

3-D Secure Best Practices Guide for Merchants

INTRODUCTION

As 3-D Secure continues to evolve and gain momentum in the marketplace, some valuable lessons can be learned from the first three years of running the service.

This guide provides Best Practices for Merchants who wish to deploy 3-D Secure in the most effective way possible.

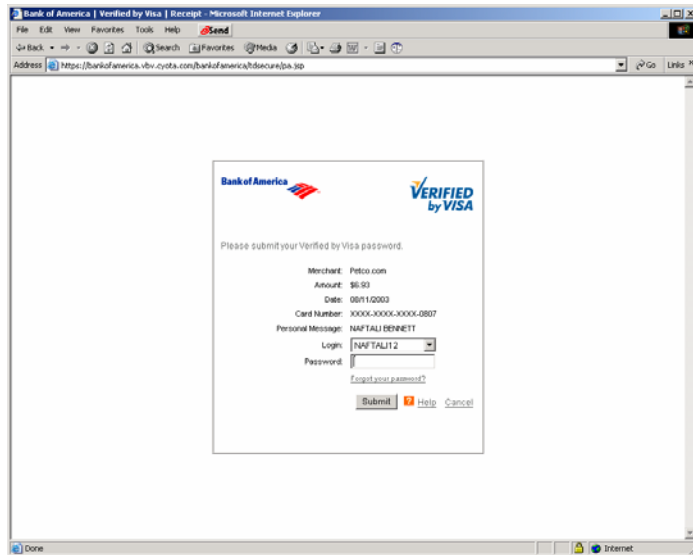
This guide is provided by Visa EU, Cyota and DataCash as a service to Merchants who have 3-D Secure and would like to get more information on implementation best practices.

BEST PRACTICES FOR MERCHANTS

Analysis of leading 3-D Secure supporting Merchants affirms that Merchants who implement the Best Practices described in this document enjoy optimal cardholder reaction to the 3-D Secure flow. Cardholders who shop at 3-D Secure Merchants view the flow as an integral part of the check-out process and are more likely to successfully authenticate themselves, compared to those shopping with Merchants who do not deploy 3-D Secure in an optimal way. The result: a higher level of purchases guaranteed and highly satisfied customers.

1. INLINE VS. POP-UP

Recommendation: deploy 3-D Secure in an inline manner, rather than popping up a new window.



Rationale: Most 3-D Secure Merchants in the past have implemented a pop-up deployment, i.e. 3-D Secure receipts and ADS (Activation During Shopping) prompts appeared in a separate window that popped-up at the appropriate time. Pop-up deployments have encountered several challenges such as pop-up killers and people who automatically close all pop-up windows.

In an in-line deployment, the 3-D Secure window is embedded in the Merchant's main window, and is presented to the cardholder as part of the shopping process. Other best practices designed for inline Merchants can further enhance the cardholder experience (see next section).

2. PRE-3-D SECURE NOTIFICATION

Recommendation: include pre-3-D Secure notification text next to the "submit order" button, on the step prior to the 3-D Secure interaction window. (Importance level: high)

Rationale: In order to increase the effectiveness of deployments, it is recommended that Merchants display a notification regarding 3-D Secure before the receipt/ADS appears. Pre-3-D Secure notifications increase cardholder awareness and prepare the cardholder for the next screen to be displayed. It is best to include a generic text and not to make any assumptions that might confuse cardholders.

An example of such a message is "When you click Submit, you may be taken to the secure Verified by Visa web site for credit card verification. You will be returned to our site when this process is complete." (see image below)

Please enter your credit card information below.

Payment Method
Payment Type:
Card Number:
Expiration Date:

VERIFIED by VISA

Your order includes:

Quantity	Item Number	Description	Unit Price	Amount
1	4170CDRW743	Maxell CD-RW 74 3 Pack Blank Re-writeable CD	\$7.99	\$7.99
Merchandise SubTotal:				\$7.99
Shipping:				\$5.99
Order Total:				\$13.98

Submit Order When you click Submit, you may be taken to the secure **Verified by Visa web site** for credit card verification. You will be returned to our secure checkout to complete your order when this process is complete.

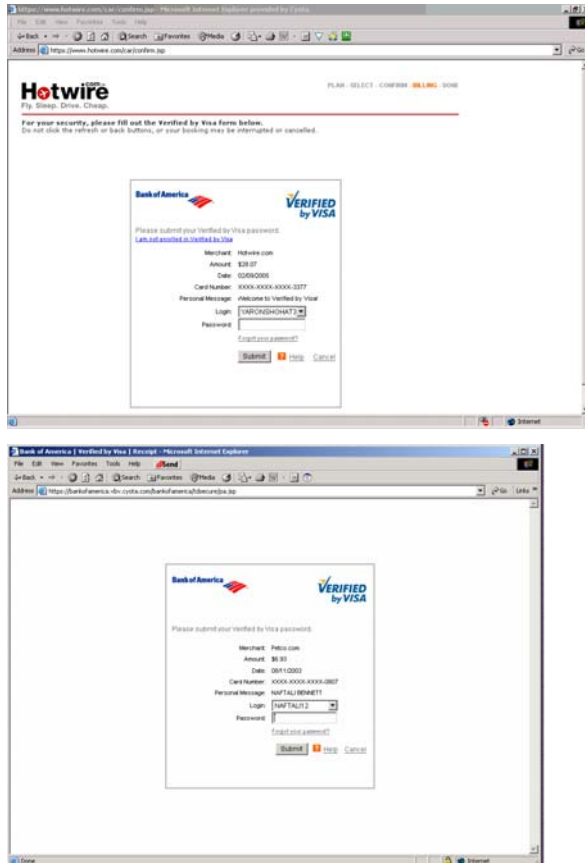
3. AWARENESS – VERIFIED BY VISA / MASTERCARD SECURECODE LOGO DURING PURCHASE

Recommendation: display Verified by Visa / MasterCard SecureCode logo during purchase.

Rationale: While the associations engage in increasing cardholder awareness of 3-D Secure on several levels through various media tracks, research has shown that the 3-D Secure process is more successful and flows more smoothly when Merchants include the Verified by Visa / MasterCard SecureCode logo on the site and particularly at the check-out page in which the cardholder inserts the PAN, in order to further increase awareness. Use of the logo in pre-3-D Secure notifications and in the last page of the checkout process is strongly recommended, since cardholders seeing it will recognize the same logo when, later on, the 3-D Secure message is displayed; as a result they will feel secure that this is a natural part of the purchase process.

4. FRAME INLINE VS. FULL INLINE

Recommendation: Tips on how to choose between the two possible inline implementation methods.



Rationale: While all inline deployments have proven to be more successful than pop-ups, Merchants can choose between two possible implementations: Frame Inline or Full Inline.

Full Inline has the benefit of a simpler implementation and less possibilities for mistakes.

However, Frame Inline has the benefit of allowing more control to the Merchants but has more possibilities for implementation errors.

Frame Inline deployments display the 3-D Secure receipts and ADS prompts in the Merchant's main window, while maintaining the Merchant's header, thus positioning the 3-D Secure process 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 & feel of the checkout process.

Points to look out for when using a Frame Inline implementation:

- Provide enough screen space so that the window can fit in. Cyota recommends using a top Frame only in order to have a less "crowded" screen. With a header Frame only, the Merchant still achieves the desired effect, while leaving enough room for the 3-D Secure page (400 X 390 pixels).
- Make sure the 3-D Secure window is not pushed out of the viewable area for low resolution screens.
- The frame should not include any other links or exit points that may distract the user from completing the 3-D Secure process (such as "search" options, standard navigation menu, etc.).
- Avoid using the HTML element iframe which can cause compatibility issues.
- All frames must be of HTTPS type. Avoid mixing HTTP and HTTPS.

See best practice #5 below.

5. INSTRUCTIONS AND LINKS ON TOP FRAME

Recommendation: when using a Frame Inline implementation, provide simple and correct instructions and allow cardholders with an easy way to go back.

Rationale: Simple text selection can improve usability instantly. The important issues to mind are:

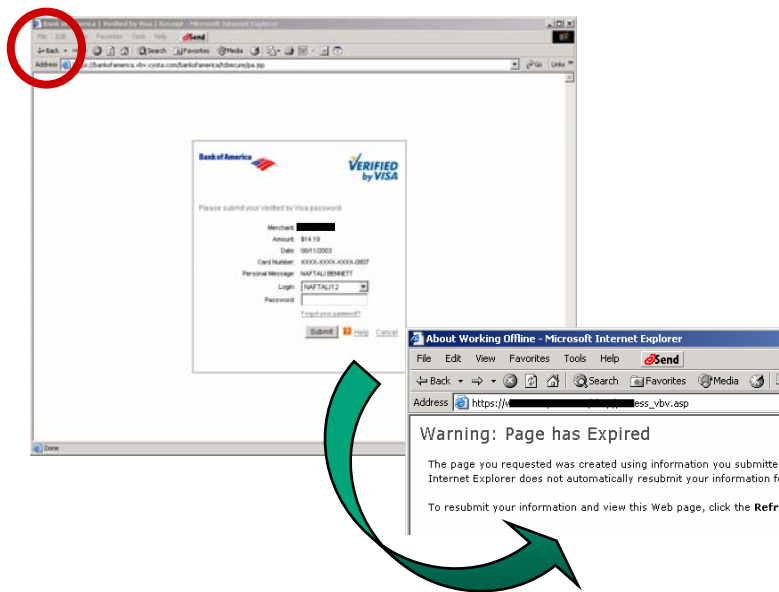
Provide short and concise explanation on the frame. Avoid making any assumptions that might confuse the user. In essence, the 3-D Secure window will provide the cardholder with all the needed instructions in order to complete the checkout process. An example text can be: "Below you will find your card issuer's 3-D Secure website. If you have not already signed up, you may be asked to do so in order to authenticate this transaction. Please follow the instructions below. These details will be visible to your card issuer only. If you do not see the details below or get stuck during the process, please click here to go back and try again."

Provide a link on the frame to allow cardholders who get stuck to get back to the payment page

6. "BACK" BUTTON FUNCTIONALITY

Recommendation: verify that the "back" button functions properly and test it thoroughly.

Rationale: An important issue Merchants should be aware of when choosing an inline deployment is handling the Internet browser "Back" button. Analysis has shown that some inline deployments do not function properly when a cardholder clicks the "Back" button on the 3-D Secure page. 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 important feature should be tested.



7. 3-D SECURE FOR SHOPPING SECTION ONLY

Recommendation: block 3-D Secure for transactions that are not initiated by web-using cardholders, but rather by the Merchant's own sales reps (importance level: low).

Rationale: Some Merchants – including those who have already implemented 3-D Secure - have a “sales reps zone” that allows sales representatives to use the web site infrastructure to key in cardholder orders as they speak to the cardholder on the phone. This makes sense as the web site infrastructure is leveraged for MOTO transactions, and the same authorization flow can be used. However, the Merchant should avoid deploying 3-D Secure at these zones, as cardholder authentication is a sensitive, individual process. The situation can be compared to someone asking for a user's ATM PIN over the phone in order to authenticate his or her identity. Typing the 3-D Secure password (in case of receipts) or Bank Details (in case of ADS messages) on behalf of the cardholder is either not practical or inconvenient for the cardholder. It is likely and reasonable that the cardholder would refuse to provide these details, and as a result will terminate the call. To avoid that, the Merchant is advised not to deploy 3-D Secure in “sales rep zones”.

**IF YOU HAVE ANY FURTHER QUESTIONS A MEMBER OF THE
DATACASH 3-D SECURE TEAM WILL BE HAPPY TO HELP YOU
TODAY**

TELEPHONE: 0870 72 74 76 1

EMAIL: 3DSECURE@DATACASH.COM