



April 12, 2004

To: Verified by Visa Merchants
Verified by Visa Acquirers
Verified by Visa Merchant Service Providers

The year 2003 was an active one for the Verified by Visa program, and 2004 promises even greater success. Verified by Visa provides Merchants with added security when accepting Visa payments over the Internet. Today, over 17,500 Merchants worldwide are processing Verified by Visa transactions with tens of thousands of others in the implementation process.

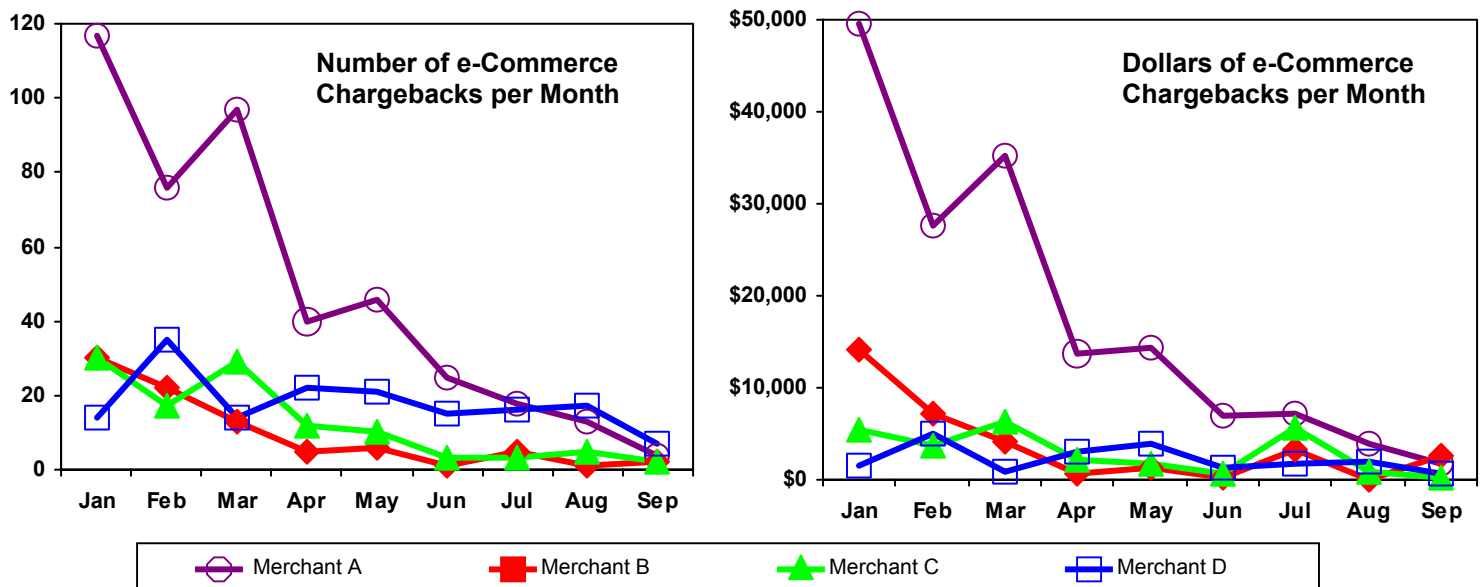
Participating Merchant¹s are protected from fraud liability for qualified purchases made with domestic and internationally issued Visa consumer credit and debit cards. Additionally, in August 2003, the interchange reimbursement rate for the CPS/e-Commerce Preferred Retail Payment Service which includes Verified by Visa transactions became five basis points lower than the Basic or standard electronic commerce transaction rate, providing an added reason for Merchants and Acquirers to participate in the program. To reiterate, if a Merchant participates in Verified by Visa, they receive these benefits regardless of whether the cardholder or Issuer participates in the qualified transaction, whether it is a Visa consumer credit or debit card, and whether the card is issued in the U.S. or overseas, with limited exceptions². The attached *Acquirer and Merchant Overview, April 2004 Update* describes the transaction qualifications in more detail.

Merchants also can benefit from reduced customer disputes and the related expenses when customers contact their card Issuer to report that they did not make a purchase. Participating Merchants that have implemented the Verified by Visa software and made changes to VisaNet processing to support the required authentication data in Visa Authorization Requests have achieved reductions in both the number of e-commerce chargebacks and dollars of chargebacks. Sales and chargeback trends for four Verified by Visa Merchants were monitored during January – September 2003. As can be seen in the graphs below, the Verified by Visa Merchants each experienced declines in fraud-related chargeback activity, leading to an overall reduction in chargeback volumes.

¹ This letter is intended for U.S. Merchants. Non-U.S. Merchants must consult with their Acquirers regarding rules governing the Verified by Visa program in other regions.

² Merchant protection from fraud related chargebacks does not apply for Visa Commercial Card and Anonymous Pre-Paid Cards, and transactions conducted in new channels (e.g., mobile phones), for transactions when the cardholder's password is not validated.

2003 Chargeback Experience – Four Verified by Visa Merchants



Verified by Visa does not completely eliminate chargebacks for electronic commerce transactions, but can have a significantly positive effect.

Security of payment card information continues to be an important factor in online shopping behavior for consumers. The third annual *UCLA Internet Report*, published in January 2003 cited the continuing security concerns as being expressed strongly by new Internet users, but also by experienced Internet users. And, in a July 25, 2003 report, *Online Credit Card Security Confidence Erodes*, Forrester Research indicated that consumer online security confidence relative to use of payment cards peaked between 2000 and 2001, declined in 2002, and remained flat in 2003 at that same level. Visa consumer research has shown that Verified by Visa increases consumer confidence. A Visa-sponsored online consumer study, completed in early 2004, clearly showed that interest in the service remains high and that Visa cardholders feel more secure about shopping when presented with the option to participate in Verified by Visa. The results indicate that with Verified by Visa, consumers are more comfortable with online shopping, more likely to shop at online stores that offer Verified by Visa, and spend more online.

Issuers continue to promote Verified by Visa to their cardholders and support activation programs through a variety of methods including web-site messaging, e-mail notifications, direct mail, and statement inserts. In the U.S. alone, over 250 million cardholders have been enabled to participate in Verified by Visa, and over 10,000 Issuers across the globe are also participating. Visa will continue Verified by Visa online advertising and promotional support in 2004, building more consumer awareness and driving online shoppers to participating Merchants. Visa will be launching different promotions throughout the year including a promotion associated with the 2004 summer Olympic games. In addition, Visa launched a new cardholder activation service, referred to as Activation Anytime, that uses a one page activation process to allow cardholders to

activate through banner advertisements, links on Issuer web-sites, and links on Merchant web-sites.

Visa has continued to actively monitor and improve the quality of the Verified by Visa program. With Visa card Issuers, Visa has established performance standards and additional product rules that assure each Issuer's implementation of Verified by Visa meets a high standard. As a result, Visa has been able to deliver significant improvements in the overall quality and consistency of the service. Visa monitors each Issuer's performance on an ongoing basis to verify that quality goals continue to be met. Each Issuer is also required to obtain pre-approval from Visa for its implementation (and any subsequent significant changes to its implementation), including such facets as the graphical User Interface and cardholder interactions, to ensure adherence to Visa's standards. Visa remains committed to providing Merchants with a high quality service.

Depending solely on Issuers to educate their cardholders and provide a high quality service is not enough. Visa-sponsored primary cardholder research, and Visa's experience working with participating Merchants, have clearly shown that participating Merchants must also actively help educate their customers on Verified by Visa to ensure success and minimize customer service calls. As a result, Visa has also modified its product rules to incorporate the following best practices:

- Implementation of an inline VbV window
- Placement of the VbV logo
- Pre-messaging at checkout to advise cardholders of Verified by Visa

Please review the attached overview for further details on these changes.

The objective of Verified by Visa is to increase security for payments in the Internet commerce environment, while reducing fraudulent use of payment cards online, in order to create a balanced value proposition for consumers and Merchants alike. The program's success relies equally upon Issuers, Merchants, and Acquirers. Visa appreciates your participation and support of Verified by Visa. The *Acquirer and Merchant Overview, April 2004 Update* summarizes the key areas on which Acquirers and Merchants will want to focus for their Verified by Visa program.

We look forward to working with you. For more information about Verified by Visa please contact your Visa or Acquirer representative.



Acquirer and Merchant Overview April 2004 Update

New Visa Root Certificate

Visa is migrating to a new root certificate (eCommerce) as a successor to the current root certificate (GP2) for all Visa-issued Verified by Visa digital certificates. Effective October 1, 2004, all new Verified by Visa digital certificates will be issued under the new eCommerce root. Merchants, Acquirers, or Merchant Processors that host the Verified by Visa service **must** take the following actions:

- *Root Certificate:* The root certificate is used by the Merchant to verify the digital signature on Payer Authentication Response messages received from Issuer Access Control Servers; this step assures Merchants that the message was received from an authorized Access Control Server. All Merchants, Acquirers, and Merchant Processors that host Verified by Visa Merchant processing **must** download and install the new eCommerce root certificate in the web server's trusted key store prior to October 1, 2004. The new eCommerce root certificate can be downloaded from the Visa website at:

<http://www.international.visa.com/fb/downloads/rootcert/main.jsp>.

Visa strongly recommends performing this step immediately. Merchants can verify the correct installation of the eCommerce root certificate via the Visa Product Integration Testing facility (PIT), at:

<https://dropit.3dsecure.net/PIT/UI?action=home>.

- *Merchant Client Certificates:* The Merchant client certificate is used by the Merchant for connections to the Visa Directory Server. Existing Merchant client certificates issued under the old GP2 root will continue to be valid until expiration (normally 2 years from the date the Merchant's certificate was issued by Visa), even if the expiration date extends beyond October 1, 2004. Therefore, no immediate action is required. However, Merchants should determine the expiration date of any existing certificates they may be using for Verified by Visa and be sure to request a new certificate well in advance of the expiration date. (Note: Visa sends a notification email to the address to which a prior certificate was fulfilled 60 days before a client certificate's expiration.)

Merchants, Acquirers and Merchant Verified by Visa Processors can direct any questions about the new root certificate by sending an email to VbVReports@visa.com.

Inline (Full Browser Window) Password Entry Page Requirement

As of April 15, 2004, presentations of Verified by Visa using a pop-up window are prohibited; instead, all Merchant implementations **must** use an inline page to present Verified by Visa. Pop-ups display as a separate, smaller window on top of the Merchant checkout page. The inline

Merchant and Acquirer Overview – April 2004 Update

page uses the full browser window of the Merchant to display the authentication page. With the announcement by Microsoft that the Internet Explorer (IE) browser will include pop-up suppression capabilities in the first half of 2004, and the growing usage and popularity of other pop-up suppression applications, pop-up implementations of Verified by Visa by Merchants are no longer viable. Existing Merchants that have implemented Verified by Visa via a pop-up presentation must convert to inline by June 30, 2004. All new Merchant implementations must use an inline approach.

Revised Merchant User Interface Product Rules and Best Practices

In recent months, Visa has conducted several user interface research studies of Verified by Visa with consumers and usability experts. Excerpts from the studies will shortly be available at www.visa.com/verified. These studies clearly demonstrate the importance of integrating Verified by Visa into the Merchant checkout process in as seamless a fashion as possible and of providing Merchant messaging and information that prepares cardholders for Verified by Visa. As a result, Visa has revised its Merchant user interface Product Rules and Best Practices for Verified by Visa and has published the revisions in a new version of the *3-D Secure Acquirer and Merchant Implementation Guide*, dated April 1, 2004. Key changes are summarized below. However, for a full description of all requirements and recommendations, Merchants should obtain the new version of the Implementation Guide from their Visa Acquirer or by downloading it from http://www.usa.visa.com/business/merchants/verified_index.html. The Product Rules identified below become effective April 15, 2004; all new implementations must adhere to the new requirements. Existing Merchants, that had begun their implementation of Verified by Visa before April 15, 2004, must comply with the Product Rules by June 30, 2004.

Key New Product Requirements:

- *Verified by Visa “learn more” Merchant symbol:* All participating Merchants **must** display the Verified by Visa “learn more” Merchant symbol during the checkout process, ideally on the checkout page near where the cardholder enters their credit card number. Visa consumer research has shown the importance of the presence of the “learn more” Merchant symbol: the Merchant symbol boosts the consumer’s confidence in making a purchase at the Merchant’s site, notifies the consumer that the Merchant participates in Verified by Visa, and provides the cardholder an easy way to learn more about the program.
- *Pre-messaging:* Participating Merchants **must** provide a concise “pre-message” on the checkout page. Visa’s usability research highlighted the importance of Merchant “pre-messaging” to help prepare users for an experience that may be new to them. Recommended wording and placement of the pre-message can be found in the Implementation Guide.

In addition to the new Product Rules, the revised *3-D Secure Acquirer and Merchant Implementation Guide* contains many new Best Practice recommendations for the Merchant user interface. Like the new Product Rules, the revised Best Practice recommendations draw upon Visa usability research that solicited feedback from consumers who shopped at existing Verified by Visa Merchants. Visa strongly recommends that Merchants follow these additional user interface recommendations. Doing so will provide the Merchant’s customers with the best possible user experience and maximize the Merchant’s benefits from participation in Verified by Visa.

Frequently Asked Questions

Why Implement Verified by Visa?

Verified by Visa was designed to increase security for online payments and reduce the fraudulent use of payment cards online by enabling Issuers to authenticate cardholders. Electronic commerce consumer transactions in which the Merchant authenticates or attempts to authenticate the cardholder are eligible to qualify as Custom Payment Service (CPS) e-Commerce Preferred transactions. Consumer transactions that are authenticated or attempted authentications are not eligible to be charged back by the Issuer for fraud-type reason codes. These include Chargeback Reason Codes 23, 61, 75 and 83 – which typically account for 50 to 70 percent of a Merchant's disputed e-commerce transactions. In addition, for Merchants that qualify transactions as CPS/e-Commerce Preferred Retail, the interchange rate applied to those transactions by Visa is five basis points lower than CPS/e-Commerce Basic Retail (standard electronic commerce without authentication data). In all events, actual pricing to Merchants is set independently at the discretion of the Acquirers.

For online purchases made with Visa Commercial Cards, transactions that are authenticated have the same chargeback protection as for Consumer Cards. Unlike for Consumer Cards, transactions in which the Merchant attempts to authenticate, but the cardholder is not enrolled, may be charged back by the Issuer if disputed as a transaction not made by the cardholder.

Note: The VisaNet processing requirements for authentication and attempted authentication transactions are important for Acquirers and Merchants – as support for these requirements **must** be in place to gain the benefits of fraud-related chargeback protection for authenticated and attempted authentication transactions and to qualify the transaction for CPS/eCommerce Preferred Retail.

What's Required to Qualify Transactions for CPS/e-Commerce Preferred?

The Authorization Request submitted by an Acquirer/Merchant for an authenticated or an attempted authentication must contain the Electronic Commerce Indicator (ECI) and Cardholder Authentication Verification Value (CAVV), returned in the Authentication Response, as proof of the authentication to qualify for chargeback protection. The Authorization Request must include the CAVV when supplied by the Issuer or by Visa, and an ECI of **5** (cardholder authenticated) or **6** (Merchant attempted to authenticate the cardholder) in the ECI field. VisaNet will qualify these authorizations for U.S. cardholders for CPS/e-Commerce Preferred for purposes of chargeback blocking³. Acquirers and Merchants will find additional information on VisaNet processing in the *3-D Secure Operations Guide for Issuers, Acquirers and Merchants*.

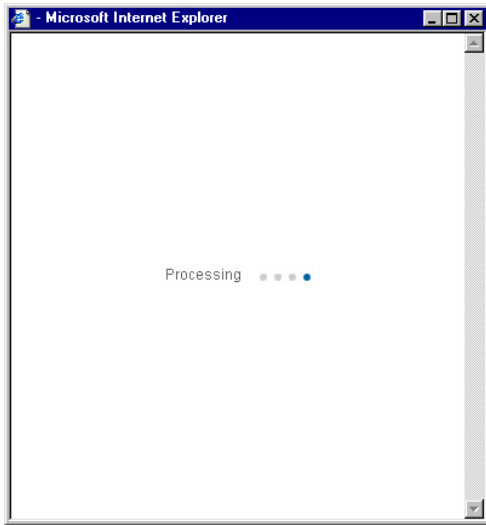
For non-U.S. cardholders, Merchants use the Verify Enrollment response of **N**, Non-Participating Issuer or cardholder, to include an ECI **6** in the Authorization Request with a blank CAVV field.

³ Merchants should contact their Visa Acquirer for further information about the qualification requirements for CPS e-Commerce Preferred.

What’s the Difference between Authenticated and Attempted Authentications?

An **Authenticated Transaction** involves a cardholder that has activated their card to participate in Verified by Visa. When the cardholder makes a purchase at a participating Merchant, the Issuer verifies the cardholder by a password or other identity information. The Merchant receives an approved Authentication Response with a CAVV and ECI of **5**.

An **Attempted Authentication Transaction** is a confirmation response that the Merchant attempted to process an authentication transaction. For an Attempt, neither the card number, nor cardholder, can be verified during authentication processing because the Issuer or cardholder are not participating in Verified by Visa. The Merchant receives an Attempts Response with a CAVV and ECI of **6**. The customer experience is shown below.



Attempts Processing Page

To ensure that participating Merchants are provided with the required proof of an attempted authentication, either the Issuer ACS or Visa will return an Attempts Response.

The processing for attempted authentications has no cardholder interaction; a “Processing” window (shown on the left) will be displayed while the Attempts Response is processed and returned to the Merchant.

When the Verified by Visa Merchant receives the Attempts Response, the message will have ECI and CAVV values for inclusion in the Authorization Request message. As noted earlier, these data elements must be included in the Authorization Request for the Merchant to receive chargeback protection.

What Chargeback Codes Are Protected by Verified by Visa?

The Chargeback Reason Codes applicable to authentication and attempted authentication transactions are shown in the chart below. These codes pertain to disputes in which the cardholder claims that they did not make the purchase. These chargebacks typically represent over half of disputes on electronic commerce transactions. All other chargeback reason codes continue to apply to e-commerce transactions.

Chargeback Reason Codes Affected by Payment Authentication

U.S. Chargeback Reason Codes	International Chargeback Reason Codes
23 Invalid T&E transaction	23 Invalid T&E transaction
61 Fraudulent mail/telephone order or electronic commerce transaction	75 Cardholder does not recognize transaction (effective October 2004 internationally)
75 Cardholder does not recognize transaction	83 Non-possession of card, fraudulent transaction

Merchant and Acquirer Overview – April 2004 Update

The Visa System averages for U.S. Acquirers/Merchants are shown below.

Percentage of Chargebacks Eligible for Verified by Visa Protection

Reason Code	% of Total Number of Chargebacks	% of Total Chargeback Dollars
23	1%	2%
61	30%	29%
75	15%	11%
83	20%	18%
Total Eligible for Verified by Visa Chargeback Protection	66%	60%
All Other	34%	40%
Total	100%	100%

Source: VisaNet System, Total e-Commerce Chargebacks, U.S. Acquirers, January/February 2004

As shown in the chart above, for U.S. Acquirers/Merchants on average, 66 percent of the total disputes/chargebacks and 60 percent of the chargeback dollars are eligible for protection by participation in Verified by Visa.

Do All e-Commerce Transactions Qualify for Attempts Chargeback Protection?

No – the Operating Regulations exclude the certain transactions types from the chargeback liability shift for attempted authentications:

- Commercial Card transactions
- Anonymous Prepaid Card transactions
- Transactions conducted in new channels (e.g., mobile phone)
- Transactions by Merchants identified through the U.S. and Global Merchant Chargeback Monitoring Program (GMCMP). Note: Acquirers of Merchants identified for U.S. or Global Chargeback Monitoring Programs **must** ensure that these Merchants do not submit Authorization Requests using an ECI of **6**; additional information will be forwarded to the Acquirers of identified Merchants.

Can Verified by Visa Merchants Eliminate Fraud Reduction Tools and Services?

No – fighting fraud is a continuing battle that requires all parties – Merchants, Acquirers, Merchant Service Providers, Issuers and Visa – to use and act on fraud detection capabilities. Verified by Visa is designed to supplement existing fraud management tools, not replace them. No one fraud tool provides the complete solution, it takes a combination of tools, including Verified by Visa, to manage fraud effectively. Verified by Visa is a new service and many cardholders are still learning about the service and so have not yet activated their card. If a cardholder is not participating, the Merchant will receive an Attempts Response. As noted above, in the case of an Attempt (ECI 6), there is no verification of the card number or

Merchant and Acquirer Overview – April 2004 Update

cardholder. Because the Merchant attempted to authenticate the cardholder, participating Merchants will be protected if the cardholder later disputes making the purchase under one of the chargeback reasons noted above.

If a Verified by Visa Merchant deactivates fraud reduction tools or services, the Merchant becomes vulnerable to fraudulent users of payment cards for Attempted Authentication transactions. Fraud rings that work the Internet are quick to identify Merchants that have removed fraud detection capabilities and target those Merchants for online purchases using lost and stolen payment cards.

What Happens if Fraud Is Reported on Authentication Transactions?

Visa has established Risk Identification Service (RIS) monitoring for reported fraud on Authenticated (ECI of 5) and Attempted Authentication (ECI of 6) transactions. Merchants that do not implement fraud detection capabilities will likely encounter higher reported fraud. If the level of reported fraud for a Merchant triggers the RIS parameters, the Merchant may be stasured as a High Risk Merchant, and they will lose the fraud-related chargeback protection afforded to Merchants participating in Verified by Visa. To avoid being stasured as a High Risk Merchant, Merchants **should always** implement and act on fraud detection/reduction capabilities. Merchants can find additional information by contacting their Visa Acquirer.

Should I continue use of Address Verification Service (AVS) and CVV2?

Merchants submitting electronic commerce transactions are required to continue to support AVS in order to qualify for CPS/e-Commerce Preferred and CPS/e-Commerce Basic. While use of CVV2 is at the Merchant's option, CVV2 is recommended for Merchant use as an additional fraud detection method. Both for AVS and CVV2, a "match" result is a positive indicator while "no match" result is a negative indicator. These fraud detection tools can assist Merchants in better identifying and reducing fraudulent transactions.