New Payment Rules Change Online Retail 2003

What merchants need to know about Verified by Visa and MasterCard SecureCode

New programs from Visa and MasterCard offer online merchants guaranteed payments and more sales.

Learn what they are, how they work, and how they'll affect the customer experience, order processes, and IT systems.

Find out how to implement wisely.

CyberSource®
www.cybersource.com
1-888-330-2300

Introduction

Currently, most merchants bear 100% of the fraud risk for online purchases—even if the transaction has been authorized by the bank. Industry studies indicate the rate of fraud online can be as high as 15 times that of in-store purchases (source:Gartner). New cardholder authentication services from Visa (Verified by Visa) and MasterCard (SecureCode) now offer merchants additional payment protection for sales transacted online.

These cardholder authentication services are designed to increase consumer confidence while shopping online and reduce merchant exposure to fraud by electronically verifying the cardholder's identity at the time of purchase.

While significant benefits can accrue to merchants who implement these programs, merchants must plan their implementation carefully. Complementary fraud protection measures are still required, and systems and processes must be thoughtfully engineered to make the most of these programs.

What Is Cardholder Authentication?

Cardholder authentication services rely on customer use of a registered password (or digital signature) which is validated by the card issuing bank at the time of check out. The following is an overview of the process.

Customers must enroll
Customers must enroll in the authentication program(s) with the card issuing bank. Note: some issuers are inviting cardholders to sign up while the customer is completing the purchase process. When these, and non-enrolled, cardholders visit an "authentication-savvy site", the following purchase process applies.

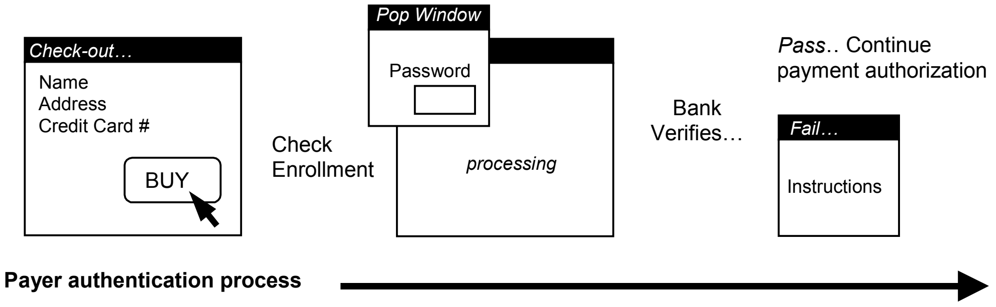
Step One: Customer initiates check-out
Customer completes merchant's check-out form as usual, supplying name, card type, card number, etc. and initiates check-out by clicking the "buy button."

Step Two: System checks cardholder enrollment
When the "buy button" is clicked, a message is sent to the appropriate card association (Visa, MasterCard) to see if the cardholder is enrolled in the program.

Step Three: Authentication window is presented
If the cardholder is enrolled, a "pop-up" window, branded by the card issuing bank, is automatically displayed and prompts the customer to enter a password. If the cardholder is not enrolled no pop-up window appears (transaction proceeds as usual).

Step Four: Password is verified with bank
The password (or digital signature) is then sent to the card issuing bank and compared to those on file.

Step Five: Transaction is accepted or rejected
If the password matches, the transaction is "authenticated" and payment processing continues. If the password does not match, the cardholder is not authenticated and the transaction is presumed to be fraudulent. (A page of the merchant's choosing is presented to the customer instructing them to contact customer service or similar follow-on actions.)



THINGS TO KNOW

Payer Authentication Programs

- Visa: Verified by Visa
- MasterCard: SecureCode

Program Objectives

- Increase consumer confidence online
- Protect online merchants from fraud

Customer Enrollment

According to Visa, more than 50% of the cardholders prompted to complete enrollment during the purchase process are completing the enrollment form.

Visa statistics indicate more than 10 million cardholders were enrolled as of early October (approximately 9 million of those enrolling during the months of August and September 2002).

Revenue and Profit Impact

Benefits

Increase in average ticket
Data released by Visa thus far suggests the average value of an online transaction initiated by a Verified by Visa enrolled cardholder is between 100-200% higher than those of non-enrolled cardholders ($206.65 compared to $88.50). Proponents of the program suggest that enrolled customers feel greater payment security and therefore are inclined to spend more.

Chargeback protection
A key benefit of authentication programs is protection from fraud-related chargebacks (sometimes known as “I didn’t do it” chargebacks which often result from identity theft or stolen card use). Without such protection, merchants lose revenue and incur other costs and fees when charges are contested. The “liability shift” represented by these programs is thus particularly beneficial to merchants.

Facts: Liability Shift

Verified by Visa
Visa’s “Verified by Visa” program (VbV) offers merchants protection from RC23, RC61, and RC75 chargebacks (chargebacks where the cardholder denies making the recorded purchase). Merchants should note that the cardholder need not be enrolled in order for the merchant to receive chargeback protection. The merchant is simply required to submit the transaction for enrollment verification. These rules are currently in place for European merchants and will apply to merchants in the USA beginning April, 2003.

MasterCard SecureCode
MasterCard’s SecureCode program similarly shifts liability away from online merchants. The liability shift in Europe is effective April 2002 and applies to European transactions (European cardholders shopping at European merchants) if the merchant is SecureCode enabled (discounts in interchange rates also apply). In the USA liability shift occurs in November 2002 for authenticated transactions (cardholder is enrolled and authenticated). Additional rule changes for US merchants are expected to be announced in the April 2003 timeframe, however the effective date for associated changes is undetermined.

Comparing liability shift requirements

	Visa	MasterCard
Merchant must be enabled and check enrollment status to receive protection	Yes	Yes
Cardholder must be enrolled and authenticated	No	EU: No USA: Yes
Effective Date Europe	April 2002	April 2002
Effective Date USA	April 2003	November 2002

Exceptions to chargeback protection
Terms and conditions do apply, and merchants are advised to consult Visa and MasterCard rules for details.

Excluded transaction types
Generally, protection does not extend to the following types of transactions:

1. Those made with procurement cards
2. Recurring billing
3. Those where payment must be “re-authorized” and the cardholder is not available to input password (such as orders requiring split shipment or backordered goods). Exceptions to this rule apply if certain transaction data (CAVV and XID) can be resubmitted with the subsequent transaction.
4. Sales transacted via “one click buy” technologies
5. Transactions that fail to authenticate.

Excluded merchant classifications

1. Protection may be contingent upon the merchant taking reasonable measures to control fraud. Although not yet specifically documented, sources at both card brands indicate merchants whose overall fraud rates exceed certain levels (likely 1%) may possibly risk not receiving chargeback protection.
2. Merchants in certain high risk categories of business, such as adult entertainment and gaming may not be covered (however each card brand may differ in this area and merchants are advised to consult card association rules for details).

Because of these exceptions and considerations, merchants are advised to review their current business rules and order processes (see later section for details).

THINGS TO KNOW

Average Ticket Increases Seen
According to Visa, statistics indicate enrolled cardholders purchase more, on average, than those who are not enrolled.

Liability Shift
Term used to indicate change in chargeback liability. Authentication programs promise merchants that the liability for chargebacks associated with fraudulent online transactions will switch from the merchant to the issuing bank.

No Need To Wait For Consumer Enrollment
Acknowledging it will take time to ramp consumer enrollment, card associations are, in many cases, not requiring cardholders to be enrolled for merchants to receive protection. In these instances merchants need only “attempt” to authenticate the transaction to receive chargeback protection.

Exceptions Apply
Chargebacks protection is only applicable to certain fraud-related chargeback types, and certain transaction types are excluded from coverage.

Customer Experience and Expectations

Preference for participating sites
The marketing messages from both Visa and MasterCard tell consumers that they can be assured of more safety when shopping online as a result of these authentication services.

To the extent the card associations are successful with these messages, consumers may develop preference for sites supporting authentication at the time of check-out. If so, merchants not offering authentication services may be at a disadvantage.

Note: Consumers have been protected from fraud since April 2000. Both Visa and MasterCard maintain "zero liability" policies in the event the card is lost or stolen (or the account fraudulently used). However, surveys indicate a certain segment of consumers continue to have security concerns regarding online card usage (see side bar). Verified by Visa and MasterCard SecureCode are intended address this concern, thus increasing consumer confidence and stimulating more online shopping.

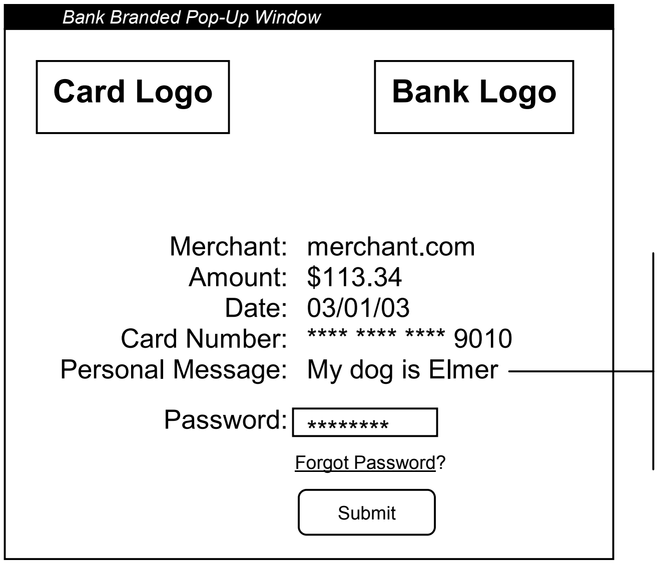
Banks prompt for enrollment
In some cases issuing banks may automatically prompt consumers to register at the time of check-out (if enrollment was checked and the cardholder was found not to be enrolled). Customers are presented with the opportunity to enroll or decline (close the window and proceed with the transaction).

Authentication added to purchase process
One key consideration for merchants is the addition of the authentication step in the purchase process. Customers will be required to enter their password into a bank-branded pop-up window after clicking "buy" (see example below). This should not be a problem for those who remember their password, but may affect transaction completion in instances where consumers forget their password or are not able to complete the authentication process (if the password is forgotten there are provisions within the user interface to help prompt the customer and this feature should minimize any risk associated with forgotten passwords).

Merchants that have one-click buy processes will now need to consider whether check-out procedures will be modified to incorporate payer authentication.

False "not able to authenticate" response
Enrolled consumers who have installed software to block pop-up windows may not be able to authenticate if the merchant has implemented using the standard pop-up authentication window approach. The system will determine that the cardholder is enrolled, but not be able to present the pop-up window to receive password information (software blocks window from "popping").

In these cases, the transaction is determined to be fraudulent because authentication could not be completed. (Similar results will occur if customers inadvertently close the pop-up window.) Actions can be taken to prevent or minimize these problems, and merchants are advised to address this in their order processing logic and IT implementation strategies (see next sections).



Merchant: merchant.com
Amount: $113.34
Date: 03/01/03
Card Number: **** **** **** 9010
Personal Message: My dog is Elmer
Password: ********

Personal message is created by the customer at the time of enrollment. Message assures customer that the window is authentic and not a false window inserted by a third party to steal personal information.

THINGS TO KNOW

How Consumers View Authentication

- 47% are now comfortable registering on web sites by providing personal information.
- 80% said they would be open to additional authentication measures to make online purchases more secure.
- 50% said they would be open to using a personal identification number (PIN).
- 32% said they would be willing to type in a portable password created by credit card company.
- 42% said they are "annoyed" at having to remember different passwords for different sites.

Source: Jupiter Media Metrix

Consumer Confidence Online Relatively Low

About one in four Web users does not trust personal information will be safe while doing personal research or communication tasks. Only 22 percent believe online purchasing data transactions are secure.

Source: NFO WorldGroup Forrester Research and the Conference Board

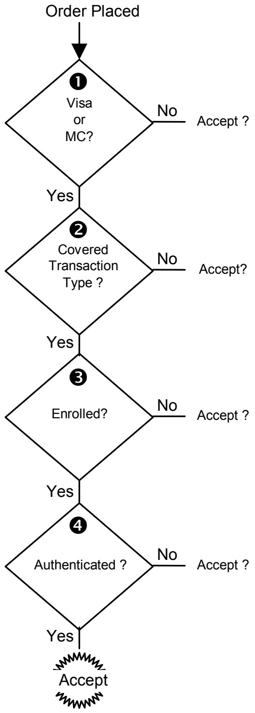
Order Process and Business Rule Considerations

On the surface, authentication programs appear to solve all fraud problems, requiring only that merchants check cardholder enrollment to gain chargeback protection. However, it is not quite this simple. Complementary fraud protection measures are still beneficial to help maximize overall revenue and profits.

Consideration One: Transactions involving non-participating card brands.
Incoming orders must be filtered based on card type used. Orders transacted with Visa or MasterCard can be forwarded for enrollment check, while those transacted with other card brands require some level of fraud screening to protect revenues.

Consideration Two: Excluded transaction types
As discussed previously, some transaction types are not covered (those made with procurement cards, and those requiring "re-authroization" when the cardholder is not present to enter their password, such as those associated with delayed or split shipments). These transactions will need to be handled differently than those covered by payer authentication programs.

Consideration Three: Acceptable fraud rates
Not all customers will be enrolled initially and it will take some time for enrollment to ramp. Though merchants theoretically receive chargeback protection on these transactions, it is unreasonable to assume banks will allow excessive levels of fraud to be incurred over a sustained period of time. To maintain program compliance and associated protections, merchants will likely need to screen "non-enrolled transactions" to hold fraud rates to an acceptable level.



Consideration Four: Non-authenticated transactions—reject or screen? The card associations recommend rejecting transactions and prompting for an alternate form of payment if the card is enrolled but the purchaser cannot be authenticated (if authentication cannot be secured for an "enrolled purchase" chargeback protection will not be extended). Merchants must consider whether they will reject these transactions or further screen them in an attempt to convert the sale. In some cases inability to authenticate may not mean the purchase is fraudulent. Consider:

- *Forgotten Password Prevents Valid Authentication*. Although password reminder features are available in the pop-up window, customers may still not be able to input correct password. Business rules must be set to handle this scenario. Will the transaction be rejected? Will it be diverted to customer service? Will complementary fraud screens be applied to determine order acceptance?

- *Technical Barriers Prevent Valid Authentication*. A growing number of customers are using "pop-up blocking software" to prevent display of pop-up windows. Because payer authentication services are most often implemented using pop-up windows for password input, persons using software which blocks these windows are unable to provide authentication information.

  Thus, even though the system has automatically performed an enrollment check and found the card to be enrolled, the transaction cannot be authenticated (the pop-up window cannot be displayed). If merchants implement using the standard pop-up window they will likely need to apply other screening technologies to attempt order conversion and minimize dissatisfaction. The alternative is to reject the order or prompt interaction with customer service—neither is optimal from a cost or revenue perspective. (See next section for IT that can help minimize this problem.)

THINGS TO KNOW

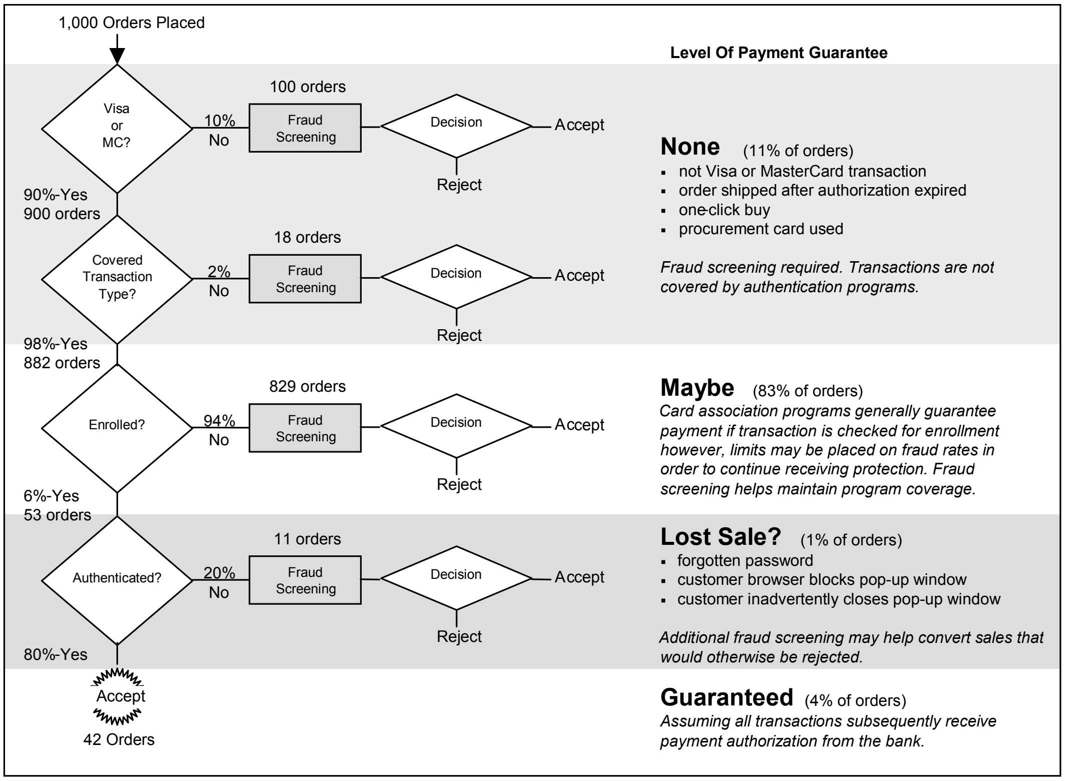
One Click Buy Considerations

Because "one click buy" does not present the opportunity for the purchaser to authenticate the transaction, merchants currently using "one click buy" technology must consider whether to modify processes or exclude such transactions from authentication.

Some Web Browsers May Block Password Window

Some consumers use software that blocks pop-up windows and interfere with authentication systems. Order processes must be designed to proactively handle these exceptions.

The following illustrates how these considerations impact the overall order flow and why payer authentication services must work hand-in-hand with other fraud screening measures. Example assumes 1,000 orders are attempted and that most transactions are standard consumer pay-per-purchase transactions with immediate shipment. Based on card brand share statistics and aggressive cardholder enrollment assumptions for the year 2003, the following distribution of orders results. (Note: businesses having higher share of procurement card orders, high percentage of split/delayed shipments, or recurring billing processes would witness a higher percentage of non-guaranteed transactions. Conversely, as cardholder enrollment increases more transactions will be "guaranteed.")



None (11% of orders)

- not Visa or MasterCard transaction
- order shipped after authorization expired
- one-click buy
- procurement card used

Fraud screening required. Transactions are not covered by authentication programs.

Maybe (83% of orders)

Card association programs generally guarantee payment if transaction is checked for enrollment however, limits may be placed on fraud rates in order to continue receiving protection. Fraud screening helps maintain program coverage.

Lost Sale? (1% of orders)

- forgotten password
- customer browser blocks pop-up window
- customer inadvertently closes pop-up window

Additional fraud screening may help convert sales that would otherwise be rejected.

Guaranteed (4% of orders)

Assuming all transactions subsequently receive payment authorization from the bank.

THINGS TO KNOW

Payment Card Share
Visa and MasterCard transactions comprise approximately 90% of online transactions in the USA.

Fraud Attempts May Shift To Card Brands Not Having Authentication Services
Success of authentication programs may drive cyber-criminals to utilize card brands which do not have authentication services. If such shift occurs, more transactions will be placed using non-covered card brands. This would result in a greater percentage of "non-guaranteed" transactions and place a greater emphasis on fraud screening orders falling into this classification.

IT Considerations

Obviously, IT systems and order processing logic are directly impacted by the decisions made regarding the customer experience and order processing. The following overview and additional IT considerations may be helpful in planning implementation of payer authentication services.

The Standard(s)
Originally Visa and MasterCard each pushed a different standard: 3-D Secure being advocated by Visa and UCAF (Universal Cardholder Authentication Field) by MasterCard. Both now support 3-D Secure, and UCAF unique features are to be implemented on top of the 3-D Secure protocol.

Systems and transaction flow

1. Upon check-out, card information is encrypted by the payer authentication service/software and sent to the card association directory server to verify enrollment status.
2. Enrollment status information is returned. If the cardholder is enrolled, a URL is supplied which prompts the display of the bank-branded pop-up window. (At this point, the session is redirected from the storefront to the bank.)
3. Customer password is again encrypted by the authentication service or software and passed to the issuing bank's server for authentication.
4. The bank returns verification code and related information (and passes the session back to the storefront). If the transaction was authenticated, appropriate information is appended to data required for payment processing. If authentication failed, the customer is presented with a page (as determined by the merchant) with an appropriate response and "next steps."
5. The transaction is submitted for payment processing, including authentication information.
6. The payment processor returns appropriate authorization code, indicating whether payment is authorized or denied.

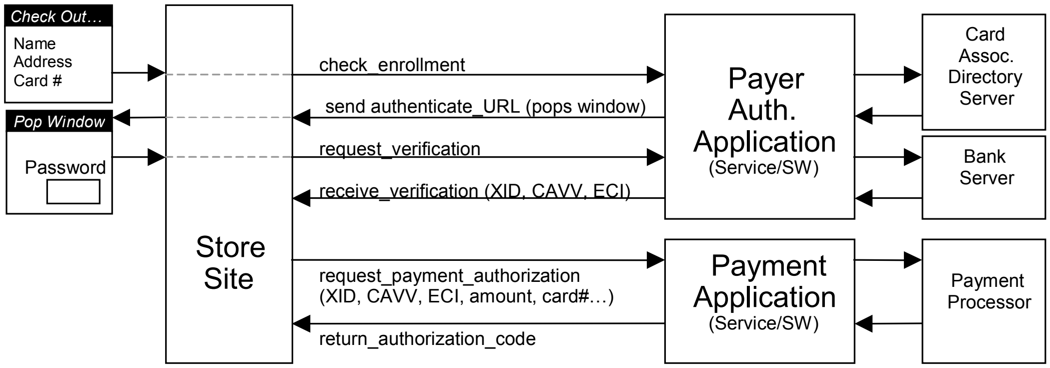
Consider: System stability
Because specifications are still being refined, and not all card brands have yet announced authentication programs or support for these standards, system stability is a concern for IT professionals. Merchants are advised to choose software or service implementations which "buffer" systems from changes. Software implementations are available which "containerize" authentication protocols such that new services from other card brands, or upgrades to current services can be accommodated without extensive re-integration. Similarly, web-based authentication services are available which almost completely buffer systems from these changes (changes occur at host data center vs. local systems).

Consider: Decision logic and service integration
Even without authentication services, decision logic associated with order screening can be quite complex. The addition of authentication services (and nuances in coverage) further highlight the need to implement decision logic that can be controlled by business managers (vs. hard coded) as business rules change. Further, payer authentication systems must be linked tightly with payment and complementary fraud screening systems for maximum processing efficiency.

Consider: How authentication window is displayed
To minimize problems regarding customers inadvertently closing the pop-up window or using pop-up blocking software, merchants are advised to consider displaying the authentication window in a frame if technically feasible.

Consider: Authentication session logic
If the pop-up window is blocked or closed the check-out process may be suspended (the storefront is waiting for the bank to return the session, but the session cannot be returned—the authentication process is incomplete). Session logic must address this and re-engage the customer with a "check-out continuance strategy" (continue on with standard authorization, prompt for an alternative payment method, etc.).

Transaction sequence and systems for authentication and payment authorization


Check Out…
Name
Address
Card #
Pop Window
Password
Store Site
check_enrollment
send authenticate_URL (pops window)
request_verification
receive_verification (XID, CAVV, ECI)
request_payment_authorization
(XID, CAVV, ECI, amount, card#…)
return_authorization_code
Payer Auth. Application
(Service/SW)
Payment Application
(Service/SW)
Card Assoc. Directory Server
Bank Server
Payment Processor

THINGS TO KNOW

Transaction Data Matters

Transactions sent for authorization to the payment processor must include key e-commerce information to qualify for protection and any applicable discounts. These transactions, termed "e-commerce preferred transactions," must include:

- ECI indicator. The transaction must be noted as the correct e-commerce transaction type.
- AVS check. A request for Address Verification Service must have been placed as a part of the authorization process.
- Verification check. A request to verify cardholder enrollment and verification of the password must have been made.
- CAVV. The "signature" generated by the bank which designates the transaction has been checked (including whether the transaction was authenticated).
- XID. The unique transaction ID generated for the transaction.

New Digital Certificate Required. Allow Time.

In most cases, authentication services or software cannot even be tested without the merchant having a digital certificate issued by the card association (Visa, MasterCard).

Merchants must first have their bank complete a form which includes the merchant ID and acquirer BIN range. Merchants then submit that information to the card association. The card association will then issue the digital certificate. Allow 2 weeks for this process.

The CyberSource Solution

CyberSource offers a convenient, hassle-free payer authentication service, giving merchants the online payment guarantees offered by major card brand programs, plus optional additional fraud screen protection, via one easy connection.

Supports all card programs
This single service supports Verified by Visa and MasterCard SecureCode, as well as future programs from major card brands, worldwide.

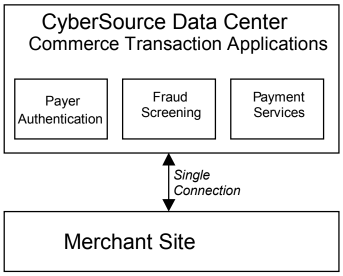
Easy installation and optional decision manager
Installs like a web service. One easy connection makes installation fast and hassle-free. Complementary payment and fraud screening services are accessible via this same connection for a fully integrated secure payment solution.

Optional decision management software is available to build and manage business rules; invoke payer authentication, fraud screening, and payment services as required; and automatically disposition and route orders based on these rules and tests.

Maintenance free
Updates and upgrades are implemented at CyberSource data centers as specifications change or new programs are introduced by other card brands. Merchants' local systems and IT resources are protected from disruption.

Works with any payment system
The service installs alongside merchant's current payment system or can be integrated with CyberSource payment solutions.

Added Payment Protection
Complementary, "transparent" fraud screening services are available via this same connection. These services help ensure merchants maintain chargeback protection under Visa and MasterCard programs and control fraud risk on purchases made with card brands not yet having authentication services.



Also available as software applications that install locally at merchant site.

Software version also available
A software version of CyberSource payer authentication service is also available. Like the hosted service, the software supports major card authentication programs and installs as a single component. "Container" architecture helps protect system stability as specifications change or new card programs are introduced.

Professional services and support
Experienced consultants and support staff are available to manage or support payer authentication service implementation.

Conclusions & Decisions

To effectively plan for the changes associated with payer authentication, merchants must:

- Revise order process flows and define new business rules associated with various transaction types, based on non participating card brands, customer experience, and exceptions to authentication coverage
- Decide whether card brands accepted will be limited only to those offering payer authentication services
- Decide which fraud screening measures will be used in conjunction with authentication services and how those will be implemented (including whether automated decision technology will be applied)
- Decide whether authentication services will be implemented using a hosted service or local software and how either integrates with current payment processing systems
- Decide, if the decision is made not to implement authentication services, how customer confidence will be maintained (e.g. what messages must be present at the time of check-out to instill confidence, knowing that card associations are heavily advertising authentication services to their cardholders)

THINGS TO KNOW

Major Companies Turn To CyberSource For Secure Transaction Solutions

- American Greetings
- Barnes & Noble
- Coldwater Creek
- Compaq
- CompUSA
- Fujitsu
- Home Depot
- Kohl's
- Nike
- OshKosh B'Gosh
- SkyMall

Questions About Payer Authentication?

Send your questions to info@cybersource.com and we will answer them promptly.

CyberSource
www.cybersource.com

United States
CyberSource Corporation
1295 Charleston Road
Mountain View, CA 94043
Tel: 888-330-2300
Tel: 650-965-6000
Fax: 650-625-9145

Europe
CyberSource International
400 Thames
Valley Park Drive
Thames Valley Park
Reading RG6 1PT.
Tel: 01189 653 484.

Japan
CyberSource KK
Toshin 24 Kudan Bldg.2F
3-2-5 Kudan-Kita, Chiyoda-ku
Tokyo 102-0073 Japan
Tel: +81-3-3511-0311
Fax: +81-3-3511-0317