

Verified by Visa: Merchant Deployment Best Practices Factsheet

The rollout of Verified by Visa (VbV) is gathering momentum across the globe. By September 2005 29,000 merchants across Europe were using the service and this number is growing quickly.

Introduction

As VbV evolves some very valuable lessons can be learned from the marketplace.

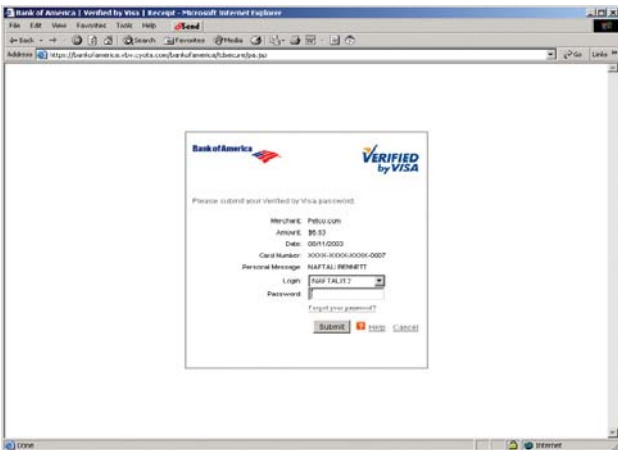
This Factsheet provides details of the way that the service should be configured and provides useful best practices information - for those merchants already using VbV, and for those who are about to deploy it.

Mandate: Inline Authentication Window

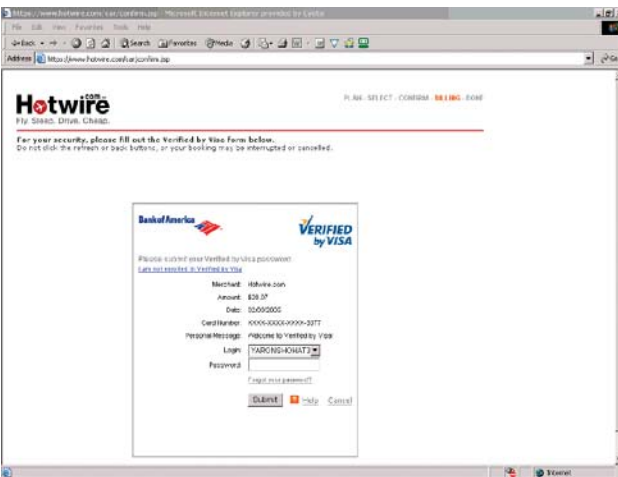
When implementing VbV, merchants have traditionally had two options in the way they configure the authentication windows - that is, pop-up windows or in-line windows.

With the pop-up authentication windows, research has shown that cardholders often mistake a new window as an advertising message, and will often close it without checking. In addition, cardholders with slower connections to the Internet are even more likely to close pop-up windows, often doing so before the window has completed loading in the browser.





Full Inline



Frame Inline

Closing a pop-up authentication window in this way impact the authentication process, cause unpredictable results and adversely affect the cardholder experience. One of the key lessons learned is that the window closure rates are substantially less with the inline authentication window.

In addition, as the rate of pop-up advertising has increased, pop-up suppression software (sometimes referred to as "pop-up killers") has gained increased market awareness and usage. Such software does not only occur in stand-alone applications, but some browsers and online service providers have begun to incorporate pop-up suppression as a standard feature of their service.

Visa strongly recommends that existing VbV merchants reconfigure the authentication page as inline windows, rather than pop-ups. New merchant deployment of VbV should only be implemented with inline windows.

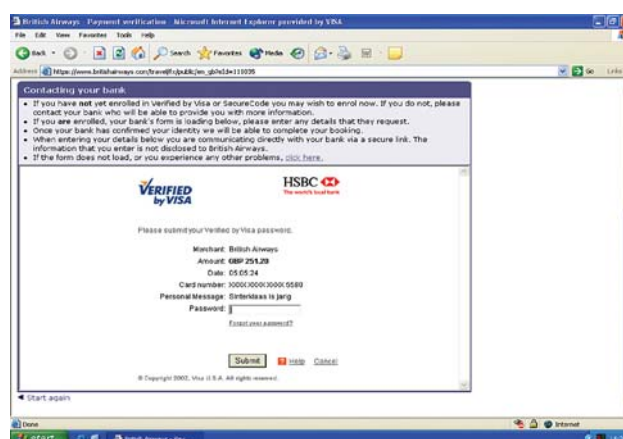
There are two possible options for deploying inline authentication windows:

Important aspects to consider when deciding on frame inline or full inline:

- > Full inline has the benefit of a simpler implementation and less scope for misunderstandings and mistakes.
- > Frame inline displays the VbV authentication page in the merchant's main window with the merchant's header. Therefore, VbV is seen as a natural part of the purchase process. It is recommended that the top frame include the merchant's standard branding in a short and concise manner and keep the cardholder within the same look and feel of the checkout process.
- > Frame inline implementation must also:
 - Provide enough screen space for the window to fit in. The recommendation is to use a top frame only in order to have a less "crowded" screen.
 - Ensure that the VbV authentication window is not pushed out of the viewable area for low-resolution screens.
 - Ensure that the frame does not include any other links or exit points that may distract the user from completing the VbV authentication process (such as "search" options, standard navigation menu, etc.).
 - Avoid using the HTML element iframe which can cause compatibility issues.
 - Ensure that all frames must be of HTTPS type. Avoid mixing HTTP and HTTPS.
 - Provide simple and correct instructions and allow cardholders with an easy way to go back.

Best Practice: 'Pre-message' Notification

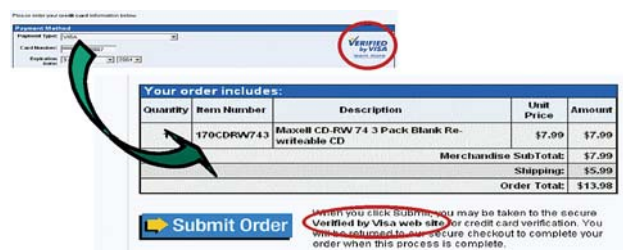
Pre-message increases cardholder awareness and prepares the cardholder for the next screen to be displayed. It is best to include generic text and not to make any assumptions that might confuse cardholders.



'Pre-message' Notification

Best Practice: VbV Logo

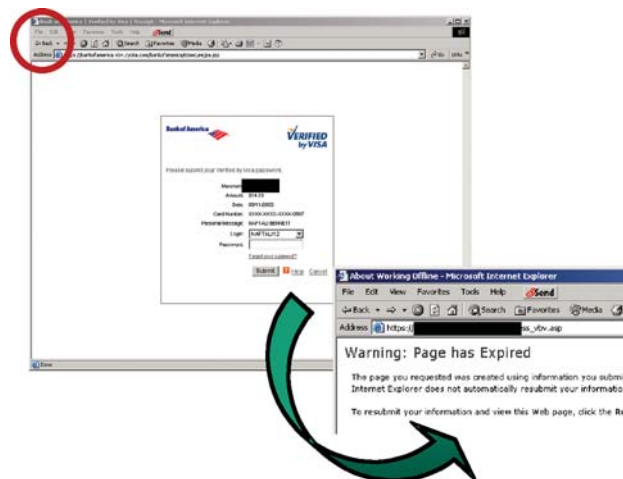
Research has shown that the VbV process is more successful and flows more smoothly when merchants include the VbV logo on the site and particularly at the checkout page.



VbV logo

Best Practice: "Back" Button Functionality

Where the policy of the merchant allows the use of the 'back' button, verify that it functions properly and test it thoroughly. Analysis has shown that some inline deployments do not function properly when a cardholder clicks the "Back" button. In some cases, when the "Back" button is clicked an alert is presented warning that the previous page has expired. Seeing this message some cardholders may close the window. Merchants should ensure that their inline deployment responds accordingly when cardholders click "Back". This feature should also be fully tested.



"Back" Button Functionality

Best Practice: Merchant Plug-In (MPI) configuration

In terms of configuring the MPI to connect to the Visa Directory Server (DS), Visa's strong recommendation is to:

- > Use Uniform Resource Locator (URL) for routing messages to the Visa DS (and not straight IP addresses)
- > Enable automatic "failover" to the alternative DS URL if receiving a network failure from the primary center.

The following table contains the Visa DS URLs for merchants based in Europe:

	URL
OCC DS	dsw.visa3dsecure.com/DSMsgServlet
OCE DS	ds.visa3dsecure.com/DSMsgServlet

Best Practice: VbV for cardholders only

Visa recommends that the use of VbV should be restricted to web-using customers.

Some early experience has shown that some multi-channel merchants operate a "sales rep zone", whereby sales representatives use the website infrastructure to process telephone order transactions. They will therefore key customer orders into the website when speaking to the cardholder on the telephone.

It is recommended that merchants should avoid deploying VbV at these zones.

Further information

For further generic information on VbV, merchants should contact their acquiring bank or visit www.visaeurope.com.

