abandonment and checkout time, increase fraud detection, and impact far fewer cardholders than with a traditional 3-D Secure implementation. A proper integration of these elements can make an implementation of MasterCard SecureCode a compelling proposition for any issuer and merchant. Results already in the market today demonstrate that success can potentially be achieved by a wide variety of issuers using an RBA approach.

ARCOT (CA TECHNOLOGIES)

Reduce Fraud with Risk-Based Authentication

RBA provides an additional layer of protection for card issuers against fraudulent online shopping transactions. This approach remains invisible to a great majority of legitimate cardholders and allows them to complete their purchase with no change in their experience. By analyzing a range of data in the context of each transaction, risk-based authentication identifies the likelihood of potentially fraudulent activity on a transaction-by-transaction basis. If the transaction matches the profile of a legitimate user and the authentication policies established by the card issuer, the transaction is allowed to continue unchallenged. Potentially risky transactions require an extra authentication step before they are allowed to be completed.

RBA also offers two significant benefits:

- **Fraud Reduction** – This approach identifies potentially fraudulent transactions and subjects them to extra scrutiny
- **Enhanced Cardholder Transaction Experience** – By challenging only a small number of risky transactions, most transactions are completed without requiring the user to do anything out of the ordinary

Balancing Risk Reduction and User Convenience

The success of RBA can be determined by three metrics:

Fraud Reduction – Clearly, the most important metric is fraud reduction. This metric is measured by computing the monthly fraud before and after deploying the RBA program. While this is a clear measure of fraud, it is difficult to attribute all changes in fraud levels to the solution. Fraud can be reported as late as 120 days after a transaction has been authorized. By then, the pattern of fraud has also changed.

Review Rate – This rate is the percentage of transactions that are flagged as potentially risky. A higher review rate potentially leads to higher fraud reduction, but also negatively impacts the cardholder's experience. In general, the review rate should not be more than 2 to 5 percent.

False Positive Ratio – This ratio is a measure of transactions that are incorrectly flagged as being potentially risky, and is related to the review rate. A higher review rate typically leads to a higher false positive ratio.

The review rate is a metric that is immediately known and easily usable to calibrate the system. The exact false positive ratio can be determined only after the true data (exact fraud information) is available (same 120-day window), but can be estimated immediately based on whether the user successfully completed the authentication challenge or failed and abandoned the transaction.

A card issuer (referred to in this case study as XYZ Bank) added Arcot RiskFort as an additional layer of fraud prevention as a supplement to its 3-D Secure program. The issuer deployed this solution to cover a small number of Bank Identification Numbers

RBA provides an additional layer of protection for card issuers against fraudulent online shopping transactions. This approach remains invisible to a great majority of legitimate cardholders and allows them to complete their purchase with no change in their experience.

(BINs) in its portfolio. During a three-month period, the issuer observed a significant reduction in fraud and expanded the solution to cover additional BINs. The issuer later deployed this solution to all BINs and cards in its debit and credit portfolio.

XYZ Bank RiskFort Implementation and Policy Decisions

XYZ Bank provided the actual fraud data that had been observed for a period of several months. Arcot divided that period into a Model Development Period (MDP) and a Model Validation Period (MVP). Using the transaction data and the actual fraud data in the MDP, Arcot developed a fraud model—a statistical function that would score each transaction with higher scores indicating a higher likelihood of fraud. This model was tested against the data in the MVP to confirm the predictive power of the model. Rules were added on top of the model, and based on the model score plus the rules, a final risk score could be generated. Then different risk score thresholds were considered for taking different actions on the transactions. The possible actions were:

During a three-month period, the issuer observed a significant reduction in fraud and expanded the solution to cover additional BINs. The issuer later deployed this solution to all BINs and cards in its debit and credit portfolio.

- Denying the transaction
- Requiring increased authentication before allowing the transaction
- Allowing the transaction, but marking it for review by a fraud analyst
- Allowing the transaction with no conditions

The **business drivers** for choosing the various thresholds were:

- Reduce monetary exposure due to the liability shift
- Lower the fraud rate
- Minimize the impact on the online consumer and irate calls from genuine users
- Control the number of abandonments by genuine users (loss of revenue)
- Control the number of cases marked for review—limited by number of available analysts

XYZ Bank elected a two-phase implementation. In the first phase, the thresholds were selected to minimize overall impact (i.e., lower review rates, fewer cases for follow-up, and lower fraud detection). Once the bank was comfortable with the numbers, the thresholds were raised to improve fraud detection, with a higher review rate and more cases for follow-up.

	PHASE 1	PHASE 2
Fraud Rate	0.045% (4.5 basis points)	0.045% (4.5 basis points)
Review Rate	0.97%	2.96%
Reject Rate	0.11%	0.11%
Total Fraud Reduction Percent	40%	66%
False Positive Ratio	1:5.8	1:4.1

MasterCard Worldwide

XYZ Bank is a very large issuer with several portfolios. The bank had implemented several other fraud prevention mechanisms and had a relatively low fraud rate of **less than five basis points** (i.e., fewer than five in 10,000 transactions were fraudulent). But given the size of the portfolio, this fraud itself was costing XYZ Bank over USD 400,000 per month and was expected to rise with increased online card usage. The bank wanted to ensure that it had a solution in place to reduce this fraud and protect against future fraud attempts.

XYZ Bank was very intent on ensuring that cardholders were not unduly impacted. Accordingly, XYZ Bank started with an initial plan to impact fewer than 1 percent of the transactions and then gradually raised it to 3 percent. The bank was satisfied with keeping the rejection rate constant while improving both the fraud reduction percentage and the false positive ratio. They achieved a 66 percent reduction in fraud when they added Arcot RiskFort RBA to their MasterCard SecureCode implementation.

Summary

Reducing financial losses and reputational damage from fraud is an undisputed goal. But fraud reduction at the expense of user convenience is not an option. RBA makes it possible to have the best of both worlds. RBA allows processors to reduce fraud and its associated costs while providing invisible authentication that doesn't disturb the online shopping experience of most legitimate users.

Resources

Documentation regarding MasterCard SecureCode implementation, best practices, and Frequently Asked Questions is available at:
www.mastercard.com/us/merchant/solutions/mastercard_securecode.html

Webinar tutorials on various aspects of MasterCard SecureCode are available at:
www.mastercard.com/securecodeonline

Contact the supplier of your existing MasterCard SecureCode service to determine your RBA options. If you are considering a new deployment, a full list of all vendors for Issuer Services is available at: **www.mastercard.com/us/merchant/solutions/securecode_vendor_list.html**