EMV®
3-D Secure

User Interface Guidelines

Version 2.1.0

April 2018

Legal Notice

This document summarizes EMVCo's present plans for evaluation services and related policies and is subject to change by EMVCo at any time. This document does not create any binding obligations upon EMVCo or any third party regarding the subject matter of this document, which obligations will exist, if at all, only to the extent set forth in separate written agreements executed by EMVCo or such third parties. In the absence of such a written agreement, no product provider, test laboratory or any other third party should rely on this document, and EMVCo shall not be liable for any such reliance.

No product provider, test laboratory or other third party may refer to a product, service or facility as EMVCo approved, in form or in substance, nor otherwise state or imply that EMVCo (or any agent of EMVCo) has in whole or part approved a product provider, test laboratory or other third party or its products, services, or facilities, except to the extent and subject to the terms, conditions and restrictions expressly set forth in a written agreement with EMVCo, or in an approval letter, compliance certificate or similar document issued by EMVCo. All other references to EMVCo approval are strictly prohibited by EMVCo.

Under no circumstances should EMVCo approvals, when granted, be construed to imply any endorsement or warranty regarding the security, functionality, quality, or performance of any particular product or service, and no party shall state or imply anything to the contrary. EMVCo specifically disclaims any and all representations and warranties with respect to products that have received evaluations or approvals, and to the evaluation process generally, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement. All warranties, rights and remedies relating to products and services that have undergone evaluation by EMVCo are provided solely by the parties selling or otherwise providing such products or services, and not by EMVCo, and EMVCo will have no liability whatsoever in connection with such products and services.

This document is provided "AS IS" without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in this document. EMVCO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AS TO THIS DOCUMENT.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to this document. EMVCo undertakes no responsibility to determine whether any implementation of this document may violate, infringe, or otherwise exercise the patent, copyright, trademark, trade secret, know-how, or other intellectual property rights of third parties, and thus any person who implements any part of this document should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, this document may provide for the use of public key encryption and other technology, which may be the subject matter of patents in several countries. Any party seeking to implement this document is solely responsible for determining whether its activities require a license to any such technology, including for patents on public key encryption technology. EMVCo shall not be liable under any theory for any party's infringement of any intellectual property rights in connection with this document.

Contents

Table of Figures

Introduction

This document provides guidelines about how the user interface (UI) is rendered based on the *EMV 3-D Secure Protocol and Core Functions Specification v 2.1.0.* The examples illustrated in this document are intended to provide guidance on implementing the EMV 3-D Secure UI.

App-based User Interface

The following section provides template examples and guidelines for building the Native and HTML User Interface (UI) to support 3-D Secure authentication for App-based implementations.

Native UI

Using Challenge Information Text

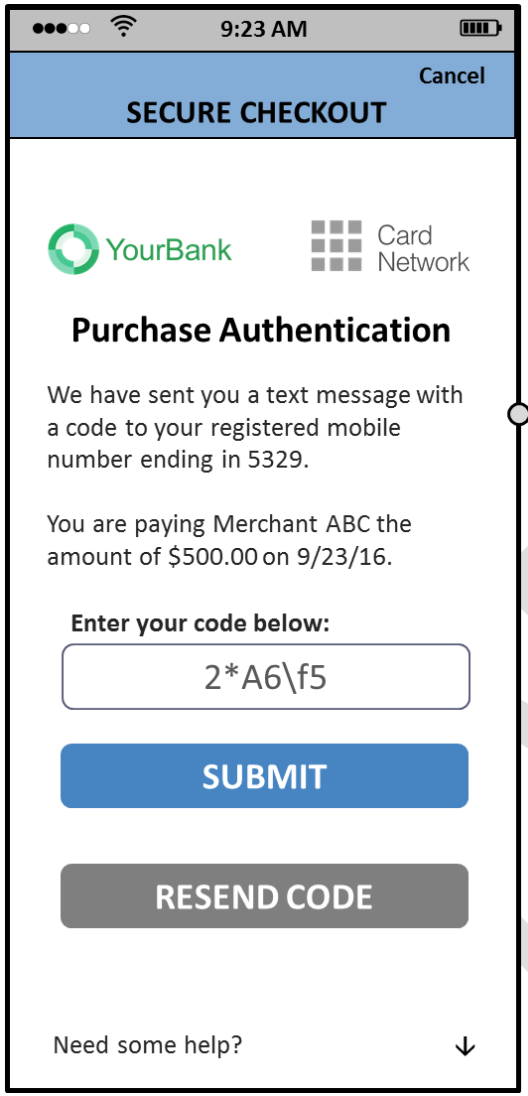
The Challenge Information Text data element is used to display additional ACS information during the challenge message exchange. Carriage returns can be utilised in this data element to enhance the user experience.

When a carriage return is required, the ACS places a carriage return symbol (“\n”) within the Challenge Information Text field as illustrated in the JSON example below.

```
"challengeInfoText":"We have sent you a text message with a code to your registered mobile number ending
in 5329\n\nYou are paying Merchant ABC the amount of $500.00 on 9/23/16"
```

The carriage return symbol (“\n”) signals the 3DS SDK to place two new lines on the screen as illustrated in Figure 1.

Figure 1: New Lines After Carriage Return Signal



Challenge Information Text (CRes)
We have sent you a text message with a code to your registered mobile number ending in 5329. \n\nYou are paying Merchant ABC the amount of $500.00 on 9/23/16.

Using Challenge Information Text Indicator

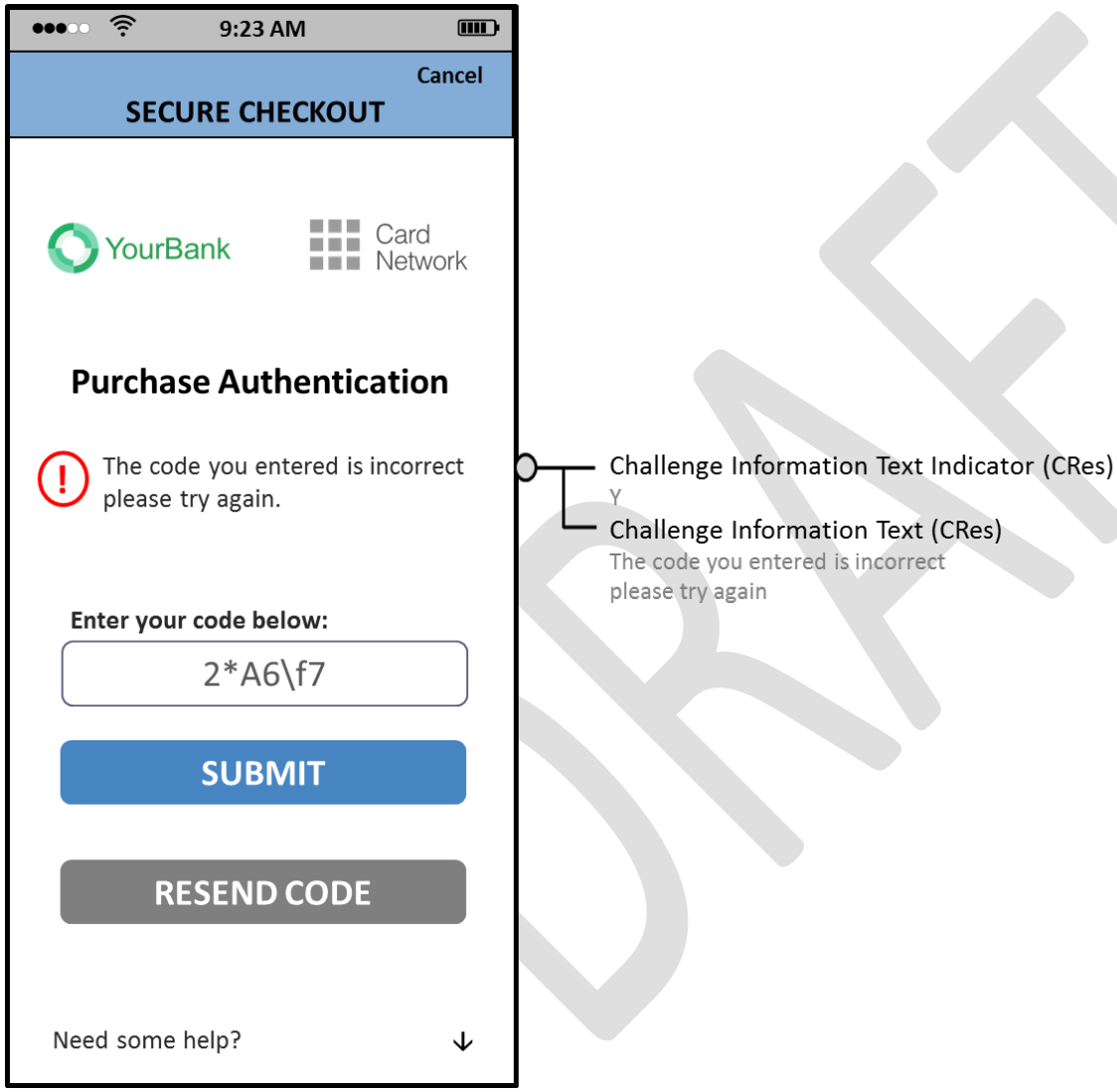
In the Native UI, the Challenge Information Text Indicator data element is utilised in the CRes message to inform the cardholder of an invalid attempt in the original CReq message.

The ACS populates the Challenge Information text field with a value = Y as illustrated in the JSON example below.

```
"challengeInfoTextIndicator":"Y"
```

Populating the Challenge Information Text Indicator field with value = Y signals the 3DS SDK to display a warning indicator as illustrated in Figure 2 below.

Figure 2: Warning Indicator



Displaying Single and Multi-select Fields

The following fields are utilised to display single and multi-select formats:

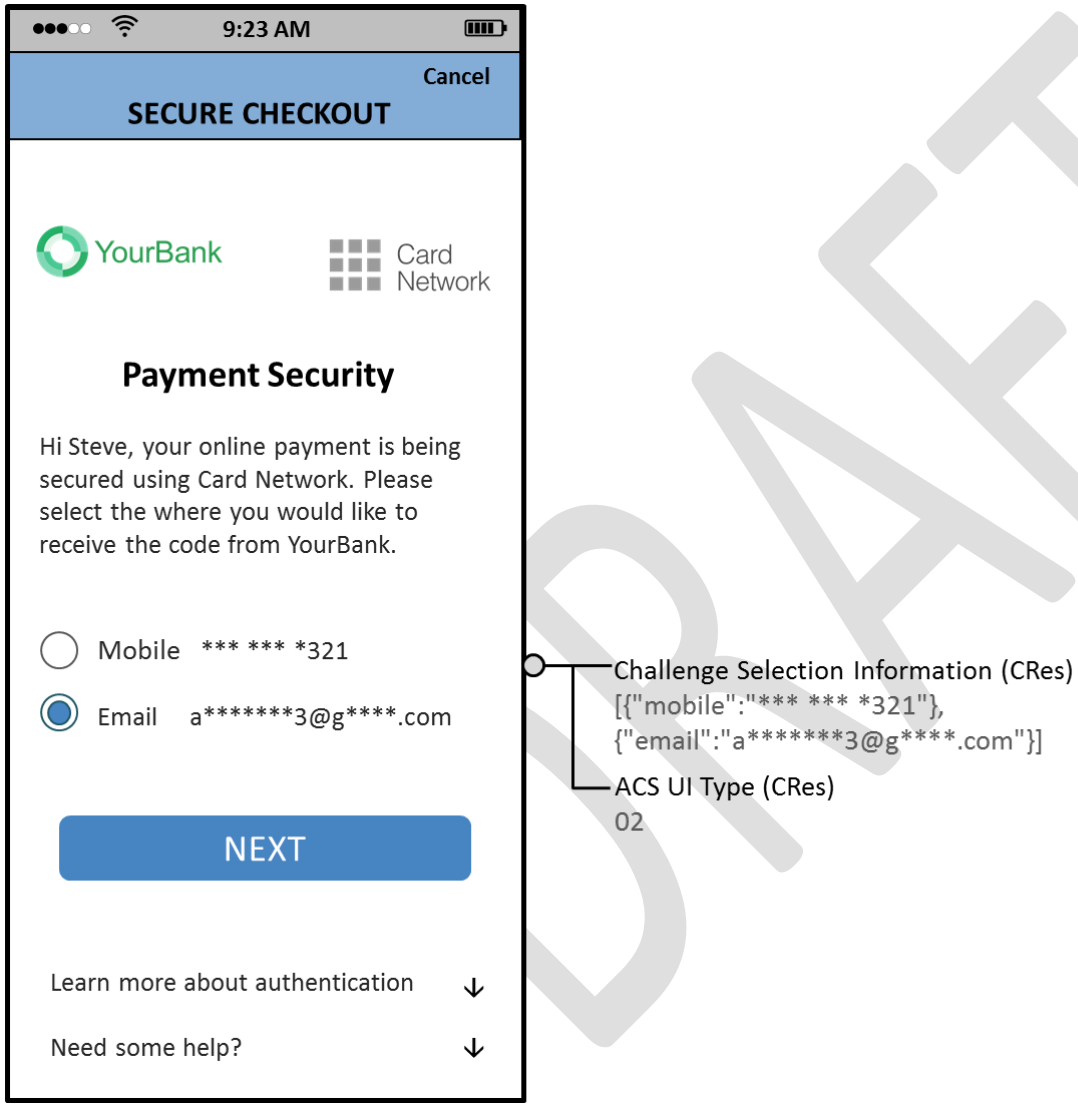
- ACS UI Type:
  - 02 = single-select
  - 03 = multi-select
- Challenge Selection Information—using an array format that includes the list of information to present

The ACS populates the ACS UI Type and Challenge Selection Information to instruct the 3DS SDK to render the single-select UI as illustrated in the JSON example below.

```
"acsUiType":"02",
"challengeSelectInfo" :[{"mobile":"*** *** *321"}, {"email":"a*******3@g****.com"}]
```

Figure 3 below illustrates how the 3DS SDK interprets the data elements to display the UI.

Figure 3: Single-select Template



Displaying Out of Band Fields

Three fields are utilised to display the Out of Band (OOB) template:

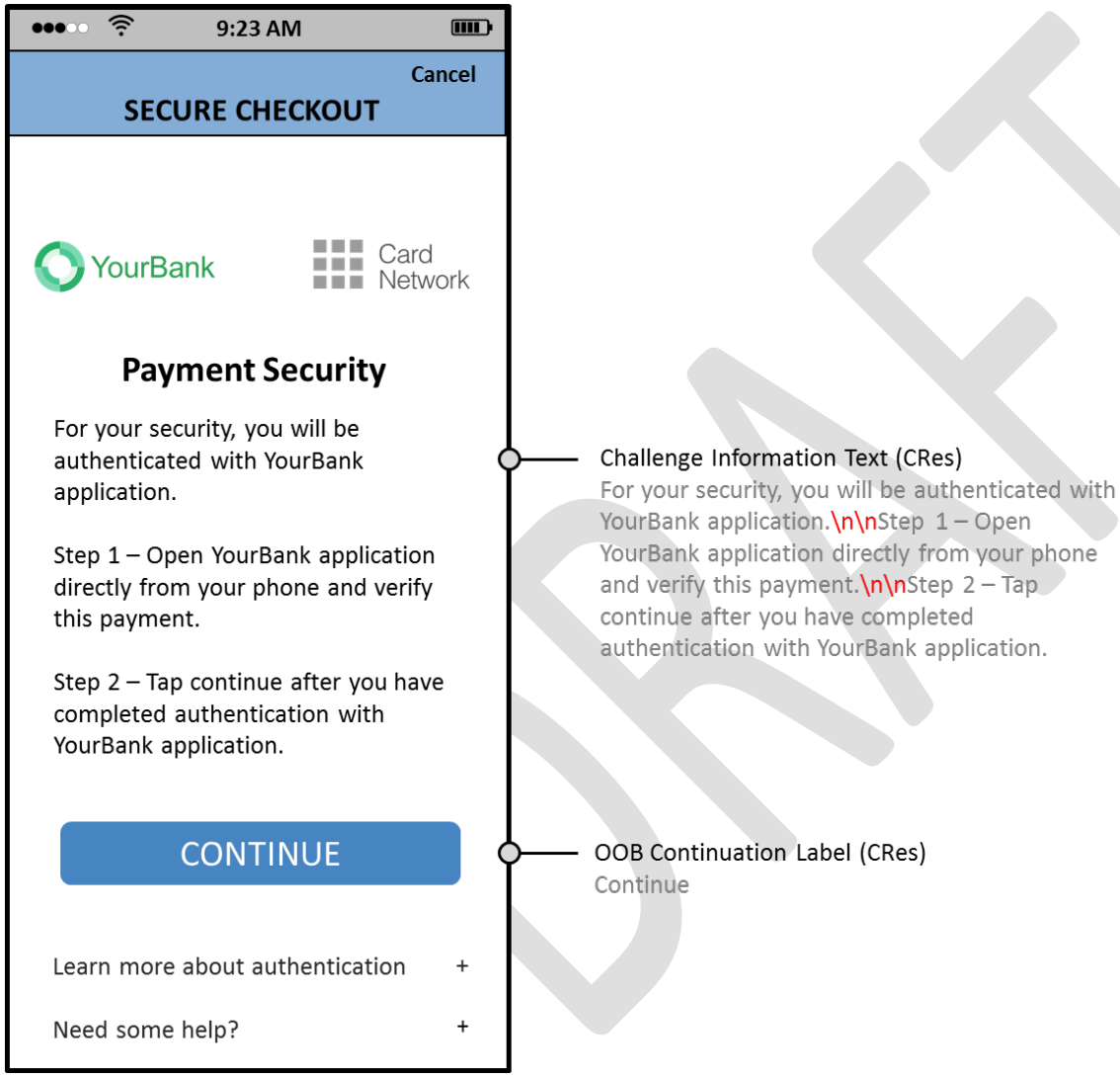
- ACS UI Type:
  - 04 = OOB
- OOB Continuation Label—3DS SDK displays the text provided on the button
- Challenge Information Text—3DS SDK displays the text provided on the screen

The ACS populates the ACS UI Type, Challenge Information Text and the OOB Continuation Label to instruct the 3DS SDK to render the OOB UI as illustrated in the JSON example below.

```
"acsUiType":"04",
"oobContinueLabel":"Continue"
"challengeInfoText":"For your security, you will be authenticated with YourBank application.\n\nStep 1 –
Open YourBank application directly from your phone and verify this payment.\n\nStep 2 – Tap continue after
you have completed authentication with YourBank application."
```

Figure 4 below illustrates how the 3DS interprets the data elements to display the UI.

Figure 4: Out of Band Template



Using Challenge Additional Information Text

In the native UI, when ACS UI type = 04 (Out of Band), cardholder instructions are displayed using the information provided by the ACS within the Challenge Information Text field.

When the 3DS Requestor App moves to the foreground, the ACS uses the Challenge Additional Information Text to provide text that will replace the Challenge Information Text and/or the warning icon (Challenge Information Text Indicator).

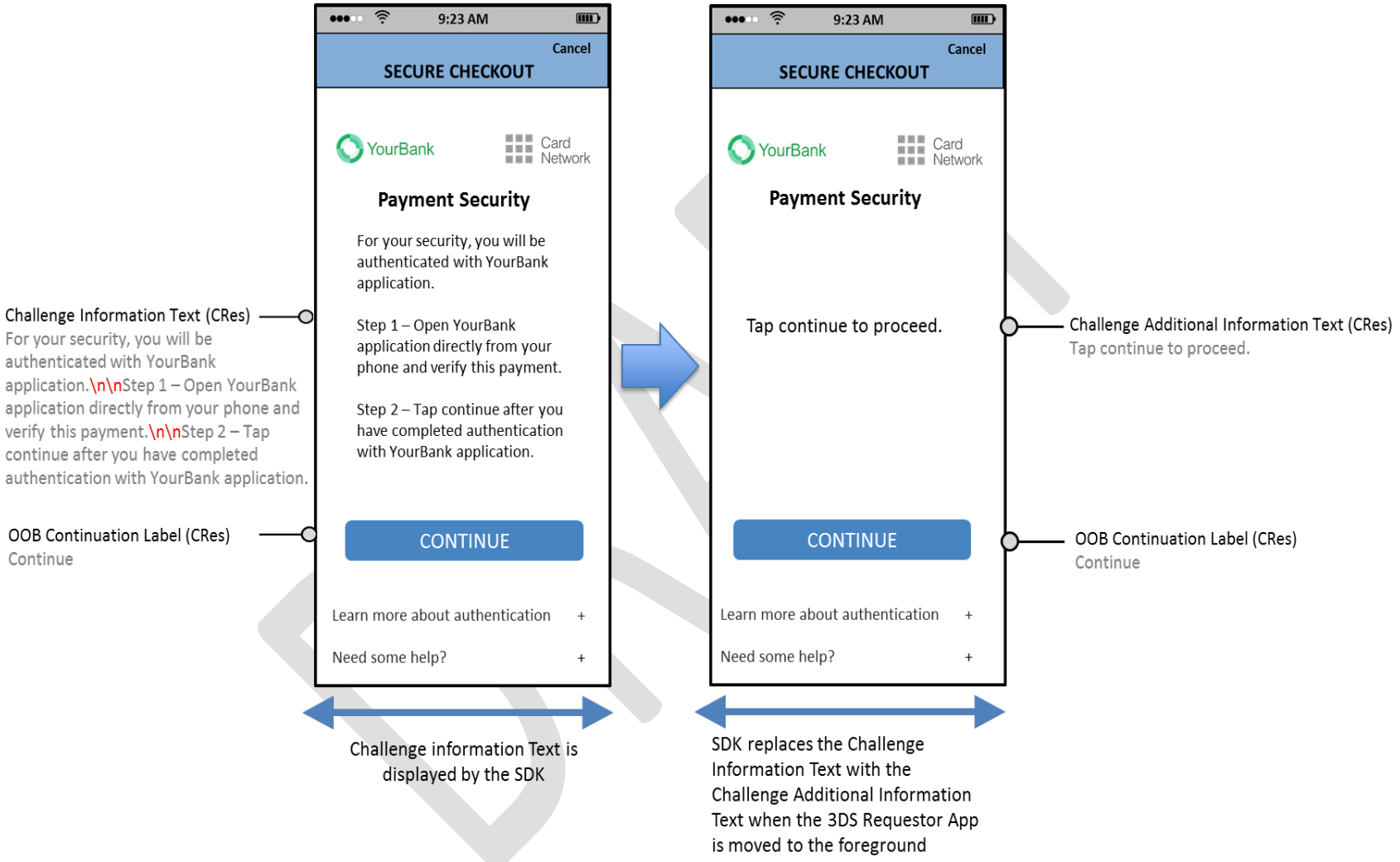
Replacing Challenge Information Text with Challenge Additional Information Text

The JSON example below illustrates the contents of the CRes message required by the 3DS SDK to display the replacement text.

```
"acsUiType":"04",
"oobContinueLabel":"Continue",
"challengeInfoText":"For your security, you will be authenticated with YourBank application.\n\nStep 1 –
Open YourBank application directly from your phone and verify this payment.\n\nStep 2 – Tap continue after
you have completed authentication with YourBank application.",
"challengeAddInfo":"Tap continue to proceed"
```

Figure 5 below illustrates the sample processing flow used by the 3DS SDK to replace the Challenge Information Text with the Challenge Additional Information Text.

Figure 5: Challenge Additional Information Text



Replacing Challenge Information Text and Warning Icon (Challenge Information Text Indicator)

The JSON example below illustrates the contents of the CRes message that allows the 3DS SDK to render the initial OOB UI using the Challenge Information Text data element.

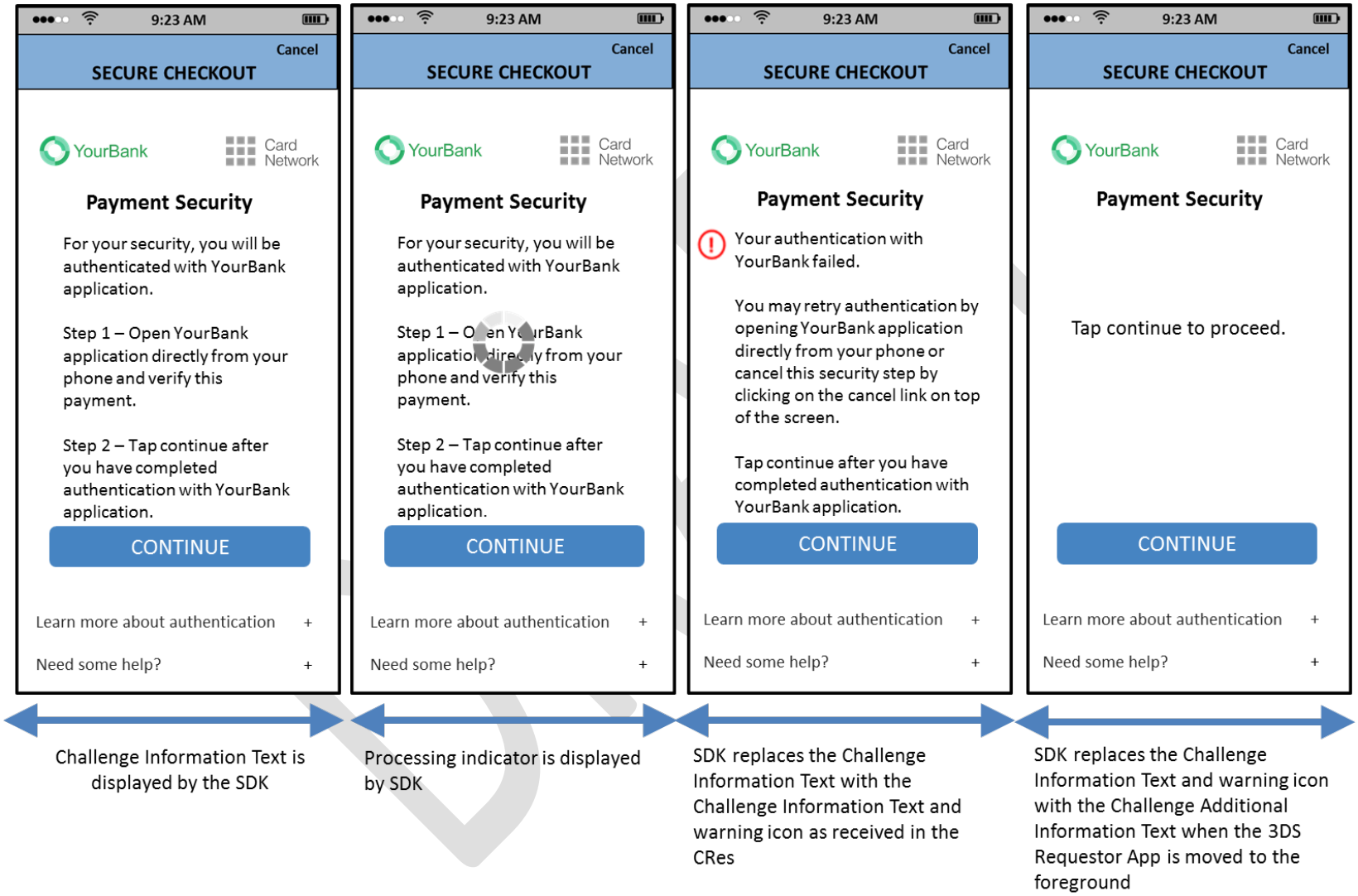
```
"acsUiType":"04",
"oobContinueLabel":"Continue",
"challengeInfoText":" For your security, you will be authenticated with YourBank application.\n\nStep 1 –
Open YourBank application directly from your phone and verify this payment.\n\nStep 2 – Tap continue after
you have completed authentication with YourBank application."
"challengeAddInfo":"Tap continue to proceed"
```

If the cardholder presses Continue but did not complete authentication with the ACS, the 3DS SDK displays a warning icon and further instructions to the cardholder. The JSON example below illustrates the contents of the CRes message that allows the 3DS SDK to display a warning icon and cardholder instructions. The ACS also provides text (Challenge Additional Information Text) to replace the warning icon (Challenge Information Text Indicator) and the cardholder instructions (Challenge Information Text).

```
"acsUiType":"04",
"oobContinueLabel":"Continue",
"challengeInfoText":"Your authentication with YourBank failed.\n\nYou may retry authentication by opening
YourBank application directly from your phone or cancel this security step by clicking on the cancel link
on top of the screen.\n\nTap continue after you have completed authentication with YourBank application.",
"challengeInfoTextIndicator": "Y",
"challengeAddInfo":"Tap continue to proceed"
```

Figure 6 below illustrates the sample processing flow used by the 3DS SDK to replace the Challenge Information Text and the warning icon (Challenge Information Text Indicator) with the Challenge Additional Information Text.

Figure 6: Challenge Additional Information Text



Displaying Expandable Information

Expandable Information can be displayed in two locations on the screen.

Two fields are utilised to display expandable information:

- Why Information Label/Expandable information Label—Presented by the 3DS SDK to appear in the cardholder UI
- Why Information Text/Expandable Information—Displayed when the Why Information Label or Expandable Information Label is selected by the cardholder

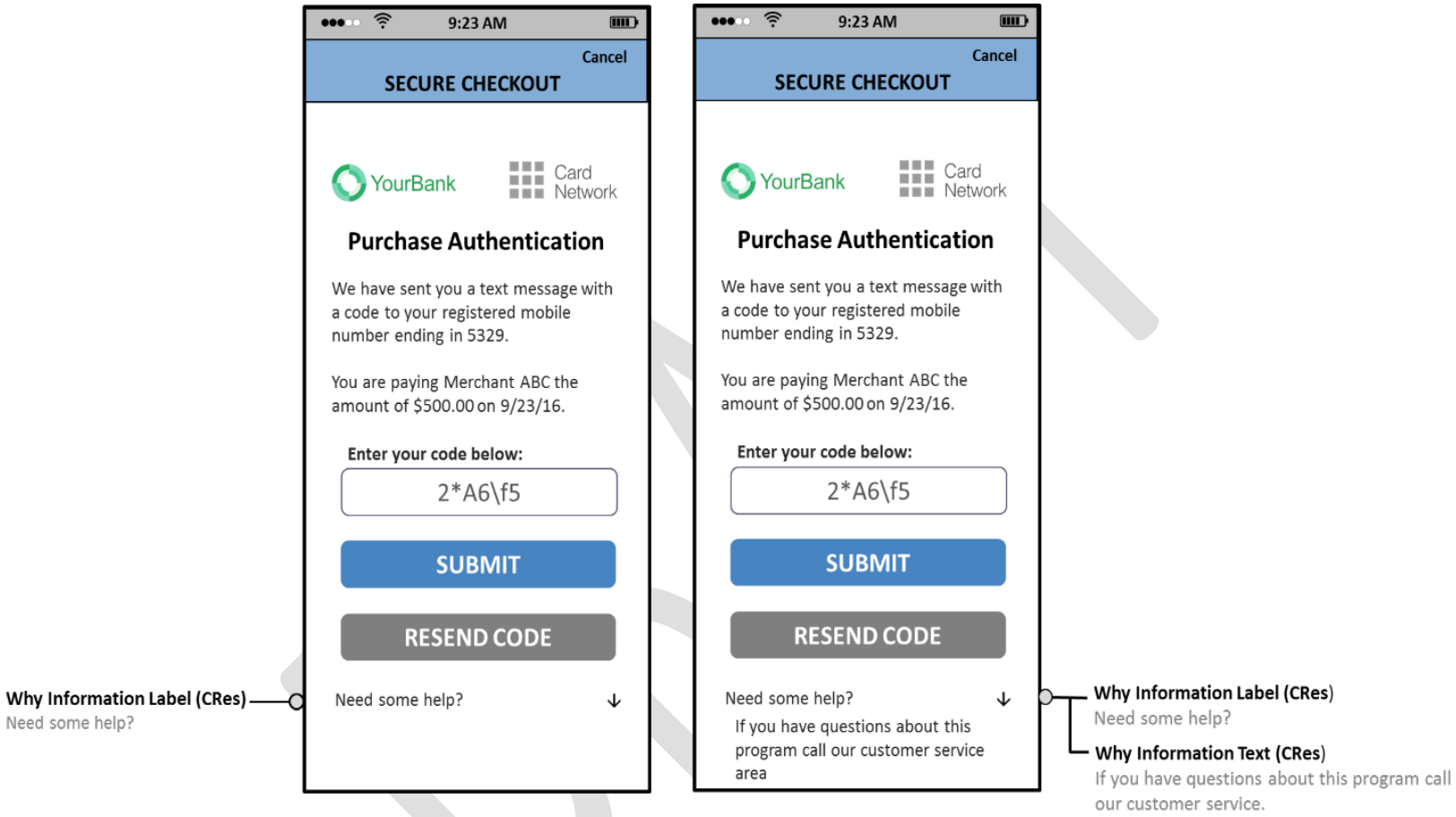
A Carriage return can also be utilised to enhance the user experience and is represented by an “\n”.

The following JSON example illustrates the contents of the CRes message that allows the 3DS SDK to render expandable information on the UI.

```
"whyInfoLabel":"Need some help?",
"whyInfoText":"If you have questions about this program call our customer service."
```

Figure 7 below illustrates the UI that is displayed when the cardholder selects or does not select the Why Information Label.

Figure 7: Why Information Text and Label

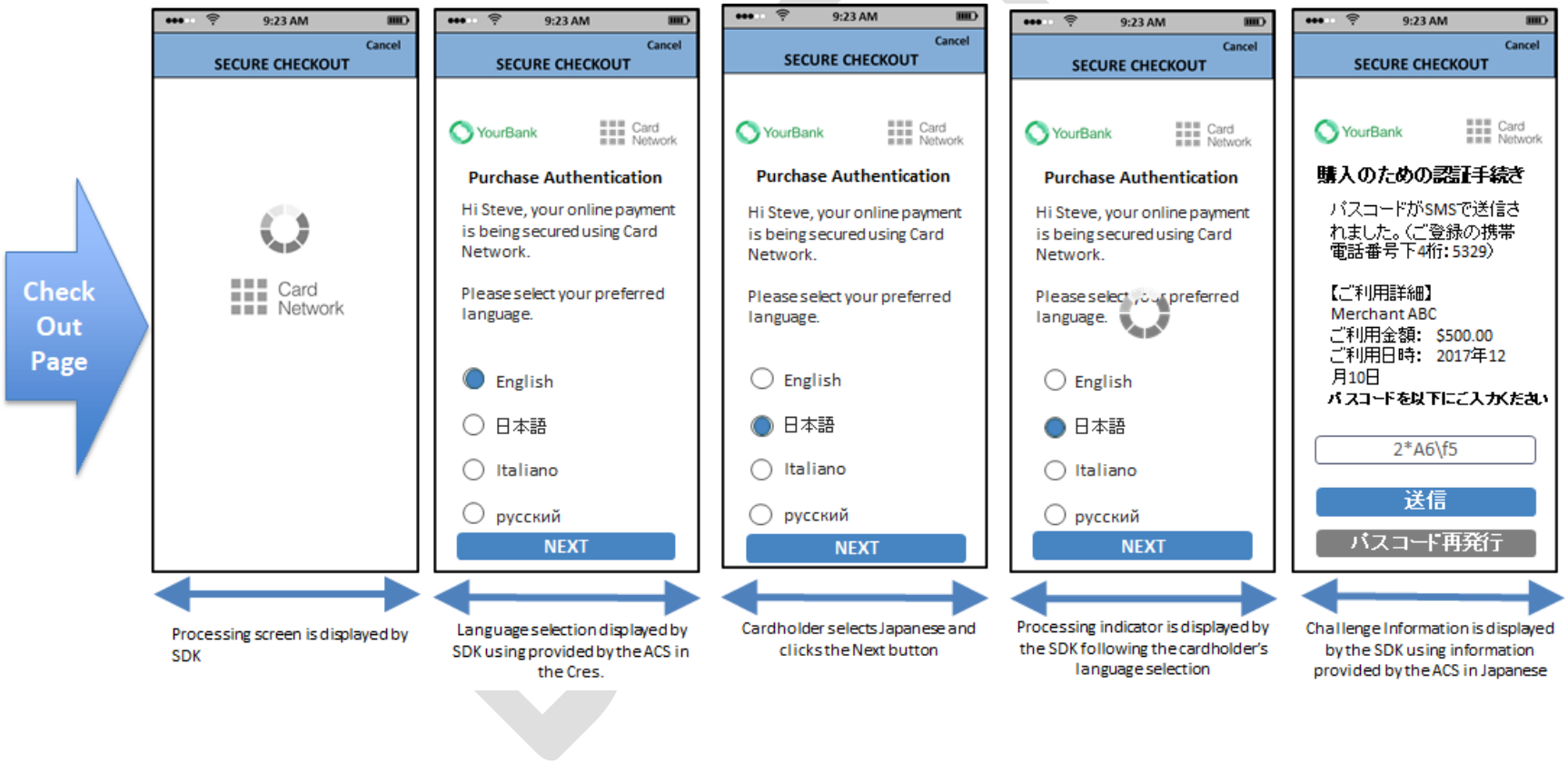


Supporting Cardholder Language Selection

The UI can be utilised by the ACS to support multiple languages during the authentication process.

Figure 8 below illustrates the cardholder user experience during an app-based transaction when the ACS supports multiple languages. The ACS supports cardholder language selection using a Single Select UI and completes the authentication in Japanese using a Text UI.

Figure 8: Multi-language Support

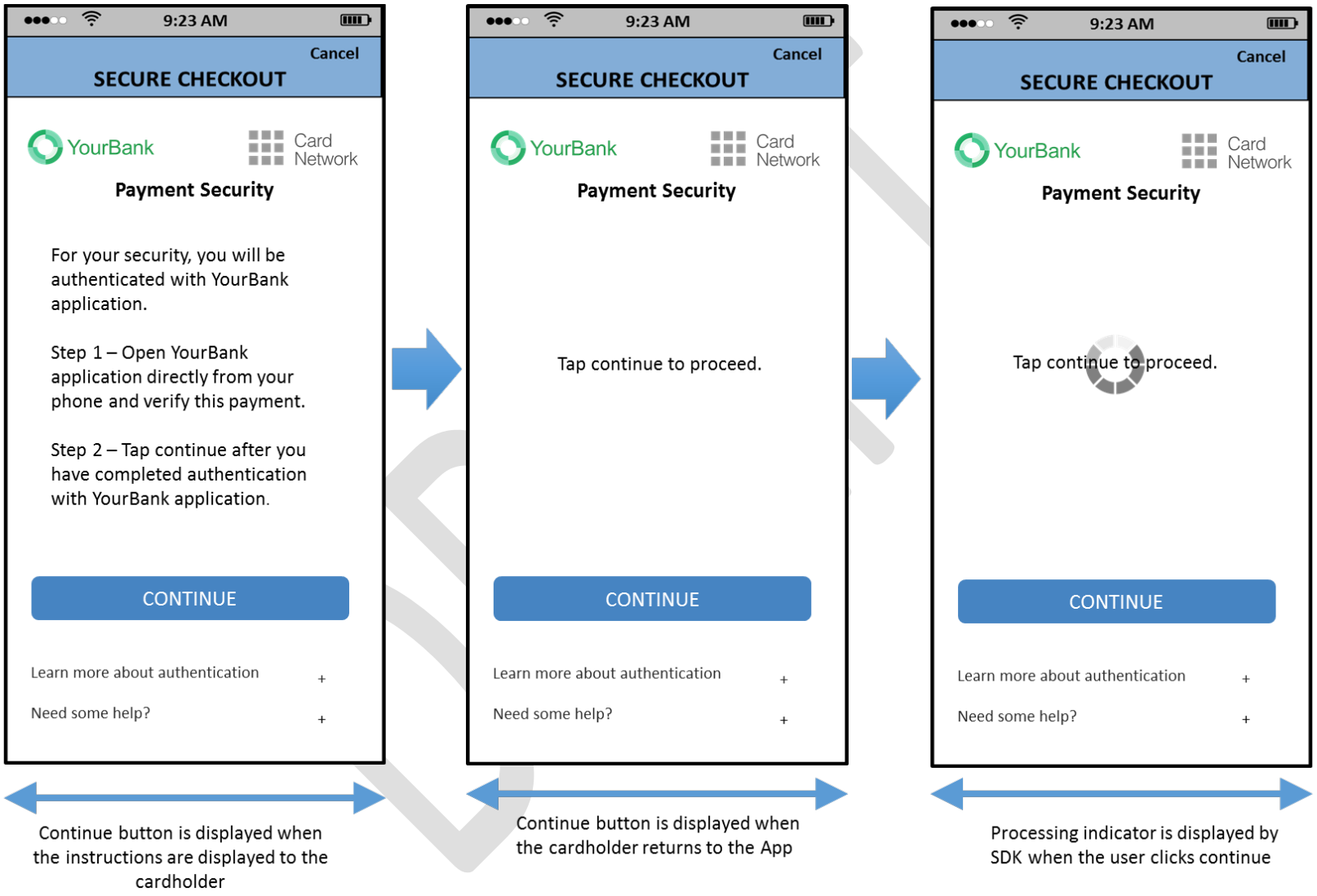


Labelling buttons

This section provides template examples and guidelines for labelling buttons on the User Interface (UI) to support 3-D Secure authentication

The button label **Continue** should be utilized when the cardholder is required to perform an action outside the current screen, then return to the screen once that action is complete. For example, during an Out of Band (OOB) challenge the cardholder receives instructions on the screen on how to complete the authentication process. Figure 9 below illustrates how the Continue label is utilised during the OOB flow.

Figure 9: Continue Label—OOB



The button label **Next** should be utilized when there are pre-defined set of screens to complete the authentication process. For example where the cardholder can select the preferred language to complete the authentication process.

The button label **Submit** should be utilized when the cardholder is submitting a final response to complete the authentication process.

If there are a series of responses to be submitted then the button label **Submit** should be utilised only when the cardholder is submitting the last response. Prior screens should utilise the **Next** button. The image below illustrates the cardholder experience using the **Next** and **Submit** button labels.

Figure 10: Next and Submit Buttons

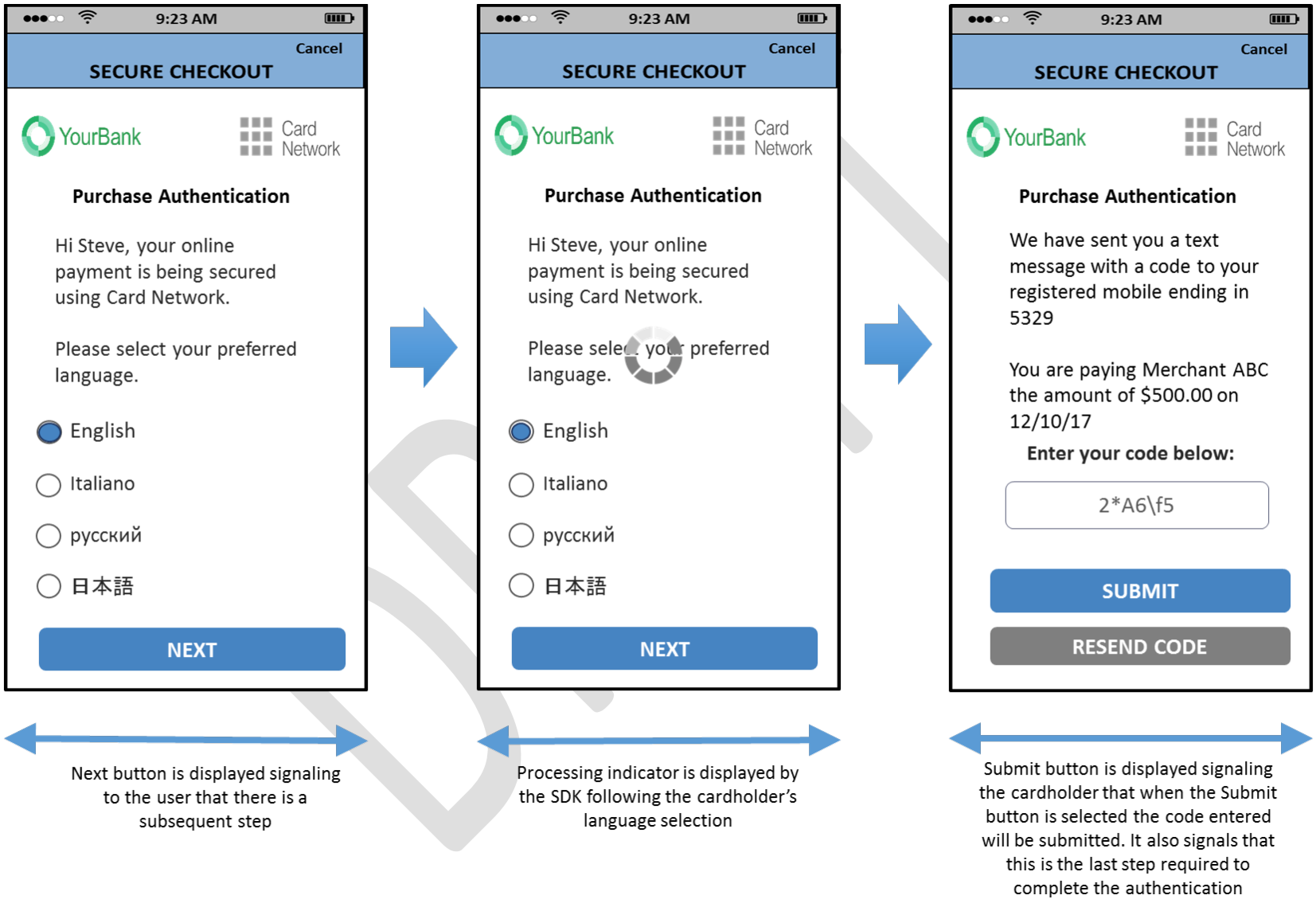
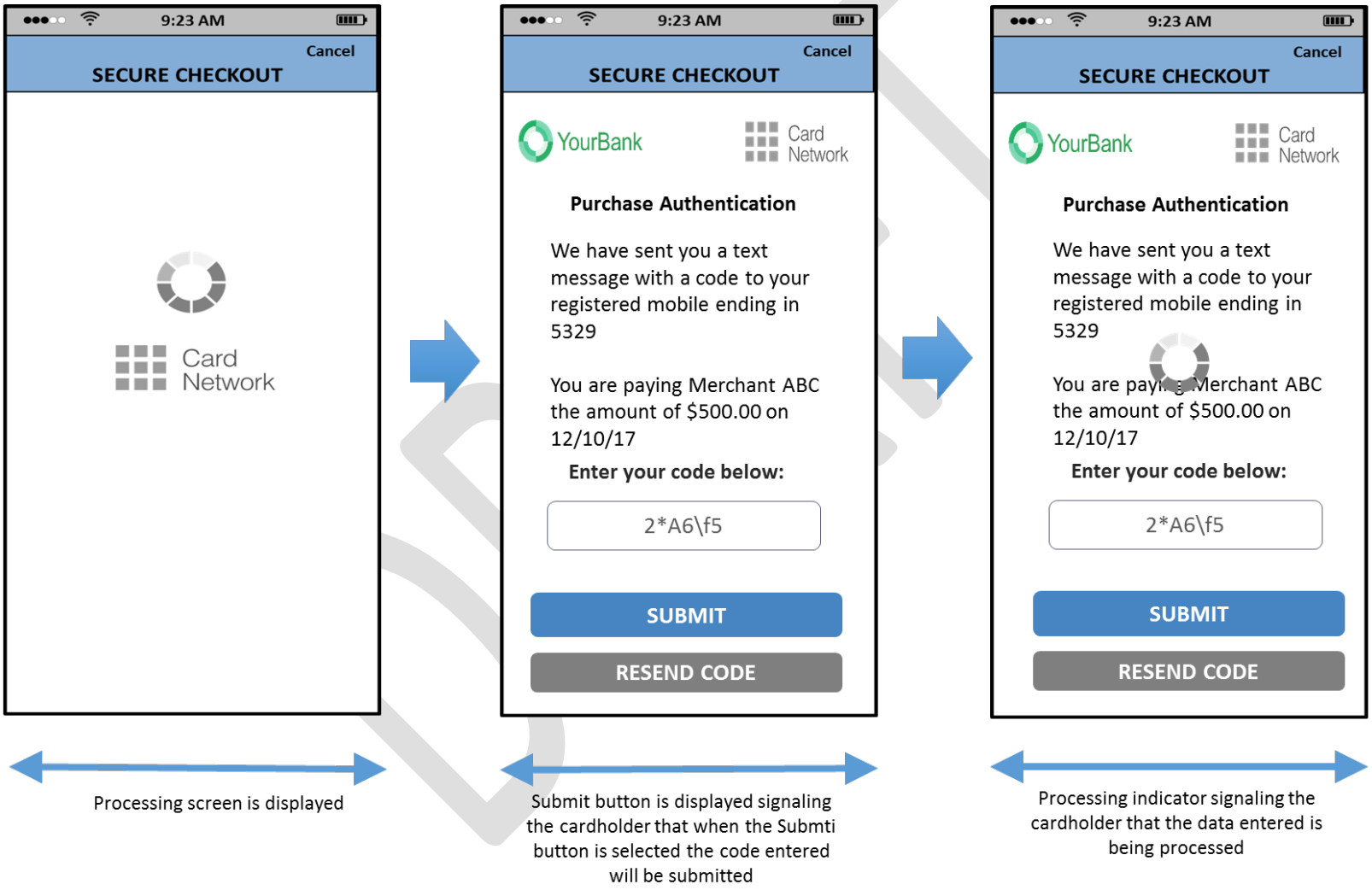


Figure 11 below illustrates the cardholder experience when only the Submit button label is utilised.

Figure 11: Submit Button



HTML UI

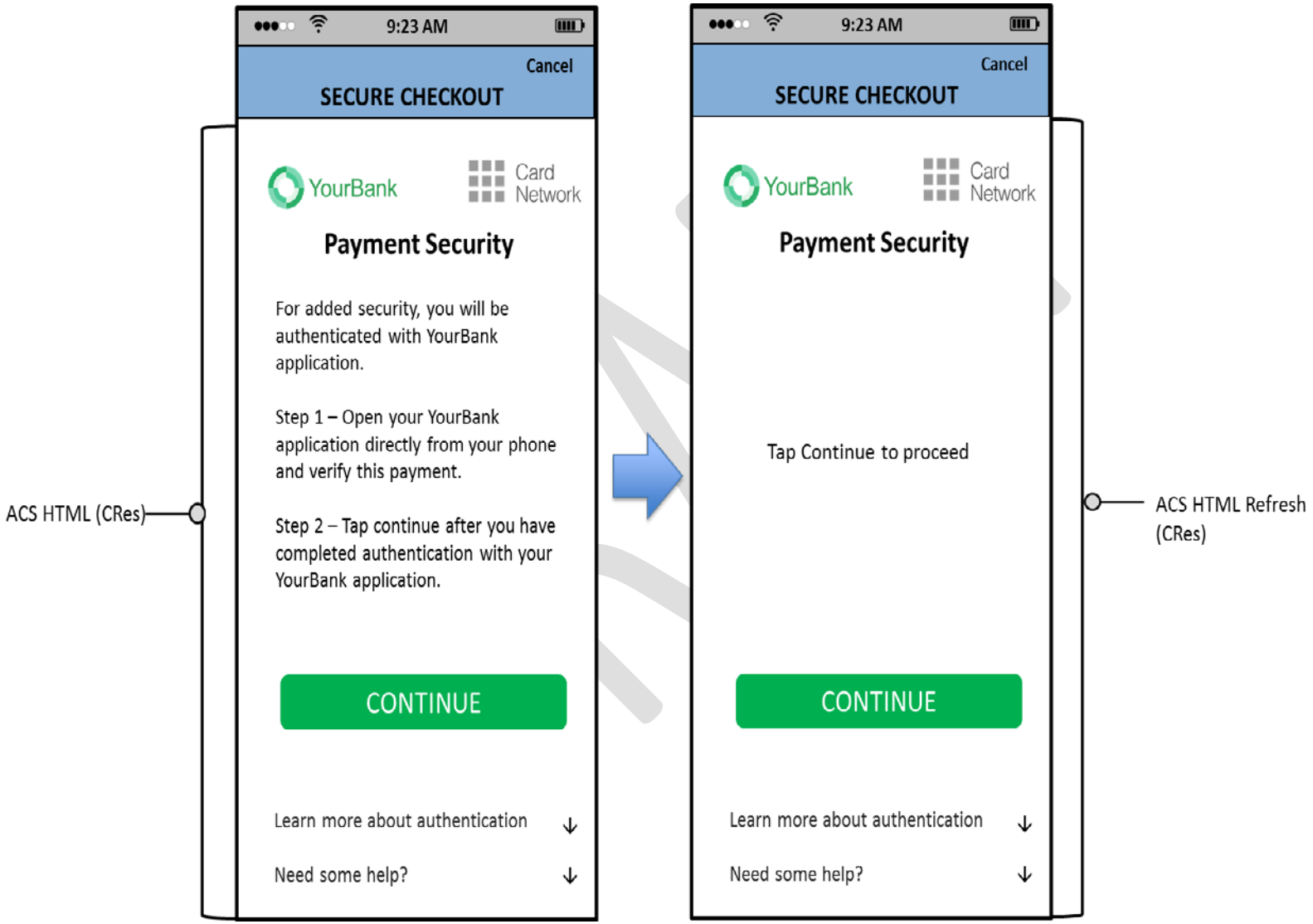
Using the ACS HTML Refresh field

When ACS UI type = 05 (HTML), information provided by the ACS within the ACS HTML field is used to provide cardholder instructions.

The ACS uses the ACS HTML Refresh field to provide text that will replace the ACS HTML when the 3DS Requestor App moves to the foreground.

Figure 12 below illustrates the sample processing flow used by the 3DS SDK to replace the ACS HTML with the information provided in the ACS HTML Refresh.

Figure 12: ACS HTML Refresh



Browser-based User Interface

This section provides template examples and guidelines for building the User Interface (UI) to support 3-D Secure authentication for Browser-based implementations.

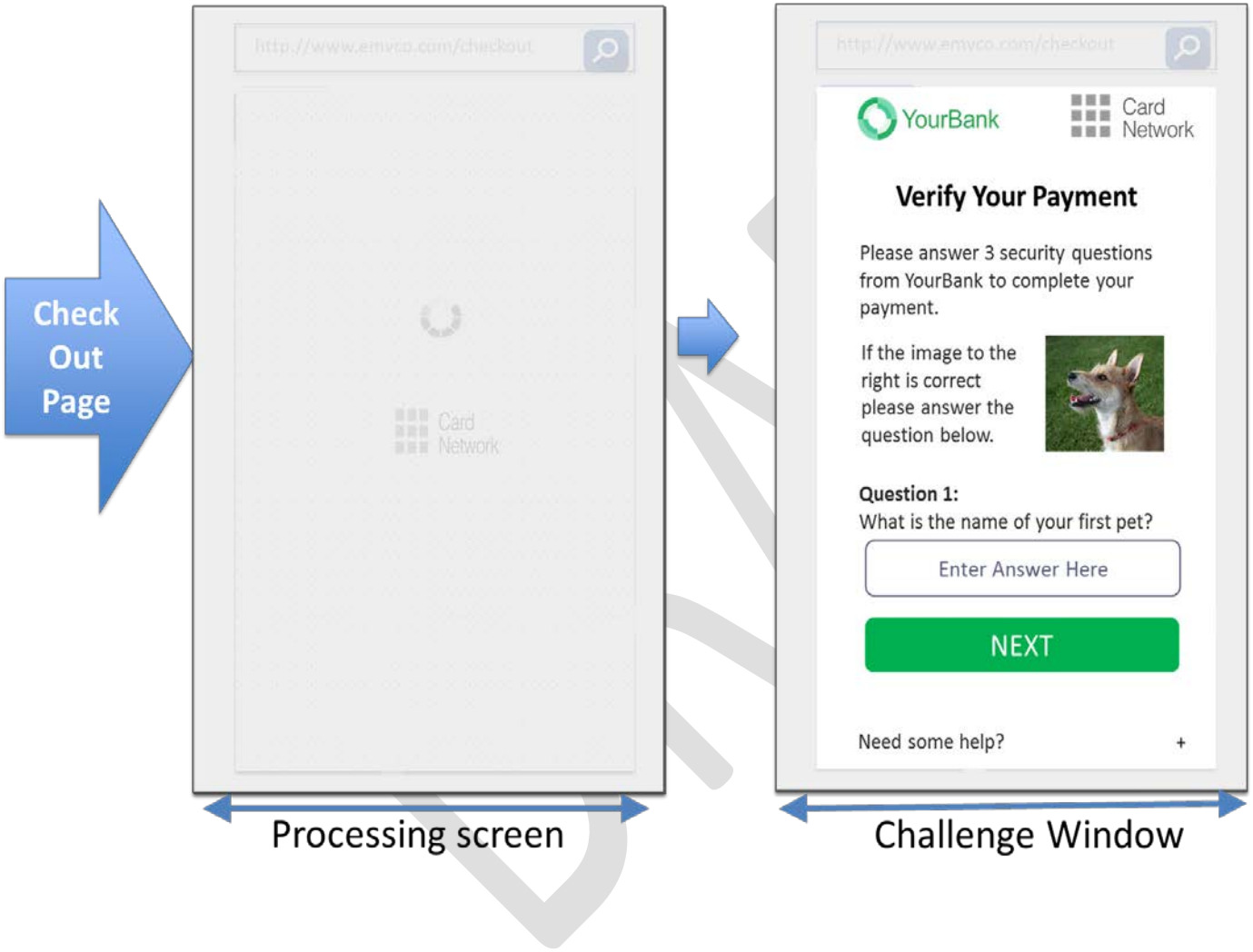
Displaying the Challenge Window in Full Screen

For smaller devices, displaying the challenge window in full screen is best utilised within a lightbox.

To enable a positive cardholder experience, cardholders should be able to view the data entry text box when the keyboard is overlaid on the authentication screen..

Figure 13 below illustrates a sample lightbox challenge window on a small mobile device with a screen size of approximately 5.5”. The challenge window size selected by the 3DS Requestor is set to Full screen.

Figure 13: Lightbox on Small Mobile Device



For Larger devices (e.g. tablets, laptops, or desktop), displaying the challenge window in full screen, pixel sizes are best utilised. Depending on the device's screen size, this can be displayed either inline or within a lightbox.

Supporting Cardholder Language Selection

The UI can be utilised by the ACS to support multiple languages during the authentication process.

Figure 14 through Figure 17 illustrate the cardholder experience during a browser-based transaction when the ACS supports multiple languages. The ACS supports cardholder language selection using a Single Select UI and completes the authentication in English using a Text UI.

Figure 14: Processing Screen After the Cardholder Completes Check out on Merchant Site

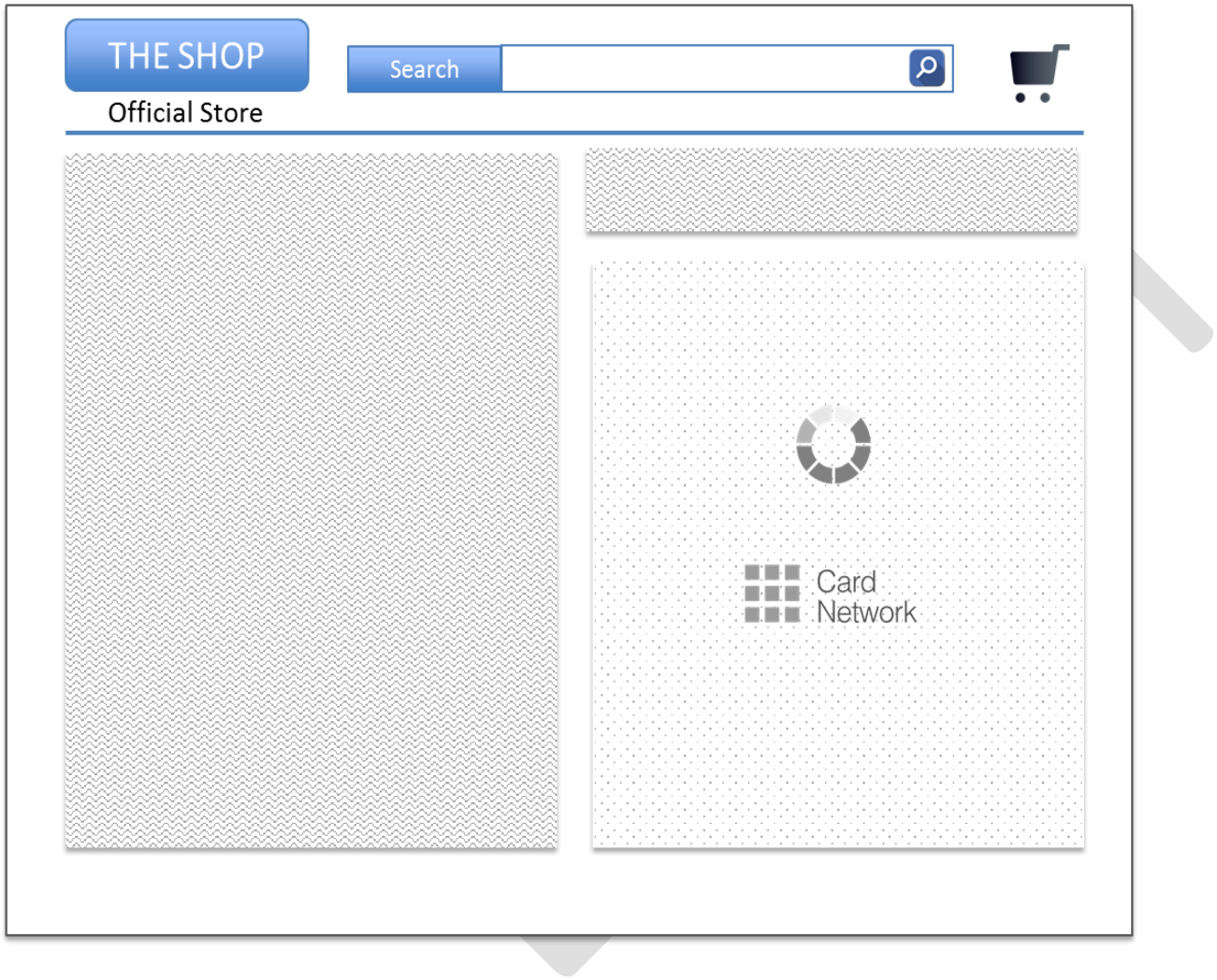


Figure 15: Cardholder Language Selection Displayed Using Single Select UI

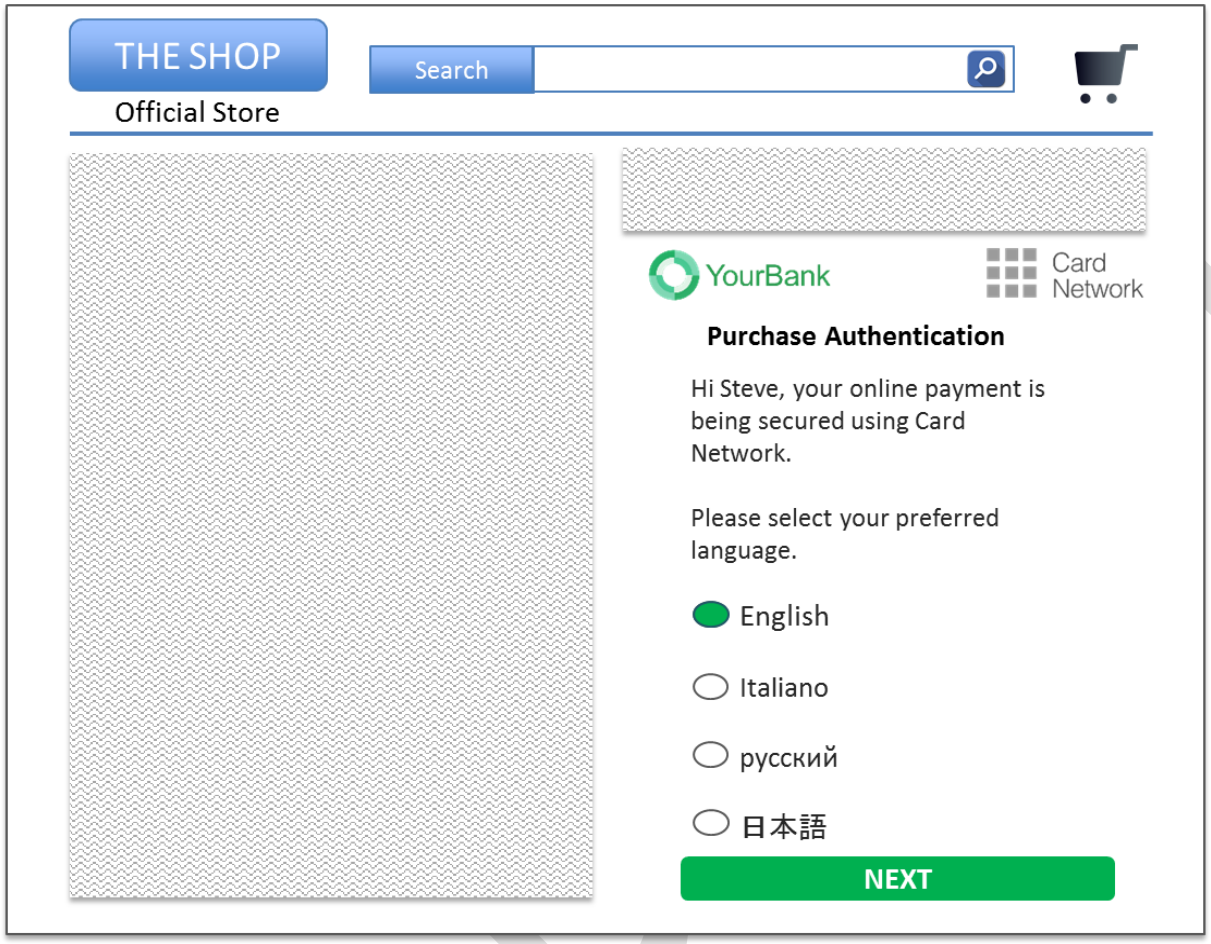


Figure 16: Processing Indicator Displayed Following Cardholder Language Selection

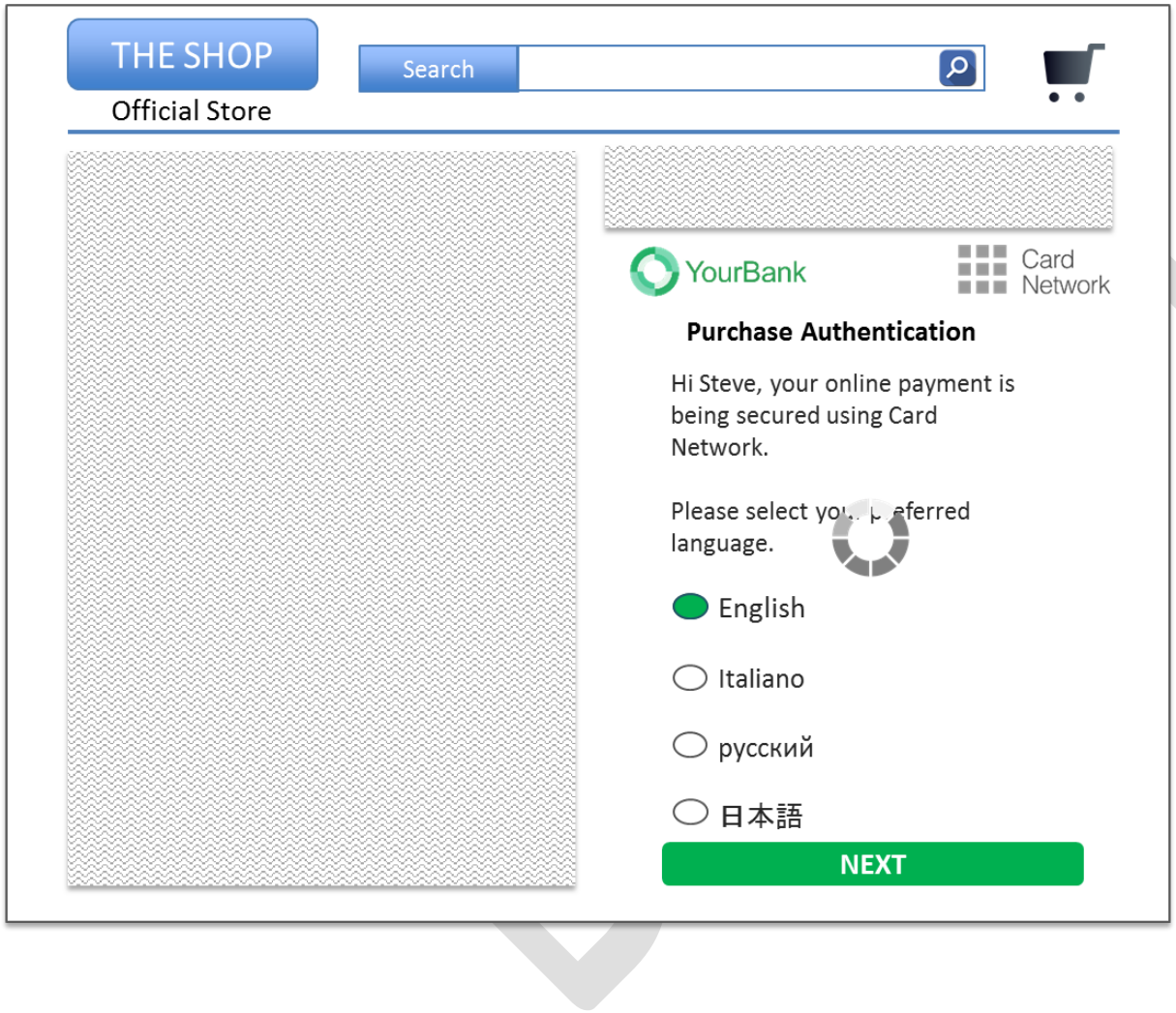


Figure 17: Challenge Displayed Using Text Template