

Sentença

Processo nº 890/2025

Reclamante:

Reclamada:

Sumário

I - O litígio versa sobre a restituição de quantias relativas a operações de pagamento supostamente não autorizadas.

II - A legislação aplicável estabelece que o prestador de serviços de pagamento deve provar que as operações foram devidamente autorizadas e autenticadas, com observância dos requisitos de autenticação forte do cliente.

III - Nos termos da lei, a responsabilidade pelo uso não autorizado de instrumentos de pagamento pode ser imputada ao utilizador, nomeadamente nos casos em que se verifica negligência grave na proteção dos dados de acesso.

IV - A jurisprudência tem entendido que a responsabilidade do prestador de serviços de pagamento está afastada quando este comprova a execução correta das operações e a inexistência de falha técnica ou operacional, cabendo ao utilizador demonstrar a ausência de negligência grave para obter a restituição.

V - Em caso de negligência grave do utilizador, este suporta integralmente os prejuízos resultantes das operações.

1. Relatório

1.1 Não foi possível a conciliação entre as partes, pelo que se passou, de imediato, à audiência de julgamento arbitral.

1.2. O Reclamante pretende que a Reclamada proceda à restituição da quantia de 3.311,57€ relativa a alegadas transferências bancárias não executadas pelo Reclamante e ao pagamento das taxas de arbitragem.

1.3. A Reclamada contestou e alegou que não pode ser responsabilizada pelas transferências ocorridas dado que o Reclamante, face a um pedido que recebeu por

SMS, para atualização de dados, acabou por fornecer a terceiros, desconhecidos, os seus dados de autenticação.

2. Objeto do Litígio

O objeto do litígio corporiza-se na seguinte questão: saber se assiste ou não ao Reclamante o direito à restituição da quantia de 3.311,57€ relativa a alegadas transferências bancárias não executadas por si e ao pagamento das taxas de arbitragem.

3. Fundamentação

3.1 Dos Factos

1. O Reclamante é cliente particular da Reclamada;
2. No dia 21.02.25, o Reclamante constatou que a Reclamada tinha autorizado diversas transferências da sua conta bancária sem o seu consentimento, doc 1;
3. Trataram-se de oito transferências bancárias, doc 1;
4. O Reclamante alegou que apenas uma única vez foi solicitado pela Reclamada uma autenticação, doc 2;
5. A Reclamada apenas procedeu à restituição da quantia de 1.104,00 €, docs 1 e 3;
6. O Reclamante referiu que a Reclamada retirou novamente o valor que tinha restituído;
7. O Reclamante exarou reclamações, nºs 000120250071206 e 000120250069590, tendo a Reclamada, através de email datado de 07.03.25, refutado qualquer responsabilidade, docs 2 a 4;
8. O Reclamante voltou a reclamar no dia 12.03.25 e no dia 21.03.25, não tendo conseguido a devolução da quantia retirada, doc 4;

9. A Reclamada alega que o Reclamante fez adesão ao serviço de pagamento Pay, sendo que essa adesão é efetuada numa primeira fase através dos dados do cartão, numero, validade e CVV;
10. Depois foi enviado para o nº de telefone do Reclamante um SMS para adesão Pay no cartão;
11. Para tal foram necessários credenciais de acesso e inserção do código recebido por SMS;
12. Colocado este Código é gerado um novo código que ao ser colocado no Wallet Pay permite a conclusão da adesão, passando o equipamento onde foi instalada a aplicação a estar apto a iniciar a sua utilização;
13. A Testemunha da Reclamada, departamento de Reclamações de Transações, explicou a situação dos autos, tendo referido que houve um pedido de atualização falso, que alguém se fez passar pela pedindo que o Reclamante atualizasse ali os seus dados;
14. A Testemunha esclareceu que o Reclamante permitiu que terceiros instalassem a sua aplicação em outro telemóvel ou dispositivo;
15. A Testemunha referiu que esta aplicação equivale a um cartão físico;
16. A Testemunha sublinhou o Reclamante deu os seus dados na suposta que depois sai um SMS, que o cliente entra na aplicação do e coloca o código, criando a aplicação um novo código;
17. A Testemunha referiu ainda que o Reclamante por desconhecimento legitimou que outrem pudesse entrar na sua conta bancaria e tivesse efetuado transferências;
18. O Reclamante referiu que o Banco mais tarde bloqueou o seu cartão e que não sabe porque não o fez antes, podendo ter evitado a situação;
19. A Testemunha da Reclamada informou que não pode precisar quando é que o Banco aciona o bloqueio, pois existem heurísticas que estão definidas para ativar suspeitas e proteção dos clientes;
20. A Testemunha declarou que no caso só pelas 2:00 da manhã foi enviada a mensagem de bloqueio ao cliente, pois só nessa altura o sistema acionou um alerta.

3.1.1 Dos Factos Provados:

Resultam provados os seguintes factos:

Prova documental: 2 (parcialmente provado que as quantias foram retiradas da conta do Reclamante), 3, 4, 5, 7, 8.

Prova por declaração: 1, 6, 9, 10 11, 12, 13, 14, 15, 16, 17, 18 (relativamente ao bloqueamento), 19, 20.

3.1.2. Dos Factos Não Provados:

Factos: 2 (relativamente ao consentimento do Reclamado); 18 (relativamente ao facto de o bloqueio dever ter sido operado mais cedo)

O Tribunal alicerçou, ainda, a sua convicção nos factos acessórios apresentados na audiência de julgamento.

3.2. Motivação

A questão central do litígio reside em determinar se o Reclamante tem ou não direito à restituição do montante de 3.311,57€, alegadamente retirado da sua conta bancária sem o seu consentimento.

Com base na prova produzida, ficou demonstrado que terceiros acederam aos dados do Reclamante por via de um esquema fraudulento, tendo este, por desconhecimento, facultado elementos que permitiram a ativação do serviço Pay noutro dispositivo.

Ainda que se reconheça a existência de transações não diretamente autorizadas pelo Reclamante, ficou igualmente provado que a sua atuação negligente contribuiu de forma relevante para a concretização das mesmas, pelo que não assiste ao Reclamante

o direito à restituição integral da quantia reclamada nem ao reembolso das taxas de arbitragem.

4. Do Direito

Nos termos do Decreto-Lei n.º 91/2018, de 12 de novembro, que transpõe para o ordenamento jurídico nacional a Diretiva (UE) 2015/2366 (PSD2), cabe ao prestador de serviços de pagamento — neste caso, a instituição bancária — demonstrar que uma operação de pagamento alegadamente não autorizada foi devidamente autenticada, registada, executada corretamente e que não foi afetada por qualquer falha técnica. É o que dispõe o artigo 116.º, n.º 1. Esta regra estabelece um ónus probatório claro a cargo da instituição financeira, exigindo-lhe que demonstre a legitimidade da operação contestada.

Contudo, o mesmo diploma, no artigo 115.º, prevê que, quando a operação resulta da perda, furto ou apropriação indevida do instrumento de pagamento, o utilizador poderá ser responsável por perdas até 50 euros, exceto quando se demonstre fraude ou negligência grave, casos em que a responsabilidade pode ser total.

A jurisprudência portuguesa tem vindo a consolidar este entendimento.

No acórdão do Supremo Tribunal de Justiça (proc. n.º 17903/19, de 8 de abril de 2025), o tribunal reafirmou que *“o banco-prestador apenas se pode exonerar de responsabilidade se provar que a operação foi autenticada e que se deveu à negligência grave do ordenante”*.¹

1

<https://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/22cd26cc9b96ce9d80258c7300322a93?OpenDocument>

Também o Tribunal da Relação do Porto, no Acórdão de 18 de abril de 2023 (proc. n.º 16900/21), considerou existir negligência grave sempre que o utilizador ignore regras básicas de segurança, designadamente ao inserir códigos de autenticação ou dados sensíveis em plataformas fraudulentas, mesmo que sob engano.²

No presente caso, ficou provado que o Reclamante, na sequência de um esquema fraudulento que simulava uma atualização da _____, forneceu os seus dados bancários, incluindo códigos enviados por SMS, permitindo a ativação da aplicação Pay num dispositivo desconhecido.

Tal ativação exige autenticação forte (Strong Customer Authentication) conforme o Decreto-Lei n.º 91/2018, artigo 2.º, alínea d), o qual define que a autenticação forte requer a utilização de dois ou mais elementos independentes das categorias:

- conhecimento (algo que só o utilizador sabe, como password ou PIN),
- posse (algo que possui, como telemóvel que receba SMS),
- inerência (algo inerente ao utilizador, como biometria).

A independência entre esses fatores garante que a violação de um não compromete os demais, assegurando a proteção dos dados de autenticação.

A prova documental e testemunhal constante nos autos demonstrou que estas condições foram cumpridas, e que as transferências resultaram de um uso regular da aplicação autorizada via autenticação forte, embora em circunstâncias resultantes de erro e desconhecimento do próprio Reclamante.

2

https://www.dgsi.pt/JTRP.NSF/56a6e7121657f91e80257cda00381fdf/15beb4204b49fe98802589b40046cb97?OpenDocument=&utm_source=chatgpt.com

Assim, apesar de o Reclamante não ter intencionalmente ordenado as transferências, ficou demonstrado que a sua conduta, ao fornecer dados de acesso a terceiros e permitir a ativação da aplicação em um dispositivo que não era o seu, foi determinante para a concretização das operações, configurando uma atuação com negligência grave, à luz do artigo 119.º, n.º 2.

Nestes termos, a instituição de crédito não é responsável pela restituição da quantia de €3.311,57 reclamada, nem pelas taxas associadas à arbitragem, pois não se verifica uma falha no serviço prestado, mas sim um uso indevido causado por comportamento do próprio cliente.

5. Decisão

Nestes termos, julga-se improcedente o pedido de restituição da quantia de €3.311,57, bem como o reembolso das taxas de arbitragem, por não se verificar qualquer atuação culposa por parte da Reclamada, absolvendo-se a Reclamada do pedido.

Notifique-se.

Porto, 20.06.25

A Juiz-Árbitro,

Manoel João Almeida