Online Processing
Addendum

Technical Specification

Online Processing Version 7.4 Revision 5.0
Addendum in Support of October 2010 Bank Card Regulations
Rev. 1
October 15, 2010

CHASE™
Paymentech

4 Northeastern Blvd. Salem, NH 03079-1952 603.896.6000 www.chasepaymentech.com

Technical Specification

Online Processing
Version 7.4 Revision 5.0
Addendum in Support of October 2010 Bank Card Regulations

Rev. 1
October 15, 2010

4 Northeastern Boulevard
Salem, New Hampshire 03079–1952
603–896–6000
www.chasepaymentech.com

This document contains confidential and proprietary information of Chase Paymentech Solutions, LLC. No disclosure or duplication of any portion of these materials may be made without the express written consent of Chase Paymentech. These materials must be used solely for the operation of Chase Paymentech programs and for no other use.

The following updates, additions, corrections have been incorporated in

Online Processing Version 7.4 Revision 5.0

Addendum In Support of October 2010 Bank Card Regulations Rev. 1

Page No(s)	Action	Description of Change
Additional Request Processing Formats		
1	Updated	Record note pertaining to MARP for the MasterCard Authentication Format Indicator (MA).
Appendix I: MasterCard SecureCode		
3	Updated	Appendix to show that MC is now a supported MOP in the MARP functionality.
7	Updated	Supported Currency to include MasterCard.

TECHNICAL SPECIFICATION
FOR ONLINE PROCESSING

Table of Contents

MasterCard Authentication Format Indicator (MA)

Length	Data Type	Field Name	Comments
2	A	Format Indicator	"MA" Constant – MasterCard SecureCode information. Specifies this record as an additional processing format of the Chase Paymentech standard format.
32	A	Accountholder Authentication Value (AAV)	Unique transaction token generated by the Issuer and presented to the merchant each time an accountholder conducts an electronic transaction using MasterCard SecureCode. Left justified/blank filled **Notes:** Must be sent in Base 64 Encoding or the transaction rejects with Response Reason Code 245 (Missing or Invalid Secure Payment Data). This is the same format used by MasterCard when returning the AAV data to the merchant during the authentication step. **DO NOT MANIPULATE** this value in any way.

Notes: This Format Indicator can be sent when MOP = IM or MC.

Transaction division level flag must be set in order to process MasterCard Authentication transactions, or the transaction rejects with Response Reason Code 246 (Merchant Not MasterCard SecureCode Enabled).

When using this Format Indicator, the Transaction Type field should be populated with the ECI value that the merchant received back from the merchant plug-in software.

When using this Format Indicator, if a European merchant is using International Maestro (IM) or MasterCard (MC), is participating in the Maestro Advanced Registration Program (MARP), and chooses to use static AAV, the Transaction Type field should be populated with a "5."

See *Appendix I: MasterCard SecureCode* for product information.

Sample

```
8    9         0         1
5678901234567890123456789012345678
MAgodlOEAxmL4wH7108KtV0QkAQAS=Rx1o
```

APPENDIX I: MASTERCARD SECURECODE

Introduction

MasterCard SecureCode is a solution designed to authenticate accountholders when paying online. SecureCode offers a mechanism for securing the Internet channel by strongly authenticating the accountholder at the point of interaction by providing a unique transaction-specific token that provides evidence that the accountholder originated the transaction. SecureCode uses MasterCard’s Universal Cardholder Authentication Field (UCAF) infrastructure to communicate the authentication information among the accountholder, Issuer, merchant and Acquirer.

MasterCard SecureCode supports the 3-D Secure Protocol. MasterCard SecureCode requires merchants to install a 3-D Secure v1.0.2 compliant Merchant Server Plug-In software application.

International Maestro supports the same SecureCode features as MasterCard.

How It Works

The accountholder shops at a participating SecureCode Internet Merchant with no changes to the shopping or checkout. The accountholder selects the merchandise to be purchased and proceeds to the checkout. At the checkout, the accountholder may complete the purchase and payment information in a variety of ways, including self-entered, electronic wallet, merchant one-click, or using other checkout capabilities.

After the purchase and payment information is entered, the customer hits the "buy" button and the Confirmation page goes back to the merchant.

The merchant plug-in (MPI) activates and checks its local cache and the MC Directory Server to determine if the customer card number is part of a participating MasterCard SecureCode BIN range. If so, a Verify Enrollment Request message is sent from the MPI, to the MC Directory Server and forwarded to the Issuer Access Control Server (ACS) to determine if authentication is available for the accountholder’s account number. The MC Directory Server sends the Issuer ACS response to the MPI. If authentication is available, the message response provides the web address for the Issuer ACS where the accountholder authentication begins. (If authentication is not available, the merchant server receives an "authentication not available" message and returns the transaction to the merchant’s commerce server to proceed with a standard Authorization Request.)

The MPI sends a message and script directing the accountholder’s browser to establish a session with the Issuer ACS to perform authentication. The in-line authentication window displays Issuer-specific and MC branding, transaction details – including merchant name and sale amount, and prompts the accountholder to enter their secure code (e.g. password). If the password is entered correctly, the transaction continues.

Continued on next page

How It Works, (Continued)

The accountholder is allowed a limited number of password attempts, typically three to five, as defined by the Issuer ACS. If unable to correctly enter the password, the accountholder may access the password hint that was established during registration. If the password is incorrectly entered more times than the Issuer limit, a failed Payer Authentication Response is returned to the merchant.

The Issuer ACS retrieves the authentication information and compares it against the data that was registered during the initial accountholder registration process. If the data matches, a success page is presented to the accountholder and the Issuer ACS sends a message through the browser to the merchant providing evidence of accountholder authentication, including a 28-byte AAV. This AAV is generated cryptographically using Issuer-specific secret keys that are synchronized with keys at the Issuer's authorization platform.

For a fully authenticated transaction, the merchant sends the AAV with Transaction Type = 5 to Chase Paymentech.

If the MasterCard Authentication record is sent without the CAVV, the CAVV is not sent in Base 64 encoding, or is sent for a non-e-Commerce transaction, Response Reason Code 245 (Missing or Invalid Secure Payment Data) is returned.

Chase Paymentech passes the AAV and Transaction Type to MasterCard with the authorization request. These fields are used during authorization processing to verify that authentication, or attempted authentication, was performed and to qualify for the e-Commerce Custom Payment Services.

Activation During Shopping (ADS): Accountholders that are not enrolled in SecureCode may be presented with an enrollment window while shopping at a SecureCode merchant's website. Unlike the traditional enrollment process, ADS does not require the customer to visit an enrollment web site before shopping. This type of enrollment takes place during the shopping process. When an eligible customer goes to checkout, the card-issuing bank asks a series of questions – similar to the traditional enrollment process. Providing the correct answers results in both a successful enrollment and a successful authentication response returned to the merchant. The merchant must send the AAV they receive to Chase Paymentech, along with Transaction Type of 5. If the accountholder chooses to opt-out of enrollment during shopping, the Issuer passes an AAV to the merchant. In this case, the merchant is not required to submit the AAV with the authorization, but must send Transaction Type of 6.

Continued on next page

How It Works, (Continued)

Non-participating MasterCard SecureCode Issuers: Participating MasterCard SecureCode merchants that attempt to authenticate an accountholder where the Issuer is not participating in MasterCard SecureCode do not receive an AAV. Merchants must pass these transactions with Transaction Type = 6.

Processing Requirements for Merchants Using International Maestro and the Maestro Advanced Registration Program or the MasterCard Advanced Registration Program (MARP)

Both the Maestro Advanced Registration Program and the MasterCard Advanced Registration Program (MARP) allow enrolled merchants to accept Maestro and MasterCard cards for e-commerce transactions without using SecureCode for every transaction. However, merchants are required to perform a full authentication on the first transaction they perform for any individual accountholder. An enrolled MARP merchant is provided with a static Accountholder Authentication Value (AAV) for use with transactions that are processed without SecureCode authentication.

Once a merchant has registered in the MARP (either the Maestro program, the MasterCard program, or both), all accountholders must go through the SecureCode process again, regardless of whether the accountholder has gone through SecureCode prior to the merchant's registration. After the accountholder has gone through SecureCode and has been approved, the accountholder is not required to go through SecureCode for subsequent transactions. The Method of Payments affected are IM (International Maestro) and MC (MasterCard) for European merchants.

For the first International Maestro or MasterCard e-commerce transaction, the merchant must request SecureCode authentication before submitting the transaction for authorization. If that transaction is subsequently authorized by the issuer, it is guaranteed to the merchant, regardless of whether the Issuer or accountholder participates in SecureCode.

The merchant populates the first SecureCode transaction as they do any SecureCode transaction.

Continued on next page

Processing Requirements for Merchants Using International Maestro and the Maestro Advanced Registration Program or the MasterCard Advanced Registration Program (MARP), (Continued)

Fully Authenticated Transactions

For the first transaction that is fully authenticated, the merchant populates:

1. Transaction Type field with "5" (ECI Indicator – Secure Electronic Commerce Transaction), and
2. AAV field with what was returned at authentication.

Attempted Authentication Transactions

For the first transaction that is an attempted authentication, the merchant populates:

1. Transaction Type field with "6" (ECI Indicator – Non-Authenticated Electronic Commerce Transaction), and
2. AAV field with blanks.

If the first International Maestro or MasterCard e-commerce transaction for the accountholder who has registered with the merchant is authorized by the Issuer, the merchant can skip the SecureCode authentication on subsequent transactions by the same customer using the same International Maestro or MasterCard account.

Subsequent Transactions

For subsequent transactions, the merchant populates:

1. Transaction Type Field with "5" (ECI Indicator – Secure Electronic Commerce Transaction), and
2. AAV field with the assigned static AAV.

If a registered accountholder uses a different International Maestro or MasterCard account for a transaction, the merchant must request SecureCode authentication before submitting the transaction for authorization.

The merchant always has the option of requesting SecureCode authentication for any International Maestro transaction, in which case the transaction is governed by Maestro rules. If the transaction is subsequently authorized by the Issuer, it is guaranteed to the acquirer or its merchant, regardless of whether the Issuer or accountholder participates in SecureCode as determined by the merchant request.

Issuers may chargeback transactions that are processed using the static AAV.

Continued on next page

Merchant Requirements

The merchant must install a certified 3-D Secure Merchant Plug-in software application.

The merchant must verify that Merchant Plug-in provides AAV in Base 64 encoding. If not, the merchant must convert to Base 64 before sending to Chase Paymentech.

In the settlement of a MasterCard SecureCode transaction, merchants are strongly encouraged to submit the MasterCard Authentication Extension Record. In the event that Chase Paymentech has to perform a new authorization, the authentication data (AAV) is included in the new authorization. By doing so, the merchant maintains the MasterCard SecureCode chargeback liability shift for authenticated transactions.

Merchants must map the MasterCard Electronic Commerce Indicator (ECI) they receive via their MPI to the appropriate Chase Paymentech Transaction Type:

Transaction Description	MasterCard ECI Returned in MPI	Chase Paymentech Transaction Type
Fully Authenticated	02	5
Attempted Authentication	01	6
Authentication Failed or Not Available	No ECI returned	7

Merchants must test and certify with Chase Paymentech to become MasterCard SecureCode enabled.

Continued on next page

Merchant Guidelines

- Merchants are required to request authorization for all SecureCode e-Commerce transactions.
- For International Maestro, it is highly recommended that merchants send SecureCode for e-Commerce transactions.
- Merchants must supply the AAV on all authorization attempts.
- Initial SecureCode authorization requests with AAVs older than 30 calendar days may be declined by the Issuer.
- Subsequent authorization attempts must include the AAV.
- Recurring payments should include AAV data for the initial authorization request only. Merchants must not provide authentication data in recurring payment authorizations as these are not considered electronic commerce transactions by MasterCard and subsequently are not eligible for MasterCard SecureCode processing.

Card Types / Supported Currencies

International Maestro, MasterCard / All currencies

MARP – International Maestro, MasterCard (for European merchants only)

Response Reason Codes

Appendix A: Response Reason Code Description/Usage

To Get Started

Contact your Chase Paymentech Representative.

END OF THE TECHNICAL SPECIFICATION

Online Processing Version 7.4 Revision 5.0
Addendum In Support of
October 2010 Bank Card Regulations Rev. 1

10/15/2010