Release Documentation

PAYWATCH

OnlineBanking

FPaaS

Versão: 01.00

Data: 2018-11-29

Estado: Final

Classificação: Restrito

Referência: DCSIBS180370

ISO 9001
ISO 20000
BUREAU VERITAS
Certification

Certificação no âmbito dos serviços AT2, SEPA e SWIFT

SIBS Forward Payment Solutions, S.A.
Rua Soeiro Pereira Gomes, Lote 1, 1649-031 LISBOA, PORTUGAL
Telefone: +351-217 813 000 / Fax: +351- 217 935 755

Ficha Técnica

Referência:	DCSIBS180370
Título do Documento:	PAYWATCH Online Banking (FPaaS)
Versão:	01.00
Estado:	Final
Classificação:	Restrito
Tipo de Documento:	Release Documentation
Área Funcional Responsável:	AF Controlo de Fraude

Documentos Relacionados

Referência	Título	Origem
n.a.		

Revisões

Versão	Data	Descrição	Autor
01.00	2018-11-29	Criação do documento	AF Controlo de Fraude

Índice

Índice de Figuras

Índice de Tabelas

1 Introdução

A SIBS FPS disponibiliza para os canais e-banking (*homebanking*), m-banking (*mobilebanking*) e t-banking (banca telefónica) dos Bancos, um serviço de prevenção e deteção de fraude da PAYWATCH num modelo *as-a-service* (*Fraud Prevention as-a-Service*, FPaaS). O Modelo é suportado numa plataforma tecnológica sustentada em algoritmos de *machine learning*, adaptados especificamente à deteção de fraude com recurso ao *profiling* de clientes e contas, endereçando de modo transversal tipologias de fraude em canais não presenciais.

A PAYWATCH, suportada na sua plataforma e nas suas equipas dedicadas, realiza a análise de risco através do *screening* em *real time* das transações efetuadas nos canais o*nlinebanking* acima referidos, permitindo ao Banco, no âmbito da Diretiva Europeia de Serviços de Pagamento (PSD2), poder isentar transações de autenticação forte (*Strong Customer Authetication,* SCA).

A PAYWATCH disponibiliza serviços opcionais e complementares ao serviço base, nomeadamente a investigação de casos de fraude, contacto ao cliente final para despiste de fraude e respostas a reclamações operacionais do cliente.

No presente documento é efetuada uma apresentação minuciosa do serviço e são descritos de forma detalhada os requisitos necessários para utilização do serviço pelos Bancos.

1.1 Âmbito do Serviço

O serviço de deteção e prevenção de fraude para o canal *onlinebanking* disponibilizado pela PAYWATCH contempla:

1) em *real time*, o *screening* das transações, devolvendo um *score* de risco tendo em conta o *profiling* do cliente/conta, assim como uma sugestão de avanço ou recusa da transação tendo em conta entidades comprometidas, exemplo contas mulas (ver mais detalhes no Arquitetura Funcional);
2) em *near real time*, a identificação de transações suspeitas de fraude que o Banco deverá analisar e dar *feedback* na plataforma confirmando ou não a ocorrência de fraude (ver mais detalhes na Arquitetura Funcional);
3) o acesso à plataforma, com o transacional do o*nlinebanking* do Banco, os alertas gerados com transações suspeitas de fraude, com os *dashboards* de gestão e com o acesso a listas de sugestão de bloqueio (entidades comprometidas) ou listas de sugestão de isenção (entidades para as quais o Banco pretende fazer um *bypass* ao *score* de risco) (ver mais detalhes no Arquitetura Funcional);
4) comités de gestão do serviço e comité de administração do serviço, a reunir anualmente; e comité de coordenação técnica do serviço, a reunir trimestralmente (ver mais detalhe no Modelo de Governance).

O Modelo analítico de risco é propriedade intelectual da SIBS, sendo elaborado com *inputs* fundamentais do Banco, pelo que não há previsão de partilha de risco/penalizações decorrentes da não deteção de fraude pelo Modelo.

1.1.1 Tipos de Fraude

A deteção de fraude no âmbito do serviço, está focada em ataques do tipo *account takeover*, *Man-in-the-Browser* (MiB) e *Man-in-the-App* (MiA).

Para este tipo de fraudes, os criminosos comumente têm recorrido às seguintes estratégias:

1. Ataques de engenharia social:
    - Roubo de credenciais
    - Execução de transações ilícitas (ex. pagamentos de serviços)
    - Execução de pedidos (cartões, cheques, etc)
    - Alteração de dados críticos (nº de tlm, etc)
    - Instalação de *malware*
    - Instalação de *bogus apps*
2. Ataques por *malware*:
    - Roubo de credenciais
    - Execução de transações ilícitas
    - Execução de pedidos (cartões, cheques, etc)
    - Alteração de dados críticos (nº de tlm, etc)
3. Ataques de compromisso:
    - SIM swapping
    - Desvio de SMS
    - Interceção de SMS
4. *Mobile app reverse engineering*:
    - Roubo de credenciais
    - Execução de transações ilícitas
    - Execução de pedidos (cartões, cheques, etc)
    - Alteração de dados críticos (nº de tlm, etc)

A PAYWATCH monitoriza as estratégias acima listadas através de desvios comportamentais.

1.1.2 Tipos de Operações

A deteção de fraude no âmbito do serviço está focada na monitorização de operações financeiras e de operações não financeiras. Importa referir que, ao abrigo deste serviço, a monitorização de dados de sessão está focada nos *logins* e respetivo desvio comportamental. Não contempla a deteção de *malware* no dispositivo do cliente, ainda que a análise comportamental permita recolher indícios deste tipo de situações.

1.2 PSD2

Um dos objetivos da *PSD2* consiste em tornar os pagamentos mais seguros, para tal os acessos às contas, os pagamentos *online*, e todas as operações nos canais remotos que possam implicar risco de fraude, necessitam de S*trong Customer Authentication*, SCA. Assim, é necessário obter dois de três fatores de autenticação:

- Algo que sei (*knowledge*)**:** *passwords* estáticas, PIN, *user*
- Algo que tenho (*ownership*): OTP, *token*, *smart card*, dispositivo
- Algo que sei (*inherence*)**:** *biometric*, ex. impressão digital

A SCA é obrigatória para todas as operações, no entanto existem algumas exceções, das quais se destacam:

- Transações de baixo valor: pagamentos remotos até 30€ (com limite de 100€ ou 5 pagamentos)
- Operações *contactless* até 50€ (com limite de 100€ ou 5 pagamentos)
- Operações em "*unnatended terminals*" como Via Verde ou parques de estacionamento
- Operações para destinatários certificados (*trusted beneficiary*)
- Operações em que o destinatário e ordenante são a mesma entidade
- Operações recorrentes/periódicas – aplicável na primeira e isento nas seguintes
- Operações de empresas, feitas em canais dedicados automáticos (FTP/SIBS, terminal bancário, etc.), desde que a autoridade nacional certifique estes canais e esteja de acordo com o seu nível de segurança
- Consulta de saldos e movimentos, depois do consentimento, no máximo de 90 dias

Estão também excecionadas operações do Banco sempre que este mantenha níveis de fraude abaixo do determinado pelos *Regulatory Technical Standards on Strong Costumer Authentication and Common and Secure Communication*, *RTS*. Estas variáveis que condicionam o tipo de autenticação requerida, das quais são exemplo o valor do pagamento, o número e montantes acumulados e o tempo decorrido desde a última autenticação forte para o tipo de transação, são variáveis que não serão controladas pelo Modelo matemático, devendo ser controladas pelo Banco de acordo com o nível de risco que o mesmo quer assumir.

O Banco pode ajustar o tipo de autenticação tendo em conta o risco da operação, a PAYWATCH analisa o risco das transações permitindo ao Banco adaptar o tipo de autenticação que pretende aplicar à transação, podendo no limite isentar as transações de baixo risco de autenticação forte. Com este serviço, o Banco pode melhorar a experiência de utilização do cliente nos canais de *onlinebanking* e evita possíveis impactos da imagem, de custos de recuperação de fundos ou de perda de clientes num cenário de fraude.

2 Apresentação do Serviço

2.1 Arquitetura Funcional

A figura seguinte ilustra os fluxos de informação e as atividades previstas no contexto do serviço proposto.

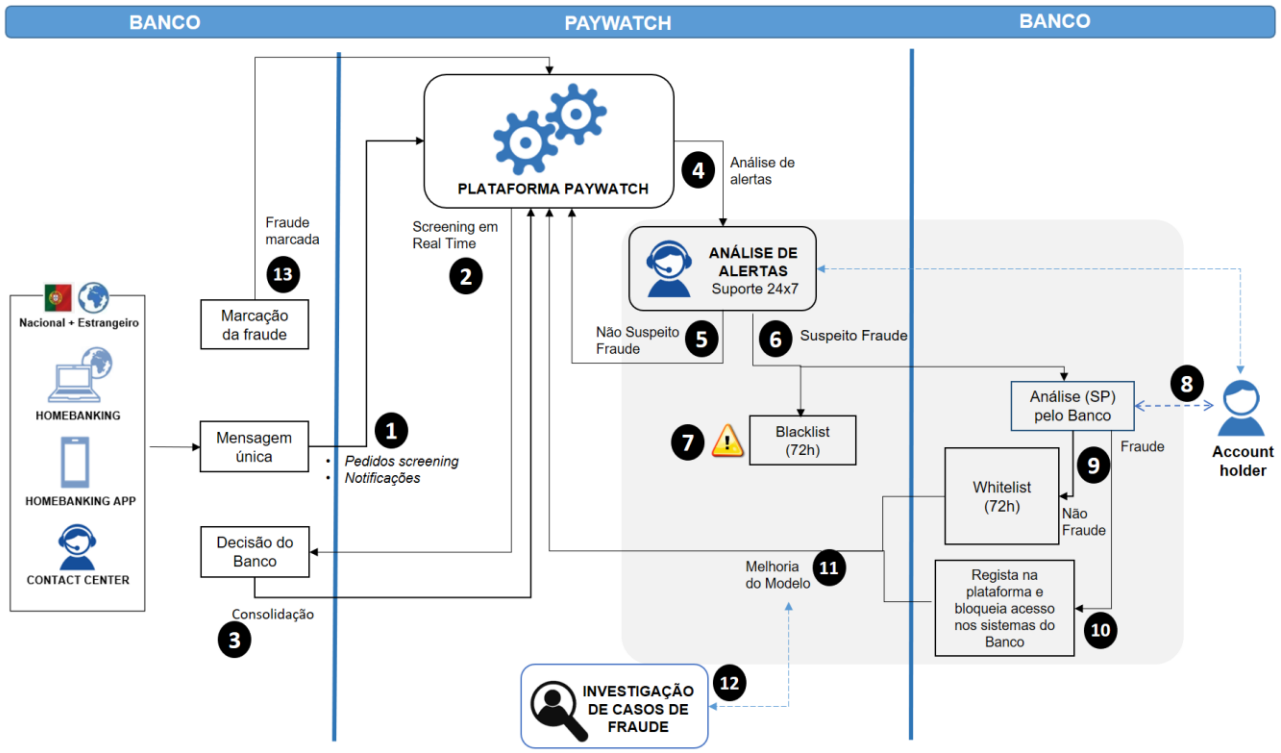

Figura 1 - Fluxos de Informação e Atividades

No contexto da PAYWATCH, devem ser observadas as responsabilidades operacionais que se encontram detalhadas na tabela seguinte:

Tabela 1 - Responsabilidades Operacionais (*Real Time*)

ID	Real Time / Near Real Time	TÓPICO	DESCRIÇÃO
1	**REAL TIME**	Pedido de *screening* / notificações	Pedido de escrutínio automatizado das operações submetidas pelo Banco à PAYWATCH. Para efetuar a análise de risco, a SIBS sugere que o Banco envie para a plataforma de deteção de fraude as transações das seguintes tipologias: ▪ Tentativas *login*; ▪ Transações financeiras; ▪ Consultas; ▪ Ativação e cancelamento de produtos e serviços; ▪ Gestão de informação de cliente. <u>Notificação</u> Caso o Banco não pretenda uma análise de risco para determinada transação, mas considere que a informação é relevante para influenciar a modelação, então esta informação é enviada como notificação (posteriormente e não em *real time*)
2		Resposta ao pedido de *screening*	Através do *screening* das transações dos canais referidos efetuadas nos *backends* aplicacionais do Banco, a PAYWATCH devolve em *real time*: ▪ Um *score* de risco de fraude (de 0 a 999); ▪ Uma sugestão de *go*/*no-go* da operação; ▪ Informação sobre o nome da regra preponderante; Se a transação não der *hit* positivo numa lista, envia-se o nome da regra preponderante para o cálculo do *score* da transação. No caso da transação dar *hit* positivo numa lista, envia-se o nome da regra (lista) preponderante.
3		Decisão do Banco / Consolidação	Sobre o trinómio enviado ao Banco, este através do sistema de processamento dos canais à distância deve decidir se: ▪ Aceita a realização da operação sem mais nenhuma diligência; ▪ Bloqueia a realização da operação; ▪ Solicita autenticação adicional para permitir a realização da operação. Para tal o Banco terá de desenvolver uma matriz adaptativa em que poderá parametrizar tendo em conta a resposta da SIBS qual o tipo de autenticação a aplicar. <u>Consolidação</u> Após a transação se realizar, o Banco deve enviar à PAYWATCH a consolidação da transação com informação do tipo de autenticação e do estado da mesma. Esta informação é necessária para manter atualizados os dados de contexto de operação que são utilizados pela plataforma para medir o risco de fraude. Assim como é através da mensagem de consolidação que a PAYWATCH sabe qual o nível de autenticação que o Banco escolheu e qual o estado da mesma, informação muito relevante para o modelo de deteção de fraude e *reporting*.

Tabela 2 - Responsabilidades Operacionais (*Near Real Time*)

ID	RT/NRT	TÓPICO	DESCRIÇÃO
4	**NEAR REAL TIME**	Análise de alertas	O output do *screening* de fraude de uma transação pode gerar alertas que serão alvo de análise detalhada, de forma a despistar a fraude e identificar os falsos positivos (análise de caso). Os analistas da SIBS terão acesso a toda a informação relevante para a validação do caso. Nos casos em que, após análise, se conclua que existem elevados indícios de fraude, a PAYWATCH envia o caso às equipas do Banco para contacto com o cliente, despiste da situação e confirmação na plataforma do resultado dessa indagação. Do mesmo modo, a informação que é enviada à PAYWATCH via notificação, pode gerar alertas e tem procedimento semelhante.
5		Alertas não suspeitos de fraude	Quando é emitido alerta que se verifica não ser suspeito de fraude, o alerta é fechado e o modelo é atualizado com essa informação.
6, 7, 8		Alertas suspeitos de fraude	Quando é emitido alerta de fraude, a conta associada é colocada temporariamente (durante 72h) numa *blacklist* da plataforma de deteção de fraude. O Banco, na plataforma, deve gerir este alerta e deve contactar o titular/utilizador do serviço associado à operação para validar se a operação foi efetivamente desencadeada por este e com os dados recebidos pelo Banco. Este contacto também pode ser assegurado pela SIBS (no âmbito dos serviços adicionais)
9, 10		*Whitelists* e *Blacklists* na PAYWATCH	O Banco deve aplicar na plataforma medidas de contenção de fraude. O serviço prevê a colocação de listas de sugestão de bloqueio (*blacklists*) ou de aceitação sem condições (*whitelist*) de transações. Com base nas listas referidas é possível, ao Banco, colocar condições de aceitação ou de recusa no *screening* das transações, em função das características das mesmas. Cada vez que uma condição de uma *blacklist* é cumprida a PAYWATCH responde ao *screening* de fraude com uma sugestão de recusa, sobrepondo-se esta avaliação ao resultado do modelo. Paralelamente, cada vez que uma condição de uma *whitelist* é cumprida, responde ao *screening* de fraude com uma sugestão de avançar, sobrepondo-se também esta avaliação ao resultado do modelo. Note-se que a *whitelist* prevalece sobre a *blacklist*. Está disponível na plataforma o carregamentos de entidades nas listas individualmente ou em *bulk*/lote.
11		Melhoria do Modelo	A melhoria do Modelo de deteção de fraude é realizada através da consolidação na ferramenta de deteção de fraude da seguinte informação: ▪ Desfecho de realização das operações; ▪ Confirmação da ocorrência ou não de fraude nos casos assinalados como alertas; ▪ Os casos de fraude que sejam do conhecimento do Banco e que tenham sido detetados de forma independente da plataforma de deteção de fraude; ▪ Eventuais anomalias observadas nas respostas da plataforma de deteção de fraude. A melhoria também acontece através da incorporação no modelo de regras/situações para modelar, como novos ou emergentes padrões de fraude, ou situações específicas para as quais importe melhorar a acuidade da deteção e reduzir taxas de falsos positivos. Estas melhorias são desencadeadas com base em vários inputs, como: ▪ Casos de fraude detetados de forma reativa; ▪ Padrões de fraude apurados em investigação; ▪ Padrões de fraude divulgados em fóruns específicos; ▪ Análise da eficácia e eficiência da plataforma de deteção de fraude; ▪ Re-treino do algoritmo preditivo com a) mais informação que contém novos padrões de fraude e por isso melhor eficácia de modelo e b) menor intervalo de tempo entre marcação e treino, que promove um maior número de re-treinos do modelo, havendo uma aprendizagem mais rápida e uma resposta mais eficaz aos padrões emergentes de fraude. À parte de outros contactos pontuais que possam existir, o comité de coordenação técnica do serviço é o fórum adequado para discutir melhorias em regras e no modelo de deteção de fraude.

ID	RT/NRT	TÓPICO	DESCRIÇÃO
12		Investigação de casos de fraudes (serviço adicional)	Internamente ao Banco ou como serviços adicionais da PAYWATCH, pode haver casos de (potencial) fraude que carecem de uma investigação mais detalhada. Na investigação devem ser reunidos elementos (como registos de operações, registos de segurança e declarações/reclamações de clientes), que devem ser avaliados para tentar determinar se: ▪ Houve fraude ou trata-se de situação que não prefigura fraude? ▪ Quem é o agente originador da situação? ▪ Houve incúria ou utilização negligente de elementos por parte de interveniente na operação que tenha contribuído de forma determinante para a fraude? ▪ Qual o método utilizado para a realização da fraude? ▪ Quais os impactos (financeiros ou outros) da fraude? ▪ Qual a total dimensão da fraude?

Tabela 3 - Responsabilidades Operacionais (*à posteriori*)

ID	RT/NRT	TÓPICO	DESCRIÇÃO
13	**EM BULK**	Marcação da fraude	Na plataforma, o Banco consegue marcar/identificar a fraude (transação a transação), para consolidar as operações como fraudulentas.

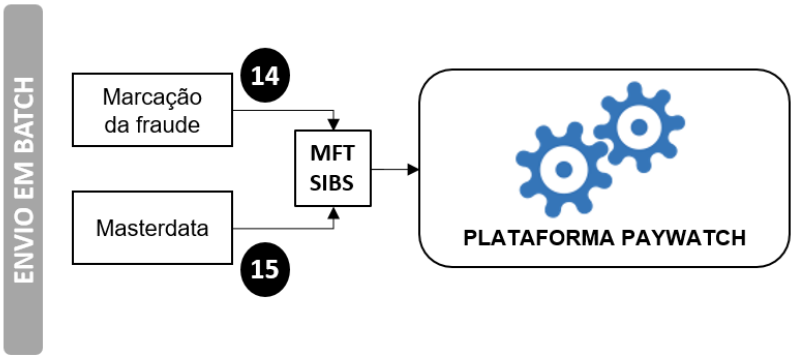

Figura 2 - Marcação de Fraude e *Masterdata*

No contexto da marcação de fraude e *masterdata*, devem ser observadas as responsabilidades operacionais que se encontram detalhadas na tabela seguinte.

Tabela 4 - Marcação de Fraude e *Masterdata*

ID	RT/NRT	TÓPICO	DESCRIÇÃO
14	**Em BULK**	Marcação da fraude	Adicionalmente à marcação de fraude transação a transação diretamente na plataforma, o Banco deve periodicamente ir enviando à PAYWATCH ficheiros de fraude marcada para consolidar as operações como fraudulentas. Esta consolidação faz-se por via de envio de ficheiro MFT com a transação ou transações fraudulentas marcadas.
15		*Masterdata*	Para contemplar alguma da informação de ordenante solicitada na transação, o Banco deve enviar ficheiros com esta informação. Esta consolidação faz-se por via envio de ficheiro MFT.

2.2 Arranque do Serviço

A abordagem da PAYWATCH baseia-se no arranque sem migração de histórico do Banco. Nesta fase de *setup* inicial, sugere-se que o Banco partilhe cinco ou seis casos de maior fraude conhecidos do último ano, de modo a simular no Modelo regras de deteção desses *modus operandi*.

À medida que for existindo histórico com fraude marcada, esse histórico vai ser utilizado como *input* para afinação de regras e para as atividades de *advanced analytics*/*machine learning*, promovendo a melhoria contínua do modelo.

No âmbito do *set-up* do serviço, os casos de fraude partilhados com a PAYWATCH deverão incluir histórico recente do cliente que contenha operações genuínas e operações fraudulentas. Para cada transação deve constar:

- Data/Hora;
- Conta;
- Montante;
- Tipo Operação;
- Tipo Autenticação;
- IP;
- Informação do *device*;
- Tipo de fraude.

2.3 Evolução do Modelo de Deteção e Prevenção de Fraude

Conforme já referido, à medida que for existindo histórico com fraude marcada, as capacidades analíticas do serviço vão evoluir. A informação histórica vai ser continuamente utilizada como *input* para afinação de regras e, quando configurar um *data set* significativo, será a base para as atividades de *advanced analytics*/ *machine learning*.

A abordagem baseada em *machine learning* consiste no estudo de modelos matemáticos, que a plataforma de deteção de fraude utilizará para progressivamente melhorar a sua *performance*. Os algoritmos de *machine learning* constroem um modelo matemático baseado em dados de treino (dados históricos com indicação das transações fraudulentas) de forma a efetuar previsões e decisões sem ser explicitamente programado para efetuar a tarefa.

Devido ao aumento de informação disponível, e do poder computacional para lidar com a mesma, esta abordagem é hoje uma realidade consumada na indústria de pagamentos. Especificamente para estas atividades, a PAYWATCH utilizará *frameworks* e tecnologia com resultados comprovados.

2.4 Casos Práticos de Análise de Risco de Operações

A análise de risco das operações do canal o*nlinebanking* é realizada pela PAYWATCH através de modelos sustentados em algoritmos de *machine learning*, adaptados especificamente para a deteção de fraude recorrendo a *profiling* de cliente e conta. Para o *profiling* de cliente e conta, não havendo histórico comportamental, o início do produto e serviço baseia-se numa ótica conservadora, através de regras de gestão de risco. Pelo que, sempre que a atividade se afaste ainda que ligeiramente de um padrão considerado normal, poderá ter como consequência um *score* elevado.

Tendo em conta o *output* de *screening* (trinómio: *score*; sugestão *go/no go*; nome da regra preponderante), o Banco deve adaptar a sua matriz de autenticação à operação, definindo assim os limites de *score* baixo ou *score* elevado.

2.4.1 Transação com *score* baixo e com entidade (IBAN) em *blacklist*, exemplo:

- A transação possui o mesmo par IP+User Agent, que foi utilizado numa transação anterior e que já foi alvo de SCA;
- O montante está dentro do seu padrão de gastos da conta;
- O IBAN está numa *blacklist*, o valor de *score* mantem-se, mas a sugestão é de NO GO.

  - Nesta situação o Banco deverá parametrizar o tipo de autenticação tendo em conta o nível de risco a assumir – *score* baixo, mas aquela entidade (IBAN) está numa lista de sugestão de bloqueio

2.4.2 Transação com *score* alto e com entidade (IBAN) em *whitelist*, exemplo:

- O *Device Fingerprint* nunca foi utilizado numa transação anterior da conta;
- A conta tem histórico de ser acedida sempre com o mesmo *Device Fingerprint*;
- O montante ou o ritmo de operações não está enquadrado com o padrão de utilização da conta;
- O IBAN está numa lista de *bypass*, o valor de *score* mantem-se, mas a sugestão é de GO.

  - Nesta situação o Banco deverá parametrizar o tipo de autenticação tendo em conta o nível de risco a assumir – *score* alto, mas aquela entidade (IBAN) está numa lista de sugestão de *bypass*.

2.5 Modelo de *Governance*

Para a gestão do serviço, a PAYWATCH define duas estruturas organizativas de coordenação, formadas por elementos do Banco e da PAYWATCH com responsabilidades bem delineadas: o Comité de Administração do Serviço e o Comité de Coordenação Técnica do Serviço.

Este modelo organizativo pode, naturalmente, ser revisto durante a prestação do serviço e a decisão de eventuais alterações cabe precisamente a uma das estruturas definidas (Comité de Administração do Serviço). Descrevem-se de seguida as estruturas definidas, no que respeita a funções, intervenientes, responsabilidades e periodicidade de reuniões.

2.5.1 Comité de Administração do Serviço

Funções

- Análise da qualidade geral do serviço, no período acordado para o efeito;
- Aprovação dos entregáveis no contexto da prestação do serviço;
- Decisão sobre os momentos de *deployment* das evoluções/desenvolvimentos a efetuar;
- Decisão de revisão de indicadores ("níveis de serviço" e "tarifário") em função das propostas analisadas em sede de Comité de Coordenação Técnica do Serviço;
- Análise da estratégia futura da prestação do serviço (médio/longo prazo);
- Análise da evolução futura do contrato (evolução do serviço/contrato);
- Aprovação das alterações ao Modelo de Gestão do Contrato.

Intervenientes

- Diretores das áreas envolvidas de ambas as instituições;
- Responsáveis pelo serviço de ambas as instituições.

Resultados

- Planeamento de macro ações e *next steps*;
- Aprovação de alterações aos "níveis de serviço" e "tarifário".

Periodicidade

- Este Comité deve reunir com uma periodicidade anual;
- Quando necessário, o Comité pode reunir fora deste calendário, desde que acordado entre as Partes.

2.5.2 Comité de Coordenação Técnica do Serviço

Funções

- Acompanhamento da prestação do serviço e avaliação da atividade no período (ex.: último trimestre ou desde o último Comité de Coordenação Técnica do Serviço);
- Análise dos níveis de serviço e da faturação para os meses em causa;
- Análise da adequabilidade da "configuração do serviço contratado", "níveis de serviço" e "tarifário";
- Análise de eventuais necessidades de evolução e/ou customização dos modelos de deteção e prevenção de fraude;
- Resolução de problemas/questões genéricas e outros assuntos relacionados com a prestação;
- Análise da prestação do serviço, no que diz respeito à *performance*, qualidade e acuidade dos modelos de deteção e prevenção de fraude;
- Avaliação dos principais eventos e problemas, e discussão das ações que deverão ser tomadas para evitar a repetição dos mesmos;
- Definição, prioritização, calendarização e acompanhamento de eventuais pedidos de alteração/ evolução;
- Avaliação do impacto, ao nível tecnológico, das alterações/evoluções propostas;
- Emissão de pareceres tecnológicos e acompanhamento da implementação de alterações/ evoluções;
- Identificação e propostas de melhoria do serviço.

Intervenientes

- Responsáveis pelo serviço de ambas as Instituições (Gestor de Serviços);
- Quando necessário, responsáveis das equipas técnico-operacionais de ambas as Partes.

Resultados

- Aprovação da inclusão de alterações/evoluções, bem como do serviço ou plataforma;
- Sugestão de alterações a "configuração contratada", "níveis de serviço" e "tarifário";
- Produção/aprovação de relatórios de acompanhamento do serviço;
- Acompanhamento da gestão do serviço e análise da execução do serviço prestado.

Periodicidade

- Este Comité deve reunir com uma periodicidade trimestral;
- Quando necessário e perante necessidade justificada, o Comité pode reunir fora deste calendário, desde que acordado entre as Partes.

2.6 Níveis de Serviço

A PAYWATCH compromete-se a garantir os seguintes níveis de qualidade:

- SLA 1: 95% dos pedidos de *screening* com *report* em menos de 200ms para níveis de carga até X transações por segundo. Onde X é um valor que tem de ser definido com base em informação a fornecer pelo Banco relativamente a: (i) estatística de volume de operações por período de tempo e (ii) valores de pico de transações.
    - Este SLA cobre o serviço de *screening* de fraude das operações dos serviços à distância do Banco (Multicanal).
- SLA 2: 99,5 % de *uptime* da plataforma que suporta o *screening* de operações, emissão de alertas, gestão de listas de contenção/aceitação sem condições e marcação de fraude.
    - Este SLA cobre os serviços, de *screening* de fraude das operações dos serviços à distância do Banco (Multicanal); alertas e tratamento de casos de fraude; disponibilização de plataforma para aplicação de medidas de contenção de fraude; e revisão e melhoria do modelo de deteção de fraude.
- SLA 3: 95% de alertas com análise iniciada em menos de 30 minutos.
    - Este SLA cobre o serviço de alertas e tratamento de casos de fraude.
- SLA 4: envio de relatório mensal. Até ao 10º dia útil de cada mês.
    - Este SLA cobre o serviço de r*eporting*.

2.7 Serviços Adicionais

Os serviços que não estejam contemplados neste documento, deverão ser avaliados e ficam sujeitos a propostas comerciais específicas. São exemplos disso, a investigação de casos de contacto ao cliente final para despiste de fraude e respostas a reclamações operacionais do cliente.

3 Solução Técnica

Os serviços no âmbito da presente oferta, serão disponibilizados com base no sistema de deteção e prevenção de fraude que a PAYWATCH adotou em todos os meios de pagamento por si geridos. Esta solução caracteriza-se por permitir que os modelos sejam desenvolvidos de forma célere e disponibilizados de uma forma simples e sem impacto no serviço. Este aspeto é fundamental uma vez que os *fraudsters* estão constantemente a explorar fragilidades e a desenvolver novos esquemas de fraude.

Em traços gerais, a solução destaca-se por:

- Permitir autonomia na criação de modelos de prevenção de fraude. As ferramentas de simulação/análise/modelização são nativas da solução, sendo possível gerar modelos de prevenção de fraude eficientes, sem exigir dependência de terceiros;
- Disponibilizar capacidades de *machine learning* e geração automática de modelos;
- Suportar a operação de diferentes grupos de entidades e de utilizadores, a partir de uma única instalação da aplicação;
- Ter desempenho elevado, em tempo real, com capacidade de processamento de milhares de transações por segundo, com latências de milissegundos;
- Apresentar uma disponibilidade elevada (alcançada pela arquitetura de várias instâncias);
- Ter certificação PCI PA-DSS 3.2;
- Permitir a gestão de casos, com desenho flexível de fluxos em função da tipologia de alertas gerados.

3.1 Ambientes Aplicacionais

A SIBS FPS disponibiliza um conjunto de ambientes aplicacionais, com diferentes propósitos, que permitem evoluções estruturais da solução de forma gradual, controlada, garantido a qualidade final do produto.

- Ambiente de Desenvolvimento – Ambiente disponível apenas à equipa de sistemas/fraude da SIBS FPS, onde são efetuados os desenvolvimentos, testes unitários e testes integrados das componentes da estrita responsabilidade da SIBS PFS;
- Ambiente de Certificação/Aceitação – Ambiente utilizado para realização dos testes de aceitação com as diversas entidades que desejem integrar com a solução de deteção de fraude disponibilizado pela SIBS FPS;
- Ambiente de Modelização – Ambiente dedicado à realização de ensaios a possíveis modelos de deteção de fraude, sem que este exercício cause entropia ou sobre esforço nos ambientes de suporte a produção;
- Ambiente de Produção – Ambiente responsável pela monitorização, *screening* de fraude, gestão de alertas e *case management* dos sistemas de processamento em ambiente produtivo.

Desta forma é assegurada uma segregação entre ambientes, levando a que os dados de produção estejam estritamente limitados aos repositórios necessários, e os acessos das equipas técnicas estejam segregados de forma a cumprir o princípio de “Necessidade de Saber” (*Kneed to Know*).

3.2 Arquitetura Técnica

A arquitetura implementada pela SIBS FPS consiste num *cluster* distribuído entre os seus dois centros de processamento de dados (Lisboa e Viseu) com quatro nós (dois em cada centro). Desta forma são atingidos elevados níveis de resiliência, através da redundância local e regional, suportado em dois centros com elevados níveis de disponibilidade.

Os *links* atualmente existentes entre os centros de processamento de dados do Banco e a SIBS FPS, *links* que atualmente constituem a extranet bancária, são suficientes para suportar este serviço, quer em termos de largura de banda quer em termos de latência (ordem de grandeza das dezenas de milissegundos). Estas ligações são contratadas diretamente pelo Banco aos operadores de comunicações, pelo que a disponibilização destes serviços está fora do âmbito da presente oferta. A proteção dos dados que fluem nestas redes é assegurada pelo protocolo IPSEC, garantindo assim a confidencialidade e integridade dos dados em trânsito.

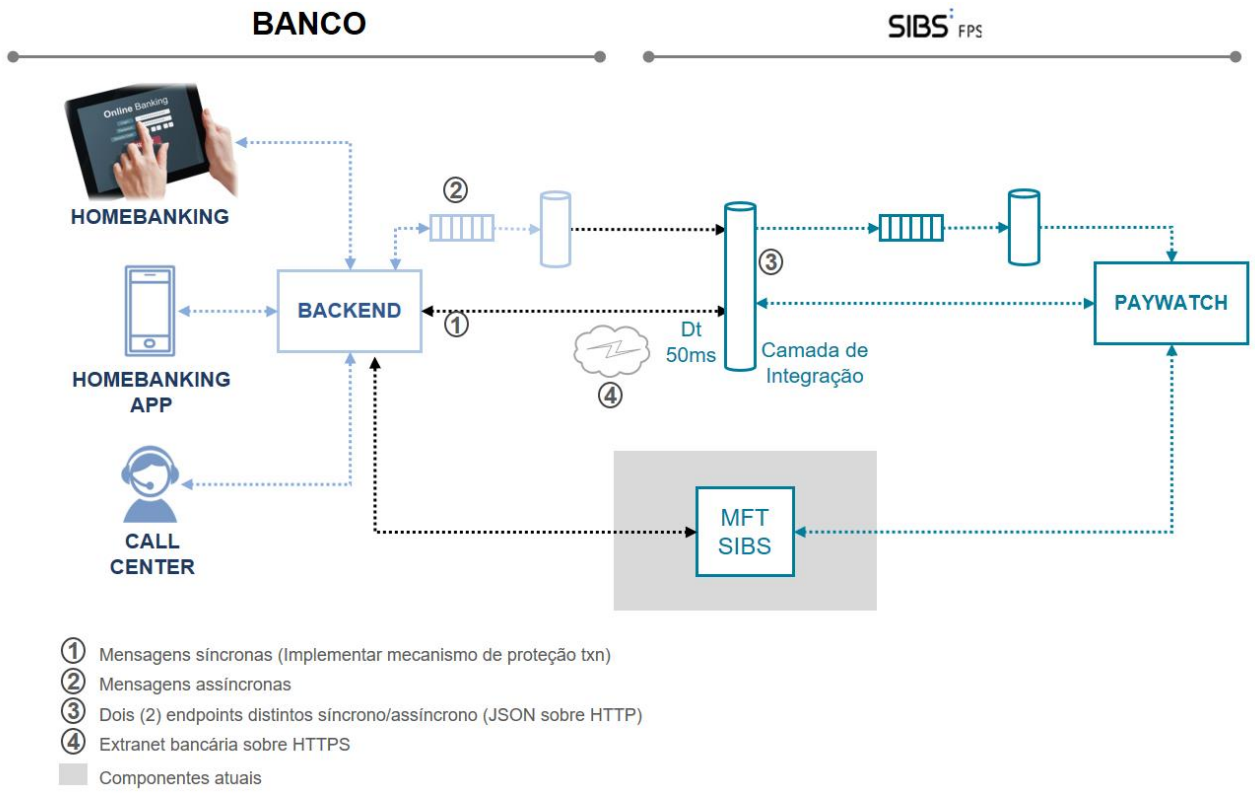

Figura 3 - Implementação de Sistemas

Para efeitos de integração entre o Banco e a solução de deteção de fraude disponibilizada pela SIBS FPS devem ser considerados os seguintes pressupostos:

1. Integração síncrona para efeitos de *screening* de fraude
    - Por este canal devem ser submetidas todas as transações sobre as quais o Banco pretenda atuar e por tal considere relevante obtenção de um *scoring* de fraude em *realtime*;
    - Sobre estas devem ser implementados, por parte do Banco, mecanismos configuráveis de *timeout* e de escusa na ida à solução de fraude, como forma de precaver a perda de serviço em contexto de intervenção programada ou problemas na plataforma de *screening* de fraude que resultem no compromisso do serviço.
2. Integração assíncrona
    - Por este canal devem ser submetidas todas as transações relevantes para a correta prestação do serviço de monitorização de fraude. Nestas incluem-se a informação complementar às transações enviadas em 1) assim como todas as transações não notificadas em 1) mas mesmo assim relevantes para uma correta monitorização do serviço;
    - O Banco deve assegurar um mecanismo de *queueing* que garanta o volume transacional de um dia, por forma a assegurar que as notificações são sempre entregues à plataforma de *screening* de fraude (isto assegura a manutenção de todo o histórico transacional, mesmo em período de *Outage* da plataforma).
3. As mensagens serão trocadas debaixo do protocolo de comunicação HTTPS com certificado *server-side* emitido por CA independente (MULTICERT) e *client-side* emitido pela SIBS.
4. Para definição da mensagem será usado o standard JSON com o principal propósito de reduzir o *payload* das mesmas.
5. A SIBS FPS disponibilizará um *endpoint* em Lisboa e outro *endpoint* em Viseu para que o Banco possa usar de acordo com as suas necessidades de serviço, sendo que deve assegurar como premissa que transações que sejam compostas por *screening realtime* (1) e notificação (2), o par deve ser entregue no mesmo *endpoint*. Abaixo identificação dos diversos *endpoints* disponíveis:
    - PRD:
      Real time: paywatch.site1.sibs.pt/onlinebanking/screening
      Assíncrono: paywatch.site1.sibs.pt/onlinebanking/notif
      Real time: paywatch.site2.sibs.pt/onlinebanking/screening
      Assíncrono: paywatch.site2.sibs.pt/onlinebanking/notif
    - QLY:
      Real time: paywatch.qly.site1.sibs.pt/onlinebanking/screening
      Assíncrono: paywatch.qly.site1.sibs.pt/onlinebanking/notif
      Real time: paywatch.qly.site2.sibs.pt/onlinebanking/screening
      Assíncrono: paywatch.qly.site2.sibs.pt/onlinebanking/notif

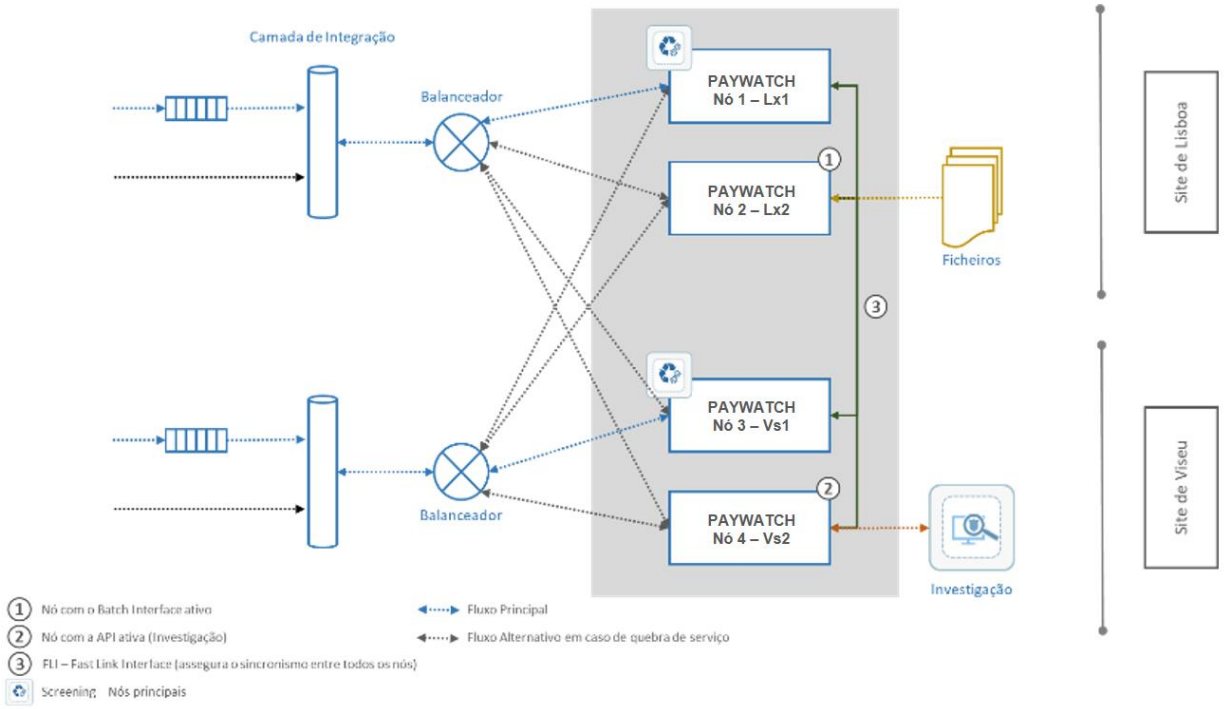

Figura 4 - Arquitetura da Solução

Os desenvolvimentos necessários nas plataformas do Banco, para viabilizar a implementação do projeto, estão fora do âmbito dos serviços disponibilizados pela PAYWATCH. Estes serão da responsabilidade das equipas do Banco.

3.3 Estrutura da Mensagem

As plataformas do Banco enviam mensagens com os atributos associados a cada transação. Como resposta às mensagens enviadas, a plataforma da PAYWATCH devolve uma mensagem com o resultado do *screening* de fraude.

As funções que se detalham abaixo são responsabilidade da entidade externa subscritora do serviço:

- Invocação do serviço de Fraude para *screening* e/ou apenas para envio de informação consolidada, para as transações que assim entender, via mensagem;
- Envio das mensagens no formato JSON com os campos identificados através das tags Plain XML definidas previamente;
- Disponibilização dos campos de acordo com as dimensões e formatos identificados nas respetivas interfaces.

3.3.1 Pedidos de *screening* e notificações/consolidação

A tabela abaixo identifica os atributos base a disponibilizar quer na mensagem de pedido de *screening* (frau.011) quer na mensagem de envio de informação consolidada/notificação (frau.012), assim como a sua representação e o respetivo *path* na mensagem:

Tabela 5 - Atributos a disponibilizar nas mensagens

Atributo	Tag	Representação	Path[1]	Descrição
Institutional Code	InstitutionalCode	Max5Numeric	.../Cntxt/InstnData/Id/Id	Código identificativo da instituição. No âmbito homebanking é código do Banco tal como é identificado no Banco de Portugal.
Operation Code	OperationCode	Max6Text	.../Tx/TxId/OprtnCd	Código identificativo da operação de acordo com a nomenclatura do subscritor do serviço.
Fraud Operation Code	FraudOperationCode	Max2Text	.../Tx/TxDtls/FrdOprtnCd	Código interno à plataforma da PAYWATCH, identificativo da operação. (ver lista de valores em Fraud Operation Codes).
External Transaction Token	ExternalTransactionToken	Max50Text	.../Tx/TxId/ExtrnlTxTkn	Identificação única da operação do ponto de vista do subscritor do serviço.
External Original Transaction Token	ExternalOriginalTransactionToken	Max50Text	.../Tx/TxId/ExtrnlOrgnlTxTkn	Identificador único da primeira operação de um conjunto de várias operações, do ponto de vista de uma instituição externa.
Originator User Name	UserName	Max100Text	.../Envt/OrgntrClnt/Usr/Nm	Nome de utilizador ordenante da operação.
Originator Alias Name	AliasName	Max150Text	.../Envt/OrgntrClnt/Als/AlsNm	Identificador alternativo do ordenante da operação.
Originator Client Identification	ClientID	Max35Text	.../Envt/OrgntrClnt/PrsnlInfrmtn/Id	Identificação do ordenante da operação.
Originator Client Token	ClientToken	Max20Text	.../Envt/OrgntrClnt/PrsnlInfrmtn/IdTkn	Token identificativo do cliente ordenante na visão corporativa.
Originator Name	OriginatorName	Max70Text	.../Envt/OrgntrClnt/PrsnlInfrmtn/Nm	Nome identificativo do ordenante da operação.
Originator Address Line	ClientOriginatorBillingAddress	Max70Text	.../Envt/OrgntrClnt/PrsnlInfrmtn/PstAdr/Adr	Morada do ordenante da operação.
Originator Country	OriginatorCountryISOAlpha2	Exact2Text	.../Envt/OrgntrClnt/PrsnlInfrmtn/PstAdr/Ctry	País do ordenante da operação no formato ISO 3166, Alpha-2 code (ex: Portugal – PT)
Originator Birth Date	OriginatorBirthDate	ISODate	.../Envt/OrgntrClnt/PrsnlInfrmtn/BrthDt	Data de nacimento do ordenante da transação no formato YYYY-MM-DD.
Originator Birth Country	OriginatorBirthCountryISOAlpha2	Exact2Text	.../Envt/OrgntrClnt/PrsnlInfrmtn/CtryOfBrth	País de nascimento do ordenante da operação no formato ISO 3166, Alpha-2 code (ex: Portugal – PT).
Originator IBAN	OriginatorIBAN	Max34Text	.../Cntxt/OrgntrData/Acct/IBAN	IBAN do ordenante da operação.
Originator BIC	OriginatorBankBIC	Max11Text	.../Cntxt/OrgntrData/Acct/BIC	BIC do ordenante da operação.

[1] Se pedido de screening substituir "…/" por "FrdOnlnBnkgVldtnReq1/". Se consolidada substituir "…/" por "FrdOnlnBnkgCnsldtdNtfctn/".

Atributo	Tag	Representação	Path[1]	Descrição
Business Type	BusinessType	Max2Text	.../Tx/TxDtls/Biztp	Identificaçao o tipo de cliente ordenante (1º byte) e destinatário (2º byte). Cada byte pode ter os seguintes valores possíveis: C – Cliente Particular B – Business (cliente corporativo) _ - Sem indicação (ex: para uma transação entre um Cliente Particular e um Cliente Corporativo, é esperado o valor CB)
Originator User Type	UserType	Max1Text	.../Envt/OrgntrClnt/Usr/tp	Identifica que tipo de utilizador é o ordenante: V – Virtual R – Real
Originator Device Identification	DeviceID	Max35Text	.../Cntxt/OrgntrData/Device/Id	Identificação do *device* do ordenante da operação.
Originator Device UID	UniversallyUniqueID	Max64Text	.../Cntxt/OrgntrData/Device/UnqIdntfr	Identificador universal único do *device* do ordenante da operação.
Originator Device OS	TerminalOperatingSystem	Max35Text	.../Cntxt/OrgntrData/Device/OSNm	Identificação do sistema operativo do *device* do ordenante da operação.
Originator Device Browser	DeviceBrowser	Max35Text	.../Cntxt/OrgntrData/Device/Brwsr	Identificação do browser do *device* do ordenante da operação.
Originator Device User Agent	UserAgent	Max254Text	.../Cntxt/OrgntrData/Device/UsrAgnt	Agente utilizador do *device* do ordenante da operação.
Originator Device IP Address	TerminalIPAddress	Max24Text	.../Cntxt/OrgntrData/Device/IPAdr	Endereço IP do *device* do ordenante da operação.
Originator Device Fingerprint	TerminalFingerprint	Max64Text	.../Cntxt/OrgntrData/Device/Fgrprnt	Fingerprint do *browser/device* do ordenante da operação.
Originator Device Timezone	OriginatorDeviceTimeZone	Max4Text	.../Cntxt/OrgntrData/Device/TmZn	Timezone do *device* do ordenante da operação, em minutos e acompanhado do respetivo sinal (ex: -060)
Originator Device Language	OriginatorDeviceLanguage	Max5Text	.../Cntxt/OrgntrData/Device/Lang	Idioma do *device* do ordenante da operação de acordo com a norma ISO 639-1 (ex: en-US, en-UK)
Originator Application Language	ApplicationLanguage	Max5Text	.../Cntxt/OrgntrData/App/Lang	Idioma da aplicação do ordenante da operação de acordo com a norma ISO 639-1 (ex: en-US, en-UK)
Originator Device Latitude	TerminalDeviceLatitude	Max10Text	.../Cntxt/OrgntrData/Device/GLctn/Lttd	Latitude do *device* do ordenante da operação, em graus no formato decimal e acompanhada do respetivo sinal (ex: 38.7166700).
Originator Device Longitude	TerminalDeviceLongitude	Max11Text	.../Cntxt/OrgntrData/Device/GLctn/Lngtd	Longitude do *device* do ordenante da operação, em graus no formato decimal e acompanhada do respetivo sinal (ex: -9.1333300).
Originator Device Rooted Indicator	OriginatorDeviceRootedIndicator	Booleano	.../Cntxt/OrgntrData/Device/RtdInd	Indica se o *device* do ordenante está *rooted/jailbroken*: 0 – Não 1 – Sim
Originator Device Charging Indicator	OriginatorDeviceChargingIndicator	Booleano	.../Cntxt/OrgntrData/Device/ChrggInd	Indica se o *device* do ordenante está em carregamento: 0 – Não 1 – Sim
Originator Device Inclination	OriginatorDeviceInclination	Max4Text	.../Cntxt/OrgntrData/Device/InclntnIndica	Inclinação do *device* do ordenante da operação, em graus e acompanhado do respetivo sinal.

Atributo	Tag	Representação	Path[1]	Descrição
Originator Device Malware Indicator	OriginatorDeviceMalwareIndicator	Booleano	.../Cntxt/OrgntrData/Device/MlwrInd	Indica se foi detetado *malware* no *device* do ordenante da operação: 0 – Não 1 – Sim
Beneficiary User Name	BeneficiaryUserName	Max100Text	.../Envt/BnfcryClnt/Usr/Nm	Nome de utilizador do beneficiário da operação.
Beneficiary Alias Name	RecipientAliasName	Max150Text	.../Envt/BnfcryClnt/Als/AlsNm	Identificador alternativo do beneficiário da operação.
Beneficiary Client Identification	BeneficiaryClientID	Max35Text	.../Envt/BnfcryClnt/PrsnlInfrmtn/Id	Identificação do destinatário da operação.
Beneficiary Client Token	BeneficiaryClientToken	Max20Text	.../Envt/BnfcryClnt/PrsnlInfrmtn/IdTkn	Token identificativo do cliente beneficiário para o subscritor do serviço de Fraude.
Beneficiary Name	Beneficiary Name	Max70Text	.../Envt/BnfcryClnt/PrsnlInfrmtn/Nm	Nome identificativo do beneficiário da operação.
Beneficiary Address Line	ClientBeneficiaryShippingAddress	Max70Text	.../Envt/BnfcryClnt/PrsnlInfrmtn/PstAdr/Adr	Morada do destinatário da operação.
Beneficiary Country	BeneficiaryCountryISOAlpha2	Exact2Text	.../Envt/BnfcryClnt/PrsnlInfrmtn/PstAdr/Ctry	País do beneficiário da operação no formato ISO 3166, Alpha-2 code (ex: Portugal – PT)
Beneficiary Birth Date	BeneficiaryBirthDate	ISODate	.../Envt/BnfcryClnt/PrsnlInfrmtn/BrthDt	Data de nacimento do beneficiário da transação no formato YYYY-MM-DD.
Beneficiary Birth Country	BeneficiaryBirthCountryISOAlpha2	Exact2Text	.../Envt/BnfcryClnt/PrsnlInfrmtn/CtryOfBrth	País de nascimento do beneficiário da operação no formato ISO 3166, Alpha-2 code.
Beneficiary IBAN	BeneficiaryIBAN	Max34Text	.../Cntxt/BnfcryData/Acct/IBAN	IBAN do destinatário da operação.
Beneficiary BIC	BeneficiaryBankBIC	Max11Text	.../Cntxt/BnfcryData/Acct/BIC	BIC do destinatário da operação.
Beneficiary Device Identification	BeneficiaryDeviceID	Max35Text	.../Cntxt/BnfcryData/Device/Id	Identificação do *device* do beneficiário da operação.
Beneficiary Device UID	BeneficiaryUniversalllyUniqueID	Max64Text	.../Cntxt/BnfcryData/Device/UnqIdntfr	Identificador universal único do *device* do beneficiário da operação.
Beneficiary Device OS	BeneficiaryTerminalOperatingSystem	Max35Text	.../Cntxt/BnfcryData/Device/OSNm	Identificação do sistema operativo do *device* do beneficiário da operação.
Beneficiary Device Browser	BeneficiaryDeviceBrowser	Max35Text	.../Cntxt/BnfcryData/Device/Brwsr	Identificação do browser do *device* do beneficiário da operação.
Beneficiary Device User Agent	BeneficiaryUserAgent	Max254Text	.../Cntxt/BnfcryData/Device/UsrAgnt	Agente utilizador do *device* do beneficiário da operação.
Beneficiary Device IP Address	BeneficiaryTerminalIPAddress	Max24Text	.../Cntxt/BnfcryData/Device/IPAdr	Endereço IP do *device* do beneficiário da operação.
Beneficiary Device Fingerprint	BeneficiaryTerminalFingerprint	Max64Text	.../Cntxt/BnfcryData/Device/Fgrprnt	Fingerprint do *browser/device* do beneficiário da operação.
Beneficiary Device Timezone	BeneficiaryDeviceTimeZone	Max4Text	.../Cntxt/BnfcryData/Device/TmZn	Timezone do *device* do beneficiário da operação, em minutos e acompanhado do sinal.
Beneficiary Device Language	BeneficiaryDeviceLanguage	Max5Text	.../Cntxt/BnfcryData/Device/Lang	Idioma do *device* do beneficiário da operação, de acordo com a norma ISO 639-1 (ex: en-US, en-UK).
Beneficiary Application Language	BeneficiaryApplicationLanguage	Max5Text	.../Cntxt/BnfcryData/App/Lang	Idioma da aplicação do beneficiário da operação, de acordo com a norma ISO 639-1 (ex: en-US, en-UK).
Beneficiary Device Latitude	BeneficiaryTerminalDeviceLatitude	Max10Text	.../Cntxt/BnfcryData/Device/GLctn/Lttd	Latitude do *device* do beneficiário da operação.

Atributo	Tag	Representação	Path[1]	Descrição
Beneficiary Device Longitude	BeneficiaryTerminalDeviceLongitude	Max11Text	.../Cntxt/BnfcryData/Device/GLctn/Lngtd	Longitude do *device* do beneficiário da operação.
Beneficiary Device Rooted Indicator	BeneficiaryDeviceRootedIndicator	Booleano	.../Cntxt/BnfcryData/Device/RtdInd	Indica se o *device* do beneficiário está *rooted/jailbroken*: 0 – Não 1 - Sim
Beneficiary Device Charging Indicator	BeneficiaryDeviceChargingIndicator	Booleano	.../Cntxt/BnfcryData/Device/PwrStts	Indica se o *device* do beneficiário está em carregamento: 0 – Não 1 – Sim
Beneficiary Device Inclination	BeneficiaryDeviceInclination	Max4Text	.../Cntxt/BnfcryData/Device/Inclntn	Inclinação do *device* do beneficiário da operação, em graus.
Beneficiary Device Malware Indicator	BeneficiaryDeviceMalwareIndicator	Booleano	.../Cntxt/BnfcryData/Device/MlwrInd	Indica se foi detetado *malware* no *device* do beneficiário da operação: 0 – Não 1 – Sim
Channel Selected Type	ChannelSelectedType	Max2Numeric	.../Cntxt/ChanlSlctdtp	Código identificativo do sub-canal de aceitação: 10 – Homebanking 11 – Mobile Banking 12 – Phone Banking
Session Identification	SessionIdentification	Max32Text	.../Cntxt/SssnId	Identificação da sessão em que estão a ser executadas as operações.
Transaction Datetime	TransactionDateTime	Timestamp	.../Tx/TxId/TxDtTm	Data/hora da operação no formato 'YYYY-MM-DD HH:MM:SS'.
Transaction Local Datetime	TerminalDatetime	Timestamp	.../Tx/TxId/TermnlDtTm	Data/hora da operação no timezone local, no formato 'YYYY-MM-DD HH:MM:SS'.
Operation Amount	OperationAmount	Decimal (fractionDigits: 5; totalDigits: 18)	.../Tx/TxDtls/TtlAmt	Montante da operação. Número de unidades monetárias especificadas numa moeda conforme a ISO4217 e em que o separador decimal é o ponto.
Operation Currency	TransactionCurrencyISONumber3	Exact3Numeric	.../Tx/TxDtls/CcyNmbr	Moeda da operação (ex: Euro – 978)
Local Operation Amount	OriginalTransactionAmount	Decimal (fractionDigits: 5; totalDigits: 18)	.../Tx/TxDtls/POITtlAmt	Montante da operação na moeda original. Número de unidades monetárias especificadas numa moeda conforme a ISO4217 e em que o separador decimal é o ponto.
Local Operation Currency	TerminalCurrencyISONumber3	Exact3NumericText	.../Tx/TxDtls/POICcyNmbr	Moeda original da operação (ex: Euro – 978)
PAN	PAN	Max23Text	.../Cntxt/OrgntrData/Crd/PAN	Primary Account Number associado à operação.
Token PAN	TokenPAN	Max23Text	.../Cntxt/OrgntrData/Crd/TknPAN	Token Primary Account Number associado à operação.
PAN Expiry Date	CardExpiryDate	Max10Text	.../Cntxt/OrgntrData/Crd/XpryDt	Data de expiração do PAN associado à operação no formato YYYYMM.
Token PAN Expiry Date	TokenPANExpiryDate	Max10Text	.../Cntxt/OrgntrData/Crd/TknPANXpryDt	Data de expiração do Token PAN associado à operação no formato YYYYMM.
Current Account Balance	CurrentBalance	Decimal (fractionDigits: 2; totalDigits: 9)	.../Tx/TxRst/Bal/CrrntBal	Saldo atual da conta. Número de unidades monetárias especificadas numa moeda conforme a ISO4217 e em que o separador decimal é o ponto.

Atributo	Tag	Representação	Path[1]	Descrição
Account Currency	AccountCurrencyISONumber3	Exact3Numeric	.../Cntxt/OrgntrData/Acct/Ccy	Identificação da moeda associada à conta (ex: Euro – 978).
Preparation User	PreparationUser	Max100Text	.../Envt/OrgntrClnt/Usr/PrprtnUsrNm	Utilizador que iniciou a operação.
User Signatures Required Counter	UserSignaturesRequiredCounter	Max2Numeric	.../Envt/OrgntrClnt/Usr/PrprtnUsrNm	Número de utilizadores necessários para a execução da operação.
Corporate Client Identification	CorporateClientID	Max35Text	.../Envt/OrgntrClnt/CrprtClntId	Identificação corporativa do cliente.
Payment Entity	PaymentEntityCode	Max7Numeric	.../Envt/PaymentEntity/Id/Id	Identificação da entidade de pagamentos.
Payment Entity Reference	PaymentEntityReferenceCode	Max15Numeric	.../Envt/PaymentEntity/PmtRef	Identificação da referência de pagamentos.
Trusted Beneficiary Indicator	TrustedBeneficiaryIndicator	Booleano	.../Envt/BnfcryClnt/TrstdBnfcryInd	Indica se o beneficiário foi identificado como de confiança pelo cliente, dispensando autenticação forte nas transações seguintes: 0 – Não 1 – Sim
Recurring Operation Indicator	RecurringOperationIndicator	Booleano	.../Tx/TxDtls/RcrrgTxInd	Indica se a operação é recorrente: 0 – Não 1 – Sim
To Self Operation Indicator	ToSelfOperationIndicator	Booleano	.../Tx/TxDtls/ToSlfOprtnInd	Indica se a operação é intra-património ou entre contas do cliente: 0 – Não 1 – Sim
User Authentication Method	UserAuthenticationMethod	Max4Text	.../Envt/OrgntrClnt/Usr/Authntcntp	Método de autenticação do utilizador (ver lista de valores User Authentication Method). Aplica-se até 4 metodos de autenticação do utilizador. Por exemplo se o utilizador utilizar os métodos “Password” e “OTP SMS” deverá ser formatado com ‘PS ‘.
Authentication Attempts Counter	AuthenticationAttemptsCounter	Max2Numeric	.../Tx/TxRst/AuthntcnAttmptsCntr	Número de tentativas de autenticação do utilizador.
Strong Customer Authentication Indicator	TransactionSCAIndicator	Booleano	.../Tx/TxDtls/SCAInd	Identifica se foi realizada uma autenticação forte: 0 – Não 1 – Sim
Transaction Description for Beneficiary	BeneficiaryTransactionDescription	Max35Text	.../Cntxt/OrgntrData/TxRltd/ToBnfcryDsc	Descrição do movimento a enviar para o beneficiário.
Transaction Description for Originator	OriginatorTransactionDescription	Max35Text	.../Cntxt/OrgntrData/TxRltd/ToOrgntrDsc	Descrição do movimento para o ordenante.
External Fraud Transaction Score	ExternalFraudTransactionScore	Max3Numeric	.../Prprtry/PrprtryExtrnlFrdRslt/TxScr	*Scoring* devolvido por uma entidade externa de gestão de fraude.
External Fraud Rule Name	ExternalFraudRuleName	Max35Text	.../Prprtry/PrprtryExtrnlFrdRslt/RlNm	Designação da regra aplicada na obtenção do *scoring*, pela entidade externa de gestão de fraude.
External Fraud Refused Indicator	ExternalFraudTransactionRefusedIndicator	Booleano	.../Prprtry/PrprtryExtrnlFrdRslt/TxRfsdInd	Resultado da avaliação do potencial de fraude da transação, pela entidade externa de gestão de fraude: 0 – Go 1 – No Go

Atributo	Tag	Representação	Path[1]	Descrição
Response Status Code	ResponseStatusCode	Max4Text	.../Tx/TxRst/RspnSttsCd	Código identificativo do estado da resposta (ver lista de valores Response Status Code).
Response Reason Code	ResponseReasonCode	Max4Text	.../Tx/TxRst/RspnRsnCd	Código de resposta (ver lista de valores Response Reason Code).
User Certificate Presence Indicator	UserCertificatePresenceIndicator	Booleano	.../Envt/OrgntrClnt/Usr/CertPrsncInd	Indica se foi utilizado um certificado digital na autenticação do utilizador.

3.3.2 Resposta ao pedido de *screening*

A tabela abaixo identifica os atributos disponibilizados na mensagem de resposta ao pedido de *screening* (frau.002)

Tabela 6 - Atributos disponibilizados na mensagem resposta ao *screening*

Atributo	Tag	Representação	Path	Descrição
Fraud Transaction Refused Indicator	FraudTransactionRefusedIndicator	Booleano	FrdVldtnRspnsOtpt/RspnData/TxRfsdInd	Indica se do ponto de vista da Fraude a transação deve ou não ser aceite: 0 – No Go 1 – Go
Fraud Transaction Score	FraudTransactionScore	Max3Numeric	FrdVldtnRspnsOtpt/RspnData/TxScr	Corresponde ao scoring de fraude da transação.
Fraud Rule Name	FraudRuleName	Max35Text	FrdVldtnRspnsOtpt/RspnData/RlNm	Identificação da regra aplicada na obtenção do scoring.
Fraud Response Datetime	FraudResponseDateTime	ISODateTime	FrdVldtnRspnsOtpt/RspnData/RspnDttm	Data/hora de resposta ao pedido de screening (no formato 'YYYY-MM-DD HH:MM:SS').

3.3.3 Validação de Mensagens

Os campos seguem uma matriz de validação, em que tendo em conta o campo e a natureza da transação o campo é mandatório ou opcional.

Tabela 7 - Matriz de validação dos campos

Atributo	Login	Transferências	Pagamentos com Referencia	Pagamentos Serviços/Compras	Operações Financeiras	Outras Operações
Institutional Code	**M**	**M**	**M**	**M**	**M**	**M**
Operation Code	**M**	**M**	**M**	**M**	**M**	**M**
Fraud Operation Code	**M**	**M**	**M**	**M**	**M**	**M**
External Transaction Token	**M**	**M**	**M**	**M**	**M**	**M**
External Original Transaction Token	**O**	**O**	**O**	**O**	**O**	**O**
Originator User Name	**M**	**M**	**M**	**M**	**M**	**M**
Originator Alias Name	**O**	**O**	**O**	**O**	**O**	**O**
Originator Client Identification	**M**	**M**	**M**	**M**	**M**	**M**
Originator Client Token	**O**	**O**	**O**	**O**	**O**	**O**
Originator Name	**O**	**M**	**O**	**O**	**O**	**O**

Atributo	Login	Transferências	Pagamentos com Referencia	Pagamentos Serviços/Compras	Operações Financeiras	Outras Operações
Originator Address Line	O	O	O	O	O	O
Originator Country	O	O	O	O	O	O
Originator Birth Date	O	O	O	O	O	O
Originator Birth Country	O	O	O	O	O	O
Originator IBAN	O	M	M	M	M	O
Originator BIC	O	O	O	O	O	O
Business Type	M	M	M	M	M	M
Originator User Type	O	O	O	O	O	O
Originator Device Identification	O	O	O	O	O	O
Originator Device UID	O	O	O	O	O	O
Originator Device OS	O	O	O	O	O	O
Originator Device Browser	O	O	O	O	O	O
Originator Device User Agent	O	O	O	O	O	O
Originator Device IP Address	O	O	O	O	O	O
Originator Device Fingerprint	O	O	O	O	O	O
Originator Device Timezone	O	O	O	O	O	O
Originator Device Language	O	O	O	O	O	O
Originator Application Language	O	O	O	O	O	O
Originator Device Latitude	O	O	O	O	O	O
Originator Device Longitude	O	O	O	O	O	O
Originator Device Rooted Indicator	O	O	O	O	O	O
Originator Device Charging Indicator	O	O	O	O	O	O
Originator Device Inclination	O	O	O	O	O	O
Originator Device Malware Indicator	O	O	O	O	O	O
Beneficiary User Name	O	O	O	O	O	O
Beneficiary Alias Name	O	O	O	O	O	O
Beneficiary Client Identification	O	O	O	O	O	O
Beneficiary Client Token	O	O	O	O	O	O
Beneficiary Name	O	M	O	O	O	O
Beneficiary Address Line	O	O	O	O	O	O
Beneficiary Country	O	O	O	O	O	O
Beneficiary Birth Date	O	O	O	O	O	O
Beneficiary Birth Country	O	O	O	O	O	O
Beneficiary IBAN	O	M	O	O	O	O
Beneficiary BIC	O	O	O	O	O	O
Beneficiary Device Identification	O	O	O	O	O	O
Beneficiary Device UID	O	O	O	O	O	O
Beneficiary Device OS	O	O	O	O	O	O
Beneficiary Device Browser	O	O	O	O	O	O
Beneficiary Device User Agent	O	O	O	O	O	O
Beneficiary Device IP Address	O	O	O	O	O	O
Beneficiary Device Fingerprint	O	O	O	O	O	O
Beneficiary Device Timezone	O	O	O	O	O	O
Beneficiary Device Language	O	O	O	O	O	O
Beneficiary Application Language	O	O	O	O	O	O
Beneficiary Device Latitude	O	O	O	O	O	O
Beneficiary Device Longitude	O	O	O	O	O	O
Beneficiary Device Rooted Indicator	O	O	O	O	O	O
Beneficiary Device Charging Indicator	O	O	O	O	O	O

Atributo	Login	Transferências	Pagamentos com Referencia	Pagamentos Serviços/Compras	Operações Financeiras	Outras Operações
Beneficiary Device Inclination	O	O	O	O	O	O
Channel Selected Type	M	M	M	M	M	M
Session Identification	M	M	M	M	M	M
Transaction Datetime	M	M	M	M	M	M
Transaction Local Datetime	O	O	O	O	O	O
Operation Amount	O	M	M	M	M	O
Operation Currency	O	M	M	M	M	O
Local Operation Amount	O	O	O	O	O	O
Local Operation Currency	O	O	O	O	O	O
PAN	O	O	O	O	O	O
Token PAN	O	O	O	O	O	O
PAN Expiry Date	O	O	O	O	O	O
Token PAN Expiry Date	O	O	O	O	O	O
Current Account Balance	O	O	O	O	O	O
Account Currency	O	M	M	M	M	O
Preparation User	O	O	O	O	O	O
Corporate Client Identification	O	O	O	O	O	O
Payment Entity	O	O	O	M	O	O
Payment Entity Reference	O	O	M	M	O	O
Trusted Beneficiary Indicator	O	O	O	O	O	O
Recurring Operation Indicator	O	O	O	O	O	O
To Self Operation Indicator	O	O	O	O	O	O
User Authentication Method	M	M	M	M	M	M
Authentication Attempts Counter	M	M	M	M	M	M
Strong Customer Authentication Indicator	M	M	M	M	M	M
Transaction Description for Beneficiary	O	O	O	O	O	O
Transaction Description for Originator	O	O	O	O	O	O
External Fraud Transaction Score	O	O	O	O	O	O
External Fraud Rule Name	O	O	O	O	O	O
External Fraud Refused Indicator	O	O	O	O	O	O
Response Status Code	M	M	M	M	M	M
Response Reason Code	M	M	M	M	M	M
User Certificate Presence Indicator	O	O	O	O	O	O

LEGENDA:
M=Mandatory O=Optional

Os campos de preenchimento obrigatório, são os campos considerados mínimos para garantir qualidade na resposta de *screening*, a falta desta informação vai enviesar o modelo, não garantindo a qualidade exigida pela PAYWATCH. Assim sendo, nos casos que os campos obrigatórios não venham preenchidos, a PAYWATCH devolverá *screening* zero e uma mensagem “INSUFFICIENT_TRANSACTION_DATA”

3.3.4 Casos Práticos de utilização dos atributos

3.3.4.1 Transação por assinatura múltipla

Num cenário onde é necessária mais de uma assinatura por transação, o fluxo esperado é:

1. Pedido de *screening*, onde:
   - ✓ User Signatures Required Counter = Número de assinaturas necessárias para executar a operação (neste exemplo, vamos considerar 3)
   - ✓ Response Status Code = PNDG
   - ✓ Preparation User = client ID do utilizador que preparou a operação (da transação em 1)
   - ✓ Response Reason Code = PD01
2. Enviar uma consolidação por cada assinatura.

   Primeira consolidação:
   - ✓ User Signatures Required Counter = 2
   - ✓ Response Status Code = PNDG
   - ✓ Preparation User = client ID do utilizador que preparou a operação (da transação em 1)
   - ✓ Response Reason Code = PD01
   - ✓ External Original Transaction Token = Da transação em 1.

   Segunda consolidação:
   - ✓ User Signatures Required Counter = 1
   - ✓ Response Status Code = ACCP
   - ✓ Preparation User = client ID do utilizador que preparou a operação
   - ✓ Response Reason Code = OP01
   - ✓ External Original Transaction Token = Da transação em 1.

3.3.4.2 Transação que envolve câmbio

Para efeitos de *profiling*, a solução da PAYWATCH vai internamente converter os montantes enviados para Euro, a fim de assegurar a normalização e criação de *profiling*. Numa primeira fase, esta componente não está disponível pelo que o Banco deve assegurar a conversão e o envio do atributo “Operation Amount” em Euro ou garantir o não envio dessa informação para não enviesar o modelo da PAYWATCH.

Assim, quando a operação for realizada numa moeda diferente da moeda da conta:

- Operation Amount = valor da transação na moeda da conta
- Operation Currency = código da moeda da conta
- Local Operation Amount = valor na moeda da transação
- Local Operation Currency = código da moeda da transação

Para mais fácil compreensão, a Tabela em baixo apresenta três exemplos.

Tabela 8 – Caso prático de transação com câmbio[2]

	Exemplo 1 **Conta em € | Transação em €**	**Exemplo 2** **Conta em € | Transação em $**	**Exemplo 3[3]** **Conta em $ | Transação em £**
Operation Amount	Se = 20€	~17,71€	~57,31$
Operation Currency	978	978	840
Local Operation Amount	{}	Se = 20$	Se = 45£
Local Operation Currency	{}	840	826

3.3.4.3 Transação com Hit Positivo em Listas

Num cenário que a transação tem um Hit Positivo nas listas, o campo Fraud Rule Name assume descrições específicas que o banco deve utilizar para preenchimento do campo Response Reason Code.

Tabela 9 – Caso prático de transação com hit positivo em listas

	Fraud Rule Name	
	Startswith(R_ONL_PAYLIST) (*Blacklist* Sistemica da PAYWATCH)	Startswith(R_ONL_BANKLIST) (*Blacklist* Sistemica da PAYWATCH)
Response Reason Code	**FR01** Transação recusada por Lista de Bloqueio da PAYWATCH	**FR02** Transação recusada por Lista de Bloqueio Privada do Banco

3.4 Masterdata

Por forma a valorizar a informação enviada nas diferentes interfaces associadas às transações, o sistema de análise e prevenção de Fraude, suporta o carregamento de dados de referência (designados também de *masterdata*). Os dados de referência correspondem a dados adicionais relacionados com um determinado atributo, que facilitam e complementam as análises a efetuar. Estes dados correspondem não só a descritivos, mas também a informação adicional sobre um determinado atributo (ex: nome e número de telefone do cliente associado a um determinado IBAN).

[2] Taxa de câmbios do Banco de Portugal a 27 de novembro de 2018.

[3] Este caso tem, numa primeira fase de ser tratado como no exemplo 2. O caso apresentado no exemplo 3 verifica-se apenas quando a PAYWATCH disponibilizar o conversor de moeda para €.

A *masterdata* é enviada pela entidade externa através de um ou mais ficheiros, no formato CSV e de acordo com o previamente acordado com a equipa da Fraude. Os ficheiros chegam à SIBS via MFT e são encaminhados para processamento direto pelo sistema de gestão de Fraude.

Os ficheiros têm que ter obrigatoriamente um *header* com os atributos respetivos de cada tabela e referidos nas tags Plain XML, seguido dos registos (detalhe) com os dados a serem carregados. Os atributos do *header* e os valores do detalhe são separados por ";" (*semicolon*), exceto no último atributo.

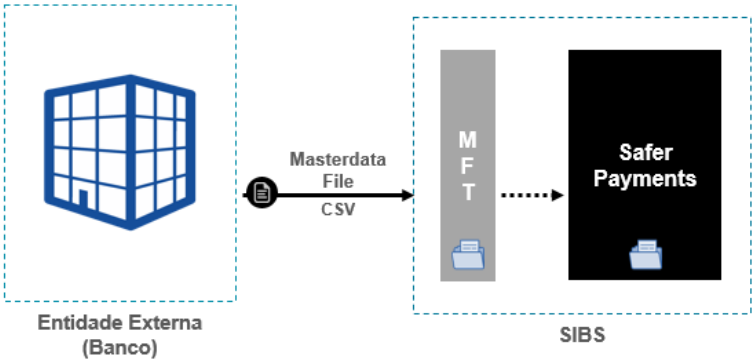

Figura 5 - Envio *Masterdata*

A Tabela abaixo identifica as tabelas de *masterdata* a serem carregadas na plataforma da PAYWATCH e que são da responsabilidade do Banco.

Tabela 10 - Tabelas *Masterdata*

Nome Ficheiro	Tabela	Descrição
FRDOPR	External Operation Code	Tabela de códigos de operação usado internamente pela instituição externa.
FRDCLI	External Cliente Identification	Tabela de identificação do cliente na instituição externa.
FRDCTI	Cliente Token IBAN	Tabela que identifica o cliente na visão corporativa SIBS e respetivos IBAN. Pode ter mais do que um IBAN.
FRDCTP	Cliente Token PAN	Tabela que identifica o cliente na visão corporativa SIBS e respetivos PAN. Pode ter mais do que um PAN.

3.5 Marcação de Fraude

À medida que for existindo histórico com fraude marcada, esse histórico vai ser utilizado como *input* para as atividades de *advanced analytics/machine learning* e para afinação de regras, promovendo a melhoria contínua do modelo. Quanto mais informação o modelo tiver, melhor é a sua eficácia e eficiência.

Para isso, a PAYWATCH disponibiliza dois métodos possíveis para a marcação de fraude. A marcação de fraude na plataforma, transação a transação. E a marcação de fraude em *batch*, pelo envio de ficheiro MFT com a transação ou transações fraudulentas marcadas.

3.5.1 Transação a transação

O Banco vai ter a possibilidade de gerir a marcação de fraude na plataforma, assinalando, transação a transação aquelas que efetivamente se verificaram como fraude.

3.5.2 Em *batch*

Outra possibilidade para a marcação da fraude, é através do envio em *batch*, de um ficheiro com a transação ou transações fraudulentas marcadas. Este envio deve ser periódico, idealmente deveria ser um envio mensal, sendo expectável que os Bancos o façam até três meses. Note-se que quanto mais cedo a PAYWATCH tiver disponível esta informação (tanto a fraude marcada na plataforma ou em *batch*), mais cedo consegue incorporar esta informação no modelo e melhorar o serviço disponibilizado ao Banco.

Estes ficheiros identificam univocamente determinadas transações e classificam-nas com o tipo de fraude associado. À semelhança do que acontece para a *masterdata*, também estes ficheiros são enviados no formato CSV e de acordo com uma estrutura previamente acordada com a equipa da Fraude. Chegam à PAYWATCH via MFT e são encaminhados para processamento pela plataforma de gestão de Fraude.

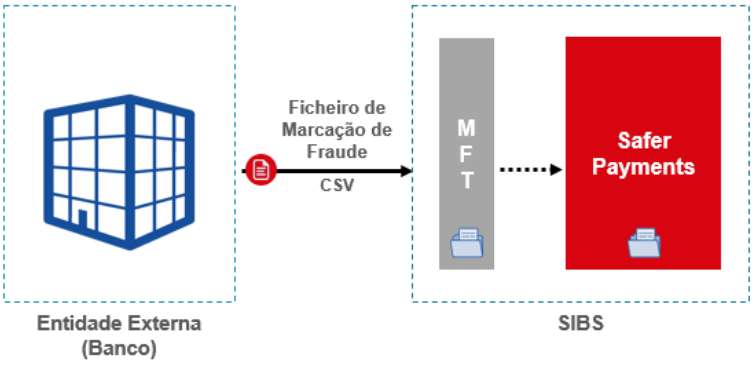

Figura 6 - Envio Marcação de Fraude

A tabela abaixo identifica os atributos contidos no ficheiro de marcação de fraude.

Nome do Ficheiro: MFRDHMB.

Tabela 11 - Atributos Ficheiro Marcação Fraude

Atributo	Tag	Representação	Descrição
Institutional Code	InstitutionalCode	Max5Numeric	Código identificativo da instituição. No âmbito *homebanking* é código do Banco tal como é identificado no Banco de Portugal.
Client Identification	ClientID	Max35Text	Identificação do ordenante da operação.
External Transaction Token	ExternalTransactionToken	Max50Text	Identificação única da operação do ponto de vista do subscritor do serviço.
Fraud Type Code	FraudTypeCode	Exact5Numeric	Identifica o tipo de fraude associado à transação (ver lista de valores Fraud Type Code).

4 Casos práticos de interação com o cliente final

4.1 Cliente reclama operação que não consegue realizar

Poderão existir diversas razões pelas quais o cliente não possa transacionar num dado momento.

Tabela 12 – Caso prático cliente não consegue realizar operação

Descrição da Situação	Ação do Banco
O cliente pode demonstrar comportamentos que o modelo interpreta como comportamentos de risco, pelo que este procede a um *score* de risco elevado. Em consequência deste *score* o Banco pode decidir não avançar com a transação.	1. O Banco deverá colocar a entidade da conta/cliente (exemplo: IBAN) em lista de isenção para que independentemente do *score* risco e da regra de decisão preponderante, a sugestão seja *GO*. 2. O Banco deverá marcar a transação como genuína de forma ao modelo ser retroalimentado.
A transação pode ter sido identificada numa *blacklist*, pelo que a Sugestão é NO GO.	O Banco deve analisar o tipo de regra que resultou na colocação da entidade em *blacklist*: 1. Se a lista em causa for Sistémica, o Banco deverá colocar a entidade em *whitelist* de modo a que o cliente possa transacionar; 2. Se a lista em causa for do Banco, este deverá remover a entidade da *blacklist*. Nestas situações o Banco deve rever os critérios de colocação em *blacklist*, dado que a situação é genuína.

4.2 Cliente reclama operação que não reconhece

Uma transação fraudulenta pode não ser identificada como tal, resultando no contacto do cliente com o Banco.

Tabela 13 – Caso prático cliente não reconhece operação

Descrição da Situação	Ação do Banco
O cliente pode demonstrar comportamentos que o modelo interpreta como comportamentos normais, pelo que este procede a um *score* de risco baixo. Em consequência deste *score* o Banco pode decidir avançar com a transação sem métodos de autenticação forte.	1. O Banco deve bloquear o acesso das credenciais da conta/cliente ao *Onlinebanking,* colocar a entidade da conta/cliente (exemplo: IBAN) em lista de bloqueio para que independentemente do *score* risco e da regra de decisão preponderante, a sugestão seja NO *GO*. 2. O Banco deve marcar a transação como fraudulenta de forma ao modelo ser retroalimentado.
A transação pode ter sido identificada numa *whitelist*, pelo que a Sugestão é GO.	O Banco deve remover a entidade da *whitelist* e rever os seus critérios de colocação nesta lista dado que a transação é fraudulenta.

5 Reporting

O *reporting* disponibiliza um *dump* com as transações com fraude efetiva com o detalhe: (1) da tipologia de fraude, (2) tipo de operação, (3) tipo de autenticação e (4) montantes. O envio é mensal, para as equipas do Banco com o acumulado dos últimos seis meses.

O tipo de relatórios a gerar, a informação que neles consta, e a periodicidade de geração/envio tem em conta o referido nas *guidelines* de *report* de fraude da EBA[4] e do Banco de Portugal[5], desde que a informação disponível na plataforma PAYWATCH assim o permita.

Numa fase inicial, o relatório será enviado por e-mail com um anexo zipado com *password* associada.

[4] EBA/GL/2018/05 - Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2).

[5] Banco de Portugal de 20 de agosto de 2013 - Informação sobre sistemas e instrumentos de pagamentos - Requisitos de reporte fraudes com instrumentos de pagamento.

6 Atividade de FPaaS

6.1 Manual Operativo

No âmbito da FPaaS, é disponibilizado um manual operacional da plataforma da PAYWATCH com a qual o Banco pode atuar na prevenção de fraude em multicanal. Como tal, nesse documento é apresentado:

- Como aceder à plataforma da PAYWATCH;
- Investigação de um caso de fraude - boas práticas e procedimentos;
- *Workflows* e exemplos de casos práticos com imagens ilustrativas da plataforma;
- Ferramentas de *Reporting.*

O acesso à plataforma da PAYWATCH é realizado via PSS, cumprindo assim as normas de segurança. O pedido de acesso à plataforma da PAYWATCH através do PSS deve ser feito pelo Administrador do PSS do Banco, seguindo os procedimentos habituais para pedido de novos tipos de intervenção no PSS.

O manual operativo será disponibilizado a partir de 30.01.2019. No âmbito do P&S incluirá a apresentação da ferramenta na forma de *workshop.*

6.2 Formulários

O Banco deve preencher dois formulários no âmbito de:

i) Configuração de endereços – necessário para contacto da PAYWATCH com o Banco no envio de informação como dados estatísticos e PAYWATCHERS, entre outros;

ii) Pedidos de acessos – necessário para que os colaboradores do Banco possam aceder e trabalhar na plataforma de deteção de fraude.

Estes formulários serão disponibilizados a partir de 30.01.2019.

A.1. Lista de Valores Possíveis

A.1.1 Códigos de Recusa

A.1.1.1 Response Status Code

Tabela 14 - Response Status Code

Código	Descrição
ACCP	Accepted
CNCL	Cancelled
EXPR	Expired
PNDG	Pending
RJCT	Rejected

A.1.1.2 Response Reason Code

Tabela 15 - Response Reason Code

Código de Erro	Descrição
CR01	Cartão inexistente ou inválido.
CR02	Cartão perdido ou roubado.
CR03	Operação não permitida para o cartão.
CR04	Operação não permitida para o estado do cartão.
CR05	Situação de cartão inválida.
CT01	Conta(s) inexistente(s) ou inválida(s).
CT02	Operação não permitida para a conta.
CT03	Operação não permitida para a conta destino.
CT04	Operação não permitida para o estado da conta.
CT05	Operação não permitida para o estado da conta destino.
CT06	Situação da conta inválida.
CT07	Situação da conta destino inválida.
DS01	Dados inválidos.
DS02	Dados insuficientes ou inexistentes.
DS03	Data limite excedida.
DS04	Data(s) inválida(s).
DS05	Entidade inexistente ou inválida.
DS06	Moeda inexistente ou inválida.
DS07	Referência de pagamento inexistente ou inválida.

Código de Erro	Descrição
OP01	Operação aceite.
OP02	Operação indisponível.
OP03	Operação inválida.
OP04	Operação não permitida.
OP05	Operação já efetuada ou em curso.
OP06	Não foi possível concluir a operação.
SM01	Saldo insuficiente ou indisponível.
SM02	Saldo inválido.
SM03	Montante(s) inválido(s).
US01	Código de autenticação incorreto.
US02	Número de tentativas de autenticação excedidas.
US03	Utilizador bloqueado.
US04	Utilizador inexistente ou inválido.
US05	Operação não permitida para o utilizador.
US06	Operação não permitida para o estado do utilizador.
US07	Estado do utilizador não permitido.
US08	Informação do utilizador desatualizada ou insuficiente.
GN01	Informação não disponível para consulta.
GN97	Erro do sistema de processamento externo.
GN98	Erro de comunicações.
GN99	Erro aplicacional.
PD01	Operação pendente de assinatura.
FR01	Transação recusada por Lista de Bloqueio da PAYWATCH.
FR02	Transação recusada por Lista de Bloqueio Privada do Banco.
FR03	Transação recusada por *score* de risco elevado.
FR04	Transação recusada por não preenchimento dos campos obrigatórios.
FR98	Transação recusada por outra componente de gestão de risco do Banco.
FR99	Transação recusada por time-out da solução de prevenção de fraude.
LM01	Limite por operação excedido.
LM02	Limite de utilização diário excedido.
LM03	Limite de utilização semanal excedido.
LM04	Limite de utilização mensal excedido.
LM05	Limite de utilização da conta/serviço destino excedido.
LM99	Limite excedido.
AL01	Ordenante sancionado.
AL02	Beneficiário sancionado.
AL99	Transação recusada por motivo de CTF/AML.

A.1.2 Fraud Operation Codes

Tabela 16 - Fraud Operation Codes

Fraud Operation Code	Fraud Operation Description	Grouped Operations
Ab	Abate	Outras Operações
Ac	Ativação	Outras Operações
Ad	Adiantamento	Operações Financeiras
Ae	Adesões	Outras Operações
Aj	Ajustamento	Outras Operações
Al	Alterações	Outras Operações
An	Anomalias	Outras Operações
Ar	Aberturas	Outras Operações
As	Associação	Outras Operações
At	Autenticação	Outras Operações
Au	Autorizações	Outras Operações
Az	Atualizações	Outras Operações
Bv	Baixo Valor	Outras Operações
Ca	Cancelamentos	Outras Operações
Cb	Chargebacks	Outras Operações
Cd	Créditos	Operações Financeiras
Cf	Confirmações	Outras Operações
Co	Compras	Operações Financeiras
Cq	Cheques	Outras Operações
Cr	Carregamentos	Pagamentos com Referência
Cs	Consultas	Outras Operações
Cv	Créditos Voucher	Outras Operações
Dd	Débitos Diretos	Outras Operações
Dp	Depósitos	Operações Financeiras
Ds	Desativações	Outras Operações
Dv	Devoluções	Operações Financeiras
Ec	Estado Cartão	Outras Operações
Fc	Fechos	Outras Operações
Fm	Fatura Manual	Outras Operações
Fr	Pagamento fracionado	Operações Financeiras
If	Informação	Outras Operações
In	Inserções	Outras Operações
Iv	Investimento	Operações Financeiras
Lc	Licenças	Outras Operações
Lg	Login	Login
Lt	Lote	Operações Financeiras

Fraud Operation Code	Fraud Operation Description	Grouped Operations
Lv	Levantamentos	Operações Financeiras
Ot	Operações Técnicas	Outras Operações
Pc	Pagamento de Compras	Pagamentos Serviços/Compras
Pe	Pedido	Outras Operações
Pg	Pagamento	Operações Financeiras
Pi	PIN	Outras Operações
Ps	Pagamento de Serviços	Pagamentos Serviços/Compras
Pt	Pagamentos ao estado	Pagamentos com Referencia
Re	Reclamações	Outras Operações
Rg	Resgate	Operações Financeiras
Sb	Substituições	Outras Operações
Se	Serviços Especiais	Outras Operações
Ss	Assinatura	Operações Financeiras
Tf	Transferências	Transferências
Tm	Transmissão	Operações Financeiras
Vb	Vendas de Bilhetes	Operações Financeiras
Vc	Verificação de Conta	Outras Operações

A.1.3 Fraud Type Code

Tabela 17 - Fraud Type Code

Fraud Type Code	Fraud Type Description
10000	Lost Card | Unknown
10100	Stolen Card | Unknown
10200	Card Not Received | Unknown
10300	Fraudulent Application | Unknown
10400	Counterfeit Card | Unknown
10500	Miscellaneous/Account Takeover | Unknown
10600	Card Not Present | Unknown
19000	Phishing/Pharming | Unknown
19100	Financing | Unknown
19200	Illegitimate Credits | Unknown
19900	Non-Accounting Transaction | Unknown
10001	Lost Card | Dishonest
10101	Stolen Card | Dishonest
10201	Card Not Received | Dishonest
10301	Fraudulent Application | Dishonest

Fraud Type Code	Fraud Type Description
10401	Counterfeit Card | Dishonest
10501	Miscellaneous/Account Takeover | Dishonest
10601	Card Not Present | Dishonest
19001	Phishing/Pharming | Dishonest
19101	Financing | Dishonest
19201	Illegitimate Credits | Dishonest
19901	Non-Accounting Transaction | Dishonest
10002	Lost Card | Modification Order
10102	Stolen Card | Modification Order
10202	Card Not Received | Modification Order
10302	Fraudulent Application | Modification Order
10402	Counterfeit Card | Modification Order
10502	Miscellaneous/Account Takeover | Modification Order
10602	Card Not Present | Modification Order
19002	Phishing/Pharming | Modification Order
19102	Financing | Modification Order
19202	Illegitimate Credits | Modification Order
19902	Non-Accounting Transaction | Modification Order
10003	Lost Card | Manipulated
10103	Stolen Card | Manipulated
10203	Card Not Received | Manipulated
10303	Fraudulent Application | Manipulated
10403	Counterfeit Card | Manipulated
10503	Miscellaneous/Account Takeover | Manipulated
10603	Card Not Present | Manipulated
19003	Phishing/Pharming | Manipulated
19103	Financing | Manipulated
19203	Illegitimate Credits | Manipulated
19903	Non-Accounting Transaction | Manipulated
20001	Unknown | Issuance of a payment order by the fraudster
20002	Unknown | Modification of a payment order by the fraudster
20003	Unknown | Manipulation of the payer by the fraudster to issue a payment order
20101	Social Engineering | Issuance of a payment order by the fraudster
20103	Social Engineering | Manipulation of the payer by the fraudster to issue a payment order
20201	Malware | Issuance of a payment order by the fraudster
20202	Malware | Modification of a payment order by the fraudster
20301	Data Breach | Issuance of a payment order by the fraudster
20302	Data Breach | Modification of a payment order by the fraudster

Fraud Type Code	Fraud Type Description
20401	Friendly Fraud | Issuance of a payment order by the fraudster
20403	Friendly Fraud | Manipulation of the payer by the fraudster to issue a payment order

A.1.4 User Authentication Method

Tabela 18 - User Authentication Method

User Authentication Method	User Authentication Method Description
N	PIN
M	Matrix Coordinates
S	OTP SMS
P	Password
C	Certificate
B	Biometric
A	CAP EMV
H	Hardware Token
T	Timebased OTP
R	Password/Code Positions
O	Others

A.2. Tabelas *Masterdata*

A.2.1 FRDOPR - External Operation Code

Tabela 19 - FRDOPR External Operation Code

Nome Atributo	Tag	Representação	Descrição
Institutional Code	InstitutionalCode	Max5Numeric	Código identificativo da instituição. No âmbito *homebanking* é código do Banco tal como é identificado no Banco de Portugal.
Operation Code	OperationCode	Max6Text	Código identificativo da operação de acordo com a nomenclatura do subscritor do serviço.
Operation Description	OperationDescription	Max60Text	Descrição do código de operação.

Exemplo ilustrativo:

InstitutionalCode;OperationCode;OperationDescription

9999;123;Transferência

9999;ABC;Login

A.2.2 FRDCLI - External Client Identification

Tabela 20 - FRDCLI External Client Identification

Nome Atributo	Tag	Representação	Descrição
Client ID	ClientID	Max35Text	ID do cliente na instituição.
Client User Name	ClientUserName	Max150Text	*Username* do cliente.
Client Alias Name	ClientAliasName	Max150Text	Identificador alternativo do cliente.
Client Token	ClientToken	Max20Text	Identificador do cliente na visão corporativa SIBS.
Client Name	ClientName	Max70Text	Nome do cliente.
Client Address Line 1	ClientAddressLine1	Max70Text	Morada do cliente.
Client Address Line 2	ClientAddressLine2	Max70Text	Localidade do cliente.
Client Country	ClientCountryISOAlpha3	Max3Text	País do cliente no formato ISO 3166, Alpha-3 *code* (ex: Portugal – PRT).
Client Phone	ClientPhone	Max30Text	Contacto telefónico do cliente.
Client Email	ClientEmail	Max55Text	Endereço e-mail do cliente.
Client Birth Date	ClientBirthDate	ISODate	Data de nascimento do cliente no formato YYYY-MM-DD.
Client Birth Country	ClientBirthCountryISOAlpha3	Max3Text	País de nascimento do cliente no formato ISO 3166, Alpha-3 code (ex: Portugal – PRT).
Client Gender	ClientGender	Max1Text	Género do cliente.
Client Profession	ClientProfession	Max30Text	Profissão do cliente.
Client Creation Date	ClientCreationDate	ISODate	Data de inicio de atividade do cliente.
Client Ratings	ClientRatings	Max5Text	Rating do cliente.
Client Active SEPADD Counter	ClientActiveSepaDDCounter	Max3Numeric	Número de autorizações de débito direto ativas do cliente
Client Debtor Posistion	ClientDebtorPosition	Max10Numeric	Montante de responsabilidades do cliente.
Client Creditor Position	ClientCreditorPosition	Max10Numeric	Montante de aplicações do cliente.

A.2.3 FRDCTI - Client Token IBAN

Tabela 21 - FRDCTI Client Token IBAN

Nome Atributo	Tag	Representação	Descrição
Client Token	ClientToken	Max20Text	Token identificativo do cliente beneficiário para o subscritor do serviço de Fraude.
Client IBAN	ClientIBAN	Max34Text	IBAN do cliente

A.2.4 FRDCTC - Client Token PAN

Tabela 22 - FRDCTC Client Token PAN

Nome Atributo	Atributo	Representação	Descrição
Client Token	ClientToken	Max20Text	Token identificativo do cliente beneficiário para o subscritor do serviço de Fraude.
PAN	PAN	Max23Text	Primary Account Number associado à operação.
Card Expire Date	CardExpiryDate	Max10Text	Data de expiração do PAN associado à operação no formato YYYYMM.