ADVANCING SECURITY IN INTERNET TRANSACTIONS.

ADVANCING COMMERCE.

Issuer-based E-Commerce Authentication Services
The explosive growth of e-commerce has given rise to security concerns from every part of the payment transaction. Cardholders worry about the safety of online transactions and the privacy of their personal information. Card issuers are concerned about the risks of payment fraud and the high-cost of managing payments.

U.S. ONLINE SHOPPING IS SET TO GROW 10% EACH YEAR TO REACH 8% OF TOTAL RETAIL SALES (BY 2014). EUROPEAN E-COMMERCE WILL GROW ABOUT 11% DURING THE SAME TIME PERIOD.*

*Forrester Forecast March 8, 2010
MasterCard® Online Authentication Service (OAS) meets the needs of all e-commerce participants by offering flexible and robust solutions for online payment authentication. This reduces fraud-related costs for issuers by allowing them to verify customers at the point of purchase online.

Recognizing that not every issuer is ready to implement an authentication solution on its own, MasterCard Worldwide provides a turnkey hosted service to facilitate issuer participation in the MasterCard® SecureCode™ and Verified by Visa programs. Each issuer can tailor OAS to meet its individual requirements while leveraging the broad technical and operational resources of MasterCard.

Operated from our Global Operations Headquarters, the MasterCard platform enables issuers of MasterCard, Maestro® and Visa to augment their fraud prevention programs with minimum internal resources. Today, dozens of issuers are using the service, representing 25 countries and ten languages.

FEATURES AND BENEFITS OF OAS

Robust Security Features
OAS is designed to satisfy the financial industry’s highest online security standards. Our platform leverages MasterCard world-class systems, technical resources and security expertise. The architecture includes the feature-rich Access Control Server (ACS), Enrollment Server, hardware security modules, and a CAP Token Validation Server. The service is built on a 3-D Secure v.1.02-compliant platform, is compliant with the Payment Card Industry (PCI) Data Security Standards and adheres to the European Union’s Safe Harbor framework. These features provide a solid framework for service provisioning, which translates into greater peace of mind for you and your cardholders.

Broad Issuer Branding and Personalization
OAS can be tailored to meet your needs. Every cardholder screen is branded prominently with your logo and can be integrated with custom graphics and text. Flexible deployment options in terms of enrollment formats and language support are also available.

Secure, Fine-Grained, Administrative Privileges
Cardholder data is protected by two-factor security. Issuer customer servicing agents can access cardholder inquiry and reporting functions through a special administrative module tied to MasterCard OnLine.® Issuer staff can call the MasterCard help desk on a 24 x 7 x 365 basis.

“…My fraud figures released show that in 2006, our fraud was split 53% Internet, 47% Counterfeit. At the end of 2007, the ratio had changed, due to ADS [Activation During Shopping] and education to 23% Internet. For half-year 2008, Internet [fraud] reduced to 13%.
It is obvious what SecureCode has done for us... Utilising ADS has made it difficult to commit fraud on CNP. I just regret we are unable to support your new two-factor system.”

Fraud Manager at a European Corporate Card Issuer
CHOICE OF AUTHENTICATION STRATEGIES
You can choose an authentication strategy that is most suitable for your fraud management objectives.

Static Password
In this most basic approach the cardholder is typically allowed to create his/her own personal password on the hosted, issuer-branded web site, after answering several enrollment questions. Cardholders may also “Activate-during-shopping” at participating merchants.

Dynamic Password Via SMS Text Message
Cardholder portfolios with high levels of mobile phone penetration are also candidates for this solution which delivers a dynamic password to the purchasing cardholder on a just-in-time basis. The MasterCard service can generate the one-time-password and route the SMS text message to the cardholder on behalf of the issuer, or send the message to the bank to handle with their SMS carrier.

Chip Authentication Program (CAP) & AA4C
EMV smart cards can be used in conjunction with a handheld card reader to provide a cryptographic signature for MasterCard SecureCode and Verified by Visa transactions. By leveraging the inherent security features of the smart card, this two-factor authentication solution provides a new level of safety and security to smart card issuers.

MasterCard also supports “Advanced Authentication For Chip” [AA4C] a new approach that works with any standard EMV card that does not have an offline PIN and lacks the Chip Authentication Program [CAP] personalization. This approach provides issuers with a two-factor solution for their legacy cards.

New Fraud Fighting Tools
MasterCard is constantly enhancing the features and functionality of OAS for the benefit of our clients. Our newest fraud management tool, Risk-Based Authentication [RBA], is a powerful, selective approach that can be used in conjunction with any authentication strategy. With this service a risk engine scores all cardholder transactions using purchase and e-commerce session parameters preset by the issuer. The most risky transactions can be treated in a segregated manner while the least risky can be “transparently authenticated”. Issuers make all key rules and policies for the system.

COUNT ON THE RELIABILITY, ENHANCED SECURITY, AND COMPREHENSIVE SERVICE OF MASTERCARD
To learn more about MasterCard Online Authentication, contact your MasterCard representative or e-mail us at securecode@mastercard.com.
HOW IT WORKS
Here is an example of how OAS authenticates a cardholder through SecureCode during a purchase at a participating merchant. The type of authentication approach used (static password, dynamic password or CAP) has no bearing on this process.

1. A cardholder submits an order at a participating online merchant.

2. The merchant sends a request to the MasterCard directory server to determine if the cardholder participates in the SecureCode program. The MasterCard directory subsequently forwards this request to the Hosted Service Access Control Server (ACS) to determine cardholder status. The enrollment response is returned to the merchant.

3. If the cardholder is participating in SecureCode, the merchant sends a request to the Hosted Service ACS to perform the actual cardholder authentication. Upon receipt of this request, the ACS will populate an issuer-branded authentication page, which is displayed to the cardholder within the merchant window. This page prompts the cardholder to submit their private SecureCode, which is then validated by the ACS.

4. The Hosted Service ACS sends a digitally signed response which contains the Accountholder Authentication Value (AAV)—back to the merchant indicating a successful cardholder verification session.

5. The merchant sends an authorization request that includes an AAV to the acquirer.

6. The acquirer sends the authorization request through the MasterCard authorization network. This authorization request will contain distinctive information about the SecureCode status of the transaction. A fully authenticated transaction will contain an AAV in the Universal Cardholder Authentication Field (UCAF™).

7. The authorization request is sent by the MasterCard authorization network to the issuer for processing.

8. The authorization response is returned to the merchant and the purchase process is complete.