Nº 1 – Setembro 2023

Sf
Serviços financeiros

Pagamentos

Fraudes e burlas

Contacte a
nossa equipa:

Paulo Fonseca
servicosfinanceiros@deco.pt

DECO
Associação Portuguesa para a
Defesa do Consumidor

FRAUDES E BURLAS NOS PAGAMENTOS

FORMAS MAIS COMUNS, CUIDADOS A TER E DIREITOS DO CONSUMIDOR

DECO
SEMPRE CONSIGO

DECO
SEMPRE CONSIGO

Voz dos Consumidores

Síntese

Com a crescente digitalização nos pagamentos e o aumento das compras online, em especial devido ao impacto da pandemia, os utilizadores de meios de pagamento eletrónicos e digitais estão a ser cada vez mais confrontados com fraudes e burlas.

A DECO recebeu um número significativo de contactos com pedidos de informação e reclamações relatando fraudes e burlas que levaram a perdas de quantias avultadas. Os media e o Banco de Portugal também reportam um crescimento de casos. As situações são diversas na sua natureza e forma, porém o resultado final é o prejuízo do consumidor sem que este tenha, de forma consciente ou voluntária, pretendido efetuar a transação ou conceder o acesso aos perpetradores da fraude.

A legislação em vigor trouxe um conjunto de medidas que procuraram incrementar a segurança nos pagamentos e introduzir mais direitos dos consumidores. Porém, há aspetos que carecem de mais intervenção e clarificação, reconhecendo as lacunas e corrigindo-as, em benefício de todos os intervenientes do ecossistema de pagamentos nacional.

Pontos de Discussão

I. Enquadramento

De acordo com o Banco de Portugal, em 2021 "*Os instrumentos de pagamento eletrónicos (cartões de pagamento, débitos diretos, transferências a crédito e transferências imediatas) continuaram a ser os preferidos dos consumidores portugueses. Estes instrumentos foram utilizados em 99,5% dos pagamentos de retalho, em número, e em 89,3%, em valor, excluindo o numerário*"[1]. Para o ano de 2022, antecipa-se um aumento desta utilização, com o reforço da

[1] Relatório dos sistemas de pagamentos, Banco de Portugal, 2021

utilização de pagamentos com a funcionalidade *contactless.* Em paralelo, o comércio eletrónico tende a manter a tendência crescente registada em 2021[2].

No Relatório dos Sistemas de Pagamento de 2022[3], o Banco de Portugal indica que "*Os consumidores portugueses continuam a preferir os instrumentos de pagamento eletrónicos (cartões de pagamento, débitos diretos, transferências a crédito e transferências imediatas). Excluindo o numerário, em 2022, estes instrumentos foram utilizados em 99,7% dos pagamentos de retalho, mais 0,2 pontos percentuais (pp) do que em 2021. Os cartões são o instrumento de pagamento eletrónico mais utilizado no dia a dia, tendo sido responsáveis por 88,0% do número de pagamentos do SICOI (86,5% em 2021). Em média, foram realizados 9 milhões de pagamentos com cartão por dia, o que corresponde a um total de 3283,1 milhões de operações em 2022*."

No mesmo relatório, o Banco de Portugal indica que as taxas de fraude em Portugal são reduzidas, mas ainda assim relevantes: "*As* ***operações com cartões****, na ótica da entidade emitente,* ***apresentaram as taxas de fraude mais elevadas****, embora o valor médio por operação fraudulenta seja o mais baixo (45 euros). Já* ***as transferências a crédito tiveram um valor médio por transação fraudulenta de 4059 euros****, mas apenas cinco em cada milhão de transferências foram fraudulentas. O valor médio da fraude por débito direto foi de 499 euros."*

Apesar deste cenário, os portugueses ainda não revelam ter um grau de conhecimento e capacidades de utilização que lhes permita estar protegidos. Os índices de literacia financeira e digital revelam que ainda há um longo caminho a percorrer, conforme identificado pela OCDE no seu relatório sobre a literacia financeira digital em Portugal[4].

Neste contexto, há um crescimento de casos de fraudes ou burlas. As formas mais frequentes de fraudes ou burlas têm como alvo os clientes, usando técnicas de engenharia social ou comportamental, incluindo o roubo dos dados dos cartões, dos códigos de autenticação ou de acesso a contas através de técnicas como o *phishing*, o *pharming*, ou o *spoofing*. Nos dois primeiros casos, os esquemas procuram obter dados sensíveis através de falsos sites ou acedendo a bases de dados. No último, os atacantes fazem-se passar por alguém conhecido ou que representa a instituição de pagamento, levando a que sejam os consumidores a atuar sob a

---

2 https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=473570976&DESTAQUESmodo=2

3 Ver https://www.bportugal.pt/sites/default/files/anexos/pdf-boletim/rsp2022.pdf

4 https://www.oecd.org/finance/financial-education/digital-financial-literacy-portugal.htm

falsa perceção de que estão a ser contactados por alguém legítimo, fornecendo dados ou códigos de acesso/transação ou efetuando transferências.

O Banco de Portugal informa que "*Nas operações com cartões, a emissão de uma ordem de pagamento por parte do infrator é* ***o tipo de fraude mais comum*** *e ocorre quando o infrator emite uma ordem de pagamento após ter obtido,* ***habitualmente através de mecanismos de engenharia social****, como é o caso do phishing, as credenciais de segurança do utilizador.* ***Este tipo de fraude aumentou em 2022, tendo sido responsável pela quase totalidade das operações fraudulentas****.*

Também ***nas transferências a crédito, a maioria das fraudes (70%)*** *resultou da emissão de uma ordem de pagamento por parte do infrator* ***após obter as credenciais de segurança do cliente lesado****. A manipulação do ordenante pelo infrator para emitir uma ordem de pagamento deixou, assim, de ser o tipo de fraude mais frequente nas transferências a crédito.*"

Nestes casos, a legislação falha aos consumidores afetados. Em casos de reclamação do consumidor "*negue ter autorizado uma operação de pagamento executada, ou alegue que a operação não foi corretamente efetuada, incumbe ao respetivo prestador do serviço de pagamento fornecer prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento*." Porém, quando um consumidor indica que foi enganado a efetuar uma transação que não pretendia, ou a partilhar códigos através dos quais foram efetuadas transações não pretendidas, esta situação acaba por ser, em muitos casos, classificada de negligência grosseira, pelo que o prestador de serviços de pagamento se recuse a reembolsar.

II. O que já foi feito

A DECO contribuiu para o desenvolvimento da legislação em vigor, acompanha os desenvolvimentos do mercado e identifica os problemas e lacunas do contexto regulatório. É o caso da Diretiva de Serviços de Pagamento revista (DSP2), transposta em Portugal pelo Decreto-Lei n.º 91/2018, de 12 de novembro. A Diretiva trouxe algumas melhorias na defesa dos interesses dos consumidores, procurando ir ao encontro de algumas das preocupações identificadas no contexto da versão anterior. Algumas das alterações verificaram-se nos direitos, como a:

- a redução da responsabilidade por operações de pagamento não autorizadas de 150 EUR para 50 EUR;

- um direito incondicional ao reembolso dos débitos diretos em euros por um período de oito semanas;
- a eliminação da cobrança de encargos suplementares pela utilização de um cartão de crédito ou de um cartão de débito de um consumidor.

Outro aspeto muito importante refere-se à introdução dos requisitos de autenticação forte, com a exigência de dois fatores de confirmação do cliente. Este requisito aplica-se no acesso à informação da conta, por exemplo no *homebanking*, ou para efetuar algumas transações, como transferências. O caso mais relevante da exigência de autenticação forte é nas compras online com cartão, em que o pagamento deve ser sujeito a dois fatores de confirmação. O objetivo desta exigência era a de redução do volume de fraudes e transações não autorizadas. Os requisitos de autenticação forte do cliente entraram em vigor a 14 de setembro de 2019, em toda a União Europeia. Desde essa data, os bancos e os demais prestadores de serviços de pagamento estão obrigados a aplicar autenticação forte dos seus clientes sempre que estes acedam online à sua conta, iniciem um pagamento eletrónico ou realizem remotamente uma ação que possa envolver risco de fraude ou outros abusos. A autenticação forte implica que o prestador de serviços de pagamento (PSP) solicite ao utilizador pelo menos dois elementos pertencentes, cada um, a uma das seguintes categorias:

- Conhecimento (por exemplo, PIN ou palavra-passe);
- Posse (por exemplo, *one-time password* (OTP), telemóvel ou cartão de pagamento);
- Inerência (por exemplo, impressão digital).

O Banco de Portugal acompanha a implementação da legislação e o seu cumprimento, bem como recebe as reclamações neste âmbito, divulgando os indicadores relativos no seu Relatório dos Sistemas de Pagamento.

III. O que está a ser feito

A DECO acompanha este tema com muita preocupação. Como tal, na sua participação no Fórum de Sistemas de Pagamento, promovido pelo Banco de Portugal, a DECO indicou que o tema deve estar no topo das prioridades da Estratégia Nacional para os Pagamentos de Retalho para os próximos anos. Em paralelo, a DECO procura apoiar os consumidores que reclamam, no sentido de saberem o que devem fazer, quais os meios de reclamação e como solicitar o ressarcimento, se possível. Adicionalmente, a DECO promove a informação e literacia dos consumidores através de artigos, entrevistas e conteúdos nos seus canais, retratando os métodos, referindo os riscos, reforçando os cuidados a ter e indicando os caminhos a seguir em caso de ser alvo de fraude.

O Banco de Portugal também refere estar preocupado com esta evolução de casos, procurando informar os consumidores.

Os media acompanham o tema de forma reativa, relatando alguns casos e procurando identificar os esquemas.

As autoridades parecem estar também a par, lançando alertas[5] e avisos para informar a população e tentando prevenir que sejam enganados nestes esquemas. A PSP indica mesmo que recebeu "mais de 36 mil queixas de burla informática e nas comunicações nos últimos quatro anos, tendo este tipo de crime aumentado 20% em 2022, ano em que se destacou a fraude "Olá pai, olá mãe". Este tipo de fraude enquadra-se no *spoofing*, mencionado atrás.

A nível europeu, o BEUC (Organização Europeia de Associações de Consumidores) também companha a preocupação com o tema, revelando que as fraudes são um problema em outros países também. Assim, preparou uma ficha[6] em que identifica algumas das principais formas de fraude, o que acontece quando se reclama e o que se exige em defesa dos interesses dos consumidores.

IV.O que queremos

A identificação das formas de fraude é um passo fundamental para a perceção dos métodos e de como se pode prevenir. Mas também é importante compreender que os ataques são levados a cabo por pessoas ou entidades que conhecem a legislação e as suas lacunas.

Por um lado, é importante que haja mais ações de alerta, com a intervenção das autoridades, do supervisor, das entidades de pagamento e dos representantes dos consumidores. Por exemplo, as campanhas devem ser preparadas para diferentes grupos de utilizadores (diferentes faixas etárias, diferentes contextos geográficos) e recorrendo a canais de divulgação distintos – TV (programas de informação, integrando o tema em programas de ficção), social media (posts, influenciadores) e jornais.

Porém, esta capacitação dos consumidores não pode servir para os responsabilizar e desresponsabilizar os prestadores de serviços de pagamento.

---

5 https://www.tsf.pt/portugal/sociedade/burla-informatica-aumentou-20-em-2022-ola-pai-ola-mae-e-uma-das-fraudes-em-destaque-15793116.html

6 https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-027_A_payment_fraud_epidemic.pdf

Deste modo, é necessário que haja um conjunto de medidas que tragam maior confiança e segurança para os consumidores, reforçando a sua proteção. Assim, a DECO considera que deve haver medidas relativas a:

- Prevenção de fraudes
  - Nas transferências a créditos haja mecanismos de confirmação do IBAN;
  - Mecanismos de monitorização de transações para detetar potenciais movimentos fraudulentos e, confirmando-se que o são, impedi-los;
  - Meios de confirmação de sites e números de telefone a fim de detetar e bloquear os canais fraudulentos;
  - Possibilitar que os consumidores possam bloquear ou impedir movimentos de pagamentos/transferências, e introduzir limites às transações;
  - Responsabilizar todos os envolvidos nas cadeias de informação e contacto - p.e. as plataformas de redes sociais no caso de promoção de lojas falsas.
- Reembolsos mais regulares em caso de fraude:
  - Compensação imediata nos casos de transações não autorizadas, conceito que deve acolher os casos de transações em que o consumidor foi enganado a fazê-las. A negligência grosseira deve ser claramente definida e ser excecionalmente aplicada;
  - Deve haver uma partilha de responsabilidade entre os prestadores de serviços de pagamento de origem e de destino nas transações, incentivando um maior envolvimento.
- Melhor supervisão do cumprimento da legislação:
  - Obrigando os PSPs a informar o consumidor dos seus direitos;
  - Adesão obrigatória a mecanismos de resolução alternativa de litígios e a aceitação das decisões;
  - Definição de um regime de sanções para os casos de não reembolso;
  - Maiores poderes para as entidades de supervisão.

No imediato, a DECO propõe **que sejam implementados mecanismos de prevenção e deteção que abordem algumas das formas mais comuns de fraudes.** Para assegurar que estes mecanismos são transversais e efetivamente implementados, esta implementação deve ser regulamentada e definida com base no supervisor – o Banco de Portugal, assegurando também a ausência de custos para os clientes.

- Marcação de IBANs fraudulentos

A criação de uma lista ou base de dados de IBANs utilizados em fraudes, com um registo centralizado – com base em denúncias e reclamações efetuadas pelos utilizadores e especialmente se houver incidências recorrentes com o mesmo IBAN.

A implementação de um sistema de alertas para esses IBANs – cada vez que haja um pedido de transferência para um IBAN constante da base de dados ou lista acima referida, a instituição de pagamentos suspende a operação e contacta o utilizador informando-o de que o IBAN indicado está numa lista de incidências. Solicita, então, a confirmação se o utilizador pretende mesmo avançar com a operação. Se o utilizador decidir avançar, a operação pode ser efetuada.

O ónus da prova de que foi efetuada esta confirmação deve estar do lado do PSP.

- Mais informação nas SMS de autenticação forte

A melhoria da informação nas SMSs, destacando a transação subjacente - os mecanismos implementados para a autenticação forte incluem as SMSs, em que são enviados códigos de utilização única (*one time password* – OTP). Esses códigos podem servir para aceder a contas ou autorizar uma transação, como uma transferência. Como referido, em muitos casos de fraude, o infrator engana o utilizador levando-o a partilhar esses códigos sob falsas premissas. Com uma melhoria da informação na SMS, dando mais destaque ao teor e finalidade dos códigos enviados, pode servir para uma melhor informação e reconhecimento dos conteúdos e de que estes não devem ser partilhados com terceiros.

- Monitorização de transações padrão

Implementação de monitorização de transações e alertas em caso de desvio do padrão – alguns PSPs implementaram a monitorização de transações dos clientes, com o devido cumprimento de proteção de dados e sigilo, estabelecendo um padrão de movimentos. Caso haja movimentos fora do padrão – pelo montante, pelo horário, ou tipo de transação - existem alertas para contactar o cliente e confirmar se está efetivamente a fazer essa operação. Essa monitorização pode recorrer a ferramentas como a inteligência artificial ou outras.

A monitorização deve ser aplicada também quanto a formas de conexão, seguindo o IP ou o IMEI habitual. EM caso de conexão em IP ou aparelho móvel diferente do habitual, acionar um alerta e contactar o cliente para confirmar.

- Estabelecimento de limites de transação

Deve ser disponibilizada a possibilidade de os utilizadores estabelecerem limites de transações, em especial em ambiente online. Esses limites só poderiam ser alterados com dupla confirmação e após um determinado período (p.e. 24 horas depois de definidos). Esta solução teria um impacto especial para os utilizadores menos habituados ao contexto digital, reforçando a sua

confiança neste contexto e impedindo que tomem decisões ou façam transações de forma precipitada, p.e. por influência de burlões.

- Reforçar a informação nas referências Multibanco (MB)

Este instrumento de pagamento tem sido usado em fraudes, sem que seja possível identificar quem a pratica. Os pagamentos com recurso a referências MB carecem de mais transparência, nomeadamente com a identificação da entidade que irá receber os fundos. Esta informação também está ausente nos extratos das contas dos pagadores. É urgente que se torne obrigatório indicar quem é o recipiente dos pagamentos, tanto no momento da instrução como no extrato de conta do pagador. As entidades que geram e comercializam essas referências deverão ter a responsabilidade de identificar e informar de quem são os recipientes.

- Marcação de referências MB fraudulentas

À semelhança da medida proposta para os IBANs, deve ser criada uma base de dados centralizada de referências MB usadas em fraudes, partilhada entre todos os PSPs, que terão a obrigação de a consultar sistematicamente.

Com base nessa lista, devem ser criados alertas para quaisquer tentativas de pagamento a essas referências, informando o pagador de que há esse registo de fraude associado.

- Criação de formas de apoio para clientes alvo de fraude

Devem ser criados pontos de contacto para os clientes, nos diferentes canais, em especial uma linha telefónica de apoio disponível a qualquer hora, para que os utilizadores de meios de pagamento possam reportar problemas, fraudes ou burlas, e solicitar o bloqueio ou suspensão de transações suspeitas. Caso este ponto de contacto não esteja disponível, o consumidor não pode ser responsabilizado pela transação fraudulenta.

- Implementação de campanhas de sensibilização e educação dos consumidores

Um passo fundamental e imediato é a criação de campanhas de informação, sensibilizando e educando os consumidores e utilizadores de meios de pagamento acerca de:

  - formas corretas de utilização
  - tipos de fraudes e burlas mais correntes, incluindo os SMS sobre produtos desalfandegar ou das autoridades e as mensagens do tipo “Olá, pai/mãe”,
  - formas de comunicação e resolução de problemas
  - procedimentos essenciais para reportar fraudes
  - procedimentos que devem seguir para assegurar que o interlocutor é efetivamente fidedigno (nos casos em que identifiquem como representando o PSP)

Os canais e programas de maior audiência deveriam servir para transmissão destas mensagens, seguindo exemplos como o *product placement* de outras áreas.

- Eliminação das limitações da legislação

A legislação é limitada no seu alcance de proteção dos utilizadores pois impede que estes tenham direito ao reembolso de transações fraudulentas em muitos casos. Assim, deve ser implementada uma alteração imediata para que haja o direito a compensação imediata nos casos de transações não autorizadas, conceito que deve acolher os casos de transações em que o consumidor foi enganado a fazê-las. A negligência grosseira deve ser claramente definida e ser excecionalmente aplicada.

Adicionalmente, deve haver um regime de partilha de responsabilidade entre os prestadores de serviços de pagamento de origem e de destino nas transações, incentivando um maior envolvimento.

- Adesão obrigatória dos PSPs a mecanismos de resolução alternativa de litígios

É importante que haja esta obrigação, permitindo que algumas situações possam ser resolvidas fora dos tribunais, assegurando maior celeridade e menores custos.

- Colaboração entre autoridades policiais, o supervisor, PSPs e organizações de consumidores

A prevenção de fraudes passa também por agir proactivamente no sentido de identificar tendências nascentes. Para esse esforço, devem contribuir colaborativamente todas as partes interessadas, incluindo as autoridades policiais e de investigação, o supervisor do setor, as entidades que oferecem os serviços (PSPs) e os representantes dos utilizadores.

V. O que já conseguimos

Neste contexto, a DECO reforçou a importância deste tema junto do Banco de Portugal, do Parlamento, da Comissão Europeia, e nos media.

Assim, a DECO conseguiu a inclusão deste tema como prioridade nos próximos anos no âmbito dos trabalhos do Fórum de Sistemas de Pagamento, do Banco de Portugal.

A nível europeu, a DECO contribuiu para a elaboração da ficha temática publicada pelo BEUC sobre o tema, identificando os tipos de fraudes e as principais reivindicações.

A DECO reportou à CE estas reivindicações e identificou as lacunas na legislação europeia no âmbito das representações que assegura.

VI.Os próximos passos

A DECO manterá o seu foco neste tema. Por um lado, promovendo a melhoria do contexto regulatório para que se possa reduzir o impacto dos ataques fraudulentos e permitir que o consumidor tenha direito ao reembolso em caso de ser alvo de fraude. Por outro, reforçará a informação e formação aos consumidores, num esforço individual e em conjunto com outras entidades, a fim de educar os consumidores quanto ao que deve fazer e o que não deve fazer.

DECO

SEMPRE CONSIGO

deco.pt

CONTACTE-NOS:

DECO LISBOA (SEDE)
R. de Artilharia Um, nº 79, 4.º
1269-160 Lisboa
Tel.: 21 371 02 00
deco@deco.pt

DECO DELEGAÇÕES

DECO MINHO
Av. Batalhão Caçadores 9,
nº 279 4900-341 Viana do Castelo
Tel.: 258 821 083
deco.minho@deco.pt

DECO NORTE
R. da Torrinha, n.º 228 H, 5.º
4050-610 Porto
Tel.: 223 391 960
deco.norte@deco.pt

DECO CENTRO
R. Padre Estevão Cabral,
n.º 79, 5.º, Sala 504
3000-317 Coimbra
Tel.: 239 841 004
deco.centro@deco.pt

DECO RIBATEJO E OESTE
R. Eng. António José Souto
Barreiros Mota, nº 6 L
Tel.: 243 329 950
deco.ribatejoeoeste@deco.pt

DECO ALENTEJO
Travessa Lopo Serrão,
n.º 15A e 15B, r/c
7000-629 Évora
Tel.: 266 744 564
deco.alentejo@deco.pt

DECO ALGARVE
R. Dr. Coelho de Carvalho, n.º 1 C
8000-322 Faro
Tel.: 289 863 103
deco.algarve@deco.pt

DECO MADEIRA
Loja do Munícipe do Caniço
Rua Doutor Francisco Peres
9125-014 Caniço
Tel: 968 800 489
deco.madeira@deco.pt

fale connosco

966 449 110