Phishing e operações não autorizadas: novos desenvolvimentos jurisprudenciais sobre a responsabilidade dos bancos

info@abreuadvogados.com
abreuadvogados.com



O Tribunal da Relação de Lisboa confirmou a condenação de um banco ao reembolso de 30.654,66€ a dois clientes vítimas de phishing, num esquema que envolveu uma falsa mensagem da Netflix e a associação não autorizada de um cartão bancário à carteira digital Apple Pay de terceiros.

O acórdão, de 22 de outubro de 2026, surge num contexto de reforço da proteção dos utilizadores de serviços de pagamento, marcado também pelo recente acórdão do Tribunal de Justiça da União Europeia (TJUE), de 15 de outubro de 2026, no processo C-70/25, Tukowiecka. Nesta decisão, o TJUE clarificou que a alegada negligência grosseira do cliente não permite ao prestador de serviços de pagamento recusar o reembolso imediato de uma operação não autorizada.

As duas decisões permitem identificar importantes orientações quanto à distribuição do ónus da prova, à avaliação da negligência grosseira, às exigências de autenticação forte e às consequências da recusa de reembolso.

1. Ónus da prova: não basta a utilização do instrumento de pagamento

No acórdão da Relação de Lisboa, o banco sustentou que a associação do cartão à Apple Pay e as operações subsequentes tinham sido realizadas com autenticação forte. Contudo, não juntou aos autos registos técnicos que demonstrassem que o cliente tivesse recebido e introduzido um segundo código de autenticação, nem que as 19 operações tivessem sido efetivamente autenticadas nos termos legalmente exigidos.

O Tribunal salientou que os registos relevantes se encontravam na esfera de controlo do banco e que a mera indicação de que as operações foram «aprovadas» não demonstrava que tivessem sido autorizadas pelo cliente.

Nos termos do artigo 113.º do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RJSPME), aprovado pelo Decreto-Lei n.º 91/2018, de 12 de novembro, cabe ao prestador demonstrar que a operação foi autenticada, devidamente registada e contabilizada, bem como a inexistência de deficiência do serviço e os factos que permitam imputar ao cliente fraude, dolo ou negligência grosseira.

O TJUE, no processo C-70/25, confirmou, igualmente, que compete ao prestador provar a negligência grosseira do cliente, não sendo suficiente invocar o incumprimento dos deveres de proteção das credenciais de segurança.

Assim, conclui-se que os registos de autenticação e os elementos técnicos que sustentam a imputação da operação ao cliente devem ser concretos, completos e aptos a fazer prova.

2. Negligência grosseira: avaliação concreta da fraude e dos deveres de informação

A Relação de Lisboa considerou que a conduta do cliente, que introduziu os dados do cartão e um código de ativação Apple Pay numa página fraudulenta, foi negligente, mas não atingiu o grau de negligência grosseira exigido pelo artigo 115.º, n.º 4, do RJSPME.

Na avaliação, o Tribunal ponderou a credibilidade do esquema, na medida em que este reproduzia fielmente a aparência do site da Netflix, o contexto de urgência criado pela mensagem e a perceção do cliente de que estava a regularizar o pagamento de uma mensalidade.

Para além disso, foi relevante o cumprimento dos deveres de informação do banco. A inclusão de advertências genéricas nas condições gerais da conta não foi considerada suficiente para demonstrar que os clientes tinham sido adequadamente alertados para os riscos de phishing. A decisão evidencia que a negligência grosseira não pode ser presumida a partir do simples facto de o cliente ter sido enganado e ter fornecido dados ou códigos. A sua apreciação exige uma análise individualizada das circunstâncias da fraude e do comportamento do utilizador.

3. Autenticação forte na associação de cartões a carteiras digitais

Um dos aspetos centrais do acórdão do Tribunal da Relação de Lisboa respeita à associação do cartão bancário a uma carteira digital instalada num equipamento de terceiros.

O Tribunal concluiu que não ficou demonstrada a aplicação de autenticação forte do cliente no processo de associação do cartão à Apple Pay. A utilização dos dados impressos no cartão e de um código recebido por SMS não permitiu, por si só, comprovar o cumprimento das exigências de autenticação forte.

Neste contexto, a Relação aplicou o artigo 115.º, n.º 5, do RJSPME, segundo o qual, quando o prestador não exige autenticação forte, o ordenante não suporta as perdas decorrentes de operações não autorizadas, salvo se tiver agido fraudulentamente.

Assim, não tendo o banco demonstrado que exigiu autenticação forte, o Tribunal considerou aplicável o artigo 115.º, n.º 5, do RJSPME, que afasta a responsabilidade do ordenante pelas perdas decorrentes de operações não autorizadas, mesmo em caso de negligência grosseira, salvo atuação fraudulenta deste.

A decisão reforça a importância de os prestadores assegurarem e documentarem a autenticação forte nos processos de associação de cartões a carteiras digitais, bem como de conservarem prova técnica que permita demonstrar o cumprimento das exigências legais.

4. Reembolso imediato: a negligência grosseira não justifica a recusa

No acórdão de 15 de outubro de 2026 (C-70/25, Tukowiecka)[1], o TJUE distinguiu expressamente a obrigação de reembolso imediato da determinação final de quem deve suportar as perdas resultantes da operação não autorizada.

Em princípio, o prestador deve reembolsar imediatamente o montante da operação não autorizada e, o mais tardar, até ao final do dia útil seguinte àquele em que teve conhecimento da operação ou foi notificado dela, desde que o cliente comunique a ocorrência sem demora injustificada.

A única exceção identificada pelo Tribunal respeita à existência de motivos razoáveis para suspeitar de fraude cometida pelo próprio cliente, comunicados por escrito à autoridade nacional competente. Em Portugal, o artigo 114.º, n.º 2, do RJSPME exige que essa comunicação seja feita às autoridades judiciárias, no prazo previsto para o reembolso.

A alegação de negligência grosseira não permite, por si só, recusar o reembolso imediato. O prestador poderá, posteriormente, exigir ao cliente o ressarcimento das perdas, desde que demonstre que estas resultaram de uma violação intencional dos seus deveres ou de uma conduta reveladora de negligência grosseira.

No caso apreciado pela Relação de Lisboa, o banco foi condenado a devolver 30.654,66€, acrescidos de juros de mora, desde 11 de fevereiro de 2025, à taxa de 14% ao ano, correspondente à taxa legal acrescida de 10 pontos percentuais, nos termos do artigo 114.º, n.º 10, do RJSPME. Foi ainda confirmada a indemnização de 1.000€ por danos não patrimoniais, considerando a ansiedade, o desgosto e o sentimento de injustiça provocados pela subtração de quantias elevadas.

5. O que devem rever os prestadores de serviços de pagamento?

As decisões evidenciam a necessidade de os bancos, instituições de pagamento e instituições de moeda eletrónica reverem os seus procedimentos internos, em particular quanto a:

- Reembolso de operações não autorizadas: assegurar o cumprimento dos prazos legais, sem fazer depender o reembolso imediato da conclusão da análise sobre eventual negligência grosseira do cliente;
- Conservação da prova: manter registos técnicos completos e acessíveis sobre autenticação, associação de cartões a carteiras digitais e execução das operações;
- Autenticação forte: verificar o cumprimento dos requisitos legais nos processos de associação de instrumentos de pagamento a dispositivos ou carteiras digitais;
- Prevenção e informação: reforçar alertas claros e eficazes sobre esquemas de phishing, evitando depender exclusivamente de cláusulas genéricas nas condições contratuais;

[1] https://curia.europa.eu/site/upload/docs/application/pdf/2026-10/cp260147pt.pdf

- Gestão de reclamações e litígios: assegurar que a recusa do reembolso imediato apenas ocorre perante suspeitas razoáveis de fraude do ordenante, comunicadas por escrito às autoridades judiciárias no prazo legal, distinguindo-a da eventual exigência posterior de ressarcimento, que depende de prova concreta.

A preparação para o futuro Regulamento relativo aos serviços de pagamento (PSR) e para a futura Diretiva relativa aos serviços de pagamento (PSD3) deve prosseguir em paralelo. Em 29 de outubro de 2026, o Conselho da União Europeia adotou as suas posições em primeira leitura sobre ambos os diplomas, cuja tramitação legislativa ainda não se encontrava concluída nessa data. O PSR e a PSD3 não substituem, por ora, o regime atualmente aplicável, mas justificam a antecipação dos ajustamentos em matéria de prevenção da fraude, prova e responsabilidade.

Em síntese, as decisões reforçam que a proteção do cliente vítima de operações não autorizadas não se limita à análise da sua conduta, exigindo também prova robusta por parte do prestador, cumprimento das obrigações de autenticação forte e respeito pela obrigação de reembolso imediato. A eventual negligência grosseira poderá relevar para a repartição final das perdas, mas não constitui fundamento autónomo para suspender ou recusar o reembolso legalmente devido.

A equipa APDFin da Abreu Advogados encontra-se disponível para apoiar os prestadores de serviços de pagamento na avaliação e adequação dos seus procedimentos internos às exigências legais aplicáveis às operações de pagamento não autorizadas, nomeadamente em matéria de autenticação forte do cliente, prevenção de fraude, conservação de prova técnica e cumprimento das obrigações de reembolso, bem como na gestão de reclamações e litígios com clientes.

Thinking about tomorrow? Let's talk today.



Diogo Pereira Duarte
diogo.p.duarte@abreuadvogados.com



Maria Eduarda Andrade
maria.e.andrade@abreuadvogados.com



Margarida Betencourt
margarida.betencourt@abreuadvogados.com



info@abreuadvogados.com
abreuadvogados.com

Abreu advogados