Antifraud System Integration

Landing Page

The landing page mode integration is made for mobile network operators, payment gateways and digital merchants who host the landing page and/or payment pages.

Integration steps to manage fraud on the flow

1- Merchant requests GetScript API from Antifraud's platform.

2- Merchant installs this script on the relevant pages to protect.

3- Events and metrics (load, click…) are sent to Antifraud's platform for deep analysis.

4- On Subscription Verification, the transaction Id (ti*) and timestamp (ts*) will be verified or blocked depending on Antifraud's platform analysis.

It is a code to be deployed on the purchase or subscription verification confirmation pages:

- Javascript code
- Non-blocking
- Dynamically generated via web service
- Low latency under 100ms RTT included

This probe will gather the necessary information for our real-time analysis.

This kit is generated at the code level that the page produces to monitor.

Get Script API

This request returns a Javascript that you will have to insert in the landing page containing theCTA (Click to Action) that you want to protect. The script must be placed before of all other scripts in the <head> tag

QUERY PARAMS:

ti* <mark>string</mark>

This is one unique identifier you have to fill to identify the transaction on our side. Onetransaction equal one identifier.

te* <mark>string</mark>

This is the targeted element you want to protect (aka your CTA DOM element to protect.) Thisparameter is not required in redirect mode integration.

ts* <mark>int32</mark>

The current timestamp of the transaction.

servicename* <mark>string</mark>

This is the service name you have to fill to identify the transaction on our side.

merchantname* <mark>string</mark>

This is the merchant name you have to fill to identify the transaction on our side.type*

<mark>string</mark>

This is the type you have to fill to identify the transaction on our side if it's "he" or "pin".

HTML Header Example Using php:

```php
<?php

$html = "http://www.social-sms.com/iq-
dcb/dcbprotect.php?action=script&ti=$ti&ts=$ts&te=%23cta_button&
servicename=$servicename&merchantname=$merchantname&type=$type";
$test = file_get_contents($html);

$test = json_decode($test)
?>
```

```html
<head>

  <script>

    <?php echo $test->s; ?>

  </script>

</head>
```

Verification will be done on the VMS level after providing the ti and ts parameters in the subscription request or redirection request

Header Enrichment Integration

Landing Page

The landing page mode integration is made for mobile network operators, payment gateways and digital merchants who host the landing page and/or payment pages.

Integration steps to manage subscription flow

1- User Enter the landing page.

2- landing Page should contain all details such as service description with price, subscription module and opt out Method.

3- User click on subscription button to subscribe into the service.

4- Subscription Button should be integrated with the Antifraud Platform if needed (Documentation should be provided separately).

5- Landing Page shall redirect the user to the below URL with the parameters provided by the SDP Team.

URL: **http://www.social-sms.com/iq-dcb/HE/v1.3/doubleclick/sub.php?serviceId=$serviceId&spId=$spId&shortcode=$shortcode&ti=$ti&ts=$ts &servicename=$servicename&merchantname=$merchantname**

6- After redirection is happened, our platform will redirect back the user either to success page or to the failure page provided by the service providers.

Service Provider shall provide the below 3 pages:

Landing Page	
Success Page	
Failure Page	

Redirect Parameters

Any parameters added other than the below, will be added to the redirected link(success or failure) automatically.

QUERY PARAMS:

serviceId* <mark>int32</mark>

Service Id, unique service Id that should be provided by the SDP Team.

spId* <mark>int32</mark>

Service provider Id, unique Id that should be provided by the SDP Team.

shortcode* <mark>int32</mark>

Short code of the service.

ti* <mark>string</mark>

This is one unique identifier you have to fill to identify the transaction on our side. One transaction equal one identifier.

ts* <mark>int32</mark>

The current timestamp of the transaction.

servicename* <mark>string</mark>

This is the service name you have to fill to identify the transaction on our side.

merchantname* <mark>string</mark>

This is the merchant name you have to fill to identify the transaction on our side.

Verification will be done on the DCB level after providing all above parameters in the redirection request.

Sample

Landing Page Provided by Merchant	http://www.landingpage.com/LP.php
Success Page Provided by Merchant	http://www.landingpage.com/success.php
Failure Page Provided by Merchant	http://www.landingpage.com/fail.php
Redirect URL Provided By SDP	http://www.social-sms.com/iq-dcb/HE/v1.3/oneclick/sub.php?serviceId=$serviceId&spId=$spId&shortcode=$shortcode&ti=$ti&ts=$ts &servicename=$servicename&merchantname=$merchantname &additionalparameter1=$addparam1&additionalparameter2=$addparam2
Success Page Redirection	http://www.landingpage.com/success.php?msisdn=964xxxxx&success=1&ti=$ti &servicename=$servicename&merchantname=$merchantname& additionalparameter1=$addparam1&additionalparameter2=$addparam2

Failure Page Redirection	http://www.landingpage.com/fail.php?reason=nohe&fail=1&ti=$ti &servicename=$servicename&merchantname=$merchantname & additionalparameter1=$addparam1&additionalparameter2=$addparam2
	
	Reason:
	    -Subscriptions Exceeded (same service time per 24 hours)
	    -Subscriptions Exceeded. Different service 1 time per 30 minutes
	    -NoHe
	    -Block
	    -UNIQID is Missing
	    -SubMaxReached
	    -Transaction Not Found in System

Integration Notes:

The Service Provider shall include the below tags in the page header in order for our system to detect the referrer. <meta name="referrer" content="unsafe-url">
If a customer was redirected to our redirection URL with a missing parameter or from a non-configured landing page, the user will get the below error. No service.