FABRÍCIO MELO SILVA

Brasileiro, solteiro, 28 anos.
Rua Júlio Cesar 837 - Jardim América - Fortaleza – CE.
Telefone: (85) 98839-0911 / (85) 99790-0885 / E-mail: fabriciomelosilva@gmail.com

FORMAÇÃO

- Graduando em Análise e Desenvolvimento de Sistemas – Universidade de Fortaleza, conclusão prevista pra 2019.

- Graduado em Ciência da Computação - Faculdade Lourenço Filho, conclusão em 2012.

EXPERIÊNCIA PROFISSIONAL

- **2018 – Grupo Edson Queiroz**

  Cargo: Programador

  Principais atividades: Realização de melhorias nos sites e aplicativos do Grupo Edson Queiroz.

  Tecnologias utilizadas: Wordpress, Laravel, Codeigniter, Android, Objective-C, Ruby on Rails.

- **2016-2018 – Grupo Edson Queiroz**

  Cargo: Estagiário (Sustentação Web)

  Principais atividades: Suporte aos sites e aplicativos do Grupo Edson Queiroz.

  Tecnologias utilizadas: Wordpress, Laravel, Codeigniter, Android, Objective-C.

- **2015-2016 – Grupo Gospel**

  Cargo: Técnico de T.I

  Principais atividades: Suporte Help Desk, administração de servidores Windows Server, suporte a telefonia, manutenção e instalação do sistema cftv.

- **2011-2012 – Instituto Iracema (IFCE)**

  Cargo: Programador (Estágio)

  Principais atividades: Responsável pela implantação das aplicações embarcadas. Configuração de um servidor em nuvem. Configuração dos servidores de sistema de controle de versão GIT e Subversion.

- **2008-2013** – **Delano Variedades**

  Cargo: Técnico de Informática

  Principais atividades: Responsável técnico por toda a rede e computadores da empresa.

QUALIFICAÇÕES E ATIVIDADES COMPLEMENTARES

- Inglês Instrumental (Yes Idiomas, 2 anos, conclusão em 2015).
- Curso Formação de Programadores Java (Instituto Evolução, conclusão em 2010).
- Curso Rede de Computadores (SOS Computadores, conclusão em 2008).
- Apresentação do painel “Controle de versão usando o Subversion” na XI Semana da Computação (Faculdade Lourenço Filho, 2012).
- Participação na palestra “Programação Funcional” realizada na Semana Acadêmica – XII Semana da Computação (Faculdade Lourenço Filho, 2012).

Antifraude

Manual de Integração

braspag
uma empresa Cielo.

10 ANOS

Versão 1.7.1

28/04/2014

SUMÁRIO

HISTÓRICO DE ALTERAÇÕES

Manual de Integração- Antifraude		
Versão	Data	* Descrição
1.0	12/04/2012	* Versão Inicial
1.1	09/05/2012	* Inserido na tabela 6.3 erro 907; Inserido classe: AntiFraudRequest.MerchantDefinedData
1.2	27/06/2012	* Retirada dos Parâmetros: **AntiFraudRequest.BillToData.DomainName;** **AntiFraudRequest.BillToData.IpNetworkAddress;** **AntiFraudRequest.CardData.Bin** * Alteração de descrição dos Parâmetros: **AntiFraudRequest.BillToData.FirstName;** **AntiFraudRequest.BillToData.LatName;** **AntiFraudRequest.DecisionManagerData. TravelData.DepartureTime** **AntiFraudRequest.DecisionManagerData. TravelData.TravelLegData.Origin**
1.3	18/10/2012	*Criação da versão 1.1 do método FraudAnalysis, que permite o envio de 95 campos de dados extras ao invés de apenas 15; Inserção dos seguintes parâmetros e respectivas descrições, na Tabela 1: **Version; AntiFraudRequest.AdditionalData [AdditionalDataCollection]**
1.3.1	28/01/2013	* Alteração da descrição dos Parâmetros: **AntiFraudRequest.BillToData.IpAddress;** **AntiFraudRequest.InvoiceHeaderData.ReturnsAccepted;** **AntiFraudRequest.PurchaseTotalsData.Currency;** * Inserção do ítem **Elo** na Tabela 5.2
1.4	05/04/2013	* Inserção do método UpdateStatus * Atualização da tabela 6.1 * Alteração no nome do método FrudAnalysisTransaction para FraudAnalysisTransactionDetails e outras informações deste método.
1.5	08/04/2013	* Inserção da url de homologação; * Inserção do link Service Description;
1.5.1	10/04/2013	* Revisão de todas as tabelas do documento; * Padronização da descrição dos campos Success e CorrelateID
1.6	19/08/2013	* Detalhamento do Serviço de Notificação de Mudança de Status; * Inserção do Anexo 1 - Adicionando Fingerprint * Inserção, no objeto FraudAnalysisRequest, dos Parâmetros: **AntiFraudRequest.CardData.AccountToken,** **AntiFraudRequest.CardData.AccountAlias** e **AntiFraudRequest.CardData.SaveAccountNumber** ***** Alteração, no objeto FraudAnalysisRequest, da descrição dos parâmetros: **AntiFraudRequest.MerchantDefinedData,**

		AntiFraudRequest.AdditionalData [AdditionalDataCollection]
1.7	03/12/2013	* Exclusão no objeto FraudAnalysisRequest, dos parâmetros: **AntiFraudRequest.MerchantDefinedData, AntiFraudRequest.MerchantDefinedData.Field1 ao AntiFraudRequest.MerchantDefinedData.Field15** * Alteração no objeto FraudAnalysisRequest, na descrição do parâmetro: **AntiFraudRequest.MerchantReferenceCode** * Inserção no objeto FraudAnalysisRequest: parâmetro **AntiFraudRequest.DeviceFingerprintID** * Alteração do Anexo 1 - Adicionando Fingerprint
1.7.1	28/04/2014	* Inclusão de observação no objeto FraudAnalysisRequest, parâmetro AntiFraudRequest.CardData.AccountNumber.

INTRODUÇÃO

A plataforma Antifraude tem a finalidade de auxiliar o estabelecimento de e-commerce na detecção de fraudes online, através da utilização de ferramentas já existentes no mercado.
O Antifraude está integrado ao gateway Pagador, facilitando o envio e processamento de transações.

OBJETIVO

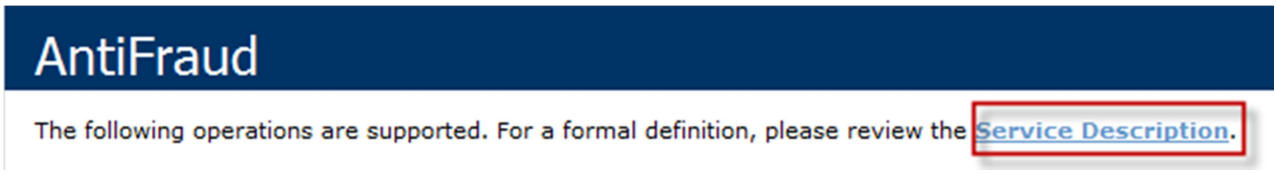
Este manual tem como objetivo orientar o desenvolvedor da loja sobre a integração com a plataforma Antifraude, descrevendo as funcionalidades existentes e os métodos a serem utilizados, listando informações a serem enviadas e recebidas e provendo exemplos. O manual detalha os fluxos de integração via *Webservice.*

Este manual atende ao seguinte fornecedor

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

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

Para acesso ao código descritivo do webservice (WSDL), acessar o link "Service Description", conforme abaixo:



A integração deve ser feita sempre usando URL e em hipótese alguma por IP ou usando nomes como www.pagador.com.br ou apenas pagador.com.br.

Para receber a URL de Produção, solicite à nossa equipe de implantação através da ferramenta Suporte.

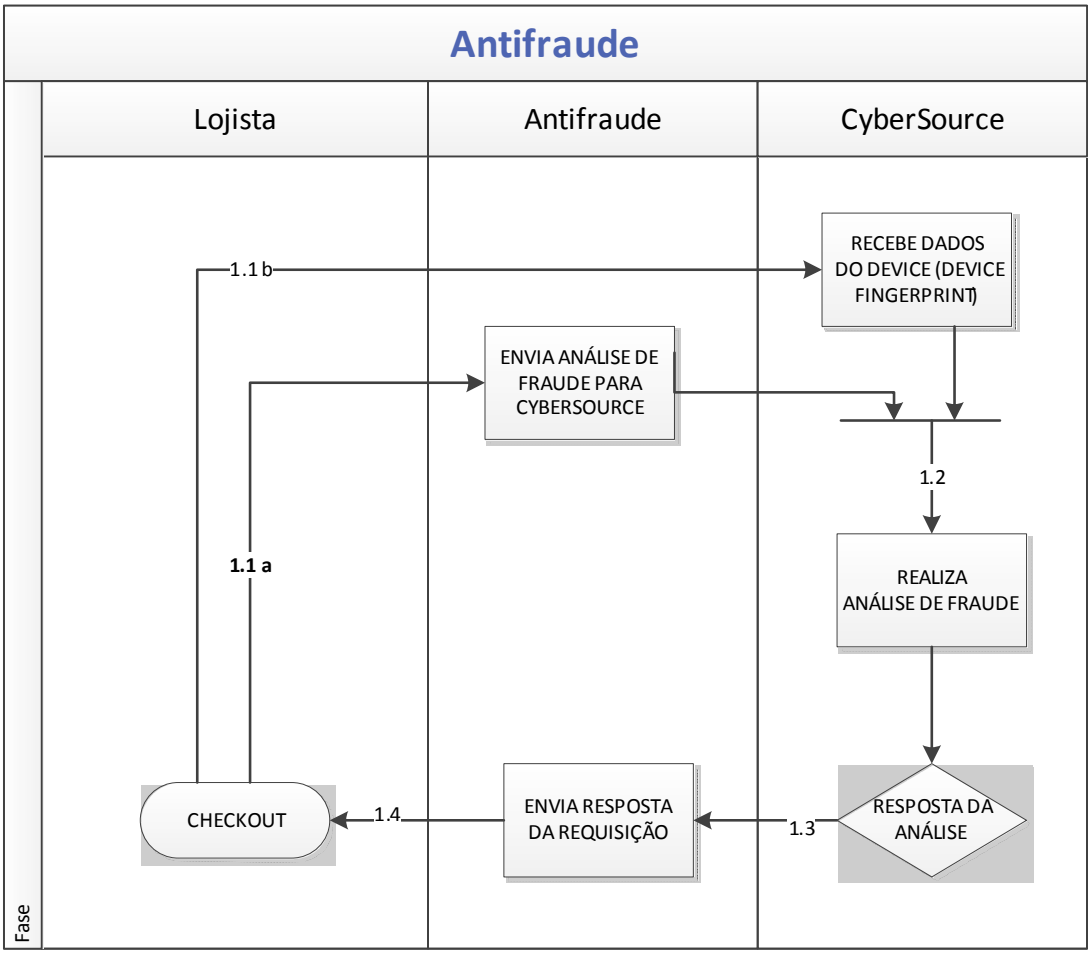
1. CENÁRIOS POSSÍVEIS

Abaixo estão representados os 3 possíveis fluxos da Plataforma Antifraude, via Webservice.

1.1. Antifraude

Envio da transação para Análise de Fraude, conforme indicado no diagrama abaixo.

Definir parâmetro AntiFraudSequenceType = AnalyseOnly.

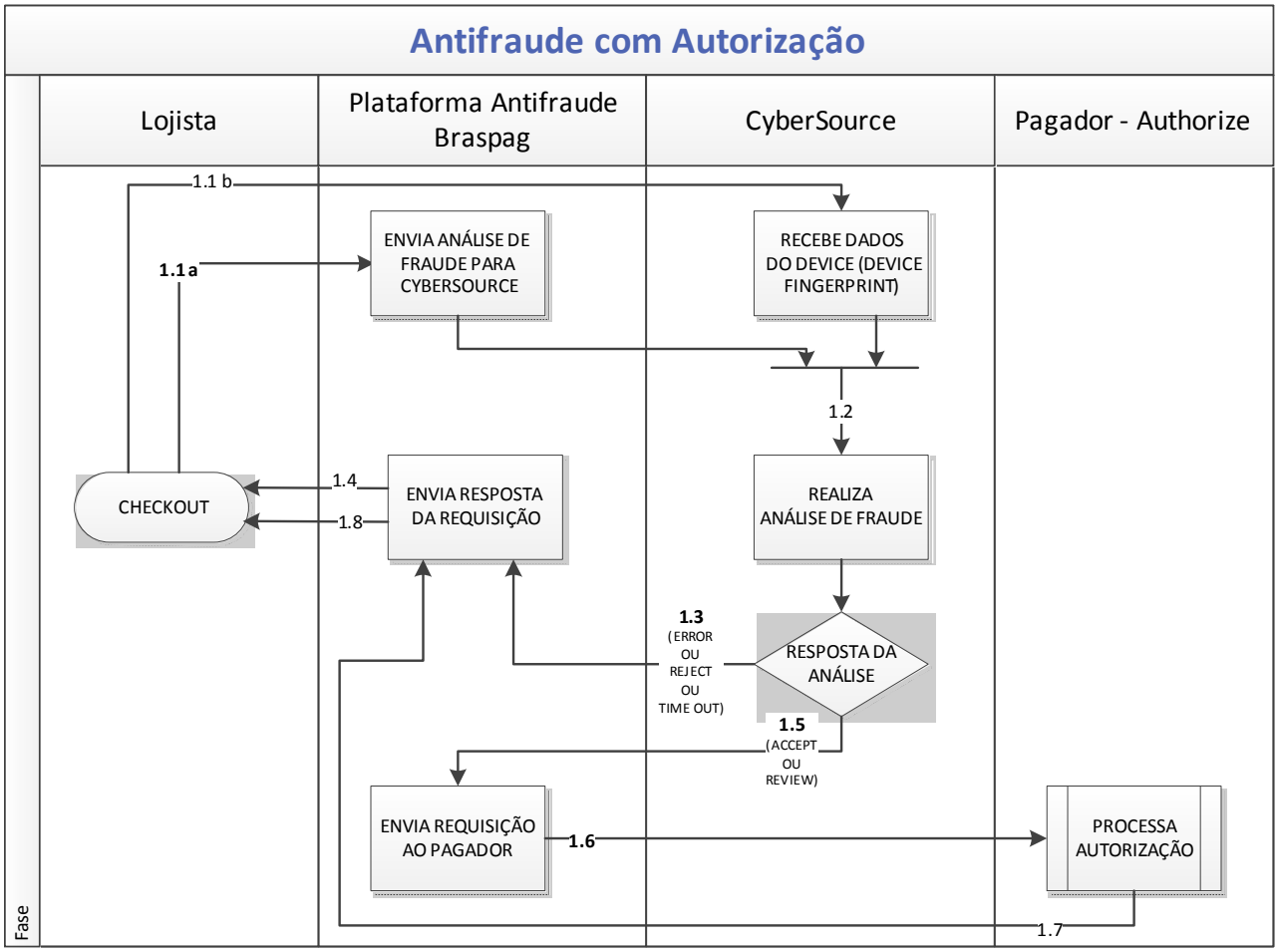


1.1 a)) Envio de requisição com dados da venda para Análise de Fraude
1.1 b) Execução do Script do DeviceFingerPrint- é enviado diretamente para Cybersource
1.2) Recebimento das informações do Device e Dados da Venda para processamento da Análise de Fraude
1.3) Envio da resposta da Análise de Fraude
1.4) Envio da resposta da Análise de Fraude

1.2. Antifraude com Autorização

Envio de transação para Análise de Fraude, caso retorne "Aprovado" ou "Revisão", a mesma será enviada para Autorização junto aos Adquirentes, utilizando o serviço de Authorize do Pagador.

Definir parâmetro AntiFraudSequenceType = AnalyseAndAuthorizeOnSuccess.



1.1 a)) Envio de requisição com dados da venda para Análise de Fraude com Autorização.
1.1 b) Execução do Script do DeviceFingerPrint- é enviado diretamente para Cybersource
1.2) Recebimento das informações do Device e Dados da Venda para processamento da Análise de Fraude
1.3) Envio da resposta da Análise de Fraude da CyberSource para o Antifraude.
1.4) Envio da resposta da Análise de Fraude.
1.5) Envio da resposta da Análise de Fraude da CyberSource para o Antifraude.
1.6) Requisição de autorização enviada ao Pagador.
1.7) Resposta da autorização enviada ao Antifraude
1.8) Resposta da Requisição enviada

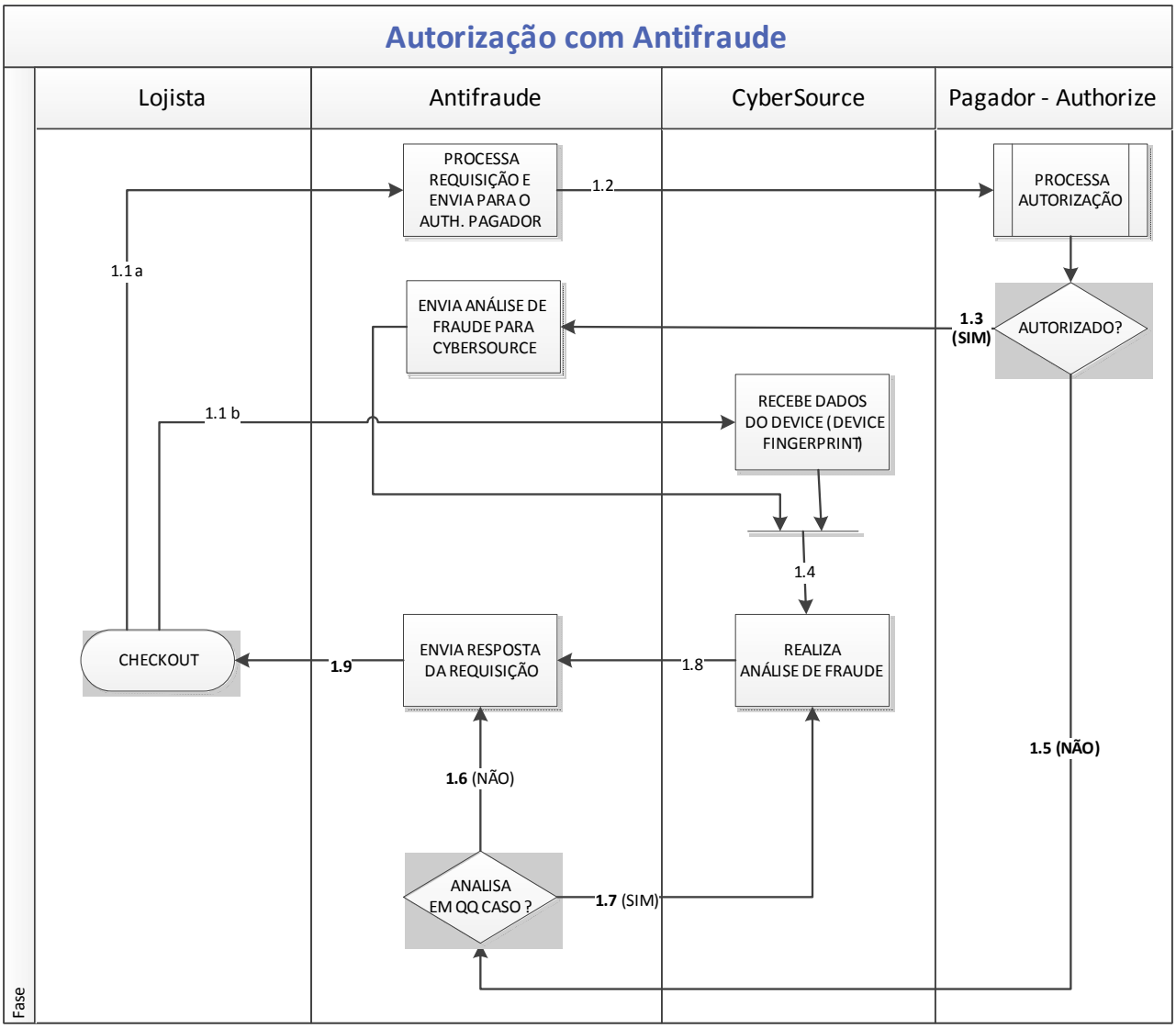
1.3. Autorização com Antifraude

Envio de transação para o Pagador, caso seja autorizada, será enviada para realização da Análise de Fraude. Caso contrário, o status da transação será armazenado no banco como "Abortado" e a Análise de Fraude não será realizada, desde que o cliente não defina que deseja a Análise de Fraude qualquer que seja o resultado do Autorizador.

Definir parâmetro AntiFraudSequenceType = AuthorizeAndAnalyseOnSuccess.

Caso se queira que a Análise de Fraude aconteça qualquer que seja o resultado do Autorizador, também é possível.

Definir parâmetro AntiFraudSequenceType = AuthorizeAndAnalyseAlways.



1.1 a) Envio da requisição com dados da venda para Autorização com Análise de Fraude
1.1 b) Execução do Script do DeviceFingerPrint- é enviado diretamente para Cybersource
1.2) Requisição enviada para o Authorize do Pagador
1.3) Requisição enviada para Análise de Fraude
1.4) Recebimento das informações do Device e Dados da Venda para processamento da Análise de Fraude
1.5) Resposta do Authorize do Pagador enviada ao Antifraude
1.6) Resposta da opção escolhida pelo cliente: NÃO
1.7) Resposta da opção escolhida pelo cliente: SIM
1.8) Envia resposta de Análise de Fraude realizada pela Cybersource , para o Antifraude
1.9) Resposta da Requisição enviada

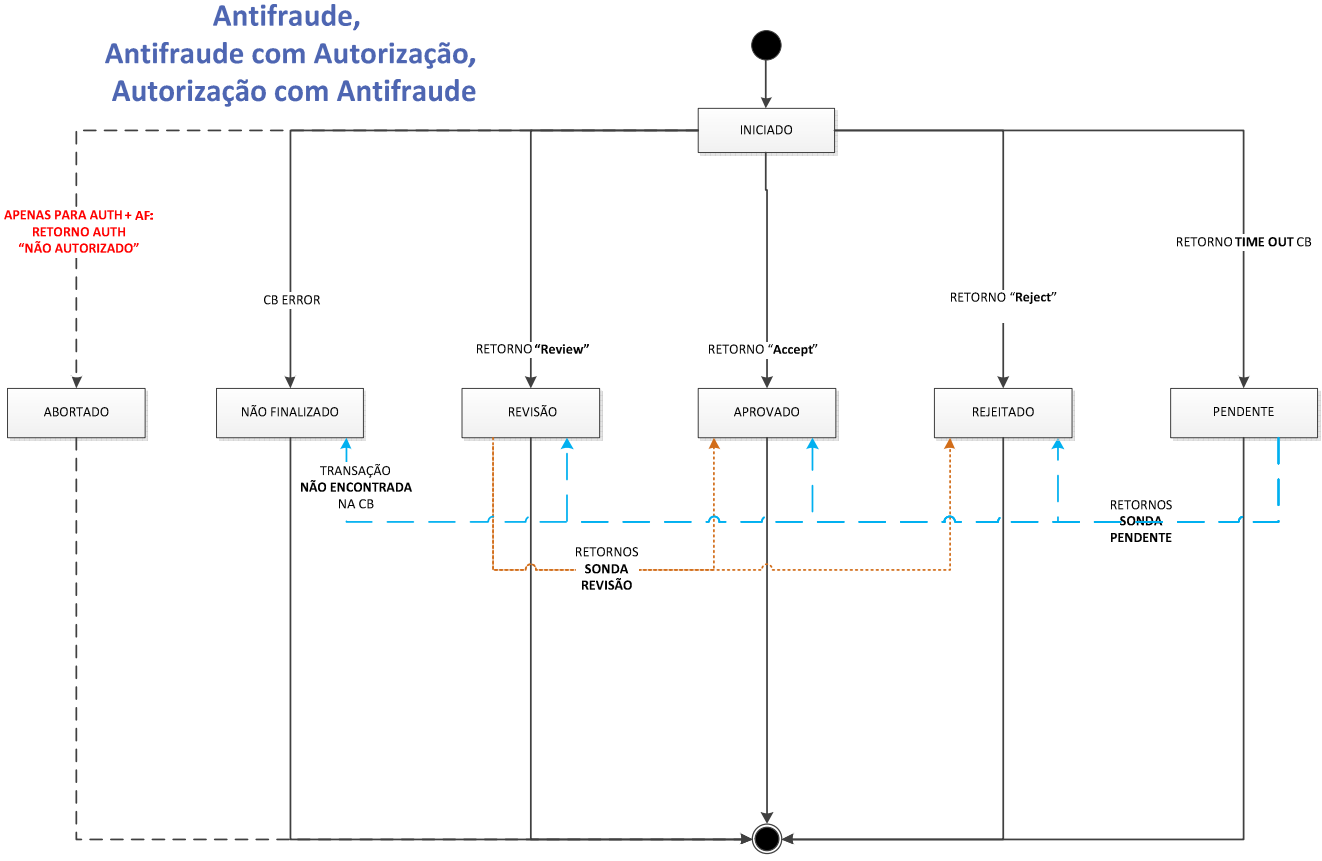
2. STATUS DA ANÁLISE DE FRAUDE

Seguem abaixo, os possíveis status que as transações enviadas para análise de fraude podem ter:

- **Iniciado** – Estado inicial das transações em Análise de Fraude;
- **Aprovado** - Transação aprovada pelo Antifraude;
- **Revisão** – Transação que será revista manualmente e após esta revisão, poderá ter seu estado alterado para "Aprovado" ou "Rejeitado";
- **Rejeitado** – Transação interpretada como fraude;
- **Pendente** – Tentativa de envio da transação para a CyberSource com retorno TIME OUT. Seu estado poderá ser alterado pela sonda ou pelo cliente para: Aprovado, Revisão, Rejeitado ou Não Finalizado;
- **Não Finalizado** – Tentativa de envio da transação para a CyberSource, com retorno de erro diferente de TIME OUT;
- **Abortado** – Indica que a solicitação de Autorização no Pagador (anterior a Análise de Fraude) obteve retorno de "Não Autorizado", fazendo com que a transação não seja enviada para Análise de Fraude.

Diagrama de Transição e Estado:

Antifraude,
Antifraude com Autorização,
Autorização com Antifraude



3. INTEGRAÇÃO VIA WEBSERVICE

3.1. Método FraudAnalysis

Para envio de uma transação de Análise de Fraude apenas, ou em conjunto com Autorização do Pagador, conforme indicado nos Diagramas do item 1.

Tabela 1 – Propriedades do objeto FraudAnalysisRequest

Parâmetro	Tipo	Tamanho	Descrição	Obrigatório?
RequestId	Guid		Id do request da requisição.	Sim
Version	String		Versão do contrato do Webservice 1.0 ou 1.1; **Obs:** Caso o valor para este parâmetro não seja informado, por padrão a versão será 1.0	Não
MerchantId	Guid		Id da loja na Braspag.	Sim
AntiFraudSequenceType	Enum		Tipo de fluxo desejado para realização da análise de fraude. Consultar tabela 5.1	Sim
DocumentData	Class		Objeto que contêm informações do comprador.	Não
DocumentData.Cpf	String	11	CPF do comprador. Enviar sem pontuação	Não
DocumentData.Cnpj	String	14	CNPJ do comprador. Enviar sem pontuação	Não
DocumentData.OtherDocument	String	0 - 20	Outro documento de identificação do comprador.	Não
AntiFraudRequest	Class		Objeto que contém todas as informações necessárias para realizar a análise de fraude.	Sim
AntiFraudRequest.BankInfoData	Class		Objeto com informações do banco do comprador. Preencher APENAS para análisar transações de débito direto.	Não
AntiFraudRequest.BankInfoData.Address	String	0 - 255	Endereço da agência bancária do comprador.	Não
AntiFraudRequest.BankInfoData.Code	String	0 - 15	Código do banco.	Não
AntiFraudRequest.BankInfoData.BranchCode	String	0 - 15	Código do banco utilizado para transferências internacionais.	Não
AntiFraudRequest.BankInfoData.City	String	0 - 35	Cidade onde o banco está localizado.	Não
AntiFraudRequest.BankInfoData.Country	String	2	País onde o banco está localizado.	Não
AntiFraudRequest.BankInfoData.Name	String	0 - 40	Nome do banco.	Não
AntiFraudRequest.BankInfoData.SwiftCode	String	0 - 30	Código SWIFT(Society for Worldwide Interbank Financial Telecommunication) do banco.	Não
AntiFraudRequest.BillToData	Class		Objeto com informações dos dados de cobrança do comprador.	Sim
AntiFraudRequest.BillToData.City	String	1 - 50	Cidade do endereço de cobrança do comprador.	Sim
AntiFraudRequest.BillToData.Country	String	2	País do endereço de cobrança do comprador.	Sim
AntiFraudRequest.BillToData.CustomerId	String	0 - 50	Id que identifica o comprador na loja.	Não
AntiFraudRequest.BillToData.DateOfBirth	DateTime		Data de nascimento do comprador.	Não
AntiFraudRequest.BillToData.Email	String	1 - 100	E-mail do comprador.	Sim

AntiFraudRequest.BillToData.HostName	String	0 - 60	Nome do host onde o comprador estava antes de entrar no site da loja.	Não
AntiFraudRequest.BillToData.HttpBrowserCookiesAccepted	Bool		True = O browser do cliente aceita cookies. False = O browser do cliente não aceita cookies.	Não
AntiFraudRequest.BillToData. HttpBrowserEmail	String	0 - 100	E-mail registrado no browser do comprador. Pode diferir do e-mail cadastrado.	Não
AntiFraudRequest.BillToData. HttpBrowserType	String	0 - 40	Nome do browser utilizado pelo comprador.	Não
AntiFraudRequest.BillToData.IpAddress	String	0 - 15	Endereço IP do comprador. Ex.: 10.1.27.15. É altamente recomendável o envio deste campo.	Não
AntiFraudRequest.BillToData.FirstName	String	1 - 60	Primeiro nome do PORTADOR (nome no cartão de crédito)	Sim
AntiFraudRequest.BillToData.LastName	String	1 - 60	Último nome do PORTADOR (nome no cartão de crédito)	Sim
AntiFraudRequest.BillToData. PhoneNumber	String	0 - 15	Telefone do comprador.	Não
AntiFraudRequest.BillToData. PostalCode	String	0 - 10	CEP ou Caixa Postal do comprador.	Não
AntiFraudRequest.BillToData.State	String	2	Sigla do estado do endereço de cobrança do comprador.	Sim
AntiFraudRequest.BillToData.Street1	String	1 - 60	Endereço de cobrança do comprador.	Sim
AntiFraudRequest.BillToData.Street2	String	0 - 60	Endereço de cobrança do comprador.	Não
AntiFraudRequest.BusinessRulesScoreThreshold	Int		Nível de risco aceitavel para ordenação de cada produto.	Não
AntiFraudRequest.CardData	Class		Objeto com informações de cartão de crédito.	Não
AntiFraudRequest.CardData.AccountNumber	String	0 - 20	Número do cartão de crédito utilizado na compra. Obs.: quando este campo for enviado, é obrigatório o envio do campos AntiFraudRequest.CardData.ExpirationMonth e AntiFraudRequest.CardData.ExpirationYear com valores válidos.	Não
AntiFraudRequest.CardData.Card	Enum		Bandeira do cartão de crédito. Consultar tabela 5.2 Obs.: Deverá ser informada caso seja realizada transação utilizando AccountToken ou AccountAlias	Não
AntiFraudRequest.CardData.ExpirationMonth	String	2	Mês de expiração do cartão de crédito, no formato MM.	Não
AntiFraudRequest.CardData.ExpirationYear	String	4	Ano de expiração do cartão de crédito, no formato YYYY.	Não
AntiFraudRequest.CardData.AccountToken	Guid		Identificador do cartão de crédito (CreditCardToken) salvo no Cartão Protegido. Este campo pode ser enviado no lugar dos campos **CardData.Account, CardData.ExpirationMonth** e **CardData.ExpirationYear.** O sistema utilizará o AccountToken para buscar e preencher estes campos. **Obs.:** o campo **CardData.Card** não será preenchido automaticamente e deve ser enviado também.	Não
AntiFraudRequest.CardData.AccountAlias	String		Identificador do cartão de crédito (CreditCardAlias) salvo no Cartão Protegido. Este campo pode ser enviado no lugar dos campos **CardData.Account, CardData.ExpirationMonth** e **CardData.ExpirationYear**. O sistema utilizará o AccountAlias para	Não

			buscar e preencher estes campos. obs: o campo **CardData.Card** não será preenchido automaticamente e deve ser enviado também.	
AntiFraudRequest.CardData.SaveAccountNumber	String		Indica se os dados do cartão de crédito serão armazenados para uso do Cartão Protegido. A ação só será feita se a loja possuir o produto Cartão Protegido contratado. O "**CreditCardToken**" gerado na plataformas Cartão Protegido associado aos dados de cartão enviados retornará no campo AntifraudRespose.AccountToken	Não
AntiFraudRequest.Comments	String	0 - 255	Comentário que o lojista pode associar a esta análise.	Não
AntiFraudRequest.DecisionManagerData	Class		Objeto onde é possível definir regras de análise. Utilize esta classe quando quiser analisar apenas alguns pedidos, ao invés de todos os pedidos enviados.	Não
AntiFraudRequest.DecisionManagerData.TravelData	Class		Objeto que contém informações de viagens, para compras de passagens e/ou pacotes de viagem.	Não
AntiFraudRequest.DecisionManagerData.TravelData.CompleteRoute	String	0 - 255	Rota da viagem. Concatenação de pernas de viagem individuais no formato ORIG1-DEST1, por exemplo: SFO-JFK: JFK-LHR: LHR-CDG.	Não
AntiFraudRequest.DecisionManagerData.TravelData.DepartureTime	DateTime		Data, hora e minuto de partida do vôo.	Não
AntiFraudRequest.DecisionManagerData.TravelData.JourneyType	String	0 - 32	Tipo de viagem. Ex.: Só ida, Ida e volta, etc.	Não
AntiFraudRequest.DecisionManagerData.TravelData.TravelLegData [TravelLegDataCollection]	List	0 - n	Coleção de dados de origem e destino das viagens do comprador.	Não
AntiFraudRequest.DecisionManagerData.TravelData.TravelLegData.Origin	String	0 - 3	Código do aeroporto do ponto de origem da viagem.	Não
AntiFraudRequest.DecisionManagerData.TravelData.TravelLegData.Destination	String	0 - 3	Número do pedido. Recomenda-se que seja o mesmo número do pedido.	Não
AntiFraudRequest.FundTransferData	Class		Objeto utilizado para análise de transferência internacional.	Não
AntiFraudRequest.FundTransferData.AccountName	String	0 - 30	Nome utilizado na conta bancária. Pode usar este campo apenas quando marcar uma operação de débito.	Não
AntiFraudRequest.FundTransferData.AccountNumber	String	0 - 30	Número da conta bancária.	Não
AntiFraudRequest.FundTransferData.BankCheckDigit	String	0 - 2	Código utilizado para validar a conta bancária.	Não
AntiFraudRequest.FundTransferData.Iban	String	0 - 2	Número internacional da conta bancária.	Não
AntiFraudRequest.InvoiceHeaderData	Class		Objeto onde é possivel especificar informações caso o comprador tenha solicitado embrulho para presente.	Não
AntiFraudRequest.InvoiceHeaderData.IsGift	Boolean		Flag que indica se o pedido é para presente ou não.	Não
AntiFraudRequest.InvoiceHeaderData.MerchantDescriptor	String	0 - 22	Descrição da loja que aparece na declaração do titular do cartão.	Não
AntiFraudRequest.InvoiceHeaderData.ReturnsAccepted	Boolean		True= Devoluções são aceitas para este pedido; False= Devoluções não são aceitas para este pedido.	Não
AntiFraudRequest.InvoiceHeaderData.Tender	Enum		Forma de pagamento utilizada para o pedido. Consultar tabela 5.3	Não
AntiFraudRequest.ItemData [ItemDataCollection]	List	1 - n	Lista de itens comprados, com seus dados.	Sim
AntiFraudRequest.ItemData.GiftCategory	Enum		Flag que avaliará os endereços de cobrança e entrega para difrentes cidades, estados ou países. Consultar tabela 5.9	Não

AntiFraudRequest.ItemData.HostHedge	Enum		Nível de importância do e-mail e endereços IP dos clientes em risco de pontuação. Consultar tabela 5.10	Não
AntiFraudRequest.ItemData. NonSensicalHedge	Enum		Nível dos testes realizados sobre os dados do comprador com pedidos recebidos sem sentido. Consultar tabela 5.11	Não
AntiFraudRequest.ItemData. ObscenitiesHedge	Enum		Nível de obscenidade dos pedidos recebedidos. Consultar tabela 5.7	Não
AntiFraudRequest.ItemData. PassengerData.FirstName	String	0 - 60	Primeiro nome do passageiro.	Não
AntiFraudRequest.ItemData .PassengerData.LastName	String	0 - 60	Último nome do passageiro.	Não
AntiFraudRequest.ItemData. PassengerData.PassengerId	String	0 - 32	Id do passageiro a quem o bilheite foi emitido.	Não
AntiFraudRequest.ItemData. PassengerData.Status	String	0 - 32	Classificação da empresa aérea. Pode-se usar valores como Gold ou Platina.	Não
AntiFraudRequest.ItemData. PassengerData.Passenger	Enum		Classificação do passageiro. Consultar tabela 5.13	Não
AntiFraudRequest.ItemData. PassengerData.Email	String	0 - 255	E-mail do passageiro.	Não
AntiFraudRequest.ItemData. PassengerData.Phone	String	0 - 15	Número do telefone do passageiro. Para pedidos fora do U.S., a CyberSource recomenda que inclua o código do país.	Não
AntiFraudRequest.ItemData. PhoneHedge	Enum		Nível dos testes realizados com os números de telefones. Consultar tabela 5.9	Não
AntiFraudRequest.ItemData. ProductData.Code	Enum		Tipo do produto. Consultar tabela 5.10	Não
AntiFraudRequest.ItemData. ProductData.Name	String	0 - 255	Nome do produto.	Não
AntiFraudRequest.ItemData. ProductData.Risk	Enum		Nível do risco do produto. Consultar tabela 5.11	Não
AntiFraudRequest.ItemData. ProductData.Sku	String	0 - 255	Código comerciante identificador do produto.	Não
AntiFraudRequest.ItemData. ProductData.Quantity	Int		Quantidade do produto a ser adquirido.	Não
AntiFraudRequest.ItemData. ProductData.UnitPrice	Decimal		Preço unitário do produto.	Sim
AntiFraudRequest.ItemData.TimeHedge	Enum		Nível de importância da hora do dia do pedido do cliente. Consultar tabela 5.12	Não
AntiFraudRequest.ItemData.VelocityHedge	Enum		Nível de importância de frequência de compra do cliente. Consultar tabela 5.13	Não
AntiFraudRequest.AdditionalData [AdditionalDataCollection]	List	1 – n	Objeto com informações adicionais a serem enviadas. As informações serão disponibilizadas no anexo Antifraude_MerchantDefinedData.pdf e irão variar de acordo com cada loja. Essas informações apesar de não obrigatórias, são de EXTREMA IMPORTÂNCIA para a análise de fraude. Obs.: Somente compatível com a versão 1.1	Não
AdditionalData.Id	String		Identificação da posição do campo Obs.: Somente compatível com a versão 1.1	Sim
AdditionalData.Value	String	0 - 255	Valor do Campo Obs.: Somente compatível com a versão 1.1	Sim
AntiFraudRequest.MerchantReferenceCode	String	1 - 50	Número do pedido. Recomenda-se que seja o mesmo número do pedido enviado para o Pagador, caso transacione pela Braspag, para facilitar o rastreamento.	Sim
AntiFraudRequest.DeviceFingerprintID	String	1 - 50	Identificador utilizado para cruzar informações obtidas pelo Browser do internauta com os dados enviados para análise. Este mesmo valor deve ser passado na	Não

			variável SESSIONID do script do DeviceFingerPrint.	
AntiFraudRequest.PurchaseTotalsData	Class		Objeto com informações de pagamento total da compra realizada.	Não
AntiFraudRequest.PurchaseTotalsData.Currency	String	0 - 3	Código da moeda utilizada no pedido. Usar Códigos ISO 4217 de Moedas. Ex: Reais=BRL; Dólar Americano=USD	Não
AntiFraudRequest.PurchaseTotalsData.GrandTotalAmount	Decimal		Valor total do pedido.	Não
AntiFraudRequest.ShipToData	Class		Objeto contendo dados de entrega do produto comprado.	Não
AntiFraudRequest.ShipToData.City	String	0 - 50	Cidade do endereço de entrega do produto.	Não
AntiFraudRequest.ShipToData.Country	String	0 - 2	Sigla do país do endereço de entrega do produto.	Não
AntiFraudRequest.ShipToData.FirstName	String	0 - 60	Primeiro nome do responsável por receber a entrega do produto.	Não
AntiFraudRequest.ShipToData.LastName	String	0 - 60	Último nome do responsável por receber a entrega do produto.	Não
AntiFraudRequest.ShipToData.PhoneNumber	String	0 - 15	Telefone do endereço de entrega do produto.	Não
AntiFraudRequest.ShipToData.PostalCode	String	0 - 10	CEP ou endereço postal do endereço de entrega do produto.	Não
AntiFraudRequest.ShipToData.ShippingMethod	Enum		Tipo de serviço de entrega do produto. Consultar tabela 5.14	Não
AntiFraudRequest.ShipToData.State	String	0 - 2	Sigla do estado do endereço de entrega do produto.	Não
AntiFraudRequest.ShipToData.Street1	String	0 - 60	Primeira linha do endereço de entrega do produto.	Não
AntiFraudRequest.ShipToData.Street2	String	0 - 60	Continuação do endereço de entrega do produto.	Não
AuthorizeCreditCardTransactionRequest	Class		Objeto que deve ser preenchido caso a loja deseje autorizar uma transação juntamente com o processo de análise. **É o mesmo request do contrato novo do Pagador.**	Dependendo do fluxo desejado.

3.2. Retorno do método FraudAnalysis

FraudAnalysisResponse além de retornar todos os dados referentes ao pedido, vai retornar também o resultado da análise de fraude.

Tabela 2 – Propriedades do objeto FraudAnalysisResponse

Parâmetro	Tipo	Tamanho	Descrição
CorrelatedId	Guid		Id que foi passado pelo request, apenas para identificação.
Success	Boolean		Flag que indica se a operação foi concluída com sucesso. NÃO indica erro.
ErrorReport [ErrorReportCollection]	List	0 - n	Lista de erros ocorridos durante o processamento. Consultar planilha de ErrorTypes.
ErrorReport.ErrorCode	Short		Código do erro.
ErrorReport.Message	String		Mensagem de erro.
AntiFraudTransactionId	Guid		Id da transação no antifraude para consultas posteriores através do método para visualizar detalhes da análise.
TransactionStatusCode	Int		Código do status da transação na Braspag. Consultar tabela 5.29
TransactionStatusDescription	String	0 - 32	Descrição do status da transação na Braspag. Consultar tabela 5.29
AntiFraudResponse.AfsReplyData	Class		Objeto com os dados da análise de fraude.
AntiFraudResponse.AfsReplyData.AddressInfoCode	String	0 - 255	Combinação de códigos que indicam erro no endereço de cobrança e/ou entrega. Os códigos são concatenados usando o caractere ^. Ex.: B^Y. Consultar tabela 5.21
AntiFraudResponse.AfsReplyData.AfsFactorCode	String	0 - 100	Combinação de códigos que indicam o score do pedido. Os códigos são concatenados usando o caractere ^. Ex.: B^Y. Consultar tabela 5.22
AntiFraudResponse.AfsReplyData.AfsResult	Int		Score total calculado para o pedido.
AntiFraudResponse.AfsReplyData.BinCountry	String	0 - 2	Sigla do país de origem da compra.
AntiFraudResponse.AfsReplyData.CardAccount	Enum		Tipo de comprador. Consultar tabela 5.15
AntiFraudResponse.AfsReplyData.CardIssuer	String	0 - 128	Nome do banco ou entidade emissora do cartão.
AntiFraudResponse.AfsReplyData.CardScheme	Enum		Tipo da bandeira. Consultar tabela 5.16
AntiFraudResponse.AfsReplyData.ConsumerLocalTime	String	0 - 8	Horário local do comprador, calculado a partir da data da solicitação e do endereço de cobrança.
AntiFraudResponse.AfsReplyData.HostSeverity	Int		Nível de risco do domínio de e-mail do comprador, de 0 a 5, onde 0 é risco indeterminado e 5 representa o risco mais alto.
AntiFraudResponse.AfsReplyData.HostListInfoCode	String	0 - 255	Sequência de códigos que indicam que as informações do comprador está associada a transações que estão na lista de positivos ou negativos. Os códigos são concatenados usando o caractere ^. Consultar tabela 5.25
AntiFraudResponse.AfsReplyData.IdentityInfoCode	String	0 - 255	Sequência de códigos que indicam que existe uma excessiva alteração de identidades do comprador. Os códigos são concatenados usando o caractere ^.

			Consultar tabela 5.23
AntiFraudResponse.AfsReplyData. InternetInfoCode	String	0 - 255	Sequência de códigos que indicam que existe um problema com o endereço de e-mail, IP ou endereço de cobrança. Os códigos são concatenados usando o caractere ^. Consultar tabela 5.24
AntiFraudResponse.AfsReplyData. IpCity	String	0 - 50	Nome da cidade do comprador a partir do endereço IP.
AntiFraudResponse.AfsReplyData. IpCountry	String	0 - 2	Sigla do país do comprador a partir do endereço IP.
AntiFraudResponse.AfsReplyData. IpRoutingMethod	Enum		Tipo de roteamento de IP utilizado pelo comprador. Consultar tabela 5.17
AntiFraudResponse.AfsReplyData. IpState	String	0 - 255	Nome do estado do comprador a partir do endereço IP.
AntiFraudResponse.AfsReplyData. PhoneInfoCode	String	0 - 255	Sequência de códigos que indicam que existe um problema com o telefone do comprador. Os códigos são concatenados usando o caractere ^. Consultar tabela 5.26
AntiFraudResponse.AfsReplyData. ReasonCode	Int		Resultado da análise. Consultar tabela 5.20
AntiFraudResponse.AfsReplyData. ScoreModelUsed	String	0 - 20	Nome do modelo de score utilizado.
AntiFraudResponse.AfsReplyData. SuspiciousInfoCode	String	0 - 255	Sequência de códigos que indicam que o comprador informou dados suspeitos. Os códigos são concatenados usando o caractere ^. Consultar tabela 5.27
AntiFraudResponse.AfsReplyData. VelocityInfoCode	String	0 - 255	Sequência de códigos que indicam que o comprador tem uma frequência de compras elevada. Os códigos são concatenados usando o caractere ^. Consultar tabela 5.28
AntiFraudResponse. Decision	String	0 - 20	Decisão tomada pela ferramenta de Antifraude. Consultar tabela 5.18
AntiFraudResponse.DecisionReplyData	Class		Objeto com os dados da decisão tomada pela ferramenta de Antifraude
AntiFraudResponse.DecisionReplyData. ActiveProfileReplyData	Class		Objeto com os dados de análise do perfil ativo.
AntiFraudResponse.DecisionReplyData. ActiveProfileReplyData.SelectedBy	String	0 - 50	Nome da regra do perfil selecionado para realizar a análise. Disponível apenas se o modo verbose estiver habilitado.
AntiFraudResponse.DecisionReplyData. ActiveProfileReplyData.Name	String	0 - 30	Nome do perfil selecionado para realizar a análise. Disponível apenas se o modo verbose estiver habilitado.
AntiFraudResponse.DecisionReplyData .ActiveProfileReplyData. DestinationQueue	String	0 - 30	Nome da fila para a qual os pedidos que não forem aceitos imediatamente são enviados. Disponível apenas se o modo verbose estiver habilitado.
AntiFraudResponse.DecisionReplyData. ActiveProfileReplyData. RulesTriggeredData	Class		Objeto com os dados de gatilho de regras para a análise de fraude.
AntiFraudResponse.DecisionReplyData. ActiveProfileReplyData. RulesTriggeredData. RuleResultItemData [RuleResultItemCollection]	List		Regras utilizadas durante a análise. Disponível apenas se o modo verbose estiver habilitado.
AntiFraudResponse.DecisionReplyData. ActiveProfileReplyData. RulesTriggeredData. RuleResultItemData.RuleNumber	Int		Id da regra.
AntiFraudResponse.DecisionReplyData. ActiveProfileReplyData.	String	0 - 20	Decisão tomada para a regra, pela ferramenta de

RulesTriggeredData. RuleResultItemData.Decision			Antifraude. Consultar tabela 5.18.
AntiFraudResponse.DecisionReplyData. ActiveProfileReplyData. RulesTriggeredData. RuleResultItemData.Evaluation	Enum		Avaliação da regra. Consultar tabela 5.19.
AntiFraudResponse.DecisionReplyData. ActiveProfileReplyData. RulesTriggeredData. RuleResultItemData.Name	String	0 - 50	Nome da regra.
AntiFraudResponse.DecisionReplyData. CasePriority	Int		Caso o lojista seja assinante do Enhanced Case Management, ele recebe este valor com o nível de prioridade, sendo 1 o mais alto e 5 o mais baixo.
AntiFraudResponse.DecisionReplyData. VelocityInfoCode	String	0 - 25	Lista de códigos acionadas pelo pedido. Esta informação foi gerada pelo request e será retornada para que seja possível relacionar ao response.
AntiFraudResponse. InvalidFieldCollection	List<string>		Lista de campos que tiveram dados inválidos.
AntiFraudResponse. MerchantReferenceCode	String	0 - 50	Código de referencia ou rastreamento gerado pelo lojista.
AntiFraudResponse. MissingFieldCollection	List<string>		Lista de campos obrigatórios que não foram enviados.
AntiFraudResponse.ReasonCode	Int		Resultado geral da análise gerado pela ferramenta de Antifraude. Consultar tabela 5.20.
AntiFraudResponse.RequestId	String	0 - 26	Identificador do request.
AntiFraudResponse.RequestToken	String	0 - 256	Identificador do request gerado pela ferramenta Antifraude

3.3. Método UpdateStatus

Método para alterar as transações em review para ACCEPT ou REJECT. A resposta deste método sempre será Fail ou Success, onde *Fail* significa que a transação não pode ser processada, e *Success* significa que a mesma está em processamento. Para obter o resultado do processamento o cliente precisará sondar a Braspag, após um período configurável que deverá ser consultado no setor de implantação e operações.

Parâmetro	Tipo	Tamanho	Descrição	Obrigatório?
RequestId	Guid		Id do request da requisição.	Sim
MerchantId	Guid		Id da loja no antifraude a ser utilizada para a consulta.	Sim
AntiFraudTransactionId	Guid		Id da transação de antifraude a ser localizada.	Sim
NewStatus	string		Novo status que a transação deverá receber. Somente poderá conter ACCEPT ou REJECT	Sim
Comment	string		Comentário associado a mudança de status.	Não

Exemplo de Xml de request:

```
<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. Retorno do método UpdateStatus

Parâmetro	Tipo	Tamanho	Descrição
AntiFraudTransactionId	Guid		Representa o ID da transação de análise de fraude que foi enviado requisição.
RequestStatusCode	String		Indica se a transação foi recebida com sucesso para processamento pela Ferramenta de Análise de Fraude. Consultar Tabela 5.30.
RequestStatusDescription	String		Contém a descrição do RequestStatusCode. Consultar Tabela 5.30.
CorrelatedId	Guid		Id que foi passado pelo request, apenas para identificação.
Success	String		Flag que indica se a operação foi concluída com sucesso. NÃO indica erro.
ErrorReportCollection	Array <string>		Coleção de string que conterá as causas do "não processamento" caso haja algum erro.

Exemplo de Xml de Response:

```
<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. CONSULTA

4.1. Notificação de Mudança de Status

Serviço que envia um post de notificação ao cliente caso haja alguma alteração de status (somente para transações com OriginalDecision **REVIEW**).

- É necessário solicitar a Equipe de Implementação o cadastramento da URL de Mudança de Status. Quando acessada pelo servidor da Braspag, enviando o POST, a URL cadastrada para Retorno de Mudança de Status, deverá exibir um código informando que recebeu a mudança de status e a processou com sucesso. **<status>OK</status>**;
- Se a URL de mudança de status da loja for acessada pelo servidor da Braspag não exibir o código de confirmação ou ocorrer uma falha na conexão, o servidor irá fazer mais 3 tentativas de envio.
- A URL de mudança de Status de Pagamento somente pode utilizar porta 80 (padrão para http) ou porta 443 (padrão para https).

Exemplo de XML:

```
<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. Método FraudAnalysisTransactionDetails

Este método deve ser utilizado para obter todas as infomações de analise de fraude referente a uma determinada transação.
O método **FraudAnalysisTransactionDetails** recebe um objeto **FraudAnalysisTransactionDetailsRequest** com as propriedades a seguir.

Tabela 3 - Propriedades do objeto FraudAnalysisTransactionDetailsRequest

Parâmetro	Tipo	Descrição	Obrigatório?
RequestId	Guid	Id do request da requisição.	Sim
MerchantId	Guid	Id da loja no antifraude a ser utilizada para a consulta.	Sim
AntiFraudTransactionId	Guid	Id da transação de antifraude a ser localizada.	Sim

4.3. Retorno do Método FraudAnalysisTransactionDetails

O método **FraudAnalysisTransactionDetails** retornará um objeto response com as propriedades abaixo:

Tabela 4 – Propriedade do objeto FraudAnalysisTransactionDetailsResponse

Parâmetro	Tipo	Tamanho	Descrição
CorrelatedId	Guid		Id que foi passado pelo request, apenas para identificação.
Success	Boolean		Flag que indica se a operação foi concluída com sucesso. NÃO indica erro.

ErrorReport [ErrorReportCollection]	List	0 - n	Lista de erros ocorridos durante o processamento. Consultar planilha de ErrorTypes.
ErrorReport.ErrorCode	Short		Código do erro.
ErrorReport.Message	String	MAX	Mensagem de erro.
AntiFraudMerchantId	Guid		Id da loja no antifraude.
AntiFraudTransactionId	Guid		Id da transação no antifraude.
AntiFraudTransactionStatusCode	Byte		Status da transação da análise de fraude. O mesmo pode sofrer alteração quando a transação é sondada ou notificada pela Cybersource a Braspag a mudança de status. Id do status da análise de fraude. Consultar tabela 5.29
AntiFraudReceiveDate	DateTime		Data em que a transação foi recebida pela Braspag.
AntiFraudStatusLastUpdateDate	DateTime		Data em que ocorreu a última atualização de status da transação.
AntiFraudAnalysisScore	Int		Score da análise de fraude.
BraspagTransactionId	Guid		Id da transação no Pagador(Braspag). Este campo somente é preenchido quando o tipo de fluxo executado for diferente de somente análise de fraude.
MerchantOrderId	String	1 - 50	Número do pedido da loja.
FraudAnalysisRequestParameter [FraudAnalysisRequestParameterCollection]	List		Lista de parâmetros enviados no request.
FraudAnalysisRequestParameter.FieldName	String	1 - 256	Nome do campo enviado no request.
FraudAnalysisRequestParameter.FieldValue	String	MAX	Valor do campo enviado no request.
FraudAnalysisResponseParameter [FraudAnalysisResponseParameterCollection]	List		Lista de parâmetros retornados pela análise de fraude.
FraudAnalysisResponseParameter.FieldName	String	1 - 256	Nome do campo retornado pela análise de fraude.
FraudAnalysisResponseParameter.FieldValue	String	MAX	Valor do campo retornado pela análise de fraude.
AntiFraudAcquirerConversionDate	Datetime		Data de alteração de status da transação quando a mesma foi analisada manualmente e teve seu status alterado na Cybersource ou sofreu alteração através da notificação da Cybersource a Braspag através do POST.
AntiFraudTransactionOriginalStatusCode	Byte		Status original da transação após a análise manual da transação na Cybersource. Este campo é retornado neste método quando a transação é sondada ou foi notificada na Braspag através do POST enviado pela Cybersource para a Braspag.

5. TABELAS DE DOMÍNIO

Tabela 5.1 – AntiFraudServiceType

Valor	Descrição
AnalyseOnly	Executa somente a análise de fraude.
AnalyseAndAuthorizeOnSuccess	O pedido de autorização será realizado somente se a análise de fraude obter sucesso.
AuthorizeAndAnalyseOnSuccess	Tenta autorizar a transação e em caso de sucesso, executa a análise de fraude.
AuthorizeAndAnalyseAlways	Tenta autorizar a transação e em caso de sucesso ou não, executa a análise de fraude.

Tabela 5.2 – Card

Valor	Descrição
Visa	Cartão Visa.
Mastercard	Cartão Mastercard.
AmericanExpress	Cartão American Express.
DInersClub	Cartão Diners Club.
VisaElectron	Cartão Visa Electron.
Elo	Cartão Elo.

Tabela 5.3 – Tender

Valor	Descrição
Consumer	Cartão de crédito pessoal.
Corporate	Cartão de crédito corpotativo.
Debit	Compra a débito.
Cod	Cobrença na entrega do produto.
Check	Cheque eletrônico.
P2P	Pagamento pessoa a pessoa.
Private1	Cartão de crédito private label.
Other	Outros meios de pagamento.

Tabela 5.4 – GiftCategory

Valor	Descrição
Yes	Em caso de divergência entre endereços de cobrança e entrega, marca com risco pequeno.
No	Em caso de divergência entre endereços de cobrança e entrega, marca com risco alto.
Off	Ignora a análise de risco para endereços divergentes.

Tabela 5.5 – HostHedge

Valor	Descrição
Low	Baixa importância do e-mail e endereço IP na análise de risco.
Normal	Média importância do e-mail e endereço IP na análise de risco.
High	Alta importância do e-mail e endereço IP na análise de risco.
Off	E-mail e endereço IP não afetam a análise de risco.

Tabela 5.6 – NonSensicalHedge

Valor	Descrição
Low	Baixa importância da verificação feita sobre o pedido do comprador, na análise de risco.
Normal	Média importância da verificação feita sobre o pedido do comprador, na análise de risco.
High	Alta importância da verificação feita sobre o pedido do comprador, na análise de risco.
Off	Verificação do pedido do comprador não afeta a análise de risco.

Tabela 5.7 – ObscenitiesHedge

Valor	Descrição
Low	Baixa importância da verificação sobre obscenidades do pedido do comprador, na análise de risco.
Normal	Média importância da verificação sobre obscenidades do pedido do comprador, na análise de risco.
High	Alta importância da verificação sobre obscenidades do pedido do comprador, na análise de risco.
Off	Verificação de obscenidade no pedido do comprador não afeta a análise de risco.

Tabela 5.8 – Passenger

Valor	Descrição
Adult	Passageiro adulto.
Child	Passageiro criança.
Infant	Passageiro infantil.
Youth	Passageiro adolescente.
Student	Passageiro estudante.
SeniorCitizen	Passageiro idoso.
Military	Passageiro militar.

Tabela 5.9 – PhoneHedge

Valor	Descrição
Low	Baixa importância nos testes realizados com números de telefone.
Normal	Média importância nos testes realizados com números de telefone.
High	Alta importância nos testes realizados com números de telefone.
Off	Testes de números de telefone não afetam a análise de risco.

Tabela 5.10 – Code

Valor	Descrição
AdultContent	Conteúdo adulto.
Coupon	Cupon de desconto.
Default	Opção padrão para análise na CyberSource quando nenhum outro valor é selecionado.
EletronicGood	Produto eletrônico.
EletronicSoftware	Softwares distribuídos eletronicamente via download.
GiftCertificate	Vale presente.
HandlingOnly	Taxa de instalação ou manuseio.
Service	Serviço.
ShippingAnd Handling	Frete e taxa de instalação ou manuseio.
ShippingOnly	Frete.
Subscription	Assinatura.

Tabela 5.11 – Risk

Valor	Descrição
Low	O produto tem um histórico de poucos chargebacks.
Normal	O produto tem um histórico de chargebacks considerado normal.
High	O produto tem um histórico de chargebacks acima da média.

Tabela 5.12 – TimeHedge

Valor	Descrição
Low	Baixa importância no horário do dia em que foi feita a compra, para a análise de risco.
Normal	Média importância no horário do dia em que foi feita a compra, para a análise de risco.
High	Alta importância no horário do dia em que foi feita a compra, para a análise de risco.

Off	O horário da compra não afeta a análise de risco.

Tabela 5.13 – VelocityHedge

Valor	Descrição
Low	Baixa importância no número de compras realizadas pelo cliente nos últimos 15 minutos.
Normal	Média importância no número de compras realizadas pelo cliente nos últimos 15 minutos.
High	Alta importância no número de compras realizadas pelo cliente nos últimos 15 minutos.
Off	A frequência de compras realizadas pelo cliente não afeta a análise de fraude.

Tabela 5.14 - Shipping Method

Valor	Descrição
SameDay	Serviço de entrega no mesmo dia.
OneDay	Serviço de entrega noturna ou no dia seguinte.
TwoDay	Serviço de entrega em dois dias.
ThreeDay	Serviço de entrega em três dias.
LowCost	Serviço de entrega de baixo custo.
Pickup	Produto retirado na loja.
Other	Outro método de entrega.
None	Sem serviço de entrega, pois é um serviço ou assinatura.

Tabela 5.15 - Customer Type

Valor	Descrição
CN	Comprador particular
CP	Comprador de negócios

Tabela 5.16- Type Flag

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

Tabela 5.17 - Type Routing

Valor	Descrição
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

Tabela 5.18 - Type Decision

Valor	Descrição
Accept	ACCEPT
Error	ERROR
Reject	REJECT
Review	REVIEW

Tabela 5.19 - Type of Evaluation of the Rule

Valor	Descrição
TRUE	T
FALSE	F
InsufficientData	N
Error	E

Tabela 5.20 – Reason Codes

Valor	Descrição
100	Operação bem sucedida.
101	O pedido está faltando um ou mais campos necessários. Possível ação: Veja os campos que estão faltando na lista AntiFraudResponse.MissingFieldCollection. Reenviar o pedido com a informação completa.
102	Um ou mais campos do pedido contêm dados inválidos. Possível ação: Veja os campos inválidos na lista AntiFraudResponse.InvalidFieldCollection. Reenviar o pedido com as informações corretas.
150	Falha no sistema geral. Possível ação: Aguarde alguns minutos e tente reenviar o pedido.
151	O pedido foi recebido, mas ocorreu time-out no servidor. Este erro não inclui time-out entre o cliente e o servidor. Possível ação: Aguarde alguns minutos e tente reenviar o pedido.
152	O pedido foi recebido, mas ocorreu time-out. Possível ação: Aguarde alguns minutos e reenviar o pedido.
202	CyberSource recusou o pedido porque o cartão expirou. Você também pode receber este código se a data de validade não coincidir com a data em arquivo do banco emissor. Se o processador de pagamento permite a emissão de créditos para cartões expirados, a CyberSource não limita essa funcionalidade. Possível ação: Solicite um cartão ou outra forma de pagamento.
231	O número da conta é inválido. Possível ação: Solicite um cartão ou outra forma de pagamento.
234	Há um problema com a configuração do comerciante na CyberSource. Possível ação: Não envie o pedido. Entre em contato com o Suporte ao Cliente para corrigir o problema de configuração.
400	A pontuação de fraude ultrapassa o seu limite. Possível ação: Reveja o pedido do cliente.
480	O pedido foi marcado para revisão pelo Gerenciador de Decisão.
481	O pedido foi rejeitado pelo Gerenciador de Decisão.

Tabela 5.21 - Address Information Codes

Valor	Descrição
COR-BA	O endereço de cobrança pode ser normalizado.
COR-SA	O endereço de entrega pode ser normalizado.
INTL-BA	O país de cobrança é fora dos U.S.
INTL-SA	O país de entrega é fora dos U.S.
MIL-USA	Este é um endereço militar nos U.S.
MM-A	Os endereços de cobrança e entrega usam nomes de ruas diferentes.
MM-BIN	O BIN do cartão (os seis primeiros dígitos do número) não corresponde ao país.
MM-C	Os endereços de cobrança e entrega usam cidades diferentes.
MM-CO	Os endereços de cobrança e entrega usam países diferentes.
MM-ST	Os endereços de cobrança e entrega usam estados diferentes.
MM-Z	Os endereços de cobrança e entrega usam códidos postais diferentes.
UNV-ADDR	O endereço é inverificável.

Tabela 5.22 - Risk Factor Codes

Valor	Descrição
A	Mudança de endereço excessiva. O cliente mudou o endereço de cobrança duas ou mais vezes nos últimos seis meses.
B	BIN do cartão ou autorização de risco. Os fatores de risco estão relacionados com BIN de cartão de crédito e/ou verificações de autorização do cartão.
C	Elevado números de cartões de créditos. O cliente tem usado mais de seis números de cartões de créditos nos últimos seis meses.
D	Impacto do endereço de e-mail. O cliente usa um provedor de e-mail gratuito ou o endereço de email é arriscado.
E	Lista positiva. O cliente está na sua lista positiva.
F	Lista negativa. O número da conta, endereço, endereço de e-mail ou endereço IP para este fim aparece sua lista negativa.
G	Inconsistências de geolocalização. O domínio do cliente de e-mail, número de telefone, endereço de cobrança, endereço de envio ou endereço IP é suspeito.
H	Excessivas mudanças de nome. O cliente mudou o nome duas ou mais vezes nos últimos seis meses.
I	Inconsistências de internet. O endereço IP e de domínio de e-mail não são consistentes com o endereço de cobrança.
N	Entrada sem sentido. O nome do cliente e os campos de endereço contém palavras sem sentido ou idioma.
O	Obscenidades. Dados do cliente contém palavras obscenas.
P	Identidade morphing. Vários valores de um elemento de identidade estão ligados a um valor de um elemento de identidade diferentes. Por exemplo, vários números de telefone estão ligados a um número de conta única.
Q	Inconsistências do telefone. O número de telefone do cliente é suspeito.
R	Ordem arriscada. A transação, o cliente e o lojista mostram informações correlacionadas de alto risco.
T	Cobertura Time. O cliente está a tentar uma compra fora do horário esperado.
U	Endereço não verificável. O endereço de cobrança ou de entrega não pode ser verificado.
V	Velocity. O número da conta foi usado muitas vezes nos últimos 15 minutos.
W	Marcado como suspeito. O endereço de cobrança ou de entrega é semelhante a um endereço previamente marcado como suspeito.
Y	O endereço, cidade, estado ou país dos endereços de cobrança e entrega não se correlacionam.
Z	Valor inválido. Como a solicitação contém um valor inesperado, um valor padrão foi substituído. Embora a transação ainda possa ser processada, examinar o pedido com cuidado para detectar anomalias.

Tabela 5.23 - Excessive Identity Changes

Valor	Descrição
MORPH-B	O mesmo endereço de cobrança tem sido utilizado várias vezes com identidades de clientes múltiplos.
MORPH-C	O mesmo número de conta tem sido utilizado várias vezes com identidades de clientes múltiplos.
MORPH-E	O mesmo endereço de e-mail tem sido utilizado várias vezes com identidades de clientes múltiplos.
MORPH-I	O mesmo endereço IP tem sido utilizado várias vezes com identidades de clientes múltiplos.
MORPH-P	O mesmo número de telefone tem sido usado várias vezes com identidades de clientes múltiplos.
MORPH-S	O mesmo endereço de entrega tem sido utilizado várias vezes com identidades de clientes múltiplos.

Tabela 5.24 - Internet Information Codes

Valor	Descrição
FREE-EM	O endereço de e-mail do cliente é de um provedor de e-mail gratuito.
INTL-IPCO	O país do endereço de e-mail do cliente é fora do U.S.
INV-EM	O endereço de e-mail do cliente é inválido.
MM-EMBCO	O domínio do endereço de e-mail do cliente não é consistente com o país do endereço de cobrança.
MM-IPBC	O endereço de e-mail do cliente não é consistente com a cidade do endereço de cobrança.
MM-IPBCO	O endereço de e-mail do cliente não é consistente com a país do endereço de cobrança.
MM-IPBST	O endereço IP do cliente não é consistente com o estado no endereço de cobrança. No entanto, este código de informação não pode ser devolvido quando a inconsistência é entre estados imediatamente adjacentes.
MM-IPEM	O endereço de e-mail do cliente não é consistente com o endereço IP.
RISK-EM	O domínio do e-mail do cliente (por exemplo, mail.example.com) está associada com alto risco.
UNV-NID	O endereço IP do cliente é de um proxy anônimo. Estas entidades escondem completamente informações sobre o endereço de IP.
UNV-RI400SK	O endereço IP é de origem de risco.
UNV-EMBCO	O país do endereço do cliente de e-mail não corresponde ao país do endereço de cobrança.

Tabela 5.25 - Customer Lists Information Codes

Valor	Descrição
CON-POSNEG	A ordem disparada bate tanto com a lista positiva e negativa. O resultado da lista positiva sobrescreve a lista negativa.
NEG-BA	O endereço de cobrança está na lista negativa.
NEG-BCO	O país de cobrança está na lista negativa.
NEG-BIN	O BIN do cartão de crédito (os seis primeiros dígitos do número do cartão) está na lista negativa.
NEG-BINCO	O país em que o cartão de crédito foi emitido está na lista negativa.
NEG-BZC	O código postal de cobrança está na lista negativa.

NEG-CC	O número de cartão de crédito está na lista negativa.
NEG-EM	O endereço de e-mail está na lista negativa.
NEG-EMCO	O país em que o endereço de e-mail está localizado na lista negativa.
NEG-EMDOM	O domínio de e-mail (por exemplo, mail.example.com) está na lista negativa.
NEG-FP	O device fingerprint está na lista negativa
NEG-HIST	A transação foi encontrada na lista negativa.
NEG-ID	ID da conta do cliente está na lista negativa.
NEG-IP	O endereço IP (por exemplo, 10.1.27.63) está na lista negativa.
NEG-IP3	O endereço IP de rede (por exemplo, 10.1.27) está na lista negativa. Um endereço de IP da rede inclui até 256 endereços IP.
NEG-IPCO	O país em que o endereço IP está localizado está na lista negativa.
NEG-PEM	Um endereço de e-mail do passageiro está na lista negativa.
NEG-PH	O número do telefone está na lista negativa.
NEG-PID	ID da conta do passageiro está na lista negativa.
NEG-PPH	O número do telefone do passageiro está na lista negativa.
NEG-SA	O endereço de entrega está na lista negativa.
NEG-SCO	O país de entrega está na lista negativa.
NEG-SZC	O código postal de entrega está na lista negativa.
POS-TEMP	O cliente está temporário na lista positiva.
POS-PERM	O cliente está permanente na lista positiva.
REV-BA	O endereço de cobrança esta na lista de revisão.
REV-BCO	O país de cobrança está na lista de revisão.
REV-BIN	O BIN do cartão de crédito (os seis primeiros dígitos do número do cartão) está na lista de revisão.
REV-BINCO	O país em que o cartão de crédito foi emitido está na lista de revisão.
REV-BZC	O código postal de cobrança está na lista de revisão.
REV-CC	O número do cartão de crédito está na lista de revisão.
REV-EM	O endereço de e-mail está na lista de revisão.
REV-EMCO	O país em que o endereço de e-mail está localizado está na lista de revisão.
REV-EMDOM	O domínio de e-mail (por exemplo, mail.example.com) está na lista de revisão.
REV-FP	O device fingerprint está na lista de revisão
REV-ID	ID da conta do cliente está na lista de revisão.

REV-IP	O endereço IP (por exemplo, 10.1.27.63) está na lista de revisão.
REV-IP3	O endereço IP de rede (por exemplo, 10.1.27) está na lista de revisão. Um endereço de IP da rede inclui até 256 endereços IP.
REV-IPCO	O país em que o endereço IP está localizado está na lista de revisão.
REV-PEM	Um endereço de e-mail do passageiro está na lista de revisão.
REV-PH	O número do telefone está na lista de revisão.
REV-PID	ID da conta do passageiro está na lista de revisão.
REV-PPH	O número do telefone do passageiro está na lista de revisão.
REV-SA	O endereço de entrega está na lista de revisão.
REV-SCO	O país de entrega está na lista de revisão.
REV-SZC	O código postal de entrega está na lista de revisão.

Tabela 5.26 - Phone Information Codes

Valor	Descrição
MM-ACBST	O número de telefone do cliente não é consistente com o estado no endereço de cobrança.
RISK-AC	O código de área do cliente está associado com risco alto.
RISK-PH	O número de telefone dos U.S. ou do Canadá é incompleta, ou uma ou mais partes do número são arriscadas.
TF-AC	O número do telefone utiliza um código de área toll-free.
UNV-AC	O código de área é inválido.
UNV-OC	O código de área e/ou o prefixo de telefone são/é inválido.
UNV-PH	O número do telefone é inválido.

Tabela 5.27 - Suspicious Data Information Codes

Valor	Descrição
BAD-FP	O dispositivo é arriscado.
INTL-BIN	O cartão de crédito foi emitido fora dos U.S.
MM-TZTLO	Fuso horário do dispositivo é incompatível com os fusos horários do país.
MUL-EM	O cliente tem usado mais de quatro endereços de email diferentes.
NON-BC	A cidade de cobrança é um desconhecida.
NON-FN	O primeiro nome do cliente é desconhecido.
NON-LN	O último nome do cliente é desconhecido.
OBS-BC	A cidade de cobrança contem obscenidades.
OBS-EM	O endereço de e-mail contem obscenidades.

RISK-AVS	O resultado do teste combinado AVS e endereço de cobrança normalizado são arriscados, o resultado AVS indica uma correspondência exata, mas o endereço de cobrança não é entrega normalizada.
RISK-BC	A cidade de cobrança possui caracteres repetidos.
RISK-BIN	No passado, este BIN do cartão de crédito (os seis primeiros dígitos do número do cartão) mostrou uma elevada incidência de fraude.
RISK-DEV	Algumas das características do dispositivo são arriscadas.
RISK-FN	Nome e sobrenome do cliente contêm combinações de letras improváveis.
RISK-LN	Nome do meio ou o sobrenome do cliente contém combinações de letras improváveis.
RISK-PIP	O endereço IP do proxy é arriscado.
RISK-SD	A inconsistência nos países de cobrança e entrega é arriscado.
RISK-TB	O dia e a hora da ordem associada ao endereço de cobrança é arriscado.
RISK-TIP	O verdadeiro endereço IP é arriscado.
RISK-TS	O dia e a hora da ordem associada ao endereço de entrega é arriscado.

Tabela 5.28 - Global Velocity Information Codes

Valor	Descrição
VEL-ADDR	Diferente estados de faturamento e/ou o envio (EUA e Canadá apenas) têm sido usadas várias vezes com o número do cartão de crédito e/ou endereço de email.
VEL-CC	Diferentes números de contas foram usados várias vezes com o mesmo nome ou endereço de email.
VEL-NAME	Diferentes nomes foram usados várias vezes com o número do cartão de crédito e / ou endereço de email.
VELS-CC	O número de conta tem sido utilizado várias vezes durante o intervalo de controle curto.
VELI-CC	O número de conta tem sido utilizado várias vezes durante o intervalo de controle médio.
VELL-CC	O número de conta tem sido utilizado várias vezes durante o intervalo de controle longo.
VELV-CC	O número de conta tem sido utilizado várias vezes durante o intervalo de controle muito longo.
VELS-EM	O endereço de e-mail tem sido utilizado várias vezes durante o intervalo de controle curto.
VELI-EM	O endereço de e-mail tem sido utilizado várias vezes durante o intervalo de controle médio.
VELL-EM	O endereço de e-mail tem sido utilizado várias vezes durante o intervalo de controle longo.
VELV-EM	O endereço de e-mail tem sido utilizado várias vezes durante o intervalo de controle muito longo.
VELS-FP	O device fingerprint tem sido utilizado várias vezes durante um intervalo curto
VELI-FP	O device fingerprint tem sido utilizado várias vezes durante um intervalo médio
VELL-FP	O device fingerprint tem sido utilizado várias vezes durante um intervalo longo
VELV-FP	O device fingerprint tem sido utilizado várias vezes durante um intervalo muito longo
VELS-IP	O endereço IP tem sido utilizado várias vezes durante o intervalo de controle curto.

VELI-IP	O endereço IP tem sido utilizado várias vezes durante o intervalo de controle médio.
VELL-IP	O endereço IP tem sido utilizado várias vezes durante o intervalo de controle longo.
VELV-IP	O endereço IP tem sido utilizado várias vezes durante o intervalo de controle muito longo.
VELS-SA	O endereço de entrega tem sido utilizado várias vezes durante o intervalo de controle curto.
VELI-SA	O endereço de entrega tem sido utilizado várias vezes durante o intervalo de controle médio.
VELL-SA	O endereço de entrega tem sido utilizado várias vezes durante o intervalo de controle longo.
VELV-SA	O endereço de entrega tem sido utilizado várias vezes durante o intervalo de controle muito longo.
VELS-TIP	O endereço IP verdadeiro tem sido utilizado várias vezes durante o intervalo de controle curto.
VELI-TIP	O endereço IP verdadeiro tem sido utilizado várias vezes durante o intervalo de controle médio.
VELL-TIP	O endereço IP verdadeiro tem sido utilizado várias vezes durante o intervalo de controle longo.

Tabela 5.29 – AntiFraudStatusCode

Código	Descrição
500	Started
501	Accept
502	Review
503	Reject
504	Pendent
505	Unfinished
506	Aborted

Tabela 5.30 – RequestStatusCode

Valor	Descrição
0	Falha no recebimento da requisição pela Ferramenta de Antifraude
1	Requisição enviada com sucesso para a Ferramenta do Antifraude, e está sendo processada.

Tabela 5.31 – RequestStatusDescription

Valor	Descrição
Fail	Falha no recebimento da requisição pela Ferramenta de Antifraude
Success	Requisição enviada com sucesso para a Ferramenta do Antifraude, e está sendo processada.

6. MAPA DE ERROS

Tabela 6.1 - Erros que podem ser gerados pelo webservice consumido pelo cliente.

Código	Descrição
101	Invalid object request or null.
102	Invalid merchant. Possibly is not registered in AntiFraude.
103	Undefined fraud analysis service credentiais or merchant is disabled.
104	Pagador merchant id is not registered.
105	The IP merchant is not allowed to access webservice.
106	Invalid sequence type.
107	RequestId was not specified
108	RequestId was not specified.
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.

Tabela 6.2 - Erros que podem ser gerados pelo Pagador e pelo serviço de Antifraude consumido pela Braspag.

Código	Descrição
301	Internal Error
302	Authorization denied

Tabela 6.3 - Erros comuns que podem ser gerados nas validações das propriedades das classes que compõem o request consumido pelo cliente.

Código	Descrição
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. ANEXO 1 – ADICIONANDO FINGERPRINT

Você precisará adicionar uma imagem de 1-pixel, que não é mostrada na tela, e 2 segmentos de código à tag <body> da sua página de checkout, se certificando que serão necessários de 10 segundos entre a execução do código e a submissão da página para o servidor.

 Se os 3 segmentos de código não forem colocados na página de checkout, seus resultados podem não ser precisos.

Colocando os Segmentos de Código

Coloque os segmentos de código imediatamente acima da tag </body> para garantir que a página Web será renderizada corretamente. Nunca adicione os segmentos de código em elementos HTML visíveis.
Os segmentos de código precisam ser carregados antes que o comprador finalize o pedido de compra, caso contrário um erro será gerado.

Substituindo as variáveis

Copie os trechos de código abaixo.
Em cada segmento, substitua as variáveis abaixo com os valores referentes à sua loja/pedido:

• **Domain**:
Testing - Use ***h.online-metrix.net***, que é o DNS do servidor de fingerprint, como apresentado no exemplo de HTML abaixo;

Production - Altere o domínio para uma URL local, e configure seu servidor Web para redirecionar esta URL para ***h.online-metrix.net***.

• ***<org ID>*:** Para obter esse valor entre em contato com a Braspag
• ***<merchant ID>*:** Para obter esse valor entre em contato com a Braspag
• ***<session ID>*:** Use o mesmo valor passado no parametro "***DeviceFingerprintID***", do serviço de requisição de análise de fraude.

Certifique-se de copiar todos os dados corretamente e de remover os sinais de tag (<>) ao substituir as variáveis.

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="">
```

Exemplo:

```
<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>
```

Exemplo:
<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>

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

Configurando seu Servidor Web

Se você não completar essa seção, você não receberá resultados corretos, e o domínio (url) do fornecedor ficará visível, sendo mais provável que seu consumidor o bloqueie.

Na seção "Substituindo as Variáveis" (Domain), todos os objetos se referem a h.online-metrix.net,que é o DNS do servidor de fingerprint. Quando você estiver pronto para produção, você deve alterar o nome do servidor para uma URL local, e configurar no seu servidor Web um redirecionamento de URL para h.online-metrix.net.