Antifraude (Antifraud)

Integration Manual

Version 1.7.1

04/28/2014

TABLE OF CONTENTS

HISTORY OF CHANGES

Integration Manual - Antifraude		
Version	Date	* Description
1.0	04/12/2012	* Initial Version
1.1	05/09/2012	* Error 907 added in table 6.3; Class added: **AntiFraudRequest.MerchantDefinedData**
1.2	6/27/2012	* Removal of Parameters: **AntiFraudRequest.BillToData.DomainName; AntiFraudRequest.BillToData.IpNetworkAddress; AntiFraudRequest.CardData.Bin** * Change Description of the Parameters: **AntiFraudRequest.BillToData.FirstName; AntiFraudRequest.BillToData.LatName; AntiFraudRequest.DecisionManagerData. TravelData.DepartureTime AntiFraudRequest.DecisionManagerData. TravelData.TravelLegData.Origin**
1.3	10/18/2012	*Creation of version 1.1 of FraudAnalysis method, which allows the sending of 95 extra data fields instead of just 15; Inserion of these parameters and their descriptions on Table 1: **Version; AntiFraudRequest.AdditionalData [AdditionalDataCollection]**
1.3.1	1/28/2013	* Change Description of the Parameters: **AntiFraudRequest.BillToData.IpAddress; AntiFraudRequest.InvoiceHeaderData.ReturnsAccepted; AntiFraudRequest.PurchaseTotalsData.Currency;** *Insert the Elo item in Table 5.2
1.4	04/05/2013	* Insert the method status UpdateStatus; * Update the table 6.1; * Change the name of the method from **FrudAnalysisTransaction** to **FraudAnalysisTransactionDetails** and other information from this method.
1.5	04/08/2013	* Insert URL homologation; * Insert Link Service Description;
1.5.1	04/10/2013	* Review of all tables in the document; * Standardization of the description of the fields Success and CorrelateID
1.6	08/19/2013	* Detailing Service Changing Status Notice; * Insert Annex 1 - Adding Fingerprint; * Insertion of Parameters in the object FraudAnalysisRequest: **AntiFraudRequest.CardData.AccountToken, AntiFraudRequest.CardData.AccountAlias** and **AntiFraudRequest.CardData.SaveAccountNumber** ***** Changing the description of the parameters, in the object FraudAnalysisRequest**: AntiFraudRequest.MerchantDefinedData, AntiFraudRequest.AdditionalData [AdditionalDataCollection]**

1.7	12/03/2013	* Deleting the following parameters, on the FraudAnalysisRequest object:**AntiFraudRequest.MerchantDefinedData, AntiFraudRequest.MerchantDefinedData.Field1 to AntiFraudRequest.MerchantDefinedData.Field15** * Changing the following parameter description, on the FraudAnalysisRequest object: **AntiFraudRequest.MerchantReferenceCode** * Insert the parameter **AntiFraudRequest.DeviceFingerprintID** on the FraudAnalysisRequest object * Changing the Annex 1 - Adding Fingerprint
1.7.1	04/28/2014	Change in object FraudAnalysisRequest, parameter AntiFraudRequest.CardData.AccountNumber

INTRODUCTION

The Antifraude platform is aimed at assisting e-commerce merchant to detect online fraud through the use of tools already available in the market.
The Antifraude integrates with the Pagador's gateway, making it easier to submit and process transactions.

OBJECTIVE

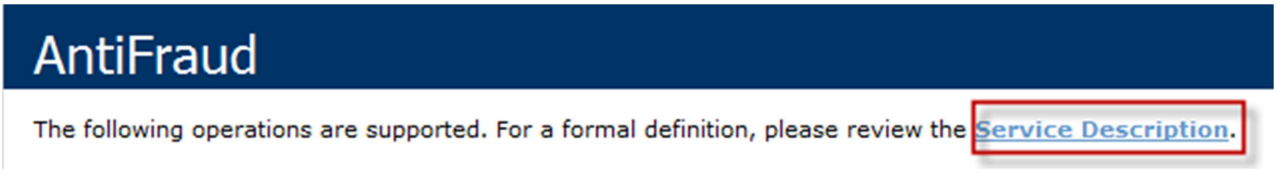
This manual aims to guide the Merchant's developer on the integration with the Antifraude platform, describing existing functions and methods to be used, listing information to be sent and received, and providing examples. The manual describes integration sequences via *Web service.*

This manual is intended for the following supplier

- ✓ **CyberSource -** http://www.cybersource.com

Url Approval: https://homologacao.braspag.com.br/AntiFraudews/antifraud.asmx

To access the webservice code description (WSDL), access the link "Service Description", as follows:



Integration always should be done using URL and under no circumstances by IP or by using names like www.pagador.com.br or just pagador.com.br.

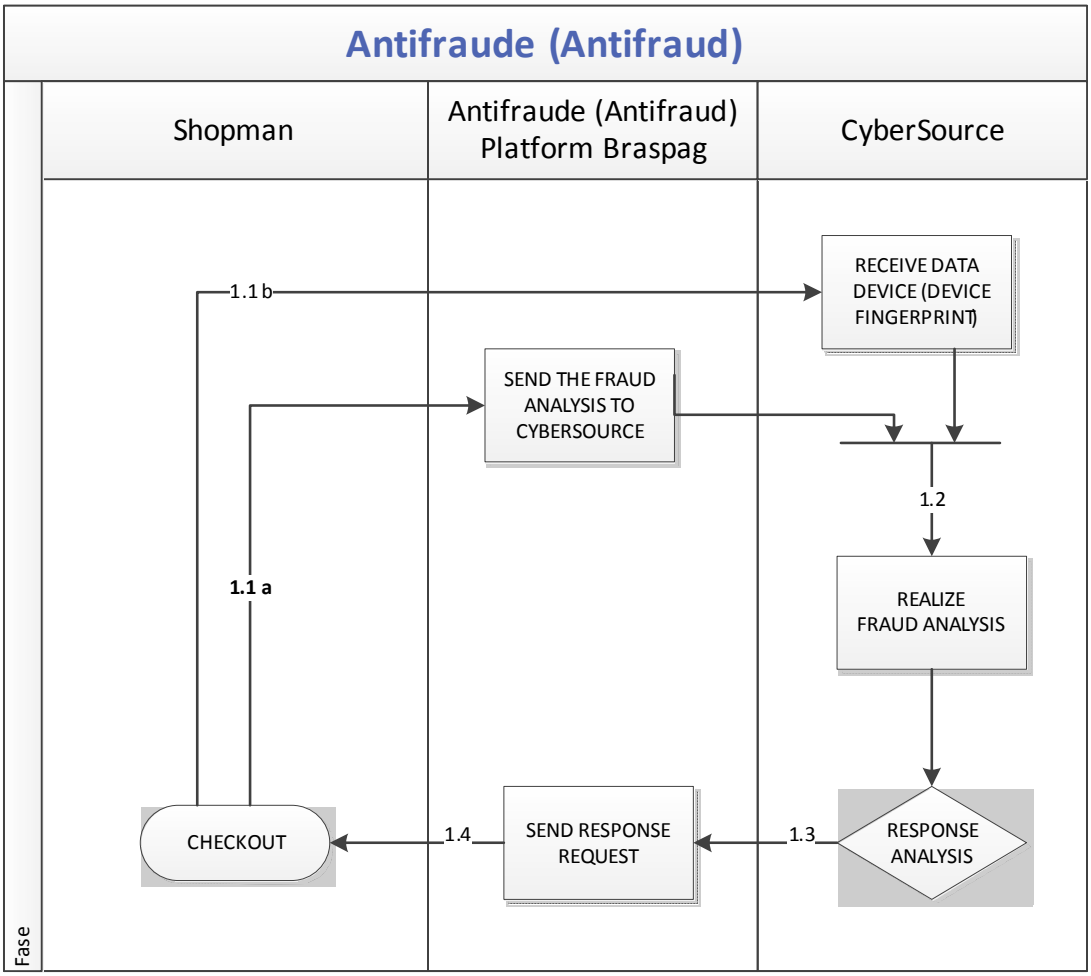
To get the production URL, please ask our implementation team through our support tool (http://suporte.braspag.com.br).

1. POTENTIAL SCENARIOS

Below are the three potential sequences for the Antifraude Platform via Web service.

1.1. Antifraude (Antifraud)

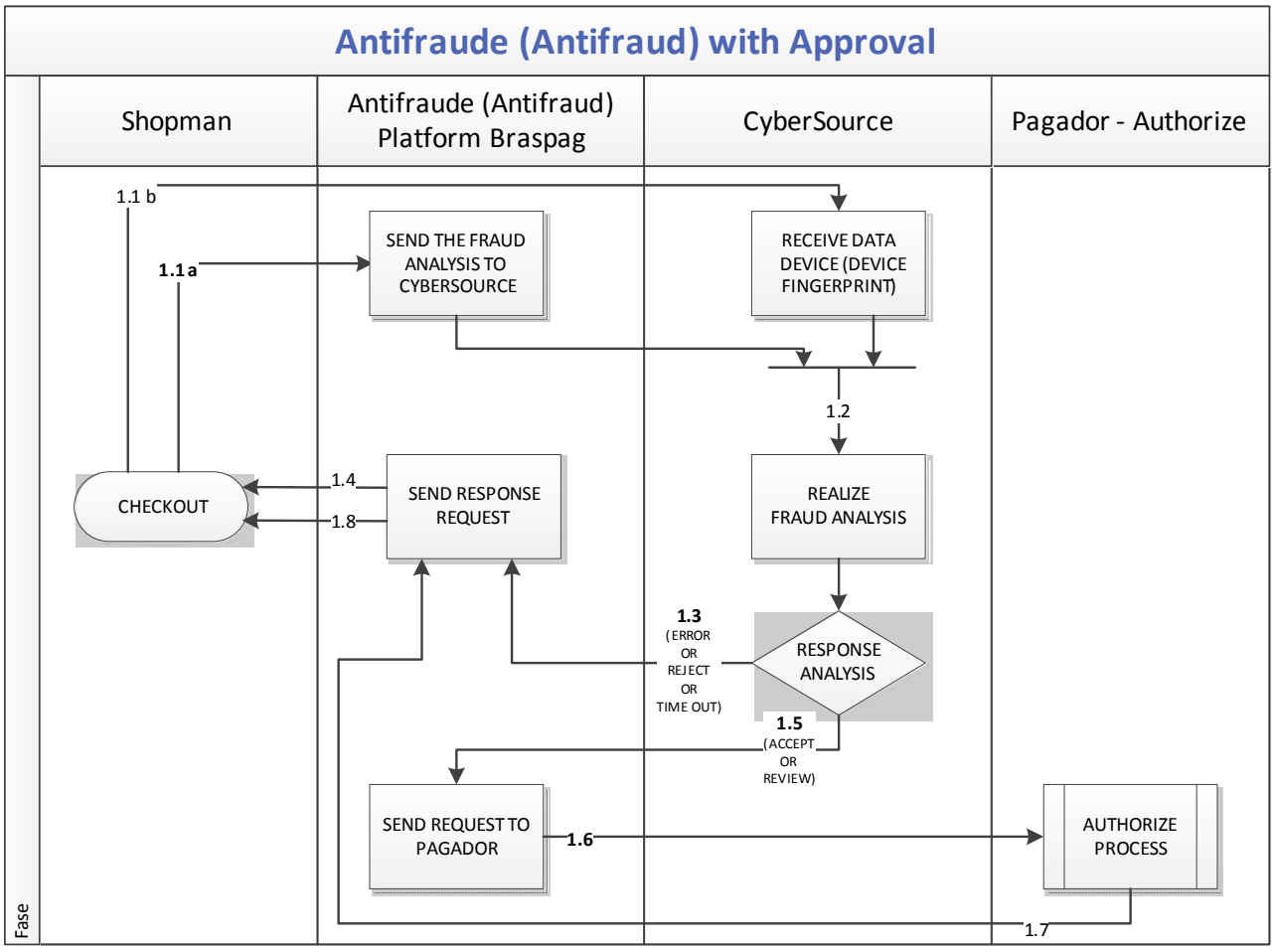
Submission of transaction for Fraud Analysis as indicated in the chart below.



1.1 a) Submission of requisition for sale with data analysis Fraud
1.1 b) Execution Script DeviceFingerPrint- is sent directly to Cybersource
1.2) Receipt of information from the device and data processing for Sale Fraud Analysis
1.3) Submission of Response Analysis of Fraud
1.4) Submission of Response Analysis of Fraud

1.2. Antifraude (Antifraud) with Approval

Submission of transaction for Antifraude (Antifraud) Analysis; if it returns "Approved" or "Review", the transaction will be sent for the Purchaser's approval via Pagador's Authorize service.



1.1 a) Submission of requisition for sale with data analysis Fraud Authorization.
1.1 b) Execution Script DeviceFingerPrint- is sent directly to Cybersource
1.2) Receipt of information from the device and data processing for Sale Fraud Analysis.
1.3) Submission of Response Analysis for CyberSource Fraud Fraud Office.
1.4) Submission of Response Analysis fraud.
1.5) Submission of Response Analysis for CyberSource Fraud Fraud Office.
1.6) Request authorization sent to the Payer.
1.7) Response of authorization sent to Fraud
1.8) Response Request sent

1.3. Approval with Antifraude (Antifraud)

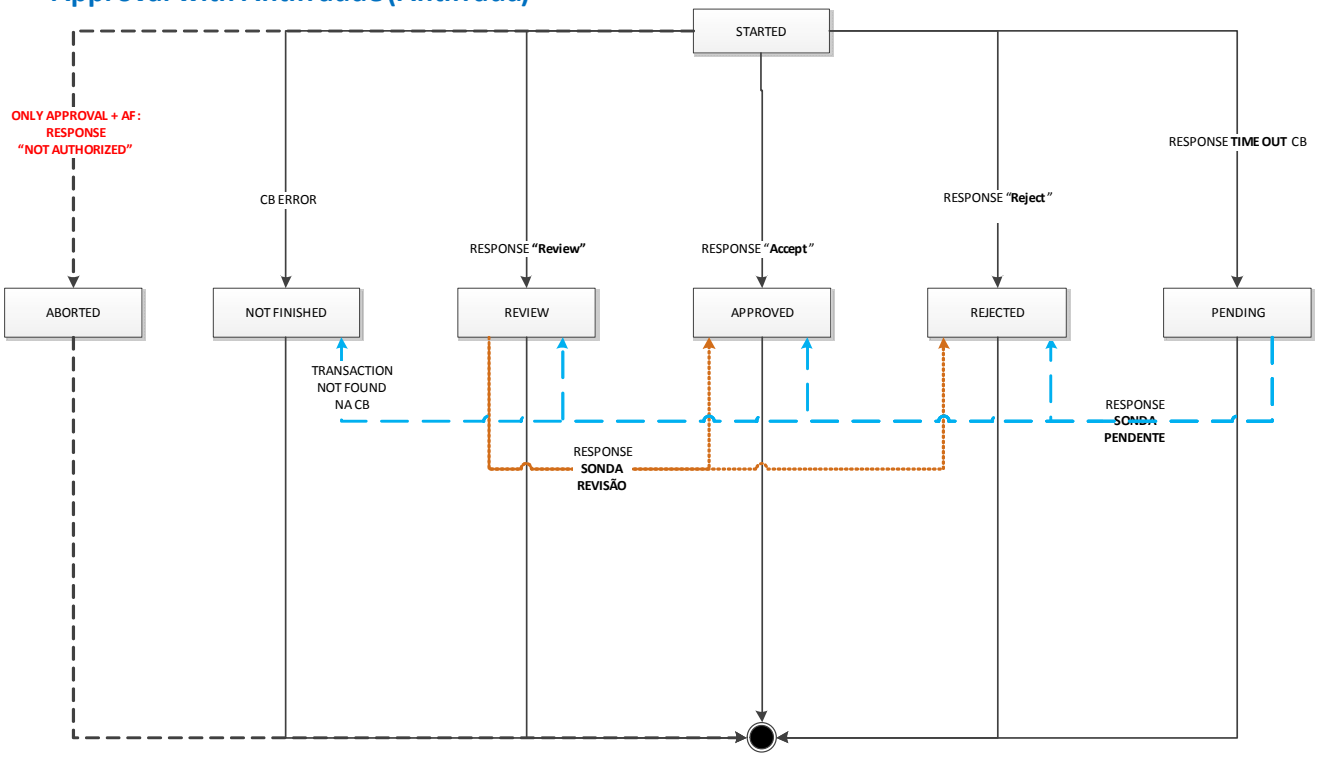
Submission of transaction for the Pagador; if approved, the transaction is sent for Fraud Analysis. Otherwise, the transaction status is stored in the database as "Aborted" and no Fraud Analysis is held, provided the customer does not indicate he wants Fraud Analysis to be held regardless of the Authorizer's result.

2. FRAUD ANALYSIS STATUS

Below are all possible status that transactions sent to Fraud Analysis might assume:

- **Initiated** – Initial status for transactions under fraud analysis;
- **Approved** - Transaction approved by Antifraude (Antifraud);
- **Review** – Transaction that will be manually reviewed, and then updated to "Approved" or "Rejected";
- **Rejected** – Transactions interpreted as fraud;
- **Pendent** – Attempt to send the transaction for CyberSource with TIME OUT return. The probe or the client can update the status for: Approved, Review, Rejected, or Not Completed;
- **Not Completed** – Attempt to send the transaction for CyberSource with an error response other than TIME OUT;
- **Aborted** – Indicates that the request for the Approval of Pagador (before Fraud Analysis) returned "Not Approved", preventing the transaction to be sent to Fraud Analysis.

State Transition Diagram:
Antifraude (Antifraud), Antifraude (Antifraud) with Approval, Approval with Antifraude (Antifraud)



3. INTEGRATION VIA WEB SERVICE

3.1. FraudAnalysis Method

Allow for the submission of a standalone Fraud Analysis transaction, or a Fraud Analysis transaction along with the Approval of Pagador, as indicated in the charts of Item 1.

Table 1 – FraudAnalysisRequest object properties

Parameter	Type	Size	Description	Required?
RequestId	Guid		Request ID.	Yes
Version	String		Version of the Webservice contract 1.0 or 1.1; **Note:** If the value for this parameter is not provided, the default version will be 1.0	No
MerchantId	Guid		Braspag Merchant ID.	Yes
AntiFraudSequenceType	Enum		Desired sequence type for Antifraud Analysis. Please see table 5.1	Yes
DocumentData	Class		Object containing purchaser info.	No
DocumentData.Cpf	String	11	Purchaser's CPF (Taxpayer ID).	No
DocumentData.Cnpj	String	14	Purchaser's CNPJ (Legal Entity ID).	No
DocumentData.OtherDocument	String	0 - 20	Identification for the purchaser.	No
AntiFraudRequest	Class		Object containing all required data to hold the Fraud Analysis.	Yes
AntiFraudRequest.BankInfoData	Class		Object containing purchaser's bank details. Fill ONLY to analyze direct-debit transactions.	No
AntiFraudRequest.BankInfoData.Address	String	0 - 255	Address of purchaser's bank branch.	No
AntiFraudRequest.BankInfoData.Code	String	0 - 15	Bank Code.	No
AntiFraudRequest.BankInfoData.BranchCode	String	0 - 15	Branch Code used for international wires transfers.	No
AntiFraudRequest.BankInfoData.City	String	0 - 35	Branch location city.	No
AntiFraudRequest.BankInfoData.Country	String	2	Branch location country.	No
AntiFraudRequest.BankInfoData.Name	String	0 - 40	Bank Name.	No
AntiFraudRequest.BankInfoData.SwiftCode	String	0 - 30	Bank SWIFT (Society for Worldwide Interbank Financial Telecommunication) code.	No
AntiFraudRequest.BillToData	Class		Object with Purchaser's billing information.	Yes
AntiFraudRequest.BillToData.City	String	1 - 50	Purchaser's billing address city.	Yes
AntiFraudRequest.BillToData.Country	String	2	Purchaser's billing address country.	Yes
AntiFraudRequest.BillToData.CustomerId	String	0 - 50	Merchant Purchaser ID.	No
AntiFraudRequest.BillToData.DateOfBirth	DateTime		Purchaser's date of birth.	No
AntiFraudRequest.BillToData.Email	String	1 - 100	Purchaser's email.	Yes
AntiFraudRequest.BillToData.HostName	String	0 - 60	Host Name of the page the purchaser was before accessing the Merchant's site.	No

AntiFraudRequest.BillToData.HttpBrowserCookiesAccepted	Bool		True = Client browser accepts cookies. False = Client browser does not accept cookies.	No
AntiFraudRequest.BillToData.HttpBrowserEmail	String	0 - 100	Email registered on purchaser's browser. May differ from the registered email.	No
AntiFraudRequest.BillToData.HttpBrowserType	String	0 - 40	Purchaser's browser name.	No
AntiFraudRequest.BillToData.IpAddress	String	0 - 15	Purchaser's IP Address. e.g.: 10.1.27.15 We highly recommend the sending of this field.	No
AntiFraudRequest.BillToData.FirstName	String	1 - 60	Purchaser's first name (Name on credit card).	Sim
AntiFraudRequest.BillToData.LastName	String	1 - 60	Purchaser's last name (Name on credit card).	Yes
AntiFraudRequest.BillToData.PhoneNumber	String	0 - 15	Purchaser's phone number.	No
AntiFraudRequest.BillToData.PostalCode	String	0 - 10	Purchaser's ZIP Code or P.O. Box.	No
AntiFraudRequest.BillToData.State	String	2	Purchaser's billing address State code.	Yes
AntiFraudRequest.BillToData.Street1	String	1 - 60	Purchaser's billing address.	Yes
AntiFraudRequest.BillToData.Street2	String	0 - 60	Purchaser's billing address.	No
AntiFraudRequest.BusinessRulesScoreThreshold	Int		Acceptable risk threshold for ordering each product.	No
AntiFraudRequest.CardData	Class		Object containing credit card info.	No
AntiFraudRequest.CardData.AccountNumber	String	0 - 20	Number of the credit card used in the purchase. Note: when this field is submitted, it is mandatory to send the fields AntiFraudRequest.CardData.ExpirationMonth and AntiFraudRequest.CardData.ExpirationYear with valid values.	No
AntiFraudRequest.CardData.Card	Enum		Credit card operator. Please see table 5.2	No
AntiFraudRequest.CardData.ExpirationMonth	String	2	Credit card expiration month, MM format.	No
AntiFraudRequest.CardData.ExpirationYear	String	4	Credit card expiration year, YYYY format.	No
AntiFraudRequest.CardData.AccountToken	Guid		Identifier of the credit card (CreditCardToken) saved in **"Cartão Protegido"**. This field may be sent instead of the fields **CardData.Account, CardData.ExpirationMonth** and **CardData.ExpirationYear.** The system uses the AccountToken to find and fill this fields. **Note**: The field **CardData.Card** not be filled automatically and must be sent as well.	No
AntiFraudRequest.CardData.AccountAlias	String		Identifier of the credit card (CreditCardAlias) saved in **"Cartão Protegido"**. This field may be sent instead of the fields **CardData.Account, CardData.ExpirationMonth** and **CardData.ExpirationYear**. The system uses the **AccountAlias** to find and fill this fields. **Note**:The field CardData.Card not be filled automatically and must be sent as well.	No

AntiFraudRequest.CardData.SaveAccountNumber	String		Indicates whether to save the data of the credit card to use the product **"Cartão Protegido"**. The action will not take place if the store does not have the product **"Cartão Protegido"** hired. The "**CreditCardToken**" generated on platforms **"Cartão Protegido"** associated with the data card sent will return in the field AntifraudRespose.AccountToken	No
AntiFraudRequest.Comments	String	0 - 255	Comment the merchant can associate with this analysis.	No
AntiFraudRequest.DecisionManagerData	Class		Object where you can define analysis rules. Use this class to analyze specific orders rather than all submitted orders.	No
AntiFraudRequest.DecisionManagerData.TravelData	Class		Object containing travel info for the purchase of tickets and/or travel packages.	No
AntiFraudRequest.DecisionManagerData.TravelData.CompleteRoute	String	0 - 255	Travel route. Concatenation of individual travel sections under the format ORIG1-DEST1, such as: SFO-JFK: JFK-LHR: LHR-CDG.	No
AntiFraudRequest.DecisionManagerData.TravelData.DepartureTime	DateTime		Travel departure date, hour and minute.	No
AntiFraudRequest.DecisionManagerData.TravelData.JourneyType	String	0 - 32	Type of journey. e.g.: One-way trip, round trip, etc.	No
AntiFraudRequest.DecisionManagerData.TravelData.TravelLegData [TravelLegDataCollection]	List	0 - n	Collection of origin and destination data of Purchaser travels.	No
AntiFraudRequest.DecisionManagerData.TravelData.TravelLegData.Origin	String	0 - 3	Airport Code of the origin point of the trip.	No
AntiFraudRequest.DecisionManagerData.TravelData.TravelLegData.Destination	String	0 - 3	Order Number. It is recommended that is the same order number.	No
AntiFraudRequest.FundTransferData	Class		Object used to analyze international wire transfer.	No
AntiFraudRequest.FundTransferData.AccountName	String	0 - 30	Bank account name. You should use this field only when booking debit transactions.	No
AntiFraudRequest.FundTransferData.AccountNumber	String	0 - 30	Bank account number.	No
AntiFraudRequest.FundTransferData.BankCheckDigit	String	0 - 2	Code used to validate the bank account.	No
AntiFraudRequest.FundTransferData.Iban	String	0 - 2	Bank account international number.	No
AntiFraudRequest.InvoiceHeaderData	Class		Object you can use to specify whether the purchaser requested gift wrap.	No
AntiFraudRequest.InvoiceHeaderData.IsGift	Boolean		Flag indicating whether or not the order is a gift.	No
AntiFraudRequest.InvoiceHeaderData.MerchantDescriptor	String	0 - 22	Merchant description shown in the cardholder's statement.	No
AntiFraudRequest.InvoiceHeaderData.ReturnsAccepted	Boolean		True = Returns are allowed for this order. False = Returns are not allowed for this order.	No
AntiFraudRequest.InvoiceHeaderData.Tender	Enum		Payment method used for the order. Please see table 5.3	No
AntiFraudRequest.ItemData [ItemDataCollection]	List	1 - n	List of items purchased with you data.	Yes
AntiFraudRequest.ItemData.GiftCategory	Enum		Flag to evaluate the billing and delivery addresses for different cities, states and countries. Please see table 5.9	No
AntiFraudRequest.ItemData.HostHedge	Enum		Significance level of email and IP address of customers at scoring risk. Please see table 5.10	No
AntiFraudRequest.ItemData.NonSensicalHedge	Enum		Level of tests performed on data of purchaser with nonsensical order. Please see table 5.11	No

AntiFraudRequest.ItemData.ObscenitiesHedge	Enum		Obscenity level of received orders. Please see table 5.7	No
AntiFraudRequest.ItemData.PassengerData.FirstName	String	0 - 60	Passenger's first name.	No
AntiFraudRequest.ItemData.PassengerData.LastName	String	0 - 60	Passenger's last name.	No
AntiFraudRequest.ItemData.PassengerData.PassengerId	String	0 - 32	Id of the passenger to whom the ticket was issued.	No
AntiFraudRequest.ItemData.PassengerData.Status	String	0 - 32	Airline company classification. You can use values such as Gold or Platinum.	No
AntiFraudRequest.ItemData.PassengerData.Passenger	Enum		Passenger classification. Please see table 5.13	No
AntiFraudRequest.ItemData.PassengerData.Email	String	0 - 255	Passenger's email.	No
AntiFraudRequest.ItemData.PassengerData.Phone	String	0 - 15	Passenger's phone number. For non-U.S. orders, CyberSource recommends to include the country code.	No
AntiFraudRequest.ItemData.PhoneHedge	Enum		Level of tests performed with the phone numbers. Please see table 5.9	No
AntiFraudRequest.ItemData.ProductData.Code	Enum		Product type. Please see table 5.10	No
AntiFraudRequest.ItemData.ProductData.Name	String	0 - 255	Product name.	No
AntiFraudRequest.ItemData.ProductData.Risk	Enum		Product risk level. Please see table 5.11	No
AntiFraudRequest.ItemData.ProductData.Sku	String	0 - 255	Product identifier merchant code.	No
AntiFraudRequest.ItemData.ProductData.Quantity	Int		Amount of product to be purchased.	No
AntiFraudRequest.ItemData.ProductData.UnitPrice	Decimal		Product unit price.	Yes
AntiFraudRequest.ItemData.TimeHedge	Enum		Customer's order placement period significance level. Please see table 5.12	No
AntiFraudRequest.ItemData.VelocityHedge	Enum		Customer's purchase frequency significance level. Please see table 5.13	No
AntiFraudRequest.AdditionalData [AdditionalDataCollection]	List	1 – n	Object with additional information to be sent. Information will be provided in Annex **Antifraude_MerchantDefinedData.pdf** and will range according to each store. This information while not mandatory, are of extreme importance for the Fraud Analysis. **Note:** Only supported by version 1.1	No
AdditionalData.Id	String		Identification of the field position **Note:** Only supported by version 1.1	Yes
AdditionalData.Value	String	0 - 255	Field Value **Note:** Only supported by version 1.1	Yes
AntiFraudRequest.MerchantReferenceCode	String	1 - 50	We recommend that this is the same number of the request sent to Pagador, if the transaction is performed by Braspag, for easier tracking	Yes
AntiFraudRequest.DeviceFingerprintID	String	1 - 50	Identifier used to to cross informations obtained by the browser of the internet user, with the data sent for analysis. This same value must be sent in the SESSIONID variable of the DeviceFingerPrint script.	No
AntiFraudRequest.PurchaseTotalsData	Class		Object with info about purchase total payment.	No
AntiFraudRequest.PurchaseTotalsData.Currency	String	0 - 3	Order currency code.	No
AntiFraudRequest.PurchaseTotalsData.GrandTotalAmount	Decimal		Order total amount.	No

AntiFraudRequest.ShipToData	Class		Object containing order delivery data.	No
AntiFraudRequest.ShipToData.City	String	0 - 50	Product delivery address city.	No
AntiFraudRequest.ShipToData.Country	String	0 - 2	Product delivery address Country code.	No
AntiFraudRequest.ShipToData.FirstName	String	0 - 60	First name of the person responsible for receiving the product delivery.	No
AntiFraudRequest.ShipToData.LastName	String	0 - 60	Last name of the person responsible for receiving the product delivery.	No
AntiFraudRequest.ShipToData.PhoneNumber	String	0 - 15	Product delivery address phone.	No
AntiFraudRequest.ShipToData.PostalCode	String	0 - 10	Product delivery address ZIP code or mailing info.	No
AntiFraudRequest.ShipToData.ShippingMethod	Enum		Product delivery service type. Please see table 5.14	No
AntiFraudRequest.ShipToData.State	String	0 - 2	Product delivery address State code.	No
AntiFraudRequest.ShipToData.Street1	String	0 - 60	Product delivery address first line.	No
AntiFraudRequest.ShipToData.Street2	String	0 - 60	Continued product delivery address.	No
AuthorizeCreditCardTransactionRequest	Class		Object that should be filled if the merchant desires to approve transactions along with the analysis process. **It is the same request as the Pagador's new contract.**	It depends on the desired sequence.

3.2. FraudAnalysis Method Return

In addition to returning all order-related data, the **FraudAnalysisResponse** will return the Fraud Analysis results.

Table 2 – FraudAnalysisResponse object properties

Parameter	Type	Size	Description
CorrelatedId	Guid		ID passed by the request only for identification.
Success	Boolean		Flag indicating whether the operation completed successfully. Do NOT indicate error.
ErrorReport [ErrorReportCollection]	List	0 - n	List of errors occurred while processing. Please see ErrorTypes sheet.
ErrorReport.ErrorCode	Short		Error code.
ErrorReport.Message	String		Error message.
AntiFraudTransactionId	Guid		Antifraud transaction ID used for later queries through the method to view analysis details.
TransactionStatusCode	Int		Braspag transaction status code. Please see table 5.30
TransactionStatusDescription	String	0 - 32	Braspag transaction status description. Please see table 5.30
AntiFraudResponse.AfsReplyData	**Class**		**Object with Fraud Analysis data.**
AntiFraudResponse.AfsReplyData.AddressInfoCode	String	0 - 255	Combination of codes that indicate error in the billing/delivery address. Codes are concatenated using the ^ character. e.g.: B^Y. Please see table 5.21
AntiFraudResponse.AfsReplyData.AfsFactorCode	String	0 - 100	Combination of codes that indicate the order score. Codes are concatenated using the ^ character. e.g.: B^Y. Please see table 5.22
AntiFraudResponse.AfsReplyData.AfsResult	Int		Order estimated total score.
AntiFraudResponse.AfsReplyData.BinCountry	String	0 - 2	Purchase origin country code.
AntiFraudResponse.AfsReplyData.CardAccount	Enum		Type of purchaser. Please see table 5.15
AntiFraudResponse.AfsReplyData.CardIssuer	String	0 - 128	Name of bank or card issuer entity.
AntiFraudResponse.AfsReplyData.CardScheme	Enum		Available operators. Please see table 5.16
AntiFraudResponse.AfsReplyData.ConsumerLocalTime	String	0 - 8	Purchaser's local time determined based on request date and billing address.
AntiFraudResponse.AfsReplyData.HostSeverity	Int		Purchaser's email domain risk level from 0 to 5, where 0 means indeterminate risk and 5 means the highest risk.
AntiFraudResponse.AfsReplyData.HostListInfoCode	String	0 - 255	Code sequence that indicates the purchaser's info is associated to transactions listed in the positive or negative list. Codes are concatenated using the ^ character. Please see table 5.25
AntiFraudResponse.AfsReplyData.IdentityInfoCode	String	0 - 255	Code sequence that indicates excessive change in purchaser identity. Codes are concatenated using the ^ character. Please see table 5.23
AntiFraudResponse.AfsReplyData.InternetInfoCode	String	0 - 255	Code sequence that indicates a problem in the email, IP or billing address. Codes are concatenated using the ^ character. Please see table 5.24

AntiFraudResponse.AfsReplyData.IpCity	String	0 - 50	Purchaser's city name obtained from IP address.
AntiFraudResponse.AfsReplyData.IpCountry	String	0 - 2	Purchaser's country code obtained from IP address.
AntiFraudResponse.AfsReplyData.IpRoutingMethod	Enum		IP routing model used by purchaser. Please see table 5.17
AntiFraudResponse.AfsReplyData.IpState	String	0 - 255	Purchaser's state name obtained from IP address.
AntiFraudResponse.AfsReplyData.PhoneInfoCode	String	0 - 255	Code sequence that indicates error in the purchaser's phone. Codes are concatenated using the ^ character. Please see table 5.26
AntiFraudResponse.AfsReplyData.ReasonCode	Int		Analysis result. Please see table 5.20
AntiFraudResponse.AfsReplyData.ScoreModelUsed	String	0 - 20	Name of the score model used.
AntiFraudResponse.AfsReplyData.SuspiciousInfoCode	String	0 - 255	Code sequence that indicates the purchaser has informed suspicious data. Codes are concatenated using the ^ character. Please see table 5.27
AntiFraudResponse.AfsReplyData.VelocityInfoCode	String	0 - 255	Code sequence that indicates the purchaser has a high purchase frequency. Codes are concatenated using the ^ character. Please see table 5.28
AntiFraudResponse.Decision	String	0 - 20	Decision made by the Antifraud tool. Please see table 5.18
AntiFraudResponse.DecisionReplyData	**Class**		**Object containing the data from the decision made by the Antifraud tool**
AntiFraudResponse.DecisionReplyData.ActiveProfileReplyData	**Class**		**Object with the data of the active profile analysis.**
AntiFraudResponse.DecisionReplyData.ActiveProfileReplyData.SelectedBy	String	0 - 50	Name of the rule of the profile selected to perform the analysis. Available only with verbose mode enabled.
AntiFraudResponse.DecisionReplyData.ActiveProfileReplyData.Name	String	0 - 30	Name of the profile selected to perform the analysis. Available only with verbose mode enabled.
AntiFraudResponse.DecisionReplyData.ActiveProfileReplyData.DestinationQueue	String	0 - 30	Name of queue for which the orders not accepted are immediately sent. Available only with verbose mode enabled.
AntiFraudResponse.DecisionReplyData.ActiveProfileReplyData.RulesTriggeredData	Class		Object with rule triggers data for Fraud Analysis.
AntiFraudResponse.DecisionReplyData.ActiveProfileReplyData.RulesTriggeredData.RuleResultItemData [RuleResultItemCollection]	List		Rules used during the analysis. Available only with verbose mode enabled.
AntiFraudResponse.DecisionReplyData.ActiveProfileReplyData.RulesTriggeredData.RuleResultItemData.RuleNumber	Int		Rule ID.
AntiFraudResponse.DecisionReplyData.ActiveProfileReplyData.RulesTriggeredData.RuleResultItemData.Decision	String	0 - 20	Decision made for the rule by the Antifraud tool Please see table 5.18
AntiFraudResponse.DecisionReplyData.ActiveProfileReplyData.RulesTriggeredData.RuleResultItemData.Evaluation	Enum		Rule evaluation. Please see table 5.19
AntiFraudResponse.DecisionReplyData.ActiveProfileReplyData.RulesTriggeredData.RuleResultItemData.Name	String	0 - 50	Rule name.
AntiFraudResponse.DecisionReplyData.CasePriority	Int		If the merchant is an Enhanced Case Management subscriber, he gets this number with the priority level, where 1 means the highest and 5 means the lowest priority.
AntiFraudResponse.DecisionReplyData.VelocityInfoCode	String	0 - 25	List of codes triggered by the order. This information was generated by the request and will be returned so that it can be related to the response.

AntiFraudResponse.InvalidFieldCollection	List<string>		List of fields that presented invalid data.
AntiFraudResponse.MerchantReferenceCode	String	0 - 50	Reference/tracking code generated by the merchant.
AntiFraudResponse.MissingFieldCollection	List<string>		List of mandatory fields that were not submitted.
AntiFraudResponse.ReasonCode	Int		Analysis overall result generated by the Antifraud tool. Please see table 5.20
AntiFraudResponse.RequestId	String	0 - 26	Request ID.
AntiFraudResponse.RequestToken	String	0 - 256	Request ID generated by the Antifraud tool

3.3. UpdateStatus Method

Method for changing transactions for review ACCEPT or REJECT. The answer of this method will always be *Success* or *Fail*, *Fail* which means that the transaction can not be processed, and Success means that it is processing. For the result of processing the customer need to probe the Braspag after a configurable period which should be consulted in real deployment and operations.

Parameter	Type	Size	Description	Required?
RequestId	Guid		Id request's request.	Yes
MerchantId	Guid		Id Store in the antifraud to be used for the query.	Yes
AntiFraudTransactionId	Guid		Id antifraud transaction to be located.	Yes
NewStatus	string		New status that the transaction should receive. May only contain ACCEPT or REJECT	Yes
Comment	string		Comment associated with the change in status.	No

Xml Request Example:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ant="http://www.braspag.com.br/antifraud/">
  <soapenv:Header/>
  <soapenv:Body>
    <UpdateStatus>
      <updateStatusRequest>
        <RequestId>00000000-0000-0000-0000-000000000000</RequestId>
        <AccessKey>00000000-0000-0000-0000-000000000000</AccessKey>
        <Version>1</Version>
        <MerchantId>00000000-0000-0000-0000-000000000000</MerchantId>
        <AntiFraudTransactionId>00000000-0000-0000-0000-000000000000</AntiFraudTransactionId>
        <NewStatus>REJECT</NewStatus>
        <Comment> Comprador não localizado nos telefones cadastrados</Comment>
      </updateStatusRequest>
    </UpdateStatus>
  </soapenv:Body>
</soapenv:Envelope>
```

3.4. UpdateStatus Method Return

Parameter	Type	Size	Description
AntiFraudTransactionId	Guid		Represents the ID of the transaction of fraud analysis that was sent in the request.
RequestStatusCode	String		I Indicates whether the transaction was successfully received for processing by the Analysis Fraud Tool. See Table 5:30.
RequestStatusDescription	String		Contains a description of RequestStatusCode. See Table 5:30.
CorrelatedId	Guid		Id that was passed by request only for identification.
Success	String		Flag that indicates whether the operation completed successfully. DO NOT indicates error.
ErrorReportCollection	Array <string>		Collection of string that will contain the causes of "not processing" in case there is an error.

Xml Response Example:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <UpdateStatusResponse xmlns="http://www.braspag.com.br/antifraud/">
      <UpdateStatusResult>
        <CorrelatedId>00000000-0000-0000-0000-000000000000</CorrelatedId>
        <Success>true</Success>
        <ErrorReportCollection/>
        <AntiFraudTransactionId>00000000-0000-0000-0000-000000000000</AntiFraudTransactionId>
        <RequestStatusCode>1</RequestStatusCode>
        <RequestStatusDescription>Request process successfully</RequestStatusDescription>
      </UpdateStatusResult>
    </UpdateStatusResponse>
  </soap:Body>
</soap:Envelope>
```

4. QUERY

4.1. Notification of Changing Status

Service that sends a post notification to the customer if there is any change in status (only for transactions with OriginalDecision **REVIEW**).

- You must request the Implementation Team, the registration of the Return URL. When accessed by the BRASPAG server, sending the POST, the registered URL should display a code indicating that received the status change and has successfully processed **<Status> OK <Status>**
- If the changing status URL of the store is accessed by the server Braspag and do not display the confirmation code or a failure occurred in connection, the server will make 3 more delivery attempts.
- The URL change status only can use port 80 (default http) or port 443 (default https).

XML Example:

```
<CaseManagementOrderStatusToPostToClient
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <Notes />
  <AntiFraudTransactionId>ce7f50c5-f9cb-4c23-8abd-f70d895e6f74</AntiFraudTransactionId>
  <MerchantReferenceNumber>310720131026</MerchantReferenceNumber>
  <OriginalDecision>REVIEW</OriginalDecision>
  <NewDecision>REJECT</NewDecision>
  <Reviewer>John J. Jr</Reviewer>
  <ReviewerComments>REVIEW PARA REJECT</ReviewerComments>
  <Queue>Fila de Revisao</Queue>
  <Profile>Perfil Retail</Profile>
</CaseManagementOrderStatusToPostToClient>
```

4.2. FraudAnalysisTransactionDetails Method

This method should be used to obtain all the information analysis of fraud relating to a specific transaction.

The **FraudAnalysisTransactionDetails** method gets a **FraudAnalysisTransactionDetailsRequest** object with the following properties.

Table 3 - FraudAnalysisTransactionDetailsRequest object properties

Parameter	Type	Description	Required?
RequestId	Guid	Request ID.	Yes
MerchantId	Guid	Antifraud merchant ID to be used for the query.	Yes
AntiFraudTransactionId	Guid	ID of the Antifraud transaction to be found.	Yes

4.3. FraudAnalysisTransaction Method Return

The **FraudAnalysisTransaction** method will return a Response object with the properties bellow:

Table 4 – FraudAnalysisTransactionResponse object properties

Parameter	Type	Size	Description
CorrelatedId	Guid		ID passed by the request only for identification.
Success	Boolean		Flag indicating whether the operation completed successfully. Do NOT indicate error.
ErrorReport [ErrorReportCollection]	List	0 - n	List of errors occurred while processing. Please see ErrorTypes sheet.
ErrorReport.ErrorCode	Short		Error code.

ErrorReport.Message	String	MAX	Error message.
AntiFraudMerchantId	Guid		Antifraud merchant ID.
AntiFraudTransactionId	Guid		Antifraud transaction ID.
AntiFraudTransactionStatusCode	Byte		Fraud Analysis status ID. Please see table 5.29
AntiFraudReceiveDate	DateTime		Date Braspag received the transaction.
AntiFraudStatusLastUpdateDate	DateTime		Date the transaction status was last updated.
AntiFraudAnalysisScore	Int		Fraud analysis score.
BraspagTransactionId	Guid		Pagador (Braspag) transaction ID. This field is filled only when the type of sequence selected is other than Only Fraud Analysis.
MerchantOrderId	String	1 - 50	Merchant order number.
FraudAnalysisRequestParameter [FraudAnalysisRequestParameterCollection]	List		List of parameters submitted in the request.
FraudAnalysisRequestParameter.FieldName	String	1 - 256	Name of the field submitted in the request.
FraudAnalysisRequestParameter.FieldValue	String	MAX	Value of the field submitted in the request.
FraudAnalysisResponseParameter [FraudAnalysisResponseParameterCollection]	List		List of parameters returned by the Fraud Analysis.
FraudAnalysisResponseParameter.FieldName	String	1 - 256	Field name returned by the Fraud Analysis.
FraudAnalysisResponseParameter.FieldValue	String	MAX	Field value returned by the Fraud Analysis.
AntiFraudAcquirerConversionDate	Datetime		The date of change of the transaction status when it was analyzed manually and had its status changed in Cybersource or was altered by notifying the Cybersource Braspag through POST.
AntiFraudTransactionOriginalStatusCode	Byte		Original status of the transaction after the manual analysis of the transaction in Cybersource. This field is returned in this method when the transaction was notified on or probed Braspag through POST sent by Cybersource for Braspag.

5. DOMAIN TABLES

Table 5.1 - AntiFraudServiceType

Value	Description
AnalyseOnly	Performs only Fraud Analysis.
AnalyseAndAuthorizeOnSuccess	The approval request shall be carried out only if the fraud analysis succeeds.
AuthorizeAndAnalyseOnSuccess	Attempts to authorize the transaction and, if successful, runs the Fraud Analysis.
AuthorizeAndAnalyseAlways	Attempts to authorize the transaction and, regardless of the result, runs the Fraud Analysis.

Table 5.2 - Card

Value	Description
Visa	Visa card.
Mastercard	Mastercard card.
AmericanExpress	American Express card.
DInersClub	Diners Club card.
VisaElectron	Visa Electron card.

Table 5.3 - Tender

Value	Description
Consumer	Personal credit card.
Corporate	Corporate credit card.
Debit	Debit purchase.
Cod	Billing in product delivery.
Check	Electronic check.
P2P	Person-to-person payment.
Private1	Private label credit card.
Other	Other payment methods.

Table 5.4 - GiftCategory

Value	Description
Yes	In case of conflict between billing and delivery addresses, mark as low risk.
No	In case of conflict between billing and delivery addresses, mark as high risk.
Off	Ignores risk assessment for conflicting addresses.

Table 5.5 - HostHedge

Value	Description
Low	Low significance of email and IP address in risk assessment.
Normal	Medium significance of email and IP address in risk assessment.
High	High significance of email and IP address in risk assessment.
Off	Email and IP address do not impact risk assessment.

Table 5.6 - NonSensicalHedge

Value	Description
Low	Low significance of the purchaser's order verification in risk assessment.
Normal	Medium significance of the purchaser's order verification in risk assessment.
High	High significance of the purchaser's order verification in risk assessment.
Off	Purchaser's order verification does not affect risk assessment.

Table 5.7 - ObscenitiesHedge

Value	Description
Low	Low significance of the purchaser's order obscenities verification in risk assessment.
Normal	Medium significance of the purchaser's order obscenities verification in risk assessment.
High	High significance of the purchaser's order obscenities verification in risk assessment.
Off	Purchaser's order obscenities verification does not affect risk assessment.

Table 5.8 - Passenger

Value	Description
Adult	Adult passenger.
Child	Child passenger.
Infant	Infant passenger.
Youth	Youth passenger.
Student	Student passenger.
SeniorCitizen	Elderly passenger.
Military	Military passenger.

Table 5.9 - PhoneHedge

Value	Description
Low	Low significance of tests performed with the phone numbers.
Normal	Medium significance of tests performed with the phone numbers.
High	High significance of tests performed with the phone numbers.
Off	Tests with phone numbers do not affect risk assessment.

Table 5.10 - Code

Value	Description
AdultContent	Adult content.
Coupon	Discount coupon.
Default	Default option for CyberSource analysis when no other value is selected.
EletronicGood	Electronic product.
EletronicSoftware	Software distributed electronically via download.
GiftCertificate	Gift voucher.
HandlingOnly	Installation or handling fee.
Service	Service.
ShippingAndHandling	Installation/handling fee and freight.
ShippingOnly	Freight.
Subscription	Subscription.

Table 5.11 - Risk

Value	Description
Low	Product has a short history of chargeback.
Normal	Product has a history of chargeback considered as normal.
High	Product has a history of chargeback above average.

Table 5.12 - TimeHedge

Value	Description
Low	Low significance for the period of day the purchased was placed for risk assessment.
Normal	Medium significance for the period of day the purchased was placed for risk assessment.
High	High significance for the period of day the purchased was placed for risk assessment.
Off	The purchase time does not affect risk assessment.

Table 5.13 - VelocityHedge

Value	Description
Low	Low significance for the number of purchases carried by the client in the last 15 minutes.
Normal	Medium significance for the number of purchases carried by the client in the last 15 minutes.
High	High significance for the number of purchases carried by the client in the last 15 minutes.
Off	The customer's purchase frequency does not affect Fraud Analysis.

Table 5.14 - Shipping Method

Value	Description
SameDay	Service of delivery on the same day.
OneDay	Service of delivery overnight or on the next day.
TwoDay	Service of delivery in two days.
ThreeDay	Service of delivery in three days.
LowCost	Low-cost delivery service.
Pickup	Product withdrawn from store.
Other	Other delivery method.
None	No delivery service, since it is a subscription or service.

Table 5.15 - Customer Type

Value	Description
CN	Particular Purchaser
CP	Business Purchaser

Table 5.16- Type Flag

Value	Description
MaestroInternational	Maestro International
MaestroUkDomestic	Maestro UK Domestic
MastercardCredit	MasterCard Credit
MastercardDebit	MasterCard Debit
VisaCredit	Visa Credit
VisaDebit	Visa Debit
VisaElectron	Visa Electron

Table 5.17 - Type Routing

Value	Description
Anonymizer	Anonymizer
AolBased	AOL, AOL dial-up, AOL POP, AOL proxy
CacheProxy	Cache proxy
Fixed	Fixed
InternationalProxy	International proxy
MobileGateway	Mobile gateway
Pop	POP
RegionalProxy	Regional proxy
Satellite	Satellite
SuperPop	SuperPOP

Table 5.18 - Type Decision

Value	Description
Accept	ACCEPT
Error	ERROR
Reject	REJECT
Review	REVIEW

Table 5.19 - Type of Evaluation of the Rule

Value	Description
TRUE	T
FALSE	F
InsufficientData	N
Error	E

Table 5.20 - Reason Codes

Value	Description
100	Successful operation.
101	Order is missing one or more required field(s). ible action: Please see the fields missing on list AntiFraudResponse.MissingFieldCollection. Please bmit order with all information.
102	One or more fields in the order are invalid. ible action: Please see invalid fields on list AntiFraudResponse.InvalidFieldCollection. Resubmit order correct information.
150	Overall system failure. ible action: Please wait a few minutes and try to resubmit order.
151	The order was received, but the server timed out. This error does not include time-out between client server. ible action: Please wait a few minutes and try to resubmit order.
152	The order was received, but timed out. ible action: Please wait a few minutes and try to resubmit order.
202	CyberSource refused order because card timed out. You can also get this code if the expiry date does match the date on the issuing bank file. If the payment processor allows issuance of credits to expired s, CyberSource does not limit this functionality. ible action: Please ask for a new card or another payment method.
231	Invalid account number. Possible action: Please ask for a new card or another payment method.
234	CyberSource merchant setup issue. Possible action: Do not submit order. Please contact the customer service to fix the setup issue.
400	Fraud score threshold exceeded. Possible action: Please review customer's order.
480	Order marked for review by the Decision Manager.
481	Order rejected by the Decision Manager.

Table 5.21 - Address Information Codes

Value	Description
COR-BA	Billing address can be normalized.
COR-SA	Delivery address can be normalized.
INTL-BA	Billing country is not the U.S.
INTL-SA	Delivery country is not the U.S.
MIL-USA	This is a military address in the U.S.
MM-A	Billing and delivery addresses have different street names.
MM-BIN	Card BIN (first six digits of the card number) do not match the country.
MM-C	Billing and delivery addresses have different cities.
MM-CO	Billing and delivery addresses have different countries.
MM-ST	Billing and delivery addresses have different states.
MM-Z	Billing and delivery addresses have different postcodes.
UNV-ADDR	Address cannot be verified.

Table 5.22 - Risk Factor Codes

Value	Description
A	Excessive address change. The customer changed his/her billing address two or more times over the last six months.
B	Card BIN or risk approval. The risk factors are related to credit card BIN and/or card approval verifications.
C	High figures of credit card. The customer used more than six credit card numbers in the last six months.
D	Email address impact. The customer uses a free email provider or the email address is suspicious.
E	Positive list. Customer is in your white list.
F	Black list. The account number, account address, email address or IP address for this purpose is in your black list.
G	Geolocalization inconsistency. The email client domain, phone number, billing address, ship address or IP address is suspicious.
H	Excessive name changes. The customer changed his/her name two or more times over the last six months.
I	Internet inconsistency. IP address and email domain not consistent with billing address.
N	Nonsensical input. Customer's name and address fields contain nonsensical words or language.
O	Obscenities. Customer's data contain obscene words.
P	Morphing identity. Several values of one identity element are linked to one value of an element of different identities. E.g., several phone numbers linked to a single account number.
Q	Phone inconsistency. Customer's phone number is suspicious.
R	Risky order. Transaction, customer and merchant present high-risk correlated information.
T	Time Coverage. The client is trying to purchase outside the expected time.
U	Address cannot be verified. Billing or delivery address cannot be verified.
V	Velocity. Account number used too much times in the last 15 minutes.
W	Marked as suspicious. Billing/delivery address é similar to an address previously marked as suspicious.
Y	The address, city, state, or country of the billing/delivery address does not match.
Z	Invalid value. Default value used, since the request had an unexpected value. Though the transaction can still be processed, please carefully check order for defects.

Table 5.23 - Excessive Identity Changes

Value	Description
MORPH-B	Same billing address used several times with multiple client identities.
MORPH-C	Same account number used several times with multiple client identities.
MORPH-E	Same email address used several times with multiple client identities.
MORPH-I	Same IP address used several times with multiple client identities.
MORPH-P	Same phone number used several times with multiple client identities.
MORPH-S	Same delivery address used several times with multiple client identities.

Table 5.24 - Internet Information Codes

Value	Description
FREE-EM	Customer's email address provided by free email provider.
INTL-IPCO	Customer's email address country is not the U.S.
INV-EM	Invalid customer's email address.
MM-EMBCO	Customer's email address domain not consistent with billing address country.
MM-IPBC	Customer's email address not consistent with billing address city.
MM-IPBCO	Customer's email address not consistent with billing address country.
MM-IPBST	Customer's IP address not consistent with billing address state. However, this information code cannot be returned when the inconsistency is between immediately adjacent states.
MM-IPEM	Customer's email address not consistent with IP address.
RISK-EM	Customer's email domain (e.g., mail.example.com) is associated with high risk.
UNV-NID	The customer's IP address is from an anonymous proxy. Those entities completely hide IP address info.
UNV-RISK	IP address from risky source.
UNV-EMBCO	The email client address country does not match the billing address country.

Table 5.25 - Customer Lists Information Codes

Value	Description
CON-POSNEG	Triggered order matches both with black and white lists. White list results overwrite black list results.
NEG-BA	Billing address found in black list.
NEG-BCO	Billing country found in black list.
NEG-BIN	Credit card BIN (first six digits of the card number) found in black list.
NEG-BINCO	Credit card issuing country found in black list.
NEG-BZC	Billing postcode found in black list.
NEG-CC	Credit card number found in black list.

NEG-EM	Email address found in black list.
NEG-EMCO	Email address country found in black list.
NEG-EMDOM	Email domain (e.g., mail.example.com) found in black list.
NEG-HIST	Transaction found in black list.
NEG-ID	Customer's account ID found in black list.
NEG-IP	IP address (e.g., 10.1.27.63) found in black list.
NEG-IP3	Network IP address (e.g., 10.1.27) found in black list. The network IP prefix may include up to 256 IP addresses.
NEG-IPCO	IP address country found in black list.
NEG-PEM	One passenger email address was found in black list.
NEG-PH	Phone number found in black list.
NEG-PID	Passenger's account ID found in black list.
NEG-PPH	Passenger's phone number found in black list.
NEG-SA	Delivery address found in black list.
NEG-SCO	Delivery country found in black list.
NEG-SZC	Delivery postcode found in black list.
POS-TEMP	Customer temporarily in white list.
POS-PERM	Customer permanently in white list.
REV-BA	Billing address found in review list.
REV-BCO	Billing country found in review list.
REV-BIN	Credit card BIN (first six digits of the card number) found in review list.
REV-BINCO	Credit card issuing country found in review list.
REV-BZC	Billing postcode found in review list.
REV-CC	Credit card number found in review list.
REV-EM	Email address found in review list.
REV-EMCO	Email address country found in review list.
REV-EMDOM	Email domain (e.g., mail.example.com) found in review list.
REV-ID	Customer's account ID found in review list.
REV-IP	IP address (e.g., 10.1.27.63) found in review list.
REV-IP3	Network IP address (e.g., 10.1.27) found in review list. The network IP prefix may include up to 256 IP addresses.
REV-IPCO	IP address country found in review list.
REV-PEM	One passenger email address was found in review list.

REV-PH	Phone number found in review list.
REV-PID	Passenger's account ID found in review list.
REV-PPH	Passenger's phone number found in review list.
REV-SA	Delivery address found in review list.
REV-SCO	Delivery country found in review list.
REV-SZC	Delivery postcode found in review list.

Table 5.26 - Phone Information Codes

Value	Description
MM-ACBST	Customer's phone number not consistent with billing address state.
RISK-AC	Customer's area code associated with high risk.
RISK-PH	U.S. or Canada phone number incomplete, or one or more parts of the number are risky.
TF-AC	Phone number uses toll-free area code.
UNV-AC	Invalid area code.
UNV-OC	Invalid area code and/or phone prefix.
UNV-PH	Invalid phone number.

Table 5.27 - Suspicious Data Information Codes

Value	Description
BAD-FP	Risky device.
INTL-BIN	Credit card issued outside the U.S.
MM-TZTLO	The device time zone do not match the country time zones.
MUL-EM	The customer has been using more than four different email addresses.
NON-BC	Unknown billing city.
NON-FN	Customer's first name not known.
NON-LN	Customer's last name not known.
OBS-BC	The billing city has obscenities.
OBS-EM	The email address has obscenities.
RISK-AVS	The AVS combined test result and the normalized billing address are risky, the AVS result indicates an exact match, but the billing address is not a normalized delivery.
RISK-BC	The billing city has duplicate characters.
RISK-BIN	In the past, the credit card BIN (first six digits of the card number) presented high fraud incidence.
RISK-DEV	Some of the device's features are risky.
RISK-FN	Customer's first and last name contain unlikely combinations of letters.

RISK-LN	Customer's middle or last name contain unlikely combinations of letters.
RISK-PIP	Risky proxy IP address.
RISK-SD	Inconsistencies between billing and delivery countries are risky.
RISK-TB	The order date and time associated with the billing address is risky.
RISK-TIP	The real IP address is risky.
RISK-TS	The order date and time associated with the delivery address is risky.

Table 5.28 - Global Velocity Information Codes

Value	Description
VEL-ADDR	Different billing and/or shipping states (USA and Canada only) have been used several times with the credit card number and/or email address.
VEL-CC	Different account numbers were used several times with the same name or email address.
VEL-NAME	Different names were used several times with the credit card number and/or email address.
VELS-CC	The account number has been used several times during the short control period.
VELI-CC	The account number has been used several times during the medium control period.
VELL-CC	The account number has been used several times during the long control period.
VELV-CC	The account number has been used several times during the very long control period.
VELS-EM	The email address has been used several times during the short control period.
VELI-EM	The email address has been used several times during the medium control period.
VELL-EM	The email address has been used several times during the long control period.
VELV-EM	The email address has been used several times during the very long control period.
VELS-IP	The IP address has been used several times during the short control period.
VELI-IP	The IP address has been used several times during the medium control period.
VELL-IP	The IP address has been used several times during the long control period.
VELV-IP	The IP address has been used several times during the very long control period.
VELS-SA	The delivery address has been used several times during the short control period.
VELI-SA	The delivery address has been used several times during the medium control period.
VELL-SA	The delivery address has been used several times during the long control period.
VELV-SA	The delivery address has been used several times during the very long control period.
VELS-TIP	The real IP address has been used several times during the short control period.
VELI-TIP	The real IP address has been used several times during the medium control period.
VELL-TIP	The real IP address has been used several times during the long control period.

Table 5.29 - AntiFraudStatusCode

Code	Description
500	Started
501	Accept
502	Review
503	Reject
504	Pendent
505	Unfinished
506	Aborted

Table 5.30 - RequestStatusCode

Value	Description
0	Started
1	Accept

Table 5.31 – RequestStatusDescription

Value	Description
Fail	Failure to receive the request for Antifraud Tool
Success	Request sent to the antifraud tool, and is being processed

6. ERROR MAP

Table 6.1 - Errors that can be raised by the web service consumed by the customer.

Code	Description
101	Invalid Request
102	Invalid Merchant
103	Undefined Fraud Analysis service credentials
104	Pagador Merchant Id is not registered
105	Access denied
106	Invalid sequence type
107	RequestId was not specified
108	OrderId cannot be null or empty
109	Your search returned no data
110	Your search returned no data.
111	Data Invalid Credit Card To Token Informed.
112	TransactionId not found for this Merchant.
113	This operation only can change status in review.

Table 6.2 - Errors that can be raised by Pagador and the Antifraud service consumed by Braspag.

Code	Description
301	Internal Error
302	Authorization denied

Table 6.3 - Common errors that can be raised at the validation of the properties of classes that comprise the request consumed by the costumer.

Code	Description
901	Parameter cannot be null or empty
902	Invalid parameter length. Valid length: <length>
903	Invalid parameter value. Valid value: <value>
904	Only numeric values are permitted
905	Parameter was not in correct format. Expected format: <format>
906	Only numeric values are permitted and/or invalid parameter length. Valid length: <length>
907	Invalid parameter

7. ANNEX 1 – ADDING FINGERPRINT

You need to add a 1-pixel image, which is not shown on the screen, and two segments of code to the tag <body> on your checkout page, making sure that it will take 3-5 seconds between the submission and execution of the code page to the server.

 If the three code segments are not placed at the checkout page, your results may not be accurate.

Putting the Code Segments

Put the code segments immediately above the tag </ body> to ensure that the Web page will render correctly. Never add the code segments in visible HTML elements.
The code segments must be loaded before the buyer finalize the purchase order, otherwise an error is generated.

Substituting variables

Copy the code snippets below.
In each segment, replace the variables with the following amounts related to your shop / order:

• **Domain**:

Testing - Use ***h.online-metrix.net***, which is the DNS server's fingerprint, as outlined in Example HTML below;

Production - Change the domain to a local URL, and configure your webserver to redirect this URL to ***h.online-metrix.net***.

- ***<org ID>*:** To get it, contact Braspag;
- ***<merchant ID>*:** To get it, contact Braspag;
- ***<session ID>*:** Use the same value passed in the parameter "***DeviceFingerprintID***" service request fraud analysis;

Be sure to copy all the data correctly and remove the signs of tag (<>) when replace the variables.

PNG image

```
<p style="background:url(https://h.online-metrix.net/fp/clear.png?org_id=<org
ID>&amp;session_id=<merchant id><session ID>&amp;m=1)"></p>
<img src="https://h.online-metrix.net/fp/clear.png?org_id=<org ID>&amp;session_
id=<merchant id><session ID>&amp;m=2" alt="">
```

Example:

```
<p style="background:url(https://h.online-metrix.net/fp/clear.png?org_id=sample_
orgID&amp;session_id=sample_merchantIDsample_sessionID&amp;m=1)"></p>
<img src="https://h.online-metrix.net/fp/clear.png?org_id=sample_orgID&amp;session_
id=sample_merchantIDsample_sessionID&amp;m=2" alt="">
```

Flash code

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

Example:
<object type="application/x-shockwave-flash" data="https://h.online-metrix.net/fp/
fp.swf?org_id=sample_orgID&session_id=sample_merchantIDsample_sessionID"
width="1" height="1" id="thm_fp">
<param name="movie" value="https://h.online-metrix.net/fp/fp.swf?org_id=sample_
orgID&session_id=sample_merchantIDsample_sessionID" />

</object>

JavaScript code

<script src="https://h.online-metrix.net/fp/check.js?org_id=***<org ID>***&session_
id=***<merchant id><session ID>***" type="text/javascript">
</script>

Example:
<script src="https://h.online-metrix.net/fp/check.js?org_id=sample_orgID&session_
id=sample_merchantIDsample_sessionID" type="text/javascript">
</script>

Setting Your Web Server

 If you do not complete this section, you will not get correct results, and the domain (url) of the supplier will be visible, it is more likely that your customer block it.

In the section "Replacing Variables" (Domain), all objects refer to h.online-metrix.net, the DNS server's fingerprint. When you are ready for deployment, you must change the server name to a local URL and configure your Web server in a URL redirect for h.online-metrix.net.