MasterCard International

MasterCard Authentication Solutions

Two-Factor Solutions Designed to Enhance Security for Online Banking and E-Commerce

Today's consumers are embracing the convenience and ease of online banking and shopping at a rapid pace. No longer are they limited to making banking transactions during "bankers' hours" at the retail branch or standing in line at a shopping mall to purchase a gift. Consumers have a choice in how they want to bank and how they want to shop—whether it is online in the privacy of their own home or in person at a bank branch or brick and mortar store.

While there is incredible opportunity for virtual transactions for both online banking and e-commerce, there are also challenges that must be overcome to continue this high-growth trajectory. There have been sharp increases in various types of fraud such as identity theft, phishing attacks, spyware, and Card Not Present (CNP) fraud.

In 2005 nearly $3 billion in estimated revenues was lost to fraudulent transactions in North America.* While many consumers forge ahead with virtual transactions unabated, many others remain wary. For example, recent MasterCard International Incorporated research found that 70% of Internet users were very concerned about Internet security and fraud issues.** This lack of confidence translates to lost revenues, while fraud-fighting efforts drive up costs.

This increase in fraud is not only eroding consumer confidence, but has prompted new government guidelines for financial institutions to implement stronger authentication efforts. Financial institutions have faced significant challenges trying to securely authenticate cardholders over the Internet and other emerging channels. Unlike the physical world, there is no signed sales receipt or physical verification associated with online banking or e-commerce transactions; consequently, there has been no sure way for an issuer to challenge a cardholder claim that he or she didn't conduct the transaction.

Regulatory Guidance

Last October the Federal Financial Institutions Examination Council (FFIEC) issued a guidance setting an end-of-2006 guideline by which U.S. banks should upgrade from single- to two-factor authentication for high-risk online transactions. To do this, banks must implement "two-factor authentication" whereby a consumer employs something he or she knows (such as a PIN) in tandem with something he or she has (such as an authentication device or mobile phone). By demanding the presence of two distinct proofs of identity, banks and retailers make it much more difficult for unauthorized parties to falsely conduct transactions on another's behalf.

MasterCard Authentication Solutions for Online Banking and E-Commerce

MasterCard has recently introduced a pair of powerful and innovative two-factor authentication tools, the MasterCard All-in-One Authentication Device and MasterCard Mobile Authentication™ (MMA), designed to enhance security for both online banking and e-commerce transactions. These solutions, based on the proven MasterCard authentication standard known as the OneSmart Chip Authentication™ Program (CAP), are currently in use in multiple countries around the globe.

* CyberSource, 2005 U.S. and Canada statictics
** MasterCard International, U.S. Internet Usage and Online Purchasing Study

MasterCard All-in-One Authentication Device

The MasterCard All-in-One Authentication Device is a slim, self-contained product that features an encased OneSmart Chip Authentication Program-compliant chip. A user enters his or her PIN into the device, which then creates a unique, one-time password. That password permits the user to conduct online banking or e-commerce transactions at MasterCard® SecureCode™-enabled merchant sites. The one-time password that is generated, based on EMV and CAP, only works once, then becomes null upon the completion of the transaction. The first instance of the MasterCard All-in-One Authentication Device is available through XIRING, a developer of products and solutions for strong authentication.

MasterCard Mobile Authentication

MasterCard Mobile Authentication allows consumers to use certain mobile phones or PDAs as one-time password generators. MMA customers download an authentication application to their J2ME-compliant mobile phone or PDA. Upon doing so, they are prompted to enter their PIN into their mobile device, which, similar to the MasterCard All-in-One Authentication Device, then generates a unique one-time password that must be entered to permit the user to conduct online banking or e-commerce transactions at MasterCard SecureCode-enabled merchant sites. The MMA solution is currently available through Cardinal Commerce, a leading provider of authentication services.

The MasterCard Suite of Online Security Solutions

For 40 years, MasterCard has pioneered security innovations and continues to be committed to providing the safest, most secure, and most reliable payment programs. The MasterCard All-in-One Authentication Device and MasterCard Mobile Authentication are the two newest additions to the MasterCard suite of online security solutions.

Existing Internet security offerings include MasterCard SecureCode, a global e-commerce solution that authenticates cardholders when they use their MasterCard payment cards to make purchases online. Before a SecureCode participant completes an online transaction, a Web page is presented by the issuer and prompts the cardholder to enter a predetermined password. Once the cardholder's identity is authorized, the transaction proceeds. SecureCode readily accommodates a broad spectrum of authentication methods ranging from passwords to unique, one-time passwords generated by the MasterCard All-in-One Authentication Device, a MasterCard Mobile Authentication-enabled mobile phone or PDA, and the OneSmart Chip Authentication (CAP) Program.

The MasterCard OneSmart Chip Authentication Program leverages a cardholder's existing chip card that is issued in EMV environments (regions such as Europe and Asia Pacific).

Meeting a Broad Array of Needs

Issuers (online banking and e-commerce)
- **Provides common approach for both online banking and e-commerce**
- **Reduces online fraud**
- **Reduces chargebacks**
- **Increases consumer confidence**
- **Reduces reputation risk**

Consumers (online banking and e-commerce)
- **Protects account information and financial assets**
- **Increases confidence in online environment**
- **Provides common tool across online banking, e-commerce, and other online financial services**

Merchants (e-commerce)
- **Provides the basis for a guaranteed online transaction**
- **Reduces chargebacks**
- **Requires minimal cost and impact on merchant and processor systems**

A cardholder inserts his or her EMV chip-enabled payment card into a smart card reader and enters his or her PIN. The hand-held or PC-connected reader then generates a unique, one-time password that must be entered to permit the user to conduct online banking or e-commerce transactions.

The Right Solution for Your Business Needs

MasterCard provides the framework for which third party vendors can offer our customers a range of flexible solutions to consider as they evaluate their authentication needs. Our authentication solutions are designed to be simple for consumers to use, provide the appropriate level of security to meet the FFIEC guidance, and give a holistic approach for online transactions including online banking and e-commerce. The MasterCard solutions are based on the OneSmart Chip Authentication Program, which has already been used to secure thousands of online transactions worldwide.

For more information on MasterCard Authentication Solutions, please contact your MasterCard representative, or visit **www.mastercardsecurity.com**

MasterCard International

6-11744 05/06