RealTransfer

INSTITUIÇÃO DE PAGAMENTO, S.A.

POLÍTICA DE GESTÃO DE FRAUDE

Índice

1. Objetivo 2
2. Definições 3

2.1. Fraude 3
3. Categorias de fraude 4
4. Tipologia de fraude 5

Fraude ao consumidor 5

Fraude à Instituição 7
5. Modelo de governo 8

5.1. Avaliação de Risco 9

5.2. Deveres e responsabilidades 11
6. Gestão de Fraude 12

6.1. Prevenção e deteção 12

6.2. Análise, classificação e resolução 13

6.3. Procedimentos de comunicação e de reporte de Fraude 13
7. Formação 15
8. Conclusão 16
9. Promulgação 16
10. Anexos 18

Anexo I 18
Fluxo do processo de gestão de fraude de consumidor 18

Anexo II 19
Fluxo do processo de gestão de fraude à instituição 19

Anexo III 20
Burlas e esquemas mais comuns 20

1. Objetivo

A "Política de Gestão de Fraude" da "RealTransfer – Instituição de Pagamento, S.A." refere-se ao conjunto de diretrizes, procedimentos e práticas implementadas para prevenir, identificar, monitorizar e tratar incidentes de fraude relacionados com os serviços de pagamento oferecidos. Desta forma, pretende-se assegurar a confiança nas operações financeiras realizadas pelos clientes, minimizando os riscos de fraudes que possam afetar tanto os clientes quanto a própria Instituição.

Em Portugal, assim como no restante da União Europeia, as Instituições de Pagamento devem cumprir a Regulamentação Europeia, em particular a Diretiva 2015/2366/UE, conhecida como PSD2 (Serviços de Pagamento 2), que estabelece requisitos de segurança e prevenção de fraude em serviços de pagamento.

Feito o exposto, encontram-se entre os principais objetivos e requisitos dessa Política os seguintes pontos:

- Identificação e prevenção de fraude:

→ Implementação de medidas técnicas e organizacionais para identificar e prevenir fraude em tempo real;

→ Uso de autenticação forte de clientes para prevenir acessos não autorizados e transações fraudulentas;

→ Análise de comportamentos e padrões para detetar atividades suspeitas, como transações fora do comum ou tentativas de acesso não autorizadas.

- Monitorização e investigação:

→ Utilização de sistemas de monitorização para detetar transações suspeitas, como transferências incomuns ou grandes volumes de movimentações financeiras;

→ Utilização de processos para investigação de eventos de fraude e reporte de incidentes às autoridades competentes, conforme exigido pela legislação.

- Responsabilidade e formação:

→ Definição clara de responsabilidades dentro da Instituição, garantindo que os colaboradores e os responsáveis pela gestão de fraude sejam devidamente formados e capacitados;

→ Adoção de práticas de sensibilização e formação regular para todos os colaboradores sobre riscos e prevenção de fraude.

- Gestão de riscos:

→ Avaliação e gestão contínua dos riscos relacionados com fraude, implementando medidas para mitigá-lo;

→ Desenvolvimento de planos de resposta a incidentes de fraude, incluindo protocolos de recuperação e comunicação com os clientes afetados.

- Conformidade regulatória:

→ A Política assegura que a Instituição cumpre com todas as normas e regulamentações pertinentes a nível nacional e europeu, incluindo a PSD2 e o Regulamento Geral de Proteção de Dados (RGPD);

→ Estabelecimento de processos para garantir a transparência na comunicação com os clientes e entidades reguladoras, especialmente no caso de incidentes de fraude.

- Colaboração com Autoridades:

→ A Política prevê a colaboração com as autoridades competentes, como o Banco de Portugal e a Polícia Judiciária, entre outras, para a investigação de fraudes mais complexas e a partilha de informações relevantes;

→ A presente Política é revista periodicamente para se ajustar às novas ameaças e exigências regulatórias. O objetivo final é proteger tanto os clientes como a própria instituição de pagamento contra os riscos de fraude, garantindo a integridade das operações e a confiança no sistema financeiro.

Os processos de gestão de fraude descritos na atual Política aplicam-se a todas as unidades de negócio da RealTransfer e vinculam todos os colaboradores ao reporte obrigatório e imediato ao responsável de Auditoria Interna de todas e quaisquer suspeitas de situações irregulares, que envolvam fraude e também condutas impróprias.

A Política de Gestão de Fraude evidencia a necessidade de as situações irregulares serem reportadas através dos canais definidos para o efeito, tão depressa quanto possível por forma a garantir o melhor tratamento e a sua rápida e eficaz resolução.

Quanto maior a eficiência do processo, mais simples será mitigar o seu risco para a Instituição.

Tendo em conta a especificidade do conceito de fraude, não é possível garantir a proteção total face à mesma. Contudo, podem ser tomadas medidas preventivas que têm como objetivo reduzir o respetivo risco de ocorrência.

2. Definições

2.1. Fraude

A fraude pode ser definida como um ato deliberado de engano, manipulação ou distorção da verdade, com a intenção de obter um benefício ou vantagem ilegítima, geralmente à custa de outra pessoa ou entidade. Esse comportamento envolve a violação de regras, leis ou normas éticas, e pode ocorrer em diversos contextos, como financeiro, comercial, jurídico ou pessoal.

Num contexto financeiro, por exemplo, a fraude pode envolver:

- → Manipulação de informações: apresentação de dados falsos ou distorcidos para enganar outra parte, como em declarações financeiras fraudulentas;
- → Roubo ou apropriação indevida: utilização de meios fraudulentos para ter acesso a dinheiro, bens ou informações pessoais sem consentimento;
- → Engano em transações: como em esquemas de vendas fraudulentas, onde o vendedor não entrega os produtos ou serviços prometidos após o pagamento;
- → Fraude digital: como o *phishing* ou *malware*, onde fraudadores tentam obter dados sensíveis, como senhas bancárias ou informações de cartão de crédito, para realizar transações não autorizadas.

A fraude é punível por Lei, sendo que as suas consequências legais variam dependendo da gravidade do ato.

O principal objetivo da fraude passa por obter uma vantagem indevida, seja em termos de dinheiro, bens ou outra vantagem, e envolve sempre uma ação deliberada de engano ou ocultação de informações relevantes. Desta forma, resulta normalmente em algum tipo de prejuízo para uma outra parte envolvida.

Relativamente à Fraude Externa, poderá definir-se como perdas potenciais resultantes de atividades com intenção fraudulenta levada a cabo por clientes da RealTransfer e terceiros (outros *stakeholders*, excluindo colaboradores). Neste sentido, a Fraude Externa ocorre quando os atos definidos no conceito de fraude são perpetrados por pessoas ou entidades externas à RealTransfer.

3. Categorias de Fraude

À semelhança de outras Instituições, a RealTransfer enfrenta várias ameaças que podem prejudicar a sua reputação e até mesmo a sua sustentabilidade financeira. Estas podem ter múltiplas origens e ser de natureza diversa e muitas delas, se não a maioria, têm origem em fontes ou agentes externos. No entanto, as fraudes levadas a cabo por agentes internos, ainda que sejam uma minoria, têm um impacto bastante mais pernicioso.

A Fraude Interna ocorre quando um membro dos Órgãos Sociais, Conselho Executivo, Diretor, Responsável ou outro Colaborador da RealTransfer participa em atividades fraudulentas.

A Fraude Externa consiste na atividade fraudulenta cometida por pessoas ou entidades externas à RealTransfer.

4. Tipologia de Fraude

A RealTransfer delineou os diferentes tipos de fraude passíveis de acontecer, de uma forma abrangente e simplista, bem como o processo de tratamento das mesmas, de acordo com o tipo de fraude.

- **Fraude ao Consumidor**

A fraude ao consumidor acontece quando o consumidor é vítima de fraudadores, sendo difícil de ser identificada, especialmente por um consumidor que acredita que está a enviar dinheiro por uma causa justa ou que está emocionalmente envolvido. Existem dois lados na fraude ao consumidor, em que o remetente é normalmente a vítima da fraude e o destinatário é o criminoso.

Seguem alguns exemplos de fraude ao consumidor:

- Burla financeira aos idosos

As razões pelas quais os burlões procuram os idosos para cometer fraude são as seguintes:

→ Cidadãos mais velhos são mais propensos a ter maiores poupanças;

→ É menos provável que denunciem fraude, porque não sabem a quem as denunciar ou não sabem que foram enganados;

→ Estarão mais interessados em produtos que prometem melhor saúde, companheirismo ou estabilidade financeira. Os autores de fraude podem tirar partido disso;

→ Alguém pode estar a forçá-los a realizar uma transação pessoalmente ou por telefone.

- Lotaria ou sorteios

A vítima deste tipo de burla pretende provavelmente enviar dinheiro para uma empresa ou organização ao invés de uma pessoa singular. É muito provável e comum que tenham recebido uma carta a notificá-los sobre o dinheiro que ganharam e, inclusive, podem ter uma cópia impressa dessa mesma carta. Neste cenário, o colaborador deve fazer perguntas do género:

→ Está a enviar dinheiro para uma empresa/organização? Onde ouviu falar deles?

→ Foi-lhe pedido para enviar dinheiro para pagamento de impostos e/ou taxas?

- Compra *online*

Se um consumidor solicita o envio de dinheiro para efetuar uma compra *online*, é muito provável que se trate de um caso típico de burla. O consumidor enviará dinheiro para o burlão e nunca mais terá notícias dessa pessoa. A maioria dos *websites* tem uma opção de pagamento diferente que proporciona um nível de proteção para o comprador e o vendedor. Neste cenário, o colaborador deve fazer perguntas como:

→ A pessoa mencionou que está a enviar dinheiro para pagar um serviço ou um item, como um cachorro que comprou *online*, por exemplo?

- Romance

Um consumidor pode mencionar que se encontrou ou foi contatado por alguém *online* e acredita estar numa relação romântica. O burlão aproveita-se das emoções do consumidor e pede que lhe envie dinheiro para que se possam encontrar, viajar, mudar de cidade/país, etc. Neste cenário, o colaborador deve fazer perguntas como:

→ Há quanto tempo conhece esta pessoa?

→ Como é que se conheceram?

→ Falou de outras opções de pagamento?

→ Qual é a urgência?

→ Já conheceu o destinatário pessoalmente, cara a cara?

- Empréstimo falso

Os esquemas de empréstimos falsos começam geralmente com um *e-mail* ou carta de uma empresa desconhecida que se oferece para emprestar dinheiro ao remetente. O consumidor solicitará o envio de dinheiro para cobrir quaisquer taxas ou pagamentos adiantados associados ao empréstimo. Neste caso, o remetente não irá receber um empréstimo e perde o seu dinheiro. Neste cenário, o colaborador deve fazer perguntas como:

→ Está a enviar dinheiro para a concessão de um empréstimo que encontrou *online*?

→ O destinatário prometeu-lhe o empréstimo depois de pagar impostos, taxas, pagamentos adiantados através de uma transferência bancária?

- Outros exemplos de fraude ao consumidor:

→ Cheque ou ordem de pagamento;

→ Desastre;

→ Anúncio de jornal.

Situações de fraude como estas são tratadas diretamente pelo departamento de Auditoria Interna com o acompanhamento do Conselho de Administração, utilizando os canais de comunicação de fraude disponibilizados pela empresa.

- **Fraude à Instituição**

As tecnologias têm provocado alterações nas diferentes práticas sociais, económicas e culturais, o que permite atingir grandes níveis de desenvolvimento associados, essencialmente, à informatização e à automatização de processos e serviços. Através de meios eletrónicos é possível realizar movimentações financeiras, tratamento de dados e armazenamento em suporte digital, o que veio potenciar novas debilidades no meio digital e conduzir à adaptação e surgimento de novos esquemas de fraude. Verifica-se, deste modo, o despertar do interesse fraudulento, maioritariamente praticado pela mesma via, e em constante acompanhamento das novas tecnologias.

As situações mais frequentes de fraude a que a RealTransfer está sujeita enquanto Instituição de Pagamento são:

- Transação de teste

Os Agentes e Correspondentes da RealTransfer não podem solicitar por telefone o registo de uma transferência-teste de dinheiro. Quaisquer chamadas de pedidos para efetuar transações de teste são fraudulentas. Neste caso, recusa-se a transação de teste e contacta-se de imediato o departamento de Auditoria Interna.

- Atualizações de *software* ou crimes informáticos

Quaisquer atualizações relacionadas com dispositivos ou *software* são feitas automaticamente pelo departamento de Sistemas de Informação da RealTransfer. O colaborador deve contactar de imediato os departamentos de Auditoria Interna e de Sistemas de Informação se achar que um *e-mail* ou *link* é suspeito. A fim de evitar este tipo de fraude, os colaboradores não devem responder ou clicar em *links* em *e-mails* fora do comum, que podem conter *malware* ou vírus. O departamento de Sistemas de Informação garante a instalação e atualização de *softwares anti-vírus e spyware*.

- Crimes cibernéticos

Phishing

É um processo utilizado por indivíduos com pretensões maliciosas e com o intuito de capturar dados pessoais e sensíveis que possam facilitar a fraude, sendo realizado através do envio de e mail ou outros tipos de mensagens (ex: SMS) preparados para serem vistos como se fossem enviados por entidades legítimas, tendo como objetivo a abertura de ficheiros que as leva para um *site* falso criado para parecer autêntico ou o contacto para linhas telefónicas falsas com o intuito de obter informações pessoais sensíveis.

Pharming

Muito idêntico ao *phishing*, ocorre quando um vírus informático instalado num dispositivo fixo ou móvel redireciona a hiperligação inscrita pelo cliente para uma página de internet falsa, em alguns casos idêntica à página oficial da instituição, permitindo a obtenção de informação confidencial. Pode acontecer quando é feito o *download* de ficheiros ou programas que parecem inofensivos.

Spyware

É um programa malicioso que é instalado no computador ou *tablet* de um indivíduo sem que este se aperceba. Uma vez instalado, deteta se está a aceder a uma página de internet protegida e regista os dados inseridos pelo utilizador.

No anexo III à presente Política, estão apresentados detalhes referentes aos tipos de fraude mais comuns na utilização dos serviços de transferências de dinheiro, sendo importante relembrar que a lista de fraudes enumeradas pretende ser meramente informativa e não exaustiva para consciencialização, sendo plausível a existência de outros tipos de fraudes.

5. Modelo de Governo

A estrutura organizacional que suporta a implementação da presente Política assenta no modelo das três linhas de defesa:

- Primeira linha de defesa, composta por todos os colaboradores;
- Segunda linha de defesa, composta pela função de Gestão de Riscos e de Conformidade;
- Terceira linha de defesa, representada pela função de Auditoria Interna.

As áreas identificadas na 2ª linha de defesa têm por objetivo assegurar o correto desenvolvimento, implementação e monitorização dos procedimentos de gestão de fraude, garantindo que todos os processos são alvo de análise e definição das ações subsequentes para o respetivo encerramento e mitigação do risco futuro.

Na 3ª linha, a função de Auditoria Interna tem por objetivo avaliar e testar de forma independente a eficiência dos processos implementados, emitindo uma opinião sobre o ambiente de controlo percecionado

e a forma como os processos são geridos. Para garantir a adequação de todas as atividades inerentes ao desenvolvimento da presente Política, a RealTransfer identificou os principais responsáveis e respetivas funções a desempenhar ao nível do desenvolvimento, validação, aprovação, monitorização e reporte.

5.1. Avaliação de Risco

A avaliação de risco de fraude é um processo crucial em qualquer Instituição, especialmente em instituições financeiras de pagamento como a RealTransfer, para identificar, analisar e mitigar os riscos associados a fraude que possam ocorrer dentro da sua atividade. Esse processo envolve a identificação de vulnerabilidades nos sistemas e procedimentos da Instituição e a implementação de medidas de prevenção e resposta adequadas para reduzir o impacto financeiro e reputacional.

O objetivo principal da avaliação de risco de fraude é entender e quantificar os riscos de fraude que a Instituição enfrenta, bem como a possibilidade de ocorrência de eventos fraudulentos e os seus potenciais impactos. Ao realizar essa avaliação, a Instituição segue as seguintes etapas:

- Identificação das fragilidades nos processos que possam ser exploradas por fraudadores;
- Desenvolvimento de medidas preventivas adequadas para mitigar ou evitar situações de fraude;
- Definição de planos de resposta e contingência para minimizar os danos em caso de ocorrência de fraude;
- Cumprimento de regulamentos legais e normativos que exigem a implementação de medidas rigorosas de segurança e a prevenção de fraude.

O risco de fraude pode emergir em diversas áreas onde não exista qualquer histórico deste tipo de ocorrência, pelo que os precedentes de fraude não são um indicador completo de todos os potenciais riscos de fraude. Assim, a RealTransfer necessita de identificar, medir/categorizar e, se necessário, implementar estratégias para mitigar este tipo de risco.

De forma a manter a avaliação de risco de fraude atualizada, o Conselho de Administração, em conjunto com a função de Gestão de Riscos, são responsáveis pela revisão anual dos riscos de fraude na Instituição, pela revisão dos procedimentos efetuados por cada uma das áreas/departamentos da Instituição e pela realização de testes de eficácia aos controlos identificados. Esta medida tem por objetivo verificar se os controlos funcionam de forma adequada e consistente ao longo de um determinado período e de acordo com os procedimentos estabelecidos para mitigar os riscos existentes.

De forma a avaliar a priorização de cada incidente, a necessidade de envolvimento da Direção de Segurança ou de Conselho de Administração e necessidade de reportar às Autoridades regulatórias e/ou judiciais de forma a salvaguardar os interesses dos consumidores e do sector financeiro em geral, cabe a função de Gestão de Riscos estimar tanto a probabilidade de ocorrência como o grau de severidade do possível impacto de acordo com os seguintes critérios.

Risco = probabilidade x consequência

Probabilidade: Hipótese de risco ocorrer num espaço de x tempo

Consequência: Grau de impacto de risco

Parâmetros de probabilidade

Avaliação	Probabilidade %	Descrição	Pontos*
Esperado	>90	Esperado que ocorra a qualquer momento	4
Muito provável	≥55≤90	Esperado que ocorra na maioria das vezes	3
Provável	≥30≤55	Ocorre com frequência	2
Pouco provável	≤30	Não ocorre com frequência	1

*Os pontos atribuídos à "Probabilidade do Risco" são definidos pela função de Gestão de Riscos, com base em valores que considera lógicos para o efeito.

Parâmetros de consequência

Grau	Pontos*
Alto	3
Médio	2
Baixo	1

*Os pontos atribuídos à "Consequência do Risco" são definidos pela função de Gestão de Riscos, com base em valores que considera lógicos para o efeito.

Assim, para graduação de risco, utiliza-se a seguinte escala:

Escala de Graduação de Risco

Probabilidade (pontos)				
4	4	8	12	
3	3	6	9	
2	2	4	6	
1	1	2	3	
	1	2	3	Consequência (pontos)

Legenda:
1-2_Reduzido_F1
3-4_Moderado_F2
5-8_Elevado_F3
9-12_Severo_F4

O grau de risco de um determinado incidente define a urgência na intervenção por parte da equipa de Auditoria Interna e/ou o desenho de medidas de mitigação imediatas ou de curto/médio prazo.

Caso a pontuação seja igual ou superior a "9" o órgão de Administração da RealTransfer terá de intervir de imediato, efetuando a denuncia as Autoridades Regulatórias e/ou Judiciais, que tomará a decisão final nesta matéria.

5.2. Deveres e Responsabilidades

A prevenção de fraude diz respeito a todos os Colaboradores da RealTransfer. No entanto, incumbe particularmente aos diretores e responsáveis das áreas atestar que todas as atividades em que se verifiquem suspeitas de fraude são imediatamente reportadas.

- Direção de Segurança

Direção de Segurança é envolvida no processo de prevenção e gestão de fraude no sentido de desenvolver ações específicas de acompanhamento da implementação das medidas descritas na presente Política e verificar constantemente a sua adequabilidade em função da normal evolução organizacional da RealTransfer.

- Função do Cumprimento Normativo

O responsável pela função do Cumprimento Normativo acompanha todas as situações de suspeita de fraude ocorridas na RealTransfer.

- Auditoria Interna

A Auditoria Interna contribui na realização de uma apropriada Política de Gestão de Fraude, no âmbito das ações de Auditoria. Nas ações de Auditoria é especificamente considerado o risco de fraude e eficácia das medidas antifraude. No caso de serem detetadas deficiências, são efetuadas recomendações com base numa avaliação de risco e tomadas as medidas preventivas e adequadas para garantir a efetividade dos controlos.

- Recursos Humanos

São da responsabilidade dos Recursos Humanos as ações relacionadas com legislação laboral a serem tomadas nos casos de fraude.

- Colaboradores

Cada colaborador estará obrigado a empenhar-se para que a RealTransfer não seja vítima de qualquer atividade fraudulenta reportando, imediatamente, nos termos já referidos anteriormente, qualquer suspeita.

6. Gestão de Fraude

6.1. Prevenção e deteção

Esta fase contempla a deteção de um evento de fraude que tanto pode ser interno por via de colaborador ou monitorização, como externo por via de cliente ou fornecedor.

A nível interno, todos os colaboradores são responsáveis pela prevenção e deteção de situações de fraude ou conduta imprópria, que possam vir a ocorrer ou tenham ocorrido na Instituição, e têm a obrigatoriedade de reportar ao departamento de Auditoria Interna. Ao nível externo, a RealTransfer possui medidas e procedimentos de proteção do cliente contra situações de fraude, disponibilizando um Formulário de contacto para reporte de incidentes.

A RealTransfer promove um ambiente ético e transparente que encoraja todos os membros dos órgãos sociais e colaboradores a participar ativamente na proteção da reputação da Instituição, promovendo uma cultura de integridade, em particular:

→ Implementando as políticas e os procedimentos que constituem os princípios e valores éticos pelos quais a Instituição se rege, o que inclui a promoção do cumprimento das normas de comportamento profissional vertidas no Código de Conduta e das políticas e procedimentos relativos aos Conflitos de Interesses;

→ Implementando políticas de recrutamento focadas na integridade dos candidatos a emprego, incluindo a realização de verificações suficientes do historial relativas ao nível e à natureza das funções a exercer.

Todos os casos de fraude detetados são geridos em linha com os processos internos definidos no âmbito da presente Política e revistos, tendo por base toda a informação disponível para determinar se é considerado um potencial incidente de fraude e os casos com suspeita de fraude são reencaminhados para um nível superior de revisão, juntamente com a documentação suporte.

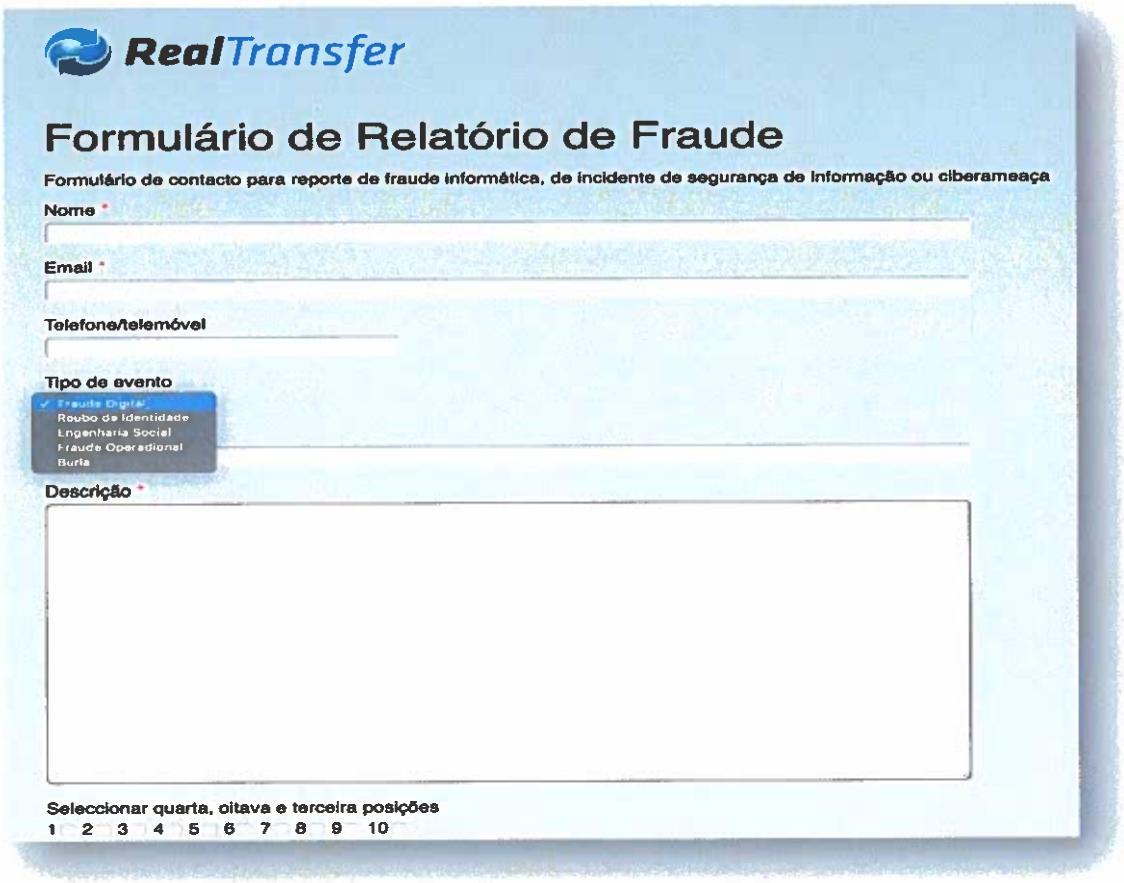
6.2. Análise, classificação e resolução

No âmbito dos incidentes de fraude detetados, o departamento de Auditoria Interna analisa os eventos reportados de acordo com a sua categoria e tipologia. A seguir os eventos serão classificados tendo por base o binómio severidade e probabilidade de ocorrência estimadas, de forma a permitir a sua correta priorização. Os eventos de fraude analisados, tanto internos como externos, são encaminhados para o departamento de Sistemas de Informação, ou para o encarregado de Proteção de Dados ou para o Conselho de Administração, dependendo da sua classificação, para o seu tratamento através de um plano de ação delineado pelo responsável de área afetada pela fraude. Após a sua resolução a documentação relativa a cada evento registado é arquivada por um período mínimo de 7 anos.

6.3. Procedimentos de comunicação e de reporte de Fraude

A RealTransfer implementou os canais adequados de comunicação e linhas de reporte que permitam a qualquer cliente, terceiro ou fornecedor, sob absoluta confidencialidade, comunicar à RealTransfer a prática de uma fraude de que tenha conhecimento ou um mero indício de que uma determinada situação possa vir a ser fraudulenta.

No sentido de contribuir para a divulgação de potenciais situações de fraude, a RealTransfer dispõe de um formulário para preenchimento *online*, ao qual poderá aceder através do *link*: https://realtransfer.pt/form_fraude.



O reporte pode também ser efetuado através do Canal de Denúncia. Este canal permite a apresentação e o seguimento seguro de denúncias, a fim de garantir a integridade e conservação da denúncia, a confidencialidade da identidade ou o anonimato dos denunciantes e a confidencialidade da identidade de terceiros mencionados na denúncia, impedindo o acesso de pessoas não autorizadas.

Tanto os consumidores, como os colaboradores ou qualquer outro *stakeholder* da RealTransfer, têm ao seu dispor os seguintes canais de denúncia ou reclamação de fraude:

- E-mail: fraude@realtransfer.pt
- Formulário *Online*: https://realtransfer.pt/form_fraude
- Telefone: +351 213 569 844
- Denúncia Anónima: https://realtransfer.anonimizado.org.pt/
- E-mail da função de Auditoria Interna: auditoria.interna@realtransfer.pt

As situações suspeitas de fraude deverão ser reportadas logo que se verifique a sua ocorrência ou a suspeita da sua ocorrência. Caso existam dúvidas sobre a situação a reportar deverá ser contactado o departamento de Auditoria Interna utilizando o endereço eletrónico supramencionado.

Deverão ser reportadas quaisquer suspeitas de fraude, alegadamente cometida pelos colaboradores da RealTransfer, nomeadamente qualquer alegado envolvimento de Administradores, Diretores, Responsáveis e Colaboradores em situações suspeitas de fraude, em particular os que tenham um papel significativo no sistema de Controlo Interno e/ou no processo de Reporte Financeiro da Instituição. Deverão igualmente ser reportadas quaisquer suspeitas de fraude, alegadamente perpetradas por pessoas ou entidades externas à RealTransfer.

Consoante a severidade de ocorrência do evento em mãos, o departamento de Auditoria Interna e/ou a Administração podem decidir reportar este tipo de evento aos órgãos regulatórios e/ou judiciais correspondentes e/ou encaminhando o denunciante.

Nos casos de fraude cibernética, o canal de comunicação preferencial com as entidades policiais é o seguinte:

- https://www.policiajudiciaria.pt/unc3t/
- Telefone: +351 211 967 000

Para todas as demais situações o reporte de eventos às Autoridades poderá ser feito recorrendo às seguintes hiperligações ou contactos nelas contidos:

https://clientebancario.bportugal.pt/pt-pt/material/seguranca-online-prevencao-de-fraude

https://clientebancario.bportugal.pt/formulario-nova-reclamacao

https://www.cncs.gov.pt/

https://www.cncs.gov.pt/certpt/notificar-incidente/

https://www.policiajudiciaria.pt/unc3t/

https://www.consumidor.gov.pt/

https://cec.consumidor.pt/

https://cec.consumidor.pt/topicos1/praticas-comerciais-desleais/fraudes-e-burlas.aspx

7. Formação

Todos os colaboradores devem estar alertas para a possibilidade de ocorrência de situações de fraude, devendo para o efeito participar em ações de formação/sensibilização adequadas sobre a matéria com vista a estarem em melhor posição para prevenir, detetar e responder aos potenciais riscos de fraude.

A RealTransfer empenha-se em garantir que todos os seus colaboradores estão cientes das suas responsabilidades. Assim, estas ações de formação/sensibilização são uma parte essencial da prevenção da fraude e devem ser concebidas de modo a:

- Promover uma cultura de combate e prevenção à fraude desde a Administração da RealTransfer até aos colaboradores;
- Comunicar as responsabilidades definidas na presente Política a todos os colaboradores;
- Dotar os colaboradores das ferramentas necessárias que permitam identificar os sinais de alerta de fraude;
- Assegurar que os colaboradores estão conscientes dos mecanismos de comunicação de fraude conforme o documentado nesta Política e no Código de Conduta.

As ações de formação têm um caráter mínimo anual, podendo, no entanto, ter uma recorrência maior, devendo referir toda a informação relevante que esteja incluída nas políticas e procedimentos da Instituição.

8. Conclusão

Uma estratégia de sucesso para a prevenção da ocorrência de situações de fraude envolve a criação de um ambiente inibidor para este tipo de infrações, sendo da responsabilidade de cada colaborador garantir que este ambiente é criado.

Apesar das diferentes circunstâncias que as eventuais suspeitas de fraude possam assumir, é fundamental que sejam todas investigadas e que seja dada uma resposta adequada às situações que de facto se tenham materializado.

Um colaborador que esteja alerta para a possibilidade da existência de fraude ou situações irregulares é um elemento fundamental para a mitigação deste tipo de riscos.

O presente documento é da autoria do RCN e é revisto e atualizado periodicamente ou sempre que se considere necessária e imprescindível à sua revisão.

9. Promulgação

O Conselho de Administração da "RealTransfer - Instituição de Pagamento, S.A.", enquanto responsável pela gestão da Instituição, aprova a presente "Política de Gestão de Fraude".

Responsável pelo Cumprimento Normativo,

Olga Pushkarenko Tomás

Com o Conhecimento de Administração

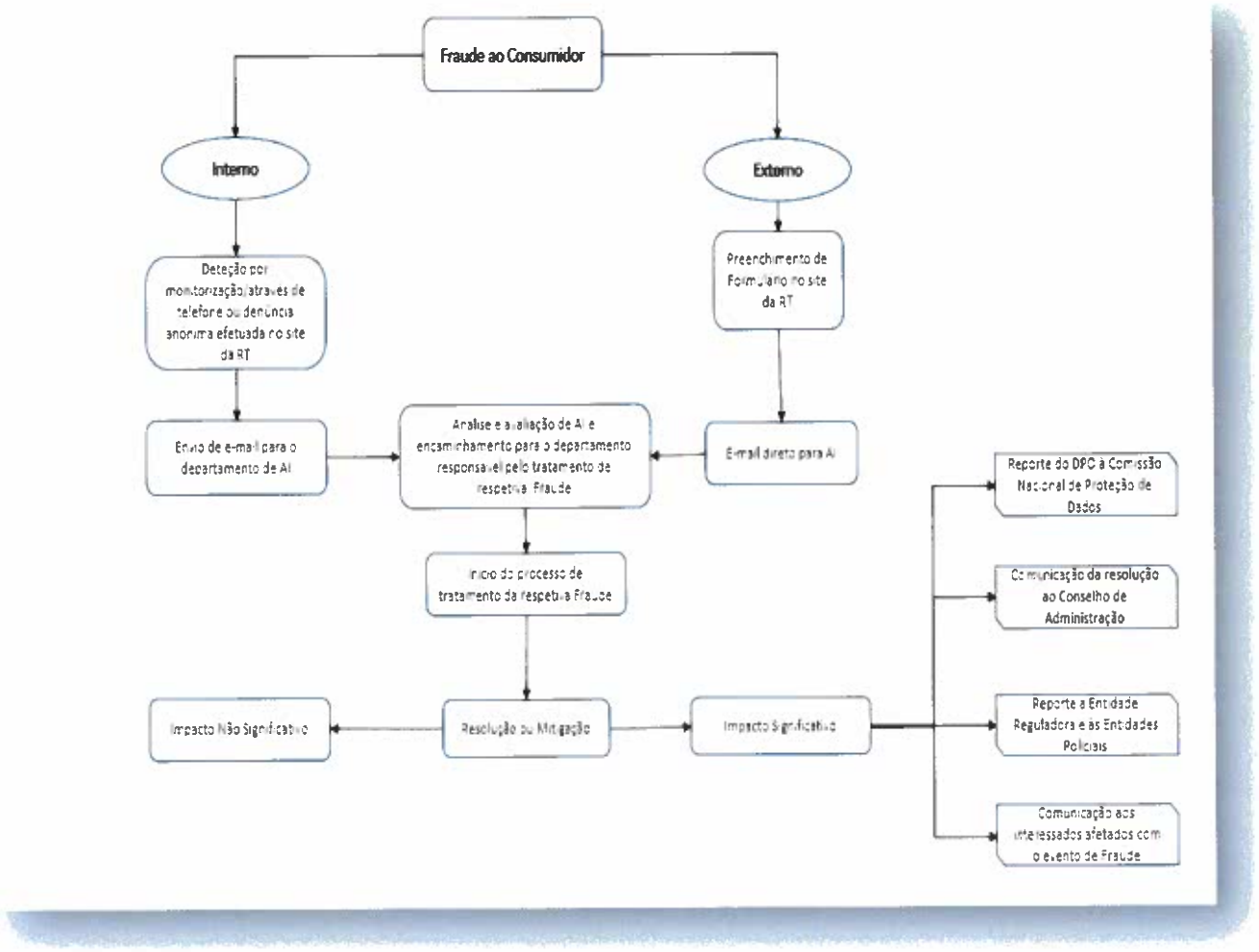
Vera Lúcia Afonso Figueira Aires

João Afonso Coelho Bettencourt da Camara

10. Anexos

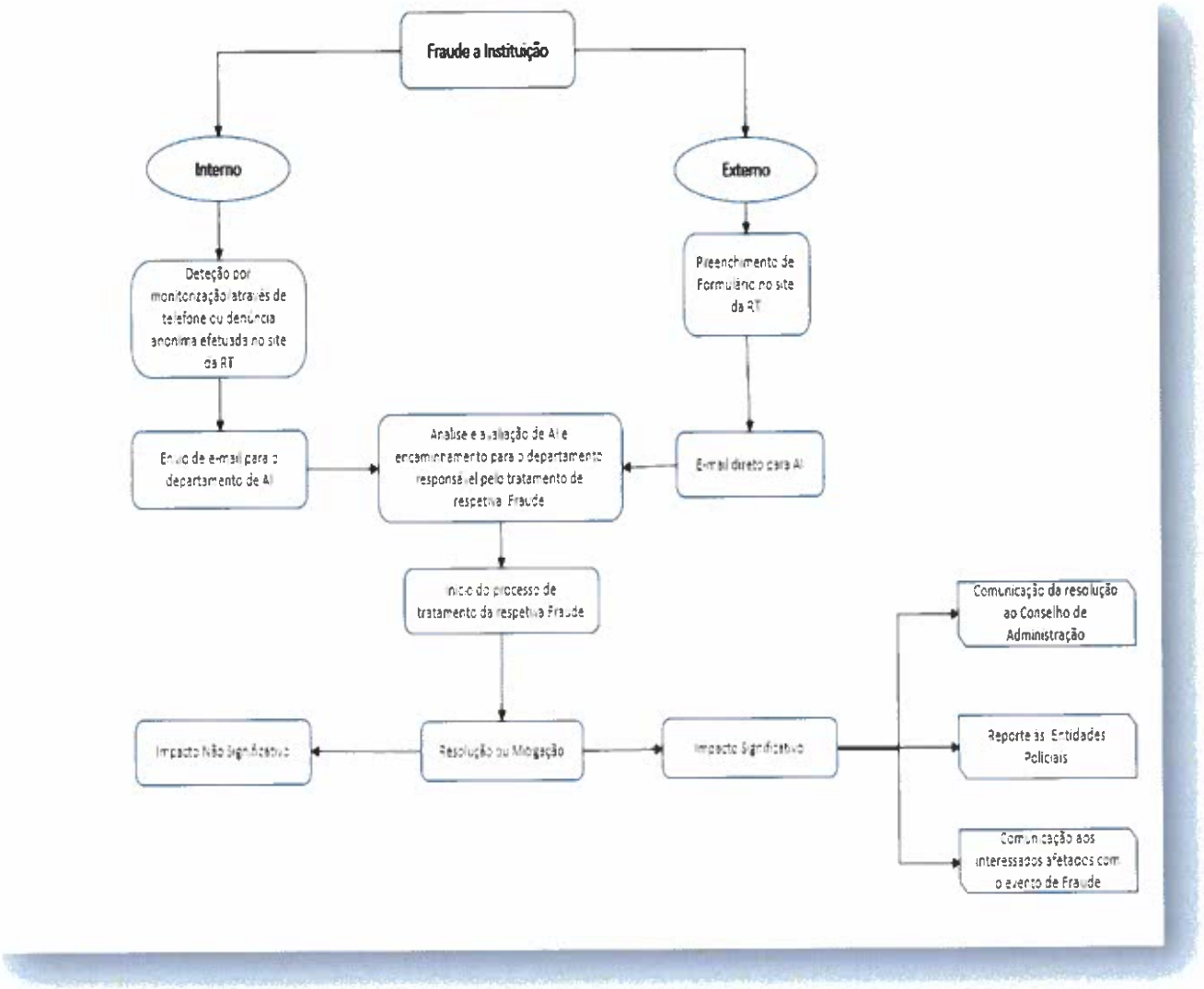
Anexo I

Fluxo do processo de gestão de fraude de consumidor



Anexo II

Fluxo do processo de gestão de fraude à Instituição



Anexo III

Burlas e esquemas mais comuns

Burlas e Esquemas mais comuns	
Doações e auxílio em catástrofes	Trata-se da realização de uma doação, aquando do acontecimento de uma catástrofe ou desastre natural, cujo destino dos fundos seja ajuda humanitária, mas que invés seja utilizado como um esquema de burla.
Reembolsos ou Indemnizações	Esquema de fraude realizado através de um terceiro fazendo-se passar por um organismo oficial (Ex: Banco de Portugal, ASAE, DECO, etc....), prometendo a prestação de auxílio na obtenção de reembolsos ou indemnizações.
Compras Online ou através de Revistas/Jornais	Trata-se da compra de um produto ou serviço fraudulento, cujo preço e condições sejam os melhores comparativamente com o mercado, utilizando o serviço de transferências de dinheiro para evitar qualquer tipo de pagamento de impostos.
Romance	Este tipo de fraude acontece não presencialmente através de um anúncio, site de encontros, email, serviços de chat ou mensagens instantâneas, por forma a ganhar um grau de intimidade ou confiança com a pessoa que irão burlar.
Prémios de Lotaria	Realiza-se através de um contacto, mensagem ou aviso a informar que ganhou a lotaria ou qualquer outro tipo de jogo oficial e que, para reclamar ou reivindicar o prémio seja necessário o pagamento de uma taxa de serviço.
Cheque	Situações de fraude em que são realizadas através da utilização de cheques falsos ou sem cobertura, em que seja necessário a realização de uma transferência de dinheiro para poder levantar os valores, o que irá gerar ao consumidor perdas e comissões de processamento por parte dos Bancos.
Abuso de idosos	Quando um terceiro se oferece para a realização da gestão de finanças, ativos ou bens, com o objetivo de manipular e condicionar a atuação, tendo em vista a tomada de posse de património para a realização de transações. Este tipo de esquemas pode assumir várias formas incluindo fraudes de telemarketing, de usurpação de identidade, empréstimos predatórios com condições extremamente desfavoráveis, esquemas relacionados com remodelações de casas ou compras de propriedades, entre outros.
Familiares em situações urgentes	Familiar distante ou terceiro fazendo-se passar por familiar que se encontra numa suposta situação de carácter urgente e que solicita o envio de dinheiro como ajuda para a resolução da mesma.
Empréstimos	Este tipo de fraude habitualmente consiste no envio de emails, cartas ou mensagens a explicar como obter um empréstimo ou mesmo a confirmar que um empréstimo que nunca se pediu já foi aprovado. Solicitam-se o pagamento de taxas de crédito, taxas de serviço, taxas de abertura de conta ou administrativas, impostos, adiantamentos ou qualquer outro tipo de custo antes de ser disponibilizado os fundos do "falso" crédito.