Transaction Risk Management Tool

PHP API – v1.0.1

Moneris SOLUTIONS

Table of Contents

**** PLEASE READ CAREFULLY****

1. **The Transaction Risk Management Tool provides additional information to assist in identifying fraudulent transactions. In order to maximize the benefits from the Transaction Risk Management Tool it is highly recommended that you:**
   a. **Carefully consider the business logic and processes that you need to implement surrounding handling the response information the Transaction Risk Management Tool provides.**
   b. **Also implement the other fraud tools available through eSelectplus (e.g. AVS, CVD, Verified by Visa and MasterCard SecureCode).**

2. **When testing the Transaction Risk Management Tool there is specific test data that you will need to use. Please carefully review and follow the testing instructions and data provided in the document.**

   Production Data should not be used in the test environment.

3. **You have a responsibility to protect cardholder and merchant related confidential account information. Under no circumstances should ANY confidential information be sent via email while attempting to diagnose integration or production issues. When sending sample files or code for analysis by Moneris staff, all references to valid card numbers, merchant accounts and transaction tokens should be removed and or obscured. Under no circumstances should live cardholder accounts be used in the test environment.**

1. About this Documentation

This documentation contains the information needed to integrate the Transaction Risk Management Tool with your website and back-end processing systems using the PHP API. In particular it describes the format for sending the requests and handling the corresponding responses you will receive.

To help prevent fraudulent activity on online transactions it is highly recommended that you also implement all of the other fraud tools available through eSelectplus which consist of AVS, CVD, Verified by Visa, MasterCard SecureCode.

- *Address Verification Service (AVS)* – Verifies the cardholder's billing address information.
- *Card validation Digit (CVD)* – Validates that cardholder has a genuine credit card in their possession during the transaction.
- *Verified by Visa and MasterCard Secure Code (VBV/SecureCode)* – Authenticate the cardholder at the time of an online transaction

For further details on implementing these additional fraud tools can be found in:

- *Moneris MPI – Verified by Visa / MasterCard SecureCode – PHP API Integration Guide*
- *Merchant Integration Guide - PHP API*

2. System and Skill Requirements

In order to use the PHP API your system will need to have the following:

1. PHP or later
2. Port 443 open for bi directional communication
3. OpenSSL
4. cURL – PHP interface – this can be downloaded from http://curl.haxx.se/download.html

As well, you will need to have the following knowledge and/or skill set:

1. PHP programming language.

Note:
Your solution may be required to demonstrate compliant with the card associations' PCI/CISP/PABP requirements. For more information on how to get your application PCI-DSS compliant, please contact our Sales Center and visit https://www.eselectplus.ca/en/downloadable-content to download the PCI_DSS Implementation Guide.

The card association has a couple of data security standards that define specific requirements for all organizations that store, process, or transmit cardholder data. As a Moneris Solutions client or partner using this method of integration, your solution must demonstrate compliance to the Payment Card Industry Data Security Standard (PCI DSS) and/or the Payment Application Data Security Standard (PA DSS). These standards are designed to help the cardholders and merchants in such ways as they ensure credit card numbers are encrypted when transmitted/stored in a database and that merchants have strong access control measures.

Non-compliant solutions may prevent merchant boarding with Moneris Solutions. For further information on PCI DSS & PA DSS requirements, please visit http://www.pcisecuritystandards.org.

3. Understanding the Transaction Risk Management Transaction Flow

A. Overview

There are 3 types of transactions associated with the Transaction Risk Management Tool.

- Session Query
- Attribute Query
- Assertion Query

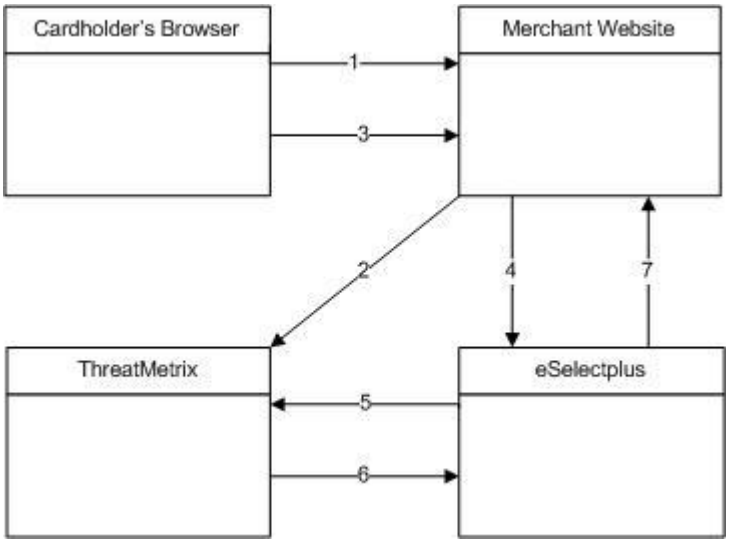
The Session Query and Attribute Query are used at the time of the transaction to obtain the risk assessment. The Assertion Query is used at a later time to provide information back into the system in regards to Suspected and/or Confirmed fraudulent transactions. This Assertion allows the system to increase its knowledge resulting in better risk assessments in the future.

It is recommended that you use the Session Query as much as possible for obtaining your risk assessment as it utilizes the device fingerprint as well as other transaction information when providing the risk scores. In order to use the Session Query you must implement two components: the tags on your website to collect the device fingerprinting information and the Session Query transaction. If you are not able to collect the needed information for the Session Query (e.g. the device fingerprint), then the Attribute Query should be used.

Since the Assertion Query impacts future transaction results, it is important that it only be used when you have valid suspicions or have confirmed that the transaction is fraudulent.

B. Transaction Flows

Session Query Transaction Flow



1. Cardholder logs onto merchant website.

2. When page is loaded in cardholder's browser, special tags within the site allow information from the device to be gathered and are sent to ThreatMetrix as the device fingerprint. The HTML tags should be placed where the cardholder is resident on the page for a couple of seconds to get the broadest data possible.

3. Customer submits a transaction.

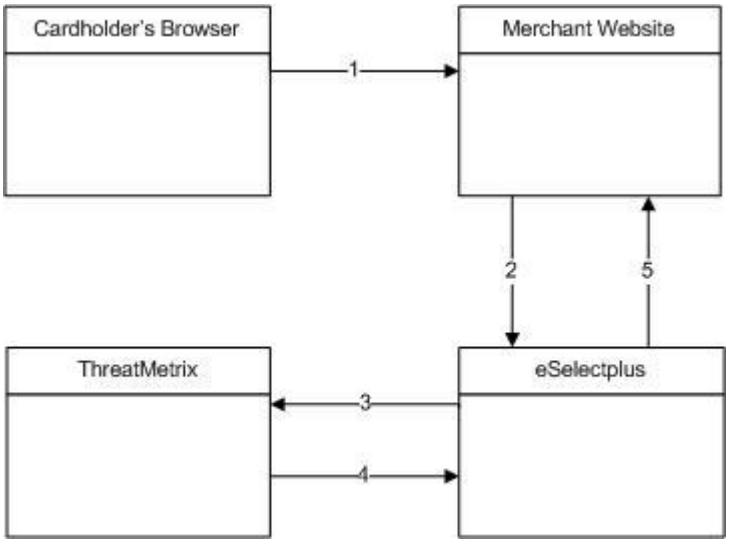
4. Merchant's web application makes a Session Query transaction to eSelectplus, including the same session id that was included in the device fingerprint. This call must be made within 30 minutes of the profiling step (#2).

5. eSelectplus submits the Session Query data to ThreatMetrix.

6. ThreatMetrix uses the Session Query data and the device fingerprint information to assess the transaction against the rules. A score is generated based on the rules.

7. The merchant will use the returned device information in its risk analysis to make a business decision. The merchant may wish to continue or cancel with the cardholder's payment transaction.

Attribute Query Transaction Flow



1. Cardholder logs onto merchant website and submits a transaction.

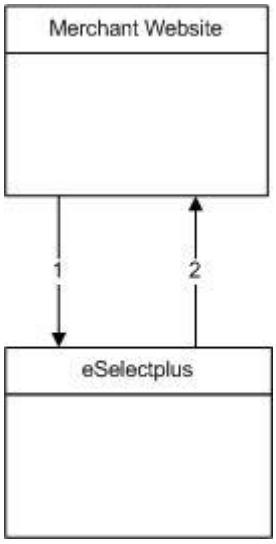
2. The merchant's web application makes an Attribute Query transaction to eSelectplus, including the session id.

3. eSelectplus submits an Attribute Query data to ThreatMetrix

4. ThreatMetrix uses the Attribute Query data to assess the transaction against the rules. A score is generated based on the rules.

5. The merchant will use the returned device information in its risk analysis to make a business decision. The merchant may wish to continue or cancel with the cardholder's payment transaction.

Assertion Query Transaction Flow



1. Merchant investigates a transaction and determines that it is fraudulent. Merchant sends an Assertion Query to eSelectplus, passing in the associated assertion data.

2. ThreatMetrix uses the Assertion Query data and updates their knowledge base so the information is included in future assessments and risk scores.

Possible Transaction flows incorporating all available fraud tools

To help prevent fraudulent activity with online transactions it is highly recommended that you implement the eSelectplus eFraud features which consist of:

- AVS and CVD
- Verified by Visa and MasterCard SecureCode
- Transaction Risk Management Tool

Please note that all responses coming back from these verification methods are intended to provide added security and fraud prevention, and the response itself will not affect the completion of a transaction. Upon receiving a response, the choice to proceed with a transaction is left entirely to the merchant.

Option A:

1. Process a **Transaction Risk Management Tool** query and obtain the response. Merchant then makes a decision to continue or to abort with the transaction.
2. Process a **VBV/SecureCode** transaction and obtain the response. Merchant then makes a decision to continue or to abort with the transaction.
3. Process a financial transaction including **AVS/CVD** details and obtain the response. Merchant then makes a decision to continue or to abort with the transaction.

Option B:

1. Process a **Transaction Risk Management Tool** query and obtain the response,
2. Process a **VBV/SecureCode** transaction and obtain the response,
3. Process a financial transaction including **AVS/CVD** details and obtain the response. Merchant then makes a one time decision based on the responses received from the eFraud tools.

4. Implementation Checklist

The following checklists provide high level tasks that will be required as part of your implementation of the Transaction Risk Management Tool. Since each organization has their own unique project requirements for implementing system and process changes, this list is a guideline only and does not cover all aspects of your project.

☐ Download and review all of the applicable APIs and Integration Guides

Document/ API	*Use the document if you are….*
Transaction Risk Management Tool Integration Guide	*Implementing or updating your integration for the Transaction Risk Management Tool*
Moneris MPI – Verified by Visa / MasterCard SecureCode – PHP API Integration Guide	*Implementing or updating Verified by Visa and MasterCard SecureCode*
Merchant Integration Guide - PHP API	*Implementing or updating transaction processing, AVS and/or CVD*

☐ Design your transaction flow and business processes.

- When designing your transaction flow, think about what scenarios you would like automated vs. which scenarios you want to be handled manually by your employees.

  The "Understand Transaction Risk Management Transaction Flow" and "How do I handle the response information? "Sections will be useful in helping you work through the design of your transaction and process flows.

  When designing your process flows, don't forget:
  - Processes for notifying impacted people within your organization when there are scheduled maintenances' for eSelectplus
  - Handling cancelled orders, refunds, etc.
  - Communicating with your customer when you will not be shipping the goods because of suspected fraud and/or because of backordered goods, etc.

☐ Complete your development and testing

This document provides the technical details required for the development and testing. Please ensure that you follow the testing instructions and data provided.

If you are an integrator:

☐ Ensure that your solution meets or exceed the requirements for PCI-DSS/PA-DSS as applicable.

☐ Send an email to eselectplus@moneris.com with the subject line "Certification Request"

☐ Develop material for your customers to help them in getting setup as quickly as possible with your solution and a Moneris account. Include information such as:

- Steps they will need to take to enter their store id/api token information into your solution
- Any optional services that you support via eSelectplus (e.g. Transaction Risk Management, AVS, CVD, VBV/SecureCode) so that they can request their account to be setup with these features.

If you are a merchant:

Ensure that you have your production account information

☐ If this is a new production account, activate your production account and setup any additional users that your organization needs.

If this is an existing production account, ensure that any changes to user profiles required to support process changes being implemented with the Transaction Risk Management Tool are completed.

☐ Plan your move to production including:

- Business Process Changes and training
- Technical implementation (see the How do I configure my store for Production? section of this document for further details)

5. How do I send Transaction Risk Management Transactions?

A. Inserting the Profiling tags into your website

The profiling tags are placed on HTML pages served by your web application which will allow ThreatMetrix to collect device information from the customer's web browser. The profiling tags will need to be placed in locations in your web application that will ensure that their devices are profiled before submitting a payment transaction.
Below is an HTML sample of the profiling tags that will require two variables (org_id, session_id). Please refer to Appendix A: Definitions of Required Fields for variable definitions.

```
<p style="background:url(https://h.online-metrix.net/fp/clear.png?org_id=my_org_id&amp;session_id=my_session_id&
amp;m=1)">
</p>

<img src="https://h.online-metrix.net/fp/clear.png?org_id=my_org_id&amp;session_id=my_session_id&
amp;m=2" alt="" >

<script src="https://h.online-metrix.net/fp/check.js?org_id=my_org_id&amp;session_id=my_session_id"
type="text/javascript">
</script>

<object type="application/x-shockwave-flash" data="https://h.online-
metrix.net/fp/fp.swf?org_id=my_org_id&amp;session_id=my_session_id"
width="1" height="1" id="obj_id">
    <param name="movie"
value="https://h.online-metrix.net/fp/fp.swf?org_id=my_org_id&amp;session_id=my_session_id" />
    <div></div>
</object>
```

B. The Session Query

Once a device profiling session has been initiated upon a client device, the Session Query API is used at the time of the transaction or even to obtain a device identifier or 'fingerprint', attribute list and risk assessment for the client device. This code can be found from the TestRiskCheckSession.php sample included in the download. Please refer to Appendix A: Definitions of Required Fields for variable definitions.

```
<?php
require "../riskClasses.php";

/********************** Request Variables ***************************/
$store_id='moneris';
$api_token='hurgle';
```

```
/********************* Transactional Variables ************************/

$type='session_query';
$order_id='risktest-'.date("dmy-G:i:s");
$session_id='abc123';
$service_type='session';
//$event_type='login';

/************************* SessionAccountInfo Variables *****************************/

$policy = '';
$device_id = '4EC40DE5-0770-4fa0-BE53-981C067C598D';
$account_login = '13195417-8CA0-46cd-960D-14C158E4DBB2';
$password_hash = '489c830f10f7c601d30599a0deaf66e64d2aa50a';
$account_number = '3E17A905-AC8A-4c8d-A417-3DADA2A55220';
$account_name = '4590FCC0-DF4A-44d9-A57B-AF9DE98B84DD';
$account_email = '3CAE72EF-6B69-4a25-93FE-2674735E78E8@test.threatmetrix.com';
$account_telephone = '5556667777';
$pan = '4242424242424242';
$account_address_street1 = '3300 Bloor St W';
$account_address_street2 = '4th Flr West Tower';
$account_address_city = 'Toronto';
$account_address_state ='Ontario';
$account_address_country = 'Canada';
$account_address_zip = 'M8X2X2';
$shipping_address_street1 = '3300 Bloor St W';
$shipping_address_street2 = '4th Flr West Tower';
$shipping_address_city = 'Toronto';
$shipping_address_state = 'Ontario';
$shipping_address_country = 'Canada';
$shipping_address_zip = 'M8X2X2';
$local_attrib_1 = 'a';
$local_attrib_2 = 'b';
$local_attrib_3 = 'c';
$local_attrib_4 = 'd';
$local_attrib_5 = 'e';
$online_tld = 'Facebook';
$online_id_handle = 'Moneris';
$transaction_amount = '1.00';
$transaction_currency = '124';

/********************** SessionAccountInfo Associative Array ************************/
$sessionAccountInfoTemplate = array
               (
                      'account_login'=>$account_login,
                      'password_hash' =>$password_hash,
                       'account_number' => $acount_number,
                      'account_name' => $account_name,
                      'account_email'=>$account_email,
                      'pan' =>$pan
                );

/************************** SessionAccountInfo Object *******************************/
$mpgSessionAccountInfo = new mpgSessionAccountInfo ($sessionAccountInfoTemplate);

/***************** Transactional Associative Array *******************/
$txnArray=array(
                      'type'=>$type,
                      'order_id'=>$order_id,
                      'session_id'=>$session_id,
                      'service_type'=>$service_type
                      );

/********************** Transaction Object ***************************/
$riskTxn = new riskTransaction($txnArray);

/************************ Set SessionAccountInfo ***************************/
$riskTxn->setSessionAccountInfo($mpgSessionAccountInfo);

/************************ Request Object ***************************/
$riskRequest = new riskRequest($riskTxn);
```

```
/********************** HTTPS Post Object ***************************/
$riskHttpsPost  =new riskHttpsPost($store_id,$api_token,$riskRequest);

/***************************** Response *****************************/
$riskResponse=$riskHttpsPost->getRiskResponse();

//print("\nResponse = " . $riskResponse);

print("\nResponseCode = " . $riskResponse->getResponseCode());
print("\nMessage = " . $riskResponse->getMessage());

$results = $riskResponse->getResults();

foreach($results as $key => $value)
{
        print("\n".$key ." = ". $value);
}

$rules = $riskResponse->getRules();

//print_r($rules);

foreach ($rules as $i)
{
        foreach ($i as $key => $value)
        {
                echo "\n$key = $value";
        }
}

?>
```

C. The Attribute Query

The Attribute Query is used to obtain a risk assessment of transaction related identifiers such as email_address, card number, etc. Unlike the Session Query, the Attribute Query does not require the device fingerprinting information to be provided. This code can be found from the TestRiskCheckAttribute.php sample included in the download. Please refer to Appendix A: Definitions of Required Fields for variable definitions.

```
<?php
require "../riskClasses.php";

/************************ Request Variables ***************************/
$store_id='moneris';
$api_token='hurgle';

/********************** Transactional Variables ***********************/
$type='attribute_query';
$order_id='risktest-'.date("dmy-G:i:s");
$service_type='session';

/************************** SessionAccountInfo Variables ****************************/
$device_id = '4EC40DE5-0770-4fa0-BE53-981C067C598D';
$account_login = '13195417-8CA0-46cd-960D-14C158E4DBB2';
$password_hash = '489c830f10f7c601d30599a0deaf66e64d2aa50a';
$account_number = '3E17A905-AC8A-4c8d-A417-3DADA2A55220';
$account_name = '4590FCC0-DF4A-44d9-A57B-AF9DE98B84DD';
$account_email = '3CAE72EF-6B69-4a25-93FE-2674735E78E8@test.threatmetrix.com';
$account_telephone = '5556667777';
//$cc_number_hash = '';
$ip_address = '192.168.0.1';
$ip_forwarded = '192.168.0.1';
$account_address_street1 = '3300 Bloor St W';
$account_address_street2 = '4th Flr West Tower';
$account_address_city = 'Toronto';
$account_address_state ='Ontario';
$account_address_country = 'Canada';
$account_address_zip = 'M8X2X2';
```

```
$shipping_address_street1 = '3300 Bloor St W';
$shipping_address_street2 = '4th Flr West Tower';
$shipping_address_city = 'Toronto';
$shipping_address_state = 'Ontario';
$shipping_address_country = 'Canada';
$shipping_address_zip = 'M8X2X2';

/********************** SessionAccountInfo Associative Array ************************/
$attributeAccountInfoTemplate = array
               (
                      'account_login'=>$account_login,
                      'password_hash' =>$password_hash,
                       'account_number' => $acount_number,
                      'account_name' => $account_name,
                      'account_email'=>$account_email
                );
/************************** SessionAccountInfo Object *******************************/
$mpgAttributeAccountInfo = new mpgAttributeAccountInfo ($attributeAccountInfoTemplate);

/***************** Transactional Associative Array *******************/
$txnArray=array(
                      'type'=>$type,
                      'order_id'=>$order_id,
                      'service_type'=>$service_type
                      );
/********************** Transaction Object ***************************/
$riskTxn = new riskTransaction($txnArray);

/************************ Set SessionAccountInfo ****************************/
$riskTxn->setAttributeAccountInfo($mpgAttributeAccountInfo);

/************************ Request Object ****************************/
$riskRequest = new riskRequest($riskTxn);

/************************ HTTPS Post Object ****************************/
$riskHttpsPost  =new riskHttpsPost($store_id,$api_token,$riskRequest);

/***************************** Response *****************************/
$riskResponse=$riskHttpsPost->getRiskResponse();

//print("\nResponse = " . $riskResponse);

print("\nResponseCode = " . $riskResponse->getResponseCode());
print("\nMessage = " . $riskResponse->getMessage());

$results = $riskResponse->getResults();

foreach($results as $key => $value)
{
       print("\n".$key ." = ". $value);
}

$rules = $riskResponse->getRules();

//print_r($rules);

foreach ($rules as $i)
{
       foreach ($i as $key => $value)
       {
              echo "\n$key = $value";
       }
}

?>
```

D. The Assertion Query

The Assertion Query is used at a later time to provide information back into the system in regards to Suspected and/or Confirmed fraudulent transactions. This Assertion allows the system to increase its knowledge resulting in better risk assessments in the future. The Assertion Query is used as a transaction or incident report consisting of transaction-related attributes and activities. The event report relates to a single device and/or multiple transaction identifiers. An Assertion Query is made with reference to impact, confidence, transaction activities and transaction attributes. This code can be found from the TestAssert.php sample included in the download. Please refer to Appendix A: Definitions of Required Fields for variable definitions.

Since the Assertion Query impacts future transaction results, it is important that it only be used when you have valid suspicions or have confirmed that the transaction is fraudulent. **An Assertion Query can only be performed once and can NOT be reversed.**

```
<?php
require "../riskClasses.php";

/************************ Request Variables ***************************/
$store_id='moneris';
$api_token='hurgle';

/********************** Transactional Variables ************************/
$type='assert';
$orig_order_id='risktest-071111-10:48:11';
$activities_description='charge_back';
$impact_description='medium';
$confidence_description='suspicious';

/***************** Transactional Associative Array *******************/
$txnArray=array       (
                      'type'=>$type,
                      'orig_order_id'=>$orig_order_id,
                      'activities_description'=>$activities_description,
                      'impact_description'=>$impact_description,
                      'confidence_description'=>$confidence_description
              );

/********************** Transaction Object ****************************/
$riskTxn = new riskTransaction($txnArray);

/************************ Request Object ******************************/
$riskRequest = new riskRequest($riskTxn);

/************************ HTTPS Post Object ***************************/
$riskHttpsPost  =new riskHttpsPost($store_id,$api_token,$riskRequest);

/***************************** Response *******************************/
$riskResponse=$riskHttpsPost->getRiskResponse();

print("\nResponseCode = " . $riskResponse->getResponseCode());
print("\nMessage = " . $riskResponse->getMessage());

$results = $riskResponse->getResults();

foreach($results as $key => $value)
{
       print("\n".$key ." = ". $value);
}

?>
```

6. How do I handle the response information?

When reviewing the response information and determining how to handle the transaction, it is recommended that you (either manually or through automated logic on your site) use the following pieces of information:

a) the risk score
b) the rules triggered (e.g. Rule Codes, Rule Names, Rule Messages) Results obtained from Verified by Visa, MasterCard Secure Code, AVS, CVD and the financial transaction authorization
c) Automated processes will also need to include the response codes for the Transaction Risk Management Transaction

A. Understanding the Risk Score

For each Session Query or Attribute Query, a score with a value between -100 and +100 will be returned based on the rules that were triggered for the transaction. Below is a table defining the different possible risk scores ranges.

Risk Score	Visa Definition
[-100 … -1]	The lowest score that can be reached is -100. The more negative the number (ie closer to -100) the more likely the transaction is fraudulent.
0	A risk score of 0 indicates a neutral transaction
[1 … +100]	The highest score that can be reached is +100. The more positive the number (ie closer to +100) the lower the risk that the transaction is fraudulent. NOTE: All ecommerce transactions have some level of risk associated with them and as a result it is rare to see transactions with a risk score in the high positive values.

When evaluating the risk of a transaction, the risk score will give you an initial indicator of the potential risk level that the transaction is or isn't fraudulent. The more negative the score, the higher the probability is that the transaction is fraudulent. Since some of the rules that are evaluated on each transaction may/may not be as relevant in your business scenario, you should also review the rules that were triggered for the transaction before determining how to handle the transaction.

B. Understanding the Rule Codes, Rule Names and Rule Messages

The rule codes, rule names and rule messages provide details on what rules were trigged during the assessment of the information provided in the Session or Attribute Query. Each Rule Code has a Rule Name and Message. The Rule Name and Rule Message will typically be very similar. The table in Appendix C provides additional information on each rule.

When evaluating the risk of a transaction, it is recommended that you review the rules that were triggered for the transaction and assess the relevancy of it to your business (e.g. how it relates to the typical buying habits of your customer base).

If you are automating some or all of the decision making process related to handling the responses, you may want to use the Rule Codes. If you are documenting manual processes you may want to refer to the more user friendly Rule Name and/or Rule Message.

C. Pulling all the information together to make a decision

Depending on your business policies and processes, you will use the information obtained from the Fraud Tools (e.g. AVS, CVD, VBV/SecureCode and Transaction Risk Management) to make an informed decision on whether you want to accept the transaction or consider it to be a potential fraudulent transaction that you do not want to continue to process.

If you do not want to continue with a transaction because it appears to risky and is likely fraudulent, you will need to:

- Let the customer know that you will not be proceeding with their order.
- Cancel the financial transaction if you have received an approved authorization. To do this you will need to send a Void/Refund for a purchase transaction or a $0.00 Capture transaction if the original transaction was a pre-authorization.

7. How Do I Test My Solution?

When testing your implementation of the Transaction Risk Management Tool you will be testing in against a test account that requires specific data to be used in some test scenarios. **It is important that you do not use Production Card information in the test environment and that the provided test data be used.**

The test environment is generally available 7x24, however since it is a test environment we cannot guarantee 100% availability. Also, please be aware that other merchants are using the test environment so in the Merchant Resource Centre you may see transactions and user IDs that you did not create. As a courtesy to others that are testing we ask that when you are processing Refunds, changing passwords and/or trying other functions that you use only the transactions/users that you created.

When testing your solution, you may use the following query test data.

Query Test Data	
Assertion Field	**Data**
IPs	150.206.192.200 150.206.192.201 150.206.192.202 150.206.192.203 150.206.192.204 150.206.192.205 150.206.192.206 150.206.192.207 150.206.192.208 150.206.192.209
Device Ids	4EC40DE5-0770-4fa0-BE53-981C067C598D C2708897-984B-44fe-BA33-839906C2B898 C88AB2FD-6492-4a8d-91A5-11AF7074E135 FE4461D3-2CEB-4606-958E-2DEEB9F1BA50 2126F23D-FD84-40a3-BF91-6E660E14D337 EAD80A88-6450-4900-8311-2D6FFFB7E7DA FA320962-E990-4265-A184-69CB50378073 34018A61-6D99-452f-99BC-4A94541F1BDC F59CBB48-BB04-40f6-8A11-5586918FBF01 92814546-DDC2-4413-B359-8ED08866AFD4
Email Address	3CAE72EF-6B69-4a25-93FE-2674735E78E8@test.threatmetrix.com A8BE4932-0F79-4897-AEEE-0BDF3B59A4DE@test.threatmetrix.com 169D66C8-7C6B-4423-9F4D-A5B8C4A15E21@test.threatmetrix.com 45D8D843-0366-4bce-B243-D1AD910DD475@test.threatmetrix.com F8344156-D3C7-4aae-A8DC-B2F41BA82CB1@test.threatmetrix.com 89A26F3A-DD2D-43f6-AB8D-82E33D64C6A7@test.threatmetrix.com

	39B07468-87C4-43e0-A0D5-54C0DD1BDC7B@test.threatmetrix.com 8DE5B299-5764-4992-A049-3D2C52E03216@test.threatmetrix.com 29B39172-FD2E-41e1-B484-5007640CD78C@test.threatmetrix.com 7212809C-BFC7-4e26-869C-88A13F6DCB50@test.threatmetrix.com
Credit Card Hashes	83297f86fc4b6d5db2cf96e653511ba41254ded4 f19c756551b50532678cd90ccacf22f9b3ef76be e84bea598a320be7d64165d11e4220e45f46e3d5 5c004039028680b0be855667082afe0695787d30 eb89318153c39e43c39f907bb4bf38e5a03e7f9d 1747e72521c74cb3394ade68c4a79df0c872c1d4 bccb4ed96a0ce7dd9b604724a78036921f3e91d8 4b2a8a693cffe4cebf92bcf24c642ce1a9d69208 18faa06eae1dfaca55ed739b96d7af535b67981c 33081886600886f500b76432b819ca8023bb5cc1

The test environment has been designed to replicate our production environment as closely as possible. One major difference is that we are unable to send test transactions onto the production authorization network and thus issuer responses are simulated. Additionally, the requirement to emulate approval, decline and error situations dictates that we use certain transaction variables to initiate various response and error situations.

To access the Merchant Resource Centre in the test environment go to https://esqa.moneris.com/mpg. And use the logins provided in the below table.

Test IDs			
store_id	**api_token**	**Username**	**Password**
store1	yesguy	DemoUser	password
store2	yesguy	DemoUser	password
store3	yesguy	DemoUser	password
store5 *	yesguy	DemoUser	password
moneris **	hurgle	DemoUser	password

* test store "store5" is intended for testing the eFraud (AVS & CVD) transactions.
** test store "moneris" is intended for testing the VbV transactions.
*** test store "moneris" is intended for testing the Transaction Risk Management Tool.

8. How Do I Configure My Store For Production?

Once you have completed testing you can move your store to production. You will need to change the Host from esqa.moneris.com to www3.moneris.com. As well you will need to change the store_id and api_token to the production values for your store.

9. How Do I Get Help?

If you require technical assistance while integrating your store, please contact the eSELECTplus Support Team:

For technical support:
Phone: 1-866-319-7450 (Technical Difficulties)

For integration support:
Phone: 1-866-562-4354
Email: eselectplus@moneris.com

When sending an email support request please be sure to include your name and phone number, a clear description of the problem as well as the type of API that you are using. **For security reasons, please do not send us your API Token combined with your store ID, or your merchant number and device number in the same email.**

10. Appendix A: Definitions of Required Fields

Required Fields		
Variable Name	**Size/Type**	**Description**
Host	an	Development = esqa.moneris.com Production = www3.moneris.com
store_id	10 / an	This is defined and provided by Moneris Solutions and is used to identify the merchant.
api_token	20 / an	This is defined and provided by Moneris Solutions and is used in conjunction with the store_id to uniquely identify your store.
order_id	50 / an	Merchant defined unique transaction identifier – Must be unique for every transaction. Allowed characters are **a-z A-Z 0-9 _ - : . @ spaces**
Session Query Required Fields		
Variable Name	**Size/Type**	**Description**
session_id	9 / decimal	The web server session identifier generated when device profiling was initiated. Allowed characters are **[a-z], [A-Z], 0-9, _, -**
service_type	session	Defines which output fields are returned. *session* -- returns IP and device related attributes.
event_type	payment	Defines the type of transaction or event for reporting purposes. *payment* -- Purchasing of goods/services.
Pan	20 / num	Credit Card Number - no spaces or dashes. Most credit card numbers today are 16 digits in length but some 13 digits are still accepted by some issuers. This field has been intentionally expanded to 20 digits in consideration for future expansion and/or potential support of private label card ranges.
AccountAddressStreet1	32 / an	The first portion of the street address component of the billing address.
AccountAddressStreet2	32 / an	The second portion of the street address component of the billing address.
AccountAddressCity	50 / an	The city component of the billing address.
AccountAddressState;	64 / an	The state component of the billing address.
AccountAddressCountry	2 / an	The 2 character ISO2 country code of the billing addresses country.
AccountAddressZip	8 / an	The zip/postal code of the billing address.
ShippingAddressStreet1	32 / an	The first portion of the street address component of the shipping address.
ShippingAddressStreet2	32 / an	The second portion of the street address component of the shipping address.
ShippingAddressCity	50 / an	The city component of the shipping address.
ShippingAddressState	64 / an	The state component of the shipping address.
ShippingAddressCountry	2 / an	The 2 character ISO2 country code of the account addresses country.
ShippingAddressZip	8 / an	The zip/postal code component of the shipping address.
LocalAttrib1 LocalAttrib2 LocalAttrib3 LocalAttrib4 LocalAttrib5	255 / an	These five attributes can be used to pass custom attribute data. These are used if you wish to correlate some data with the returned device information.
TransactionAmount	255 / an	The numeric currency amount. Must contain 2 decimals.

TransactionCurrency	10 / n	The currency type that the transaction was denominated in. If TransactionAmount is passed, the TransactionCurrency is required. Values to be used are: CAD – 124 USD – 840

Attribute Query Required Fields		
Variable Name	**Size/Type**	**Description**
service_type	session	Defines which output fields are returned. *session* -- returns IP and device related attributes but no policy information.
DeviceId	36 / an	The unique device identifier generated by a prior call to the ThreatMetrix session-query API.
Pan		Credit Card Number - no spaces or dashes. Most credit card numbers today are 16 digits in length but some 13 digits are still accepted by some issuers. This field has been intentionally expanded to 20 digits in consideration for future expansion and/or potential support of private label card ranges.
IPAddress	64 / an	The true IP address, results will be returned as true_ip_geo, true_ip_score etc
IPForwarded	64 / an	The IP address of the proxy, if the IPAddress is supplied, results will be returned as proxy_ip_geo, proxy_ip_score otherwise if IPAddress is not supplied this IP address will be treated as the true IP address and results will be returned as true_ip_geo, true_ip_score etc.
AccountAddressStreet1	32 / an	The first portion of the street address component of the billing address.
AccountAddressStreet2	32 / an	The second portion of the street address component of the billing address.
AccountAddressCity	50 / an	The city component of the billing address.
AccountAddressState;	64 / an	The state component of the billing address.
AccountAddressCountry	2 / an	The 2 character ISO2 country code of the billing addresses country.
AccountAddressZip	8 / an	The zip/postal code of the billing address.
ShippingAddressStreet1	32 / an	The first portion of the street address component of the shipping address.
ShippingAddressStreet2	32 / an	The second portion of the street address component of the shipping address.
ShippingAddressCity	50 / an	The city component of the shipping address.
ShippingAddressState	64 / an	The state component of the shipping address.
ShippingAddressCountry	2 / an	The 2 character ISO2 country code of the account addresses country.
ShippingAddressZip	8 / an	The zip/postal code component of the shipping address.

Assertion Query Required Fields		
Variable Name	**Size/Type**	**Description**
orig_order_id	50 / an	
assert_activities_desc	charge_back / payment_fraud / card_address / card_number / velocity / amount / quantity / address / geolocation / time	**Payment Activities:** *charge_back* - There has been a change back related to the entity. History of charge backs may indicate the presence of 'friendly fraud'. *payment_fraud* - Payment fraud e.g. card not present fraud was attempted from this entity. *card_address* - The billing address did not match the address held by the issuing bank. *card_number* - The card number and or expiry date was not valid for the issuing bank. *velocity* - The card/IP Address/FP has processed a suspicious volume of transactions. *amount* - Sometimes card thieves will run a test transaction to see if a card is still 'live' by running through small purchases. *quantity* - The quantity transacted is suspicious e.g. 100s of TVs of the same make

		ordered at the same time. *address* - The billing/shipping address has been associated with fraud in the past. *geolocation* - The IP Address did not match billing/shipping details. *time* - The transaction was performed during an unusual time.
assert_impact_desc	medium high	*medium* – the impact of the report is medium (e.g. an address change might be suspicious, but not high impact). *high* – The impact of the report is high (e.g. the entity has committed Card Not Present fraud).
assert_confidence_desc	suspicious / confirmed_bad	*suspicious* – Fraud is suspected, but not yet confirmed by an analyst *confirmed_bad* - A fraud incident has been manually confirmed by an analyst

11. Appendix B: Definitions of Response Fields

<table>
<tr><th colspan="3">Response Fields</th></tr>
<tr><th>Variable Name</th><th>Size/Type</th><th>Description</th></tr>
<tr><td>ResponseCode</td><td>3 / an</td><td>The response codes:
<table><tr><th>Result Value</th><th>Definition</th></tr><tr><td>001</td><td>Success</td></tr><tr><td>981</td><td>Data error</td></tr><tr><td>982</td><td>Duplicate order_id</td></tr><tr><td>983</td><td>Invalid transaction</td></tr><tr><td>984</td><td>Previously Asserted</td></tr><tr><td>985</td><td>Invalid Activity Description</td></tr><tr><td>986</td><td>Invalid Impact Description</td></tr><tr><td>987</td><td>Invalid Confidence Description</td></tr><tr><td>988</td><td>Cannot find previous</td></tr></table></td></tr>
<tr><td>Message</td><td></td><td>The response message</td></tr>
<tr><td>event_type</td><td></td><td>The type of transaction or event returned in the response.</td></tr>
<tr><td>org_id</td><td></td><td>The ThreatMetrix defined unique transaction identifier.</td></tr>
<tr><td>policy</td><td></td><td>The Policy used for the session_query will be returned with the return request. If the Policy was not included, then the Policy name default is returned.</td></tr>
<tr><td>policy_score</td><td></td><td>The sum of all the risks weights from triggered rules within the selected policy in the range [-100…100]</td></tr>
<tr><td>request_duration</td><td></td><td>Length of time it takes for the transaction to be processed.</td></tr>
<tr><td>request_id</td><td></td><td>The request identifier is a unique number and will always be returned with the return request.</td></tr>
<tr><td>request_result</td><td></td><td>success – ThreatMetrix was able to process the request successfully
fail_access – ThreatMetrix was unable to process the request due to API verification failing
fail_verification – API query limit reached
fail_incomplete – ThreatMetrix was unable to process the request due to incomplete or incorrect input data
fail_internal_error – ThreatMetrix encountered an error while processing the request
fail_temporarily_unavailable – the request fail because the service is temporarily unavailable
fail_invalid_email_address – the format of the supplied email address was invalid
fail_invalid_telephone_number – the format of the supplied telephone number was invalid
fail_invalid_device_id – the format of the supplied device_id was invalid
fail_invalid_ip_address_parameter – the format of a supplied ip_address parameter was invalid</td></tr>
<tr><td>review_status</td><td></td><td>The transaction status based on the assessments and risk scores.</td></tr>
<tr><td>risk_rating</td><td></td><td>The rating based on the assessments and risk scores.</td></tr>
<tr><td>service_type</td><td></td><td>The service type will be returned in the attribute query response.</td></tr>
<tr><td>session_id</td><td></td><td>The temporary identifier unique to the visitor will be returned in the return request.</td></tr>
<tr><td>summary_risk_score</td><td></td><td>This score is based on all of the returned values in the range [-100 … 100]</td></tr>
<tr><td>transaction_id</td><td></td><td>This is the transaction identifier and will always be returned in the response when supplied as input.</td></tr>
<tr><td>unknown_session</td><td></td><td>If present, the value is ‘yes’ and indicates the session_id that was passed was not found.</td></tr>
<tr><td>RuleName</td><td></td><td>The names of rules verified from the selected policy that have triggered. Each rule name is returned as a separate name/value pair.</td></tr>
<tr><td>RuleCode</td><td></td><td>The codes of the rules verified from the selected policy that have triggered. Each rule code is</td></tr>
</table>

	returned as a separate name/value pair.
RuleMessageEn	An English message description of the rule returned.
RuleMessageFr	A French message description of the rule returned.

12. Appendix C: Risk Management Tool Rules & Codes

The following is a list of all possible responses of Rule Names once a Query has been performed.

Rule Number and Rule Description			
Rule Name	**Rule Number**	**Message / Description**	**Rule Explanation**
White lists			
DeviceWhitelisted	WL001	Device White Listed	Device is on the white list. This indicates that the device has been flagged as always "ok". NOTE: This rule is currently not in use.
IPWhitelisted	WL002	IP White Listed	IP Address is on the white list. This indicates the device has been flagged as always "ok". NOTE: This rule is currently not in use.
EmailWhitelisted	WL003	Email White Listed	Email address is on the white list. This indicates that the device has been flagged as always "ok". NOTE: This rule is currently not in use.
Event Velocity			
2DevicePayment	EV003	2 Device Payment Velocity	Multiple payments were detected from this device in the past 24 hours.
2IPPaymentVelocity	EV006	2 IP Payment Velocity	Multiple payments were detected from this IP within the past 24 hours.
2ProxyPaymentVelocity	EV008	2 Proxy Payment Velocity	The device has used 3 or more different proxies during a 24 hour period. This could be a risk or it could be someone using a legitimate corporate proxy.
Email			
3EmailPerDeviceDay	EM001	3 Emails for the Device ID in 1 Day	This device has presented 3 different email ids within the past 24 hours.
3EmailPerDeviceWeek	EM002	3 emails for the Device ID in 1 week	This device has presented 3 different email ids within the past week.
3DevciePerEmailDay	EM003	3 Device Ids for email address in 1 day	This email has been presented from three different devices in the past 24 hours.
3DevciePerEmailWeek	EM004	3 Device Ids for email address in 1 week	This email has been presented from three different devices in the past week.
EmailDistanceTravelled	EM005	Email Distance Travelled	This email address has been associated with different physical locations in a short period of time.
3EmailPerSmartIDHour	EM006	3 Emails for SmartID in 1 Hour	The SmartID for this device has been associated with 3 different email addresses in 1 hour.
GlobalEMailOverOneMonth	EM007	Global Email over 1 month	The e-mail address involved in the transaction over 30 days ago. This generally indicates that the transaction is less risky. Note: This rule is currently set currently set so it does not impact the policy score or risk rating.
ComputerGeneratedEmailAddress	EM008	Computer Generated Email Address	This transaction used a computer generated email address.
Account Number			
3AccountNumberPerDeviceDay	AN001	3 Account Numbers for device in 1 day	This device has presented 3 different user accounts within the past 24 hours.
3AccountNumberPerDeviceWeek	AN002	3 Account Numbers for device in 1 week	This device has presented 3 different user accounts within the past week.

3DevciePerAccountNumberDay	AN003	3 Device IDs for account number in 1 day	This user account been used from three different devices in the past 24 hours.
3DevciePerAccountNumberWeek	AN004	3 Device IDs for account number in 1 week	This card number has been used from three different devices in the past week.
AccountNumberDistanceTravelled	AN005	Account Number distance travelled	This card number has been used from a number of physically different locations in a short period of time.
Credit Card / Payments			
3CreditCardPerDeviceDay	CP001	3 credit cards for device in 1 day	This device has used three credit cards within 24 hours.
3CreditCardPerDeviceWeek	CP002	3 credit cards for device in 1 week	This device has used three credit cards within 1 week.
3DevicePerCreditCardDay	CP003	3 device ids for credit card in 1 day	This credit card has been used on three different devices in 24 hours.
3DevciePerCreditCardWeek	CP004	3 device ids for credit card in 1 week	This credit card has been used on three different devices in 1 week.
CredtCardDistanceTravelled	CP005	Credit Card has travelled	The credit card has been used at a number of physically different locations in a short period of time.
CreditCardShipAddressGeoMismatch	CP006	Credit Card and Ship Address do not match	The credit card was issued in a region different from the Ship To Address information provided.
CreditCardBillAddressGeoMismatch	CP007	Credit Card and Billing Address do not match	The credit card was issued in a region different from the Billing Address information provided.
CreditCardDeviceGeoMismatch	CP008	Credit Card and device location do not match	The device is located in a region different from where the card was issued.
CreditCardBINShipAddressGeoMismatch	CP009	Credit Card issuing location and Shipping address do not match	The credit card was issued in a region different from the Ship To Address information provided.
CreditCardBINBillAddressGeoMismatch	CP010	Credit Card issuing location and Billing address do not match	The credit card was issued in a region different from the Billing Address information provided.
CreditCardBINDeviceGeoMismatch	CP011	Credit Card issuing location and location of the device do not match	The device is located in a region different from where the card was issued.
TransactionValueDay	CP012	Daily Transaction Value Threshold	The transaction value exceeds the daily threshold.
TransactionValueWeek	CP013	Weekly Transaction Value Threshold	The transaction value exceeds the weekly threshold.
Proxy Rules			
3ProxyPerDeviceDay	PX001	3 Proxy Ips in 1 day	This device has used three different proxy servers in the past 24 hours.
AnonymousProxy	PX002	Anonymous Proxy IP	This device is using an anonymous proxy
UnusualProxyAttributes	PX003	Unusual Proxy Attributes	This transaction is coming from a source with unusual proxy attributes.
AnonymousProxy	PX004	Anonymous Proxy	This device is connecting through an anonymous proxy connection.
HiddenProxy	PX005	Hidden Proxy	This device is connecting via a hidden proxy server.
OpenProxy	PX006	Open Proxy	This transaction is coming from a source that is using an open proxy.
TransparentProxy	PX007	Transparent Proxy	This transaction is coming from a source that is using a transparent proxy.

DeviceProxyGeoMismatch	PX008	Proxy and True GEO Match	This device is connecting through a proxy server that didn't match the devices geolocation.
ProxyTrueISPMismatch	PX009	Proxy and True ISP Match	This device is connecting through a proxy server that doesn't match the true IP address of the device.
ProxyTrueOrganizationMismatch	PX010	Proxy and True Org Match	The Proxy information and True ISP information for this source do not match.
DeviceProxyRegionMismatch	PX011	Proxy and True Region Match	The proxy and device region location information do not match.
ProxyNegativeReputation	PX012	Proxy IP Flagged Risky in Reputation Network	This device is connecting from a proxy server with a known negative reputation.
SatelliteProxyISP	PX013	Satellite Proxy	This transaction is coming from a source that is using a satellite proxy.
GEO			
DeviceCountriesNotAllowed	GE001	True GEO in Countries Not Allowed blacklist	This device is connecting from a high-risk geographic location.
DeviceCountriesNotAllowed	GE002	True GEO in Countries Not Allowed (negative whitelist)	The device is from a region that is not on the whitelist of regions that are accepted.
DeviceProxyGeoMismatch	GE003	True GEO different from Proxy GEO	The true geographical location of this device is different from the proxy geographical location.
DeviceAccountGeoMismatch	GE004	Account Address different from True GEO	This device has presented an account billing address that doesn't match the devices geolocation.
DeviceShipGeoMismatch	GE005	Device and Ship Geo mismatch	The location of the device and the shipping address do not match.
DeviceShipGeoMismatch	GE006	Device and Ship Geo mismatch	The location of the device and the shipping address do not match.
Device			
SatelliteISP	DV001	Satellite ISP	This transaction is from a source that is using a satellite ISP.
MidsessionChange	DV002	Session Changed Mid-session	This device changed session details and identifiers in the middle of a session.
LanguageMismatch	DV003	Language Mismatch	The language of the user does not match the primary language spoken in the location where the True IP is registered.
NoDeviceID	DV004	No Device ID	No device ID was available for this transaction.
Dial-upConnection	DV005	Dial-up connection	This device uses a less identifiable dial-up connection.
DeviceNegativeReputation	DV006	Device Blacklisted in Reputational Network	This device has a known negative reputation as reported to the fraud network.
DeviceGlobalBlacklist	DV007	Device on the Global Black List	This device has been flagged on the global blacklist of known problem devices.
DeviceCompromisedDay	DV008	Device compromised in last day	This device has been reported as compromised in the last 24 hours.
DeviceCompromisedHour	DV009	Device compromised in last hour	This device has been reported as compromised in the last hour.
FlashImagesCookiesDisabled	DV010	Flash Images Cookies Disabled	Key browser functions/identifiers have been disabled on this device.
FlashCookiesDisabled	DV011	Flash Cookies Disabled	Key browser functions/identifiers have been disabled on this device.
FlashDisabled	DV012	Flash Disabled	Key browser functions/identifiers have been

			disabled on this device.
ImagesDisabled	DV013	Images Disabled	Key browser functions/identifiers have been disabled on this device.
CookiesDisabled	DV014	Cookies Disabled	Key browser functions/identifiers have been disabled on this device.
DeviceDistanceTravelled	DV015	Device Distance Travelled	The device has been used from multiple physical locations in a short period of time.
PossibleCookieWiping	DV016	Cookie Wiping	This device appears to be deleting cookies after each session.
PossibleCookieCopying	DV017	Possible Cookie Copying	This device appears to be copying cookies.
PossibleVPNConnection	DV018	Possibly using a VPN Connection	This device may be using a VPN connection

13. Appendix D: Example of Risk Response

A. Session Query

```
<?xml version=”1.0”?>
<response>
<receipt>
      <ResponseCode>001</ResponseCode>
      <Message>Success</Message>
<Result>
      <session_id>abc123</session_id>
      <unknown_session>yes</unknown_session>
      <event_type>payment</event_type>
      <service_type>session</service_type>
      <policy_score>-25</policy_score>
      <transaction_id>riskcheck42</transaction_id>
      <org_id>11kue096</org_id>
      <request_id>91C1879B-33D4-4D72-8FCB-B60A172B3CAC</request_id>
      <risk_rating>medium</risk_rating>
      <request_result>success</request_result>
      <summary_risk_score>-25</summary_risk_score>
      <Policy>default</policy>
      <review_status>review</review_status>
</Result>
<Rule>
      <RuleName>ComputerGeneratedEMail</RuleName>
      <RuleCode>UN001</RuleCode>
      <RuleMessageEn>Unknown Rule</RuleMessageEn>
      <RuleMessageFr>Regle Inconnus</RuleMessageFr>
</Rule>
<Rule>
      <RuleName>NoDeviceID</RuleName>
      <RuleCode>DV004</RuleCode>
      <RuleMessageEn>No Device ID</RuleMessageEn>
      <RuleMessageFr>null</RuleMessageFr>
</Rule>
</receipt>
</response>
```

B. Attribute Query

```
<?xml version=”1.0”?>
<response>
<receipt>
      <ResponseCode001</ReponseCode>
      <Message = Success</Message>
<Result>
      <org_id>11kue096</org_id>
      <request_id>443D7FB5-CC5C-4917-A57E-27EAC824069C</request_id>
      <service_type>session</service_type>
      <risk_rating>medium</risk_rating>
      <summary_risk_score>-25</summary_risk_score>
      <request_result>success</request_result>
      <policy>default</policy>
      <policy_score>-25</policy_score>
      <transaction_id>riskcheck19</transaction_id>
      <review_status>review</review_status>
</Result>
<Rule>
      <RuleName>ComputerGeneratedEMail</RuleName>
      <RuleCode>UN001</RuleCode>
      <RuleMessageEn>Unknown Rule</RuleMessageEn>
      <RuleMessageFr>Regle Inconnus</RuleMessageFr>
</Rule>
<Rule>
```

```
        <RuleName>NoDeviceID</RuleName>
        <RuleCode>DV004</RuleCode>
        <RuleMessageEn>No Device ID</RuleMessageEn>
        <RuleMessageFr>null</RuleMessageFr>
</Rule>
</receipt>
</response>
```

C. Assertion Query

```
<?xml version=”1.0”?>
<response>
<receipt>
        <ResponseCode>001</ResponseCode>
        <Message>Successful Assertion</Message>
<Result>
        <request_id>967F1AB1-4F19-4A13-9945-B5B19D784305</request_id>
        <request_result>success<request_result>
        <request_duration>51</request_duration>
</Result>
</receipt>
</response>
```