17 de outubro 2018

Serviços de Deteção e Prevenção de Fraude nos Canais Onlinebanking

SIBS Partner in Payments

Agenda

- Experiência PAYWATCH
- Sinergias Cartão/Online Banking
- Prevenção de Fraude no Online Banking

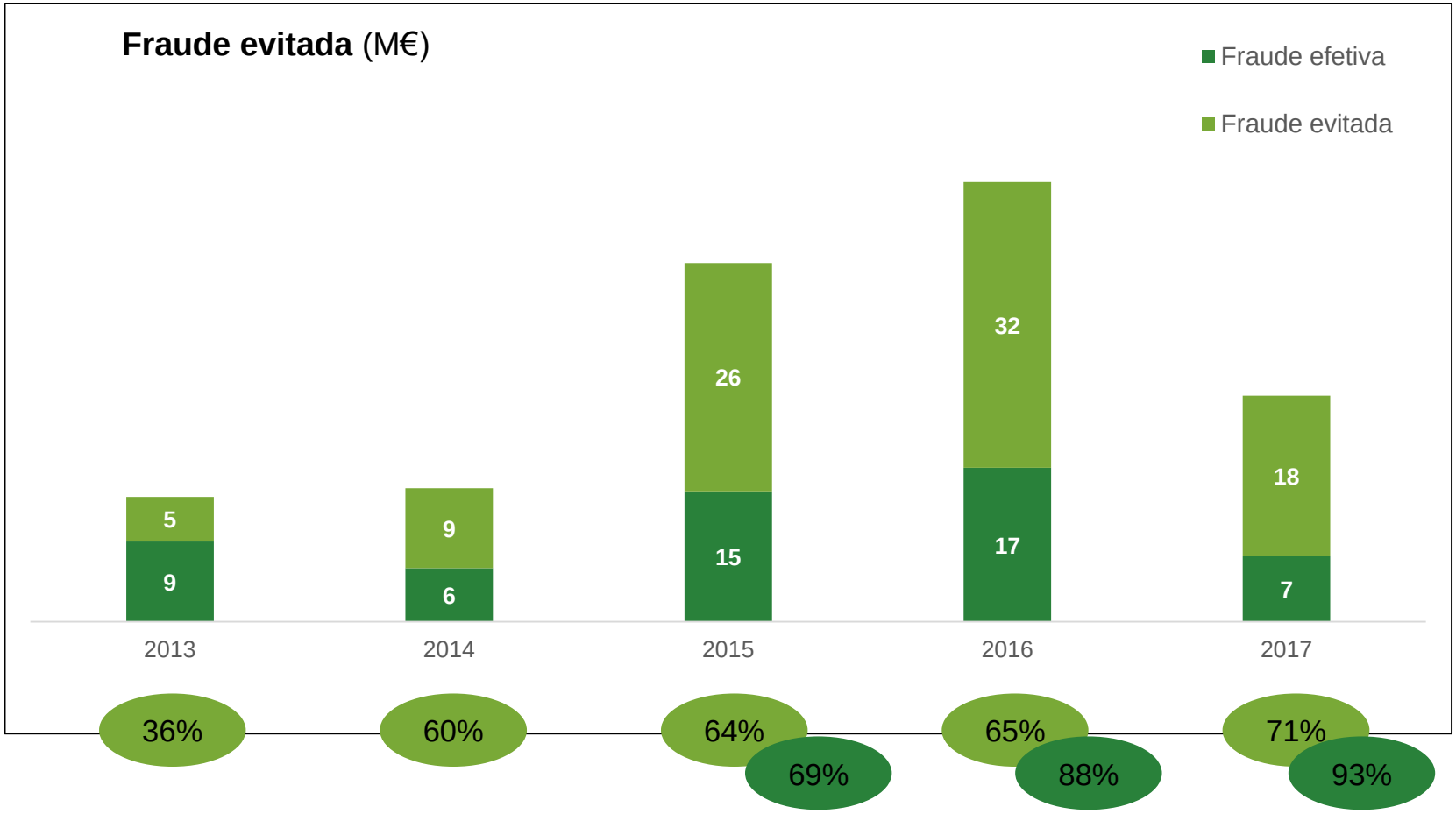
Agenda

- Experiência PAYWATCH
- Sinergias Cartão/Online Banking
- Prevenção de Fraude no Online Banking

Atuais capacidades da PAYWATCH são distintivas ao longo de toda a cadeia de valor da gestão de fraude

	Proposta de valor SIBS
Estrutura de dados	Base de dados compreensiva de cartões (emissão e *acquiring*) em ambiente multicanal, com potencial de agregação de estrutura de dados complementar dos bancos (com IBAN como identificador único)
Data Lake	Plataforma integrada (em arquitetura de IT redundante e escalável) de análise e gestão de dados em tempo real, capacitada para agregação de BDs complementares
Analytic engine	Experiência consolidada em gestão de acervo de regras (“expert rules”) baseada em mais de 20 anos de histórico, atualmente operado sobre plataforma de última geração com capacidade de gestão dinâmica e monitorização de impacto das regras, estando igualmente preparada para adoção de *advanced analytics*
Monitorização e intervenção	Equipa de mais de 30 pessoas dedicada à gestão de fraude, com modelo operativo de deteção, análise e reporte testado em escala
Impacto	Performance histórica distintiva com reduzida incidência de fraude sobre o sistema de cartões: 4x inferior à média europeia nos ATMs, 3x inferior à media europeia no CNP, com taxa de fraude evitada de 71 %

Evolução de níveis fraude com cartão em Portugal



Total

BCTL

Fonte: Dados PAYWATCH 2017

PAYWATCH – Serviços Integrados de Gestão e Prevenção de Fraude

Gestão de Regras & Modelação

- Criação de modelos de prevenção de fraude
- Otimização de modelos
- Capacidade de simulação
- Modelos adaptativos aos diferentes canais (cartões, ATM, POS, MB WAY, Via Verde)

Análise & Gestão de alertas (24x7)

- Investigação operacional de 1ª linha
- Aplicação de medidas de contenção imediatas
- Colocação de cartão / terminal em listas de bloqueio

PAYWATCH

Relatórios & Ações de mitigação

- Recomendações e principais eventos detalhados
- Revisão regular dos eventos de fraude e definição de melhores práticas
- Relatórios e métricas de fraude para bancos

Investigação de casos

Análise por peritos de casos especiais

- Investigação para determinação de pontos de compromisso
- Canais diretos com as forças policiais nacionais e internacionais
- Representação de casos junto das entidades judiciais

Suporte *Corporate*

Suporte *Cardholder*

Agenda

- Experiência PAYWATCH
- Sinergias Cartão/Online Banking
- Prevenção de Fraude no Online Banking

Experiência da PAYWATCH na gestão de fraude de cartões é um importante ativo para prevenção de fraude no Online banking

Metodologias base para deteção de fraude

- *Profiling* comportamental:
  - Velocidades de transações Origem
  - Velocidades de transações Destino
  - Velocidades de Montantes Origem
  - Velocidades de Montantes Destino
- Padrões atípicos:
  - Incompatibilidades cronológicas
  - Incompatibilidades geográficas

Área	Tipo	Descrição
Cartões – *Card present*	• LSNR • *Skimming* • Cash trapping with transaction reversal • Manipulação de mensagem	• Perdidos, Roubados e Não Recebidos • Contrafação de pista • Manipulação de dispensadores de ATMs • Simulação de transações
Cartões – *Card not present*	• Extrapolação • *Data Breaches & Botnets*	• Geração de Número cartão + Data Exp (+CVV) • Compromisso de dados de cartão em comerciantes,…
Online banking	• *Social engineering* • *Malware* • SIM *Swaps* • *E-Mules*	• *Phishing*, *vishing*, etc. • MIB, *Trojans*, *Bogus* Apps, etc. • Interseção de SMS *Token* • Exfiltração de fundos

A estrutura de dados do canal Cartão é semelhante à do canal Online banking

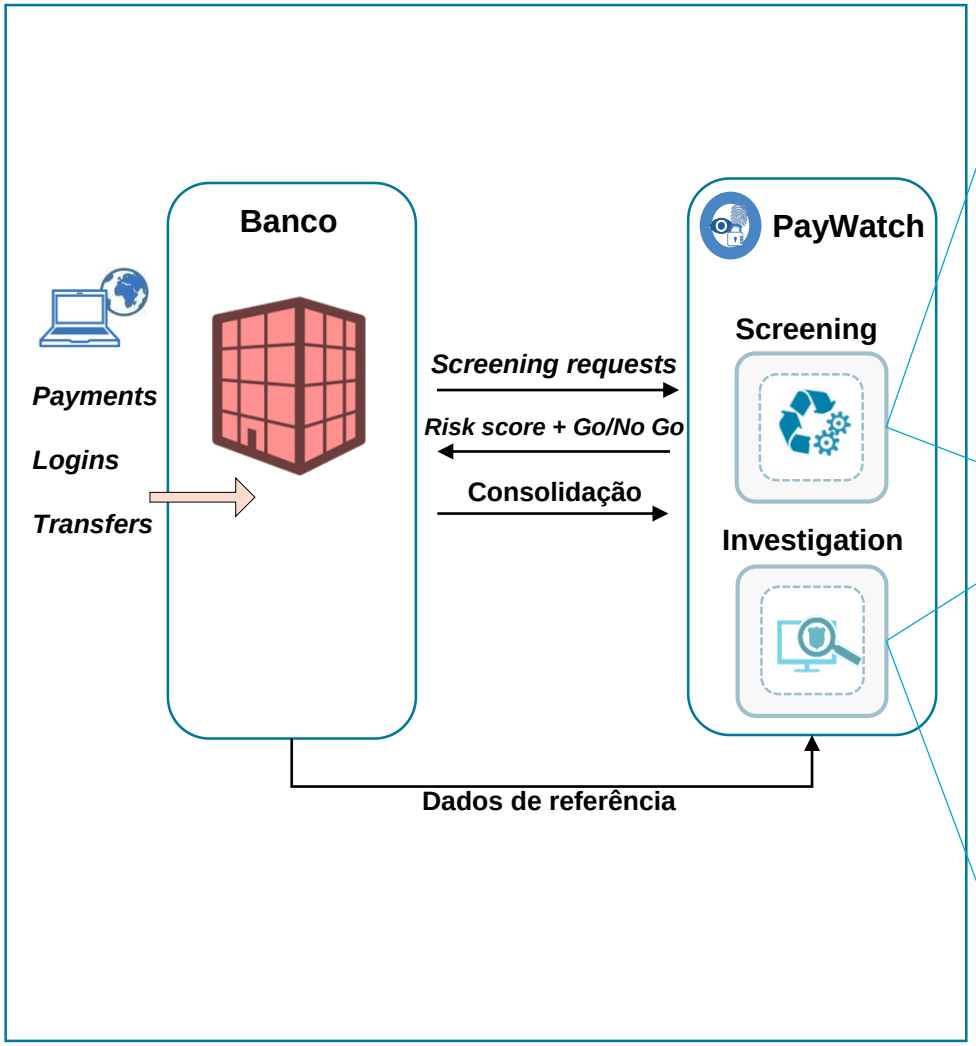
Dados da Transação	Canal: Cartão	Canal: Online banking
Contexto de origem	• País Cartão • Banco Cartão • BIN Cartão • PAN • Data Expiração • Tec *Chip/Contactless* • Suporte 3D Secure	• País IBAN • Banco IBAN • BIC IBAN • IBAN • Nome • Morada • User ID
Contexto de destino	• País Terminal • *Acquirer* ID Terminal • *Merchant* ID Terminal • ID Terminal • MCC • Tec *Chip/Contactless* • Suporte 3D Secure	• País IBAN • Banco IBAN • BIC IBAN • IBAN • Entidade (Pag Serviços) • Referência(Pag Serviços)
Estrutura da transação	• Canal (ATM/POS) • Operação (Lev, Compra) • Resultado • Montante • Autenticação PIN • Autenticação Chip/Mag • IP & *User Agent*	• Canal (m-, e-, t- *banking*) • Operação (login, transf) • Resultado • Montante • Autenticação SCA/No SCA • Destinatários Frequentes • IP & *User Agent* • *Device Fingerprint* • GPS

Regras de natureza análoga

- Valor acumulado transacionado para Entidade/Ref num período temporal
- Velocidade de montantes para um determinado IBAN destino (conta mula)
- Número de transações efetuadas pelo IBAN por semana
- IBAN destino novo recebe transações de um número excessivo IBANs origem
- Tempo entre logins de determinado *device fingerprint* incompatível com ação humana (script)

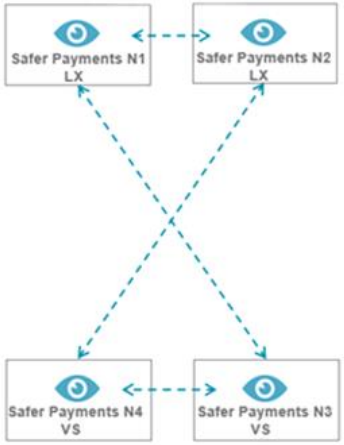
A arquitetura e serviços adotados para Cartão são a base para o canal Online banking

Arquitetura funcional



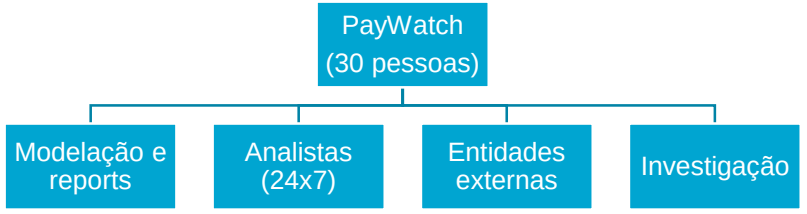
Arquitetura IT

- Redundância local e geográfica
- Ativo-Ativo
- Tempo de resposta em ~50 ms
- 6.5 M transações/dia
- Histórico de 3 anos



Equipa de gestão de fraude end-to-end

- Cerca de 500 investigações / ano resultando em 25 pessoas detidas
- Mais de 300 atributos e 400 perfis
- *Workflows* flexíveis e integrados
- Priorização de regras e simulação de impactos



Agenda

- Experiência PAYWATCH
- Sinergias Cartão/Online Banking
- Prevenção de Fraude no Online Banking

A PAYWATCH disponibiliza um P&S para permitir isentar as transações de baixo risco de autenticação forte

SIBS Partner in payments

Obrigações PSD2

A PSD2 tem como um dos objetivos tornar os pagamentos mais seguros, sendo que para tal os acessos às contas, os pagamentos online, e todas as operações nos canais remotos que possam implicar risco de fraude terão de ter autenticação forte.

- **ALGO QUE SEI (KNOWLEDGE) |** Password estáticas, PIN, user
- **ALGO QUE TENHO (OWNERSHIP) |** OTP, token, smart card, dispositivo
- **ALGO QUE SOU (INHERENCE) |** biometric, ex. impressão digital

Exceções

- Transações de **BAIXO VALOR** – pagamentos remotos até 30€ (com limite de 100€ ou 5 pagamentos)
- Em operações **CONTACTLESS** até 50€ (com limite de 100€ ou 5 pagamentos)
- Em operações "**UNNATENDED TERMINALS**" como Via Verde ou parques de estacionamento
- Em operações para **DESTINATÁRIOS CERTIFICADOS** (*white list*)
- Em operações em que o destinatário e ordenador é a **MESMA ENTIDADE**
- Operações **RECORRENTES** (periódicas – aplicável na primeira e isento nas seguintes)
- Em operações, de Empresas, feitas em canais dedicados automáticos (FTP/SIBS, canal multibancário, etc), desde que a autoridade nacional certifique estes canais e esteja de acordo com o seu nível de segurança
- Em consulta de saldos e movimentos, depois do primeiro consentimento, e durante cada 90 dias

Estão excecionadas também operações do PSP sempre que este mantenha níveis de FRAUDE abaixo do determinado pelos RTS. Para tal terá de existir Risk Base Analises em real time.

PAYWATCH cognitive security services

O P&S disponibilizado pela PayWatch realiza o screening em real time das operações

Para cada pedido de Screening ao Safer Payments, são devolvidos 3 campos: Score, Regra e Indicador de Go/NoGo.

Score, indicação do nível de risco da transação, sobre o qual o banco pode optar por incrementar os níveis de autenticação, isentar de Autenticação Forte, ou mesmo bloquear

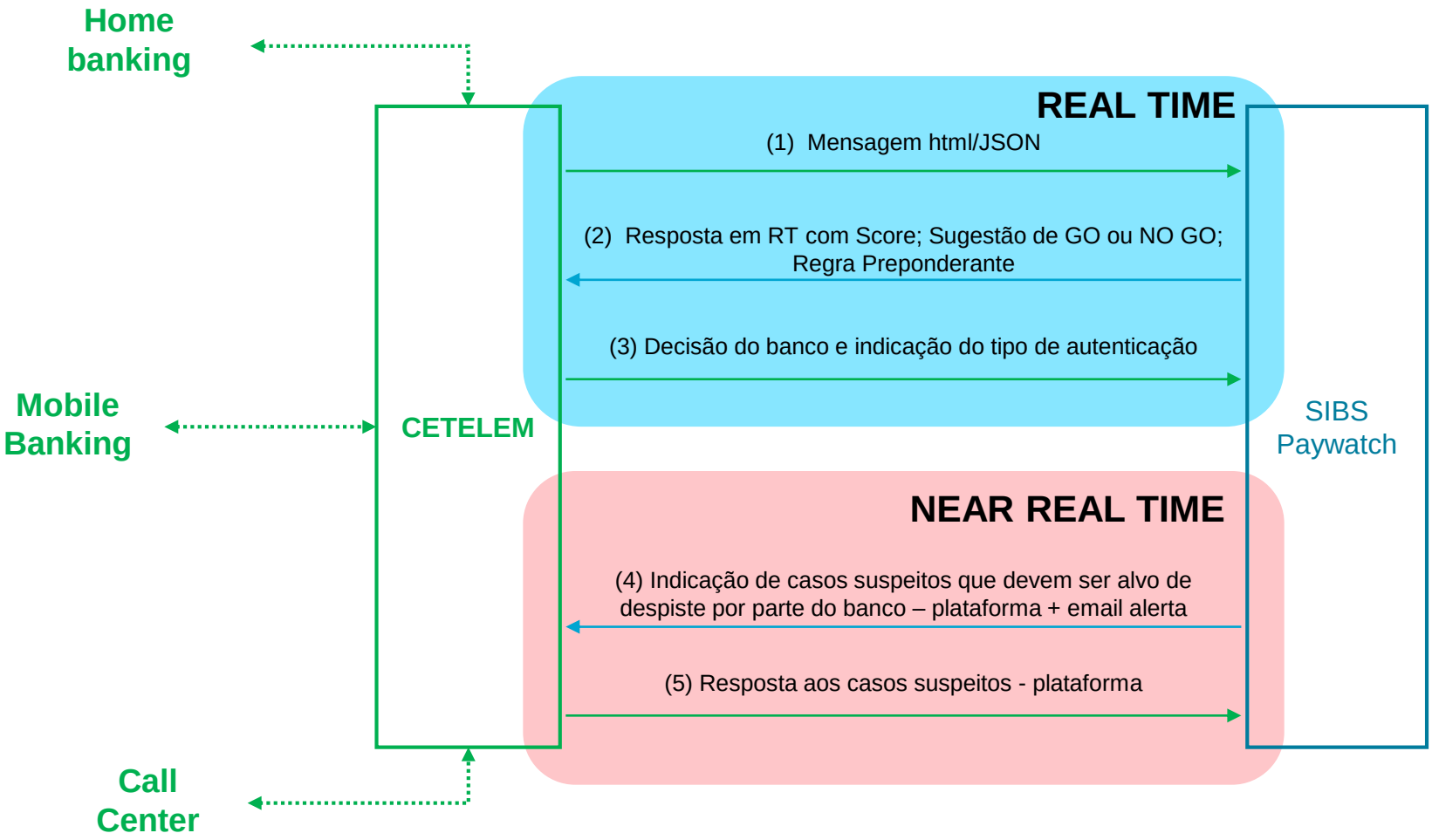
Regra, indicação da condição mais preponderante, que levou ao bloqueio ou bypass

Go/NoGo, indicação da monitorização de fraude se a transação deve ou não ser bloqueada, baseada na aplicação do modelo de regras

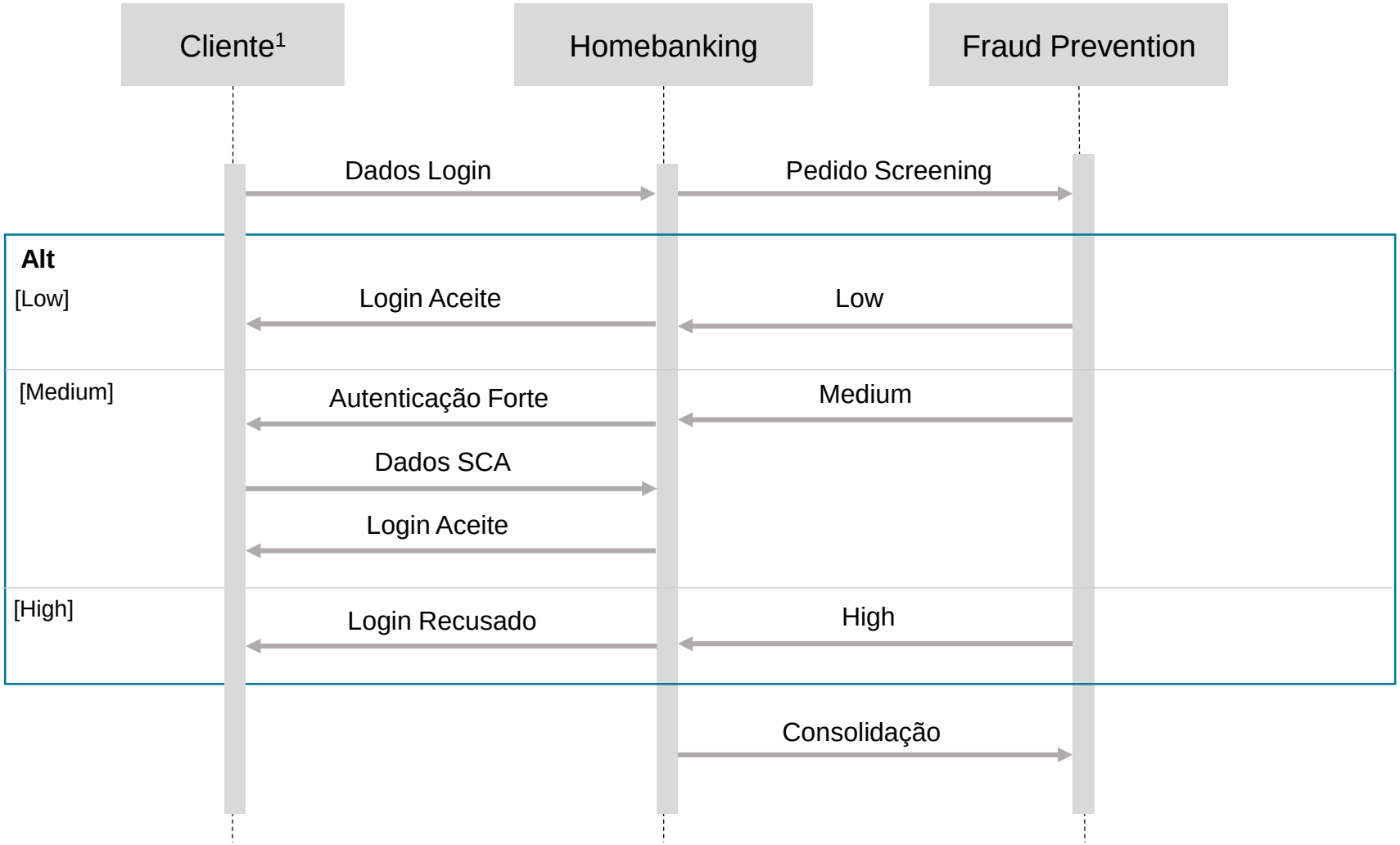
Ex. 998, Whitelist IBAN(O), Go; ex: 3, Blacklist IP , NoGo

A solução da PAYWATCH permite ao banco decidir em real time para cada transação o tipo de autenticação que quer solicitar ao cliente, tendo em conta a analise de risco da transação.

Funcionamento da solução de Prevenção de Fraude no Online banking

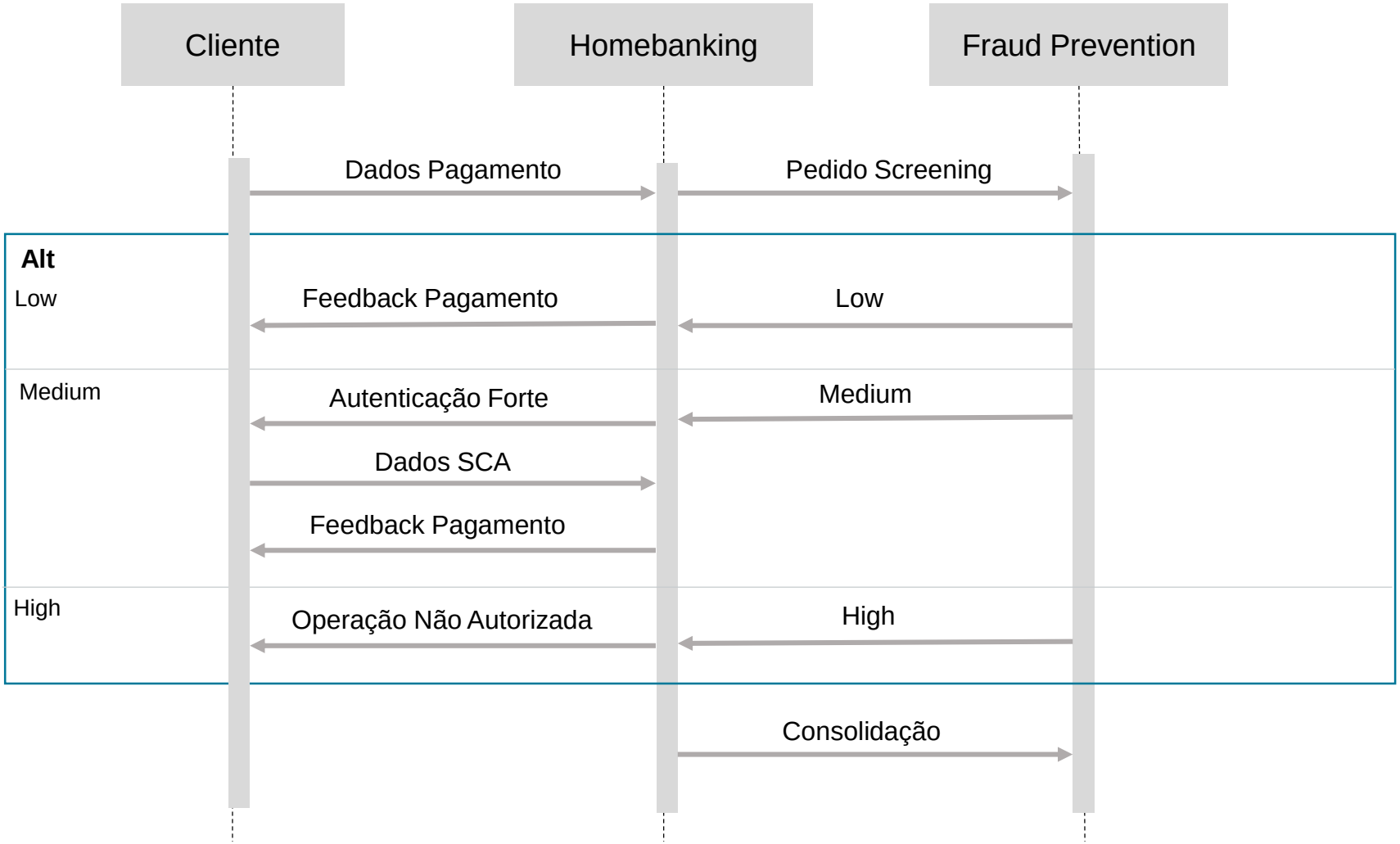


Flow Login



1 Clientes em Whitelist, necessário decidir o que fazer quando o score de risco é alto

Flow Pagamento Serviços



Tipos de Operações a monitorizar o risco

Operações Financeiras	Inclui todas as operações realizadas nos canais que impliquem movimentação de fundos, entrada ou saida. Ex. Transferência, Pagamentos de Serviços, Carregamentos.
Operações Não Financeiras	Inclui todos os tipos de operações que não são financeiras, mas que estão relacionadas com a utilização de uma conta, como por exemplo: - Tentativas de Login - Alteração de contactos (email/telefone) - Alteração de password ou do método de autenticação - Alterações de limites ou dos beneficiários
Dados de Sessão	Dados de sessão incluem todos os cliques/caminhos percorridos pelo utilizador durante a sessão. Este tipo de eventos não é utilizado no contexto do Safer Payments.

Tipos de Dados que o banco deve disponibilizar para a analise de risco

	Operações Financeiras	Operações Não Financeiras
Obrigatórios	• Montante • Data/hora transação • Conta Origem • Conta Destino • Canal (web/mobile/phone)	• ID Conta • Tipo de operação • Data/hora transação • Canal (web/mobile/phone)
Opcionais	• Endereço IP • Informação device/browser (ex. Resolução ecrã, sistema operativo, timezone, ...) • ID Sessão	

Estratégia de implementação para a prevenção de fraude no canal Onlinebanking

Estrutura de dados

- Apresentação formato standard de mensagem (*Release Documentation*) – Data proposta Nov.18
- Testes de integração com o Banco – Data proposta Jan.19

Data Lake

- Não haverá migração de dados. Haverá análise conjunta (SIBS/Banco) dos maiores casos de 2017/2018

Analytic engine e Case Management

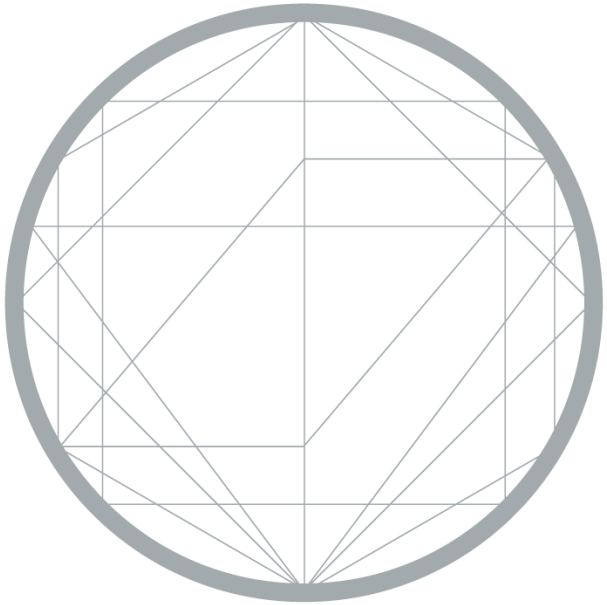
- Package 1.0 em fevereiro 2019 e 2.0 9 a 12 meses depois (detalhado no próximo slide);
- A SIBS disponibilizará os interfaces para um screening em realltime, o qual, o mais tardar, aquando do lançamento do package 2.0, entregará sugestão de GO/NO GO, Score de Risco e o Nome da regra preponderante (possibilidade de entregas parciais entre 1.0 e 2.0, com visibilidade ao incremento de accuracy dos parâmetros);
- O CETELEM terá acesso à ferramenta podendo, em realtime, atuar com bloqueio ou desbloqueio de IBANs/IPs/Entidades(Referência)/User.

Monitorização e intervenção

- A SIBS realizará a análise do caso, encaminhando as situações de potencial fraude para despiste do Banco junto do cliente final
- A SIBS dispõe de equipa operacional dedicada de prevenção de fraude 24x7, assim como *data scientist* para modelização e implementação de novas regras previamente simuladas

Projeto de implementação

Onlinebanking	Responsabilidade	Data
Adjudicação do cliente	Banco	1.11
Disponibilização da Release Documentation – Arquitetura e Estrutura de Mensagem	SIBS	30.11
Desenvolvimento de Mensagem e tratamento do score de risco	Banco	TBD
Disponibilização dos 5/6 maiores casos de fraude 17/18	Banco	03.12
Disponibilização de Manual de Serviço	SIBS	30.01
Inicio de testes de QLY com bancos (testar ligação SIBS/Banco)	SIBS	01.02
Disponibilização do modelo de prevenção e fraude 1.0	SIBS	28.02
Inicio de testes de PRD com bancos (testar analise de score e analise de alertas)	SIBS	01.03



SIBS

Partner in payments

Estrada Casal do Canas
Lote 3
2720 - 092 Amadora
PORTUGAL