

# FACT SHEET: Payer Authentication

Verified by Visa, MasterCard SecureCode, J/Secure

## Lower Processing Costs and Fraud Risk. Implement Payer Authentication Services Quickly and Easily.

### Program Overview

Payer Authentication services are based on the 3D-Secure standard. Programs include Verified by Visa, MasterCard SecureCode and JCB's J/Secure. These programs provide services to authenticate the purchaser at the time of an online sale via use of a cardholder-defined password. Merchants using these services receive fraud-related chargeback protection and lower processing rates as defined by the card association programs (see table below).

### How Payer Authentication Works

- When the "buy button" is clicked, a message is sent to the card brand's enrollment server to see if the cardholder is enrolled.
- If cardholder is enrolled, a form is presented within your checkout page which prompts for a password. If not enrolled, checkout proceeds as usual (or cardholder is prompted to enroll, "Activation During Shopping").
- The password is sent to the cardholder's bank for verification. If verified the transaction is "authenticated." If not authenticated, cardholder may be prompted to contact customer service or use an alternate payment method.

### Implementation Considerations

- *Messaging.* Usability studies show transaction completion is optimized when messaging regarding authentication is presented during the checkout process (Visa rules also require this).
- *Web/Call Center Interfaces.* If you use your web store payment screens for call center orders, separate interfaces will now be required. Payer Authentication screens cannot be supported in a call center environment (staff cannot enter password on behalf of cardholder as it would compromise cardholder security).
- *Split Shipments.* Systems must be able to store and re-submit authentication codes in case payment must be re-authorized (as in the case of split or delayed shipments).
- *Complementary Fraud Screening.* To maintain program compliance and protect against fraud perpetrated via the use of other card brands, complementary risk management tools and policies should be actively used.

Item	MasterCard	Visa
Chargeback Codes Covered by Liability Shift	RC37	RC75 RC83 (RC23, RC6)
Chargeback Protection (USA)	Fully authenticated transactions only	All transactions except excluded card types (e.g. Purchase Cards)
Chargeback Protection (Non-USA)	Fully authenticated transactions and attempts	All transactions except excluded card types (e.g. Purchase Cards)
Chargebacks Issued on Validated Transaction (US)?	Yes always issued, but merchant can re-present and reverse chargeback.	Chargeback is usually truncated (merchant gets no notification). Merchants classified in high risk categories receive chargebacks but can reverse by supplying authentication and enrollment check data.
Interchange Savings (basis points saved if payer authentication services are used)	<u>Credit Card</u> 22bps lower if enrolled 32bps lower if not enrolled <u>Debit Card</u> 49bps + \$0.01 lower if enrolled 50bps + \$0.01 lower if not enr. <i>Note: Issuer-dependent</i>	5 bps
Card Types Covered	Credit and Purchase Cards	Credit Cards
Activation During Shopping?	Yes	Yes
Merchant Options If Transaction Fails Auth.	Accept or Cancel.	Must Cancel.

#### Other Notes:

- Merchants with chargeback rates over 1% may not be eligible for chargeback protection.
- Does not work with "one-click-buy" or recurring billing programs

### CyberSource Solutions

CyberSource offers a hassle-free hosted service that supports Verified by Visa, MasterCard SecureCode, and J/Secure programs and can be implemented with any payment system.

1-888-330-2300

[www.cybersource.com](http://www.cybersource.com)

**CyberSource®**  
the power of payment