Fraud Genius Fraud Score API 1.0 Specification

Document version 1.13 (1/2014)

The following API specification is used to obtain a fraud score for an e-commerce transaction by a merchant website or back-end payment processing servers. The fraud score value returned is 0 through 100 indicating the risk factor of the submitted transaction (low values are lower risk). Sample code is provided by Fraud Genius illustrating a properly formatted call to the Fraud Genius API (Application Programming Interface) using the following specification. If the sample code language is not in use by your organization, you can use the following to construct an API call.

Calling the Fraud Genius API

The Fraud Genius HTTP API requires you to pass a set of field/value pairs as an HTTP POST over an HTTPS (port 443) connection. The URI for this service is: **https://api.fraudgenius.com/api.php**
The post field names and expected values are in the input table below.

Some fields below are -required- in order to process a fraud score API call. Missing required fields will result in an error being returned by the API. It is strongly recommended that all supported fields are sent to the API as this will increase the accuracy of the fraud score to maximum.

Address and other entry fields physically typed by the end-user (customer) on your website order form SHOULD NOT be trimmed, scrubbed or capitalization changed before sending to the API. If you perform capitalization correction or whitespace trimming on your webpage order form (e.g., with javascript) - before doing this - it is strongly recommended to retain the original entry text in a separate variable for passage to the Fraud Genius API. For example, if the customer types the address line: "123 MAIN street " - Retain the full line including capitalization and any trailing or leading spaces. Use the original text to send to the API in the appropriate field.

The API supports returning a fraud score for PayPal type transactions (see billcountry field instructions) - with most fields not sent that are typically used with a credit card transaction.

PCI DSS Note: Some optional values indicated below containing customer information are used for score determination. This credit card billing information is not stored by Fraud Genius - it is only used to determine score, then discarded - and so should not impact your PCI DSS compliance beyond the security of the API call. The API call is PCI DSS compliant secured forced HTTPS using a trusted signed root certificate.

API INPUT FIELDS (POSTed Variables)

Field Variable Name	Type/Expected Value (Maximum Length)	Description
Required INPUT Fields - The following fields are required.		
merchid	string (255)	Your merchant ID is supplied by Fraud Genius during your account creation.
merchkey	string (255)	Your initial merchant key is supplied by Fraud Genius during account creation. The key can be changed in your account management area.
apiversion	string (255) If missing, assumed API 1.0 call (value: 1.0)	String indicating the API version that this call is formatted for. If using this specification in your API call - the value should be: 1.0
transactionid	string (255)	Your internal identifier for this transaction. This value is echoed back in the API response for confirmation on your end that the score is matching the submitted transaction. This is also used in your account management area to identify transactions for further score review/reports. If you do not maintain internal transaction identifiers, it is recommended that you submit a unique number for each API call in any case (such as a unix timestamp).
billcountry	string (2)	The 2 letter (ISO 3166-1) billing country code supplied by the end-user customer on your website order form for this transaction. For PayPal type transactions where you do not have access to the billing country being used, use PP as the country code.
remoteip	string (255)	The source IP address of the customer connection to your website (e.g.; PHP variable $_SERVER['REMOTE_ADDR']) - IPv4 expected for API 1.0 calls.

OPTIONAL INPUT Fields - the following fields are optional, but recommended for score accuracy.		
testtrans	integer (1)	Used for testing your website communication with the Fraud Genius API. If this field is included, and set to value 1, the transaction sent to the API will be treated as a test transaction only. The API will not record a test transaction against monthly totals or for reporting. The API will always return a score of "123456789" for test transactions. Note: Certain features, like transaction velocity settings, may not work with a test transaction.
fname	string (255)	The customer first name exactly as typed in your website order form (no case changes or whitespace trimming).
lname	string (255)	The customer last name exactly as typed in your website order form (no case changes or whitespace trimming).
ccname	string (255)	The full name on the credit card exactly as typed (no case changes or whitespace trimming) by the customer on your website order form. Do not construct this on your end by combining first and last names - leave blank if the full credit card name is not available.
ccnumber	string (255)	The first 6 digits of the credit card used for the transaction. Do not include dashes or spaces. If the full credit card number is supplied, this will be truncated by the API to the first 6 digits.
billstreet1	string (255)	The billing street address line one exactly as typed (no case changes or whitespace trimming) by the customer on your website order form.
billstreet2	string (255)	The billing street address line two exactly as typed (no case changes or whitespace trimming) by the customer on your website order form.
billcity	string (255)	The billing city exactly as typed (no case changes or whitespace trimming) by the customer on your website order form.

billstate	string (255)	The billing state/provence exactly as typed (no case changes or whitespace trimming) by the customer on your website order form.
billpostalcode	string (255)	The billing postal code supplied by the customer on your website order form.
custemail	string (255)	The customer email supplied for your website order processing.
custpass	string (255)	The customer password supplied for your website order processing.
agent	string (255)	The User-Agent HTTP header for the customer connection to your website order form (e.g.; supplied by the PHP variable $_SERVER['HTTP_USER_AGENT'])
acceptlang	string (255)	The Accept-Language HTTP header for the customer connection to your website order form (e.g.; supplied by the PHP variable $_SERVER['HTTP_ACCEPT_LANGUAGE'])
accept	string (255)	The Accept HTTP header indicating the browser content types for the customer connection to your website order form (e.g.; supplied by the PHP variable $_SERVER['HTTP_ACCEPT'])
acceptencode	string (255)	The encoding HTTP header indicating the accepted browser compression types supported for the customer connection to your website order form (e.g.; supplied by the PHP variable $_SERVER['HTTP_ACCEPT_ENCODING'])
proxyip	string (255)	The IP address included in any standard proxy HTTP headers for the customer connection to your website order form. This field should only be included if different than the remoteip field. Note that this header value is typically blank. See API sample code for sending recommendation. For example, this value can be included in the following PHP $_Server keys: 'HTTP_X_FORWARDED_FOR', 'HTTP_X_FORWARDED', 'HTTP_X_CLUSTER_CLIENT_IP', 'HTTP_FORWARDED_FOR', 'HTTP_FORWARDED'

Optional Informational Fields Below - Maintained for post transaction review/reports and for custom merchant account preferences (example, how score is affected by dollar amounts or black/whitelisting). Otherwise, omitting will not affect fraud score accuracy.		
cost	decimal (20,2)	The total dollar amount of the transaction. Can be in any value/currency - as this is used for merchant side reports and setting limits (see your account management preferences) - it is not directly used by the 1.0 API.
quantity	integer (11)	The item quantity of the transaction.
itemcode	string (255)	Your internal item code of the product(s) ordered in the transaction.
customerid	string (255)	Your internal customer ID of the customer entering the transaction on the website order form. Can be used for whitelisting, for example, in your merchant account preferences.

API Returned Values

The API will return a delimited set of values back through the calling HTTPS connection. The API v1.0 uses the | character (ASCII #124, HTML |) as the delimiter. Example: value1|value2|value3|...

Field names for the values ARE NOT returned. All values are returned in the specified order regardless of error condition or a successfully derived fraud score. See the sample code for constructing forward compatible API calling code (for future API versions). Assume an error if an incorrect amount of fields are returned for the indicated field apiversion call value. Example, API v1.0 calls all return the four (4) values indicated in the output table below.

API OUTPUT VALUES - 4 total for API v1.0

Returned over HTTPS connection from API call - delimited by | character (ASCII #124, HTML |)

Value Order	Type	Name	Description
1	integer	Response Code	This is returned as 1 for a successful fraud score derived from the transaction. Value of 2 for error condition returned from API (see Message Text value below). Note if using the Fraud Genius sample code API calling class, this value is returned from the API calling function getfraudscore() - A 3 is returned from getfraudscore() if connecting to the API was unsuccessful.
2	string	Message Text	If an error condition exists from the API call (Response Code is 2 or 3) - the Error reason text will be indicated here. Example: "Merchant key incorrect" Also, if there is a score override triggered because of your account preferences, the reason will be indicated. Example: "BLOCK ALL TRIGGERED: Region <shown> - See account preferences"
3	string	Transaction ID	This is the transactionid field from the API call echoed back as confirmation that the return information is associated with the called transaction. If the call was processed normally, it will equal the transactionid field.
4	signed integer	Fraud Score	The fraud score for the transaction if successfully derived (Response Code is 1). Returned Fraud Score values are 0 (low risk) through 100 (high risk of fraud) for the API v1.0 calls. A fraud score of -1 indicates an error condition (see Message Text value). Note that if your account preferences triggered a score override (e.g.; transaction is from an IP you whitelisted), the Message Text return value will indicate this. An override issues a Fraud Score of either 0 (Allow all triggered) or maximum of 100 (block all triggered).

Order Detail XML Query

Fraud Genius provides informational order and score details on any transaction previously passed to the fraud score API under your account. This order details query returns similar information that is provided in your Transaction History on the Fraud Genius website account management area (log into www.fraudgenius.com customer area to see this). The Order Detail interface is accessed by passing your merchant ID, merchant key, and transaction ID using an HTTP POST over an HTTPS (port 443) connection. The URI for this service is: **https://api.fraudgenius.com/orderdispxml.php**

An XML description for the order is returned, as described below.

The POST field names and expected values to the URI for this service are in the input table below:

ORDER DETAIL INPUT FIELDS (POSTed Variables)

Field Variable Name	Type/Expected Value (Maximum Length)	Description
merchid	string (255)	Your merchant ID is supplied by Fraud Genius during your account creation.
merchkey	string (255)	Your Fraud Genius account merchant key.
transactionid	string (255)	The transaction ID that you are requesting details for is supplied in this field. This is the same ID that was previously passed to the fraud score API in the transactionid field. IMPORTANT NOTE: You must be using unique transaction IDs in your previous fraud score API calls to successfully access this XML query. If there are duplicate IDs for the transaction you are querying, an error will be returned by this call.
version	string (255) If missing, assumed details version 1.0 call (value: 1.0)	Optional string indicating the version of order details expected to be returned for this call - the default value is 1.0 if missing and the XML block of version 1.0 is described below.

ORDER DETAIL OUTPUT

An XML document is returned by a properly formatted call to the Order Detail service.

Below is a sample XML returned from a call to the Order Detail service for transaction ID ORD123456789:

Order Detail XML Output Sample

```
<?xml version="1.0" encoding="UTF-8"?>
<order transactionid="ORD123456789" xmlns="FraudGeniusOrderDetail"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:SchemaLocation="FraudGeniusOrderDetail https://api.fraudgenius.com/orderdisp.xsd">
  <time>2013-01-29 21:56:08</time>
  <score>87</score>
  <connection>
    <risklevel>high</risklevel>
    <note>The order originates from a country with high fraudulent activity.</note>
    <ip>41.66.207.0</ip>
    <country>Ghana</country>
  </connection>
  <billingcountry>US</billingcountry>
  <email>
    <risklevel>medium</risklevel>
    <note>The customer email domain is considered medium risk.</note>
    <orderemail>sample@hotmail.com</orderemail>
  </email>
  <customerid>mycustomer3789737</customerid>
  <cost>99.89</cost>
  <quantity>2</quantity>
  <itemcode>myspeaker-9in subwoofer</itemcode>
  <bininfo>
    <unknown>false</unknown>
    <issuer>SAMPLE BANK, LTD.</issuer>
    <issuercountry>COSTA RICA</issuercountry>
    <brand>MASTERCARD</brand>
    <cardtype>DEBIT</cardtype>
    <category>PREPAID</category>
    <website>HTTP://WWW.SAMPLEBANKLTD.COM/</website>
    <telephone>502.213.6951</telephone>
  </bininfo>
  <indicators>
    <indicator>
      <risklevel>high</risklevel>
      <note>The order has characteristics in text entry that indicate fraud.</note>
    </indicator>
    <indicator>
      <risklevel>medium</risklevel>
      <note>The credit card issuing bank is not in the same country as the order origin, or
has other anomalies that indicate the card may have a higher risk of fraudulent use.</note>
    </indicator>
    <indicator>
      <risklevel>medium</risklevel>
      <note>The billing country is not matching order connection source IP.</note>
    </indicator>
  </indicators>
</order>
```

The schema description for this XML is below (also available from the following URL: **https://api.fraudgenius.com/orderdisp.xsd**). The schema can be used by the merchant retail system's XML parser or as a guide to manually process an Order Detail output. Note the following from the Schema:

- The <bininfo> element will not be returned in the XML if the credit card BIN was not supplied with the original order.
- If the BIN was supplied but <unknown> is **`true`**, the following fields in the <bininfo> type are not returned.
- The connection city may not be supplied (depending upon confidence).
- There can be multiple <indicator> elements provided for the order in the XML.
- <risklevel> is a string with the following available values: info | low | medium | high
- Either <error>, on failure, or <order>, on success, will be returned as the root XML element.

Order Detail Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
targetNamespace="FraudGeniusOrderDetail" xmlns="FraudGeniusOrderDetail"
elementFormDefault="qualified">

  <xsd:annotation>
    <xsd:documentation xml:lang="en">Order Detail Display for Fraud Genius (v1.0)
Copyright 2014 FraudGenius.com. All rights reserved.</xsd:documentation>
  </xsd:annotation>

  <xsd:simpleType name="risklevelType">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="info"/>
      <xsd:enumeration value="low"/>
      <xsd:enumeration value="medium"/>
      <xsd:enumeration value="high"/>
    </xsd:restriction>
  </xsd:simpleType>

  <xsd:complexType name="orderType">
    <xsd:sequence>
      <xsd:element name="time" type="xsd:dateTime"/>
      <xsd:element name="score" type="xsd:int"/>
      <xsd:element name="connection">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element name="risklevel" type="risklevelType"/>
            <xsd:element name="note" type="xsd:string"/>
            <xsd:element name="ip" type="xsd:string"/>
            <xsd:element name="country" type="xsd:string"/>
            <xsd:element name="city" type="xsd:string" minOccurs="0"/>
          </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="billingcountry" type="xsd:string"/>
      <xsd:element name="email">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element name="risklevel" type="risklevelType"/>
            <xsd:element name="note" type="xsd:string"/>
```

```
            <xsd:element name="orderemail" type="xsd:string"/>
          </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="customerid" type="xsd:string"/>
      <xsd:element name="cost" type="xsd:decimal"/>
      <xsd:element name="quantity" type="xsd:int"/>
      <xsd:element name="itemcode" type="xsd:string"/>
      <xsd:element name="bininfo" minOccurs="0">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element name="unknown" type="xsd:boolean"/>
            <xsd:element name="issuer" type="xsd:string"  minOccurs="0"/>
            <xsd:element name="issuercountry" type="xsd:string"  minOccurs="0"/>
            <xsd:element name="brand" type="xsd:string"  minOccurs="0"/>
            <xsd:element name="cardtype"  minOccurs="0">
              <xsd:simpleType>
                <xsd:restriction base="xsd:string">
                  <xsd:enumeration value=""/>
                  <xsd:enumeration value="DEBIT"/>
                  <xsd:enumeration value="CREDIT"/>
                  <xsd:enumeration value="CHARGE CARD"/>
                </xsd:restriction>
              </xsd:simpleType>
            </xsd:element>
            <xsd:element name="category" type="xsd:string"  minOccurs="0"/>
            <xsd:element name="website" type="xsd:string"  minOccurs="0"/>
            <xsd:element name="telephone" type="xsd:string"  minOccurs="0"/>
          </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="indicators">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element name="indicator" minOccurs="0" maxOccurs="unbounded">
              <xsd:complexType>
                <xsd:sequence>
                  <xsd:element name="risklevel" type="risklevelType"/>
                  <xsd:element name="note" type="xsd:string"/>
                </xsd:sequence>
              </xsd:complexType>
            </xsd:element>
          </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
    </xsd:sequence>
    <xsd:attribute name="transactionid" type="xsd:string"/>
  </xsd:complexType>

  <xsd:element name="order" type="orderType"/>
  <xsd:element name="error" type="xsd:string"/>
</xsd:schema>
```

For questions or comments on this document, please email support@fraudgenius.com