Acórdão do Tribunal da Relação de Lisboa

Processo:	**2035/25.6T8LSB.L1-2**
Relator:	**RUTE SOBRAL**
Descritores:	**RESPONSABILIDADE BANCÁRIA** **OPERAÇÕES NÃO AUTORIZADAS** **AUTENTICAÇÃO FORTE** **UTILIZADOR** **NEGLIGÊNCIA GROSSEIRA** **FRAUDE** **DOLO** **DANOS NÃO PATRIMONIAIS**
Nº do Documento:	**RL**
Data do Acordão:	**22-10-2026**
Votação:	**UNANIMIDADE**
Texto Integral:	**S**
Texto Parcial:	**N**
Meio Processual:	**APELAÇÃO**
Decisão:	**IMPROCEDENTE**
Sumário:	**Sumário (elaborado nos termos do disposto no artigo 663º, nº 7, CPC):** **I. Nas operações de pagamento não autorizadas realizadas por autenticação de terceiro através de dados e credenciais de segurança obtidas ilicitamente por prática de *phishing*, incumbe ao prestador de serviços de pagamento (Banco) demonstrar que a operação foi autorizada pelo utilizador, ou que este atuou com fraude, dolo ou negligência grosseira, não bastando a mera prova de que a operação foi registada ou autenticada no sistema.** **II. A introdução pelo utilizador dos dados do cartão bancário e de um código recebido por SMS numa página fraudulenta que reproduz de forma convincente o sítio oficial de uma entidade prestadora de serviços de *streaming* conhecida, na sequência de mensagem enganosa concebida para induzir a regularização de um alegado pagamento em dívida, traduz comportamento negligente, mas não integra, sem mais, negligência grosseira para efeitos dos artigos 113º e 115º do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica.** **III. A negligência grosseira pressupõe um grau particularmente intenso de desrespeito pelos deveres de cuidado, correspondente a uma atuação que um utilizador médio, razoavelmente informado e prudente, não adotaria.** **IV. Para a aferição da existência de negligência grosseira do utilizador, deve averiguar-se se, no caso concreto, a sua conduta é especialmente censurável, tendo em consideração a aparência fidedigna ou não da mensagem de correio eletrónico, a ingenuidade que manifestou, e o cumprimento pelo banco das obrigações de informação e esclarecimento dos clientes impostas pela lei.** **V. Não se pode qualificar como grosseiramente negligente a conduta de quem fornece credenciais de segurança em resultado de uma prática fraudulenta capaz de ludibriar um grande número de pessoas, e não apenas as extremamente descuidadas ou incautas.**

VI. Não demonstrando o Banco que, no procedimento de associação do cartão bancário a uma carteira digital (*Apple Pay*), foi efetivamente aplicada autenticação forte do cliente, nos termos legalmente exigidos, não pode fazer recair sobre o utilizador as perdas resultantes de operações de pagamento não autorizadas, salvo prova de atuação fraudulenta deste.
VII. A mera alegação e afirmação por testemunha de que o sistema interno exigia etapas adicionais de validação não é suficiente quando o Banco não junta aos autos os registos técnicos suscetíveis de comprovar a concreta realização dessas etapas pelo utilizador.
VIII. Verificada a realização de operações de pagamento não autorizadas, sem prova de fraude, dolo ou negligência grosseira do utilizador, e sem demonstração do cumprimento do dever de autenticação forte, responde o prestador de serviços de pagamento pelo reembolso integral dos montantes debitados, acrescido dos juros previstos no artigo 114º do RJSPME, sem prejuízo do direito de indemnização.
IX. Os danos de ansiedade, desgosto e sentimento de injustiça sofridos pelo titular da conta em consequência da subtração fraudulenta de quantias elevadas do seu património constituem danos não patrimoniais merecedores de tutela indemnizatória, também no âmbito da responsabilidade contratual bancária.

Decisão Texto Parcial:

Decisão Texto Integral:

Acordam os juízes da 2ª secção cível do Tribunal da Relação de Lisboa que compõem este coletivo:

I - RELATÓRIO

Os autores AA e BB, identificados nos autos, instauraram em 29-08-2025, no Juízo Local Cível do Seixal, a presente ação declarativa de condenação, com forma de processo comum, contra o réu Banco Comercial Português, SA, igualmente identificado nos autos, formulando os seguintes pedidos:
- Condenação do réu no pagamento da quantia de € 30.654,66, que alegaram ter-lhes sido ilicitamente subtraída de conta bancária de que eram titulares no banco réu;
- Condenação do réu no pagamento da quantia de € 6.000,00, a título de indemnização por danos não patrimoniais.
Fundamentando os pedidos, alegaram que o autor recebeu uma SMS no seu telemóvel no dia 10-02-2025, de uma entidade identificada como *netflix,* informando-o da rejeição do pagamento da mensalidade do respetivo serviço, e exigindo-lhe o pagamento imediato, a partir de um link ali fornecido, sob pena de suspensão do serviço a partir de 12-02-2025. O Autor, acreditando na legitimidade da SMS, acedeu ao link fornecido, inserindo os dados do seu cartão bancário. De seguida, recebeu nova SMS com o teor "*O seu cartão **…51 está pronto para usar Apple Pay. Pode utilizar sempre que vir o símbolo contactless ou a marca Apple Pay*". Embora o autor não fosse possuidor de qualquer equipamento da marca Apple, presumiu que a mensagem correspondia à confirmação da operação de pagamento da

mensalidade do serviço netflix que acabara de realizar. Em 11-02-2025, os Autores verificaram que os dados do respetivo cartão bancário haviam sido associados a um dispositivo da marca Apple pertencente a terceiros desconhecidos, que os utilizaram para fazer 19 transações comerciais, no montante global de € 30.654,66. Tais transações comerciais traduziram-se em aquisição de criptomoeda e compras online na loja IKEA em França, e ocorreram num período inferior a 24 horas.
Os autores mantinham uma relação bancária com o banco réu de mais de 20 anos, nunca tendo efetuado operações bancárias eletrónicas em montantes equiparáveis aos indevidamente subtraídos, nem tampouco quaisquer transações ou aquisições relacionadas com criptoativos.
Concluíram que o réu não adotou as diligências adequadas para garantir a máxima segurança dos valores depositados na sua conta à ordem, consentindo na realização de diversas operações bancárias em montantes exorbitantes num intervalo inferior a 24 (vinte e quatro) horas, circunstância que, pela sua natureza e valor, diverge manifestamente do seu padrão habitual de movimentação.
O réu contestou a ação, pugnando pela sua improcedência, alegando que a responsabilidade pelas operações que levaram à subtração do montante em causa é do titular do cartão, uma vez que foram efetuadas com recurso a autenticação forte, através do serviço 3D secure associado ao telemóvel do Autor, com envio de notificação para a aplicação.
Considerou ainda o contestante que o Autor incumpriu o dever de sigilo e de não divulgação dos códigos de acesso que sobre si recaía, conforme estipulado nas Condições Gerais dos Serviços de Meios de Comunicação à Distância que havia subscrito.
Por intermédio do requerimento apresentado em 25-10-2025 (referência 53790463), os autores pronunciaram-se sobre a defesa por exceção, reiterando ter o réu violado os seus deveres de vigilância, diligência e segurança, por não ter reagido prontamente perante a realização de operações atípicas, bloqueando a conta.
Foi dispensada a realização de audiência prévia e proferido despacho saneador, afirmando-se a validade e regularidade da instância, e enunciando-se o objeto do litígio e os temas de prova, sem qualquer reclamação.
Finda a audiência de julgamento, foi proferida sentença que julgou a <u>ação parcialmente procedente</u>, reproduzindo-se o seu dispositivo:
"*Nestes termos, o Tribunal julga a ação parcialmente procedente, por provada e, em consequência:*
a. ***a) Condena o Réu Banco Comercial Português S.A a pagar aos Autores AA e BB a quantia de € 30.654,66 (trinta mil seiscentos e cinquenta e quatros euros e sessenta e seis cêntimos) acrescidas dos juros à de 14% ano, desde 11.02.2025 até efetivo e integral pagamento;***
b) Condena o Réu Banco Comercial Português S.A a pagar ao Autor AA a quantia de € 1.000,00 (mil euros) a título de danos não patrimoniais;
c) Absolve o Réu Banco Comercial Português S.A do demais peticionado;
d) Condena Autores e Réu, na proporção dos respetivos decaimentos, que se fixam em 90% para o Réu e em 10% para os Autores. "

Não se conformando com tal decisão, o réu da mesma interpôs recurso de apelação, ao qual pediu que fosse atribuído efeito suspensivo, mediante caução que ofereceu (por garantia autónoma, irrevogável e à primeira solicitação, no valor máximo de € 45.000,00) transcrevendo-se as respetivas conclusões:

"a) O presente recurso vem interposto da sentença que julgou a ação parcialmente procedente e condenou o Banco Comercial Português, S.A. a pagar aos Autores a quantia de €30.654,66, acrescida de juros à taxa de 14% ao ano desde 11.02.2025 até efetivo e integral pagamento, bem como a pagar ao Autor AA a quantia de €1.000,00 a título de danos não patrimoniais.

b) O Recorrente não se conforma com a decisão recorrida, por entender que a mesma incorre em erro de aplicação do direito aos factos provados.

c) A fraude em causa teve origem numa mensagem identificada como "netflix" e num link externo, renovaperfil.com, alheios à esfera de domínio do Banco, não tendo sido demonstrada qualquer falha inicial dos sistemas, canais ou comunicações do Recorrente.

d) O simples facto de o prejuízo se ter materializado através de movimentos numa conta bancária não permite imputar automaticamente ao Banco a responsabilidade por uma fraude externa, desencadeada por uma página que aparentava pertencer à "netflix".

e) Ao responsabilizar o Banco, apesar de a captação dos dados ter ocorrido fora dos seus canais e apesar de o Autor ter inserido dados de cartão e código de ativação Apple Pay numa página externa, a sentença recorrida converteu indevidamente o dever de segurança bancária numa responsabilidade objetiva.

f) A conduta do Autor, e não qualquer falha de segurança do Banco, constitui o fator causal decisivo da associação do cartão ao Apple Pay de terceiros e das subsequentes operações. A esse título veja-se o depoimento prestado pela Testemunha CC, que prestou o seu depoimento no dia 27.06.2026, a título de exemplo, minutos [00:09:03]; [00:10:03].

g) O presente recurso não depende da alteração da matéria de facto.

h) Pelas razões suprarreferidas nos Pontos 31 a 107, que aqui se dão por integralmente reproduzidas, a alteração da matéria de facto quanto aos factos C e D, dados pelo Tribunal Recorrido, como Não Provados, reforça ainda mais a conclusão de que o Autor não se limitou a ser vítima de phishing, tendo antes praticado os atos necessários à ativação de uma Wallet Apple Pay em equipamento de terceiros, em violação grave dos deveres de guarda, sigilo, cautela e confidencialidade.

i) O facto C, dado como não provado, deveria ter sido dado como provado, porquanto a testemunha CC explicou que a adesão à Apple Pay exigia a receção de um primeiro código por SMS, a sua introdução na App do Banco, a geração de um segundo código pela App e a introdução desse segundo código na Wallet, testemunha CC, minutos [00:02:30]; [00:03:15]; [00:05:17]; [00:05:50]

j) A mesma testemunha afirmou que sem tais passos não seria possível efetuar a adesão à Apple Pay, minutos [00:09:03]; [00:10:03]; [00:11:34]

k) A testemunha esclareceu ainda que, no caso concreto, existia registo desses passos e que todos os passos haviam sido cumpridos, minutos [00:09:03];

l) O facto D deveria igualmente ter sido dado como provado, porquanto a

testemunha CC, no seu depoimento afirmou que as 19 transações foram efetuadas com validação forte, minutos [00:16:30]; [00:18:23]; [00:18:34]; [00:18:37]; [00:39:08]; [00:39:15]; [00:39:54].
m) A testemunha explicou que, depois de concluída a adesão à Wallet, as validações das transações Apple Pay passam a ser efetuadas no equipamento onde a Wallet está instalada, minutos, [00:40:36]; [00:41:01]; [00:38:33]; [00:43:10]; [00:43:45]; [00:45:11]; [00:45:59], por PIN ou biometria, sem emissão de novo código pelo Banco para cada operação, testemunha CC, minutos, [00:16:40]; [00:41:22]; [00:41:46].
n) A sentença recorrida deu ainda como provado que o serviço prestado pelo Réu não foi afetado por qualquer avaria técnica ou deficiência suscetível de originar falha de segurança.
o) Assim, impunha-se decisão diversa quanto aos factos C e D, devendo os mesmos ser eliminados do elenco dos factos não provados e aditados à matéria de facto provada.
p) Deve, por isso, ser aditado à matéria de facto provada que, na sequência da inserção do código de ativação Apple Pay, o Autor recebeu através da App do Réu um novo código, que permitiu a associação do cartão à Wallet Apple Pay instalada em equipamento de terceiros, a esse título e designadamente veja-se o depoimento prestado pela testemunha CC [00:35:28]; [00:36:48]; [00:38:33]
q) Deve ainda ser aditado à matéria de facto provada que as transações identificadas no facto provado n.º 15 foram efetuadas com recurso a autenticação forte, no âmbito do serviço Apple Pay, Testemunha CC, minutos [00:21:32]; [00:25:55]; [00:34:32].
r) Ainda que não se altere a matéria de facto, sempre os factos provados n.ºs 4 e 6 a 14 impunham decisão diversa, por revelarem negligência grosseira do Autor.
s) Mesmo aceitando integralmente a factualidade dada como provada, designadamente os factos provados n.ºs 4 e 6 a 14, impunha-se decisão diversa.
t) Resultou provado que, em 10.02.2025, pelas 17h43m, o Autor recebeu no seu telemóvel uma mensagem de remetente identificado como "netflix", informando-o da rejeição do pagamento da mensalidade do serviço e exigindo-lhe pagamento imediato sob pena de suspensão do serviço.
u) Resultou provado que a referida mensagem continha o link https:// renovaperfil.com.
v) Resultou provado que o Autor acedeu a esse link, que o dirigiu a uma página web que reproduzia de forma fidedigna a aparência do site oficial da "netflix".
w) Resultou provado que o Autor inseriu os dados do seu cartão bancário nesse link.
x) Resultou provado que o Autor recebeu, de seguida, um código de ativação à Apple Pay.
y) Resultou provado que o Autor inseriu, na página web para onde o link o remetera, o código de ativação da Apple Pay.
z) Resultou provado que, um minuto depois, o Autor recebeu nova SMS com o seguinte teor: "O seu cartão ..3651 está pronto para usar Apple Pay. Pode utilizar sempre que vir o símbolo contactless ou a marca Apple Pay".
aa) Resultou provado que o Autor presumiu que tal mensagem correspondia à

confirmação da operação de pagamento da mensalidade "netflix".
bb) Resultou igualmente provado que o Autor não é possuidor de qualquer equipamento da marca Apple.
cc) Esta sequência factual não permite concluir por mera distração ou simples imprudência.
dd) O Autor não se limitou a aceder a um link fraudulento ou a inserir dados do cartão.
ee) O Autor recebeu e inseriu um código de ativação Apple Pay, apesar de pretender pagar uma mensalidade "netflix" e apesar de não possuir qualquer equipamento Apple.
ff) A divergência entre o ato que o Autor julgava praticar — pagamento de uma mensalidade "netflix" — e o ato que objetivamente lhe foi comunicado — ativação Apple Pay — era manifesta.
gg) Tal divergência impunha, segundo um padrão mínimo de diligência, que o Autor interrompesse imediatamente o procedimento, se abstivesse de introduzir qualquer código e contactasse o Banco.
hh) Acresce que as condições gerais aplicáveis, dadas como provadas no facto n.º 4, alertavam expressamente para os riscos de phishing, SMS com links, páginas fraudulentas, pedidos de dados pessoais, dados bancários, dados de cartão e códigos de autenticação.
ii) As mesmas condições gerais advertiam que o cliente deveria desconfiar de mensagens com tom de urgência, mensagens SMS com links e pedidos de fornecimento de códigos de autenticação enviados pelo Banco.
jj) A conduta do Autor violou, assim, de forma grave, os deveres de cautela, sigilo, guarda e confidencialidade associados à utilização do instrumento de pagamento.
kk) Tal conduta deve ser qualificada como negligência grosseira, para efeitos do artigo 115.º, n.º 4, do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica.
ll) Ao concluir que a atuação do Autor não configura negligência grosseira, a sentença recorrida incorreu em erro de julgamento.
mm) O Tribunal Recorrido desvalorizou indevidamente o elemento decisivo do caso concreto: a introdução de um código de ativação Apple Pay por quem pretendia apenas pagar uma mensalidade "netflix" e não possuía equipamento Apple.
nn) A sentença recorrida reconduziu o caso a uma situação genérica de phishing, quando os factos provados revelam um comportamento objetivamente gravemente descuidado.
oo) O ónus de demonstração da negligência grosseira do ordenante, previsto no artigo 113.º, n.º 4, do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, mostra-se cumprido pela própria factualidade provada.
pp) A prova da negligência grosseira não resulta apenas da utilização registada do instrumento de pagamento.
qq) Resulta da conduta concreta do Autor, tal como fixada nos factos provados.
rr) Verificando-se negligência grosseira do ordenante, este suporta as perdas resultantes das operações de pagamento não autorizadas até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, nos termos do artigo 115.º, n.º 4, do Regime Jurídico dos Serviços

de Pagamento e da Moeda Eletrónica.
ss) Consequentemente, não deveria o Banco ter sido condenado a restituir aos Autores a quantia de € 30.654,66.
tt) A sentença recorrida acabou por transformar o dever de segurança do Banco numa responsabilidade objetiva por toda e qualquer operação fraudulenta, ainda que precedida de atuação gravemente negligente do cliente.
uu) O regime legal aplicável não estabelece tal responsabilidade objetiva.
vv) Pelo contrário, o regime legal afasta a responsabilidade do prestador de serviços de pagamento quando as perdas resultem de negligência grosseira do ordenante.
ww) A sentença recorrida violou, por erro de interpretação e aplicação, os artigos 110.º, 113.º, 114.º e 115.º do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica.
xx) Deve, por isso, a sentença ser revogada e substituída por acórdão que julgue a ação improcedente, absolvendo o Banco do pedido de pagamento da quantia de € 30.654,66.
yy) Revogada a condenação principal, deve igualmente ser revogada a condenação no pagamento de juros de mora à taxa de 14% ao ano.
zz) Com efeito, a condenação em juros pressupõe a existência de uma obrigação de reembolso pelo prestador de serviços de pagamento.
aaa) Verificando-se negligência grosseira do ordenante, inexiste obrigação de reembolso e, consequentemente, inexiste fundamento para aplicação do artigo 114.º, n.º 10, do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, e, logo à partida, existindo motivos razoáveis para o Banco recusar o reembolso imediato perante a conduta do Autor, que inseriu dados do cartão e código de ativação Apple Pay numa página externa.
bbb) Deve também ser revogada a condenação do Banco no pagamento de €1.000,00 a título de danos não patrimoniais.
ccc) Verificando-se negligência grosseira do Autor, inexiste facto ilícito imputável ao Banco que possa sustentar a obrigação de indemnizar.
ddd) Os danos emocionais considerados pela sentença resultam da atuação fraudulenta de terceiros e da conduta do próprio Autor, não de qualquer incumprimento indemnizável imputável ao Banco.
eee) A matéria de facto provada quanto aos danos não patrimoniais é, além disso, limitada, tendo sido dado como Não Provado que o Autor tivesse dificuldades em dormir e que a Autora tivesse sofrido ansiedade, desgosto ou sentimento de injustiça que a abalou.
fff) Deve, consequentemente, o Banco ser absolvido também do pedido de indemnização por danos não patrimoniais.
ggg) Procedendo o presente recurso, deverá ser alterada a decisão quanto a custas, ficando as mesmas a cargo dos Autores, na proporção do respetivo decaimento.
(…)
Termos em que, deve o presente recurso ser julgado procedente e, em consequência, ser revogada a sentença recorrida, absolvendo-se o Recorrente de todos os pedidos contra si formulados, com as demais consequências legais."
Os autores apresentaram resposta, pugnando pela manutenção da decisão

recorrida e concluindo nos seguintes termos:
"1. O Recurso objeto dos presentes autos deve ser julgado totalmente improcedente, mantendo-se integralmente a sentença recorrida, por não padecer dos alegados erros de julgamento da matéria de direito ou de facto invocados pelo Recorrente.
2. A douta sentença recorrida procedeu a uma correta e criteriosa apreciação da prova produzida e a uma adequada subsunção jurídica da factualidade apurada, não padecendo de qualquer dos erros de julgamento que lhe são imputados pelo Recorrente.
3. O recurso interposto assenta, essencialmente, na pretensão de qualificar como negligência grosseira a conduta do Autor AA e, subsidiariamente, na alteração dos factos C) e D) julgados não provados pelo Tribunal a quo.
4. Nenhuma dessas pretensões encontra suporte bastante na matéria de facto definitivamente apurada ou na prova produzida em audiência de julgamento.
5. Resultou provado que o Autor recebeu uma mensagem cujo remetente se apresentava identificado como "Netflix", comunicando-lhe a rejeição do pagamento de uma mensalidade e a iminente suspensão do serviço.
6. Resultou igualmente provado que o Autor, convicto da veracidade e autenticidade daquela comunicação, acedeu ao link nela disponibilizado, sendo direcionado para uma página que reproduzia de forma fidedigna a aparência do sítio oficial da Netflix.
7. Foi nesse contexto, e convencido de que se encontrava a regularizar uma mensalidade de reduzido valor, que o Autor introduziu os dados do cartão bancário e o código que lhe foi remetido.
8. A conduta do Autor deve ser apreciada à luz das concretas circunstâncias em que ocorreu e não a posteriori, à luz do conhecimento adquirido sobre a fraude e sobre o significado que os terceiros atribuíram aos atos praticados.
9. A jurisprudência do Supremo Tribunal de Justiça tem igualmente afastado a qualificação como negligência grosseira em situações em que o utilizador fornece elementos de segurança convencido de que os está a fornecer no âmbito de uma operação legítima, não bastando a mera circunstância de esses elementos terem chegado ao conhecimento de terceiros.
10. A circunstância de o endereço eletrónico utilizado pelos agentes fraudulentos não corresponder ao domínio oficial da Netflix não permite, por si só, qualificar a atuação do Autor como grosseiramente negligente, quando ficou provado que a página para a qual foi direcionado reproduzia fielmente a aparência daquela entidade.
11. Também a referência ao Apple Pay não permite concluir automaticamente pela existência de negligência grosseira, devendo a atuação do Autor ser apreciada no contexto concreto em que ocorreu e não à luz do conhecimento posteriormente adquirido acerca do mecanismo utilizado pelos agentes fraudulentos.
12. Não se mostra, por conseguinte, demonstrada qualquer atuação fraudulenta, dolosa ou grosseiramente negligente do Autor, nos termos exigidos pelo artigo 115.º do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica.
13. O juízo de censura não pode ser formulado a posteriori, a partir do conhecimento integral da fraude e do significado técnico dos atos praticados,

devendo antes atender às circunstâncias concretamente percecionadas pelo Autor no momento em que atuou.
14. Não resultou provado que o Autor tivesse compreendido que os atos por si praticados se destinavam à associação do cartão bancário a uma carteira digital instalada num equipamento pertencente a terceiro.
15. Muito menos resultou provado que, tendo compreendido essa circunstância, o Autor tivesse conscientemente decidido prosseguir com tal associação.
16. O Recorrente pretende ainda, subsidiariamente, a alteração da matéria de facto dada como não provada relativamente aos factos C) e D).
17. A impugnação da matéria de facto deve, contudo, improceder, porquanto a prova produzida não permite concluir, com o grau de segurança exigível, que o Autor tenha percorrido a concreta sequência de atos de adesão à Apple Pay que o Recorrente pretende ver aditada à matéria de facto provada.
18. A testemunha CC descreveu o procedimento de adesão à Apple Pay implementado pelo Recorrente, mas, quando reportada ao caso concreto, não demonstrou conhecimento direto de que o Autor tivesse praticado, um a um, os atos que o Recorrente lhe imputa.
19. Com efeito, o depoimento da testemunha CC, invocado pelo Recorrente, descreveu, em primeira linha, o funcionamento abstrato do procedimento técnico então previsto para associação de um cartão à Wallet Apple Pay.
20. A descrição abstrata dos passos que, segundo o sistema, seriam necessários à conclusão de determinada operação não constitui prova de que esses concretos passos tenham sido pessoalmente realizados pelo Autor no caso sub judice.
21. A testemunha reconheceu que o Banco dispunha de meios para demonstrar os concretos passos realizados na operação, não tendo sido apresentados nos autos elementos objetivos que demonstrassem que o Autor percorreu a sequência de atos que o Recorrente pretende ver aditada à matéria de facto.
22. A mera conclusão de que o procedimento de adesão à Apple Pay foi concluído não permite presumir, sem os correspondentes elementos objetivos, que o titular do cartão tenha praticado, um a um, todos os atos que compunham o procedimento então vigente.
23. Também as declarações prestadas pelo Autor não confirmam a sequência de atos alegada pelo Recorrente, tendo aquele confirmado apenas a receção de um código, não resultando das suas declarações qualquer confirmação da alegada introdução desse código na aplicação do Banco, nem da posterior receção e utilização de um segundo código na Wallet Apple Pay.
24. Não pode, assim, a descrição abstrata do funcionamento do sistema ser utilizada para suprir a ausência de prova sobre a concreta sequência de atos realizada no caso dos autos.
25. A prova produzida não permite dar como demonstrado, com a necessária concretização, que as 19 operações realizadas sobre a conta dos Autores tenham sido efetivamente processadas mediante o mecanismo de autenticação forte invocado pelo Recorrente.
26. A afirmação testemunhal de que as operações "teriam de ter" autenticação forte, ou de que todas "tiveram" autenticação forte, não substitui a demonstração objetiva do mecanismo de autenticação efetivamente utilizado

em cada uma das operações concretamente realizadas.
27. Deve, por conseguinte, manter-se inalterada a decisão da matéria de facto quanto aos factos C) e D), julgando-se improcedente a impugnação deduzida pelo Recorrente.
28. Nos termos do artigo 113.º, n.º 4, do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, incumbe ao prestador de serviços de pagamento apresentar elementos que demonstrem a existência de fraude, dolo ou negligência grosseira da parte do utilizador.
29. O simples registo da utilização do instrumento de pagamento não é suficiente para demonstrar que uma operação foi autorizada pelo ordenante ou que este atuou fraudulentamente, com dolo ou com negligência grosseira.
30. No caso dos autos, o Recorrente não logrou demonstrar a concreta sequência de autenticação que invoca, nem demonstrou factualidade bastante para qualificar a atuação do Autor como fraudulenta, dolosa ou grosseiramente negligente.
31. Incumbia, por conseguinte, ao Recorrente demonstrar concretamente os factos suscetíveis de integrar a alegada negligência grosseira, ónus que manifestamente não satisfez.
32. Não se mostra, assim, cumprido o ónus de prova que sobre o Recorrente impendia nos termos do artigo 113.º, n.º 4, do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica.
33. A circunstância de a fraude ter tido origem numa mensagem e numa página web externas à esfera de atuação do Recorrente não afasta, por si só, a responsabilidade deste pelas operações posteriormente realizadas através do sistema bancário.
34. A responsabilidade reconhecida na sentença não assenta na origem da fraude, mas nas concretas operações não autorizadas posteriormente realizadas sobre a conta dos Autores e no cumprimento, pelo prestador de serviços de pagamento, dos deveres de segurança e proteção que sobre si impendiam.
35. Não está em causa uma obrigação de o Banco impedir toda e qualquer fraude praticada por terceiros, mas a obrigação de observar os deveres de segurança que lhe incumbem perante operações de pagamento concretamente realizadas através dos seus sistemas.
36. A responsabilidade reconhecida na sentença não constitui, por conseguinte, uma responsabilidade objetiva do Recorrente, antes decorrendo da aplicação do regime legal às operações não autorizadas e da apreciação do cumprimento dos deveres que sobre o prestador de serviços de pagamento impendiam nas concretas circunstâncias dos autos.
37. A articulação dos artigos 114.º e 115.º do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica não permite, por si só, afastar a responsabilidade do prestador: o artigo 115.º estabelece as situações em que as perdas podem ser imputadas ao ordenante, designadamente quando exista atuação fraudulenta, incumprimento deliberado ou negligência grosseira, pressupostos que, no caso concreto, não foram demonstrados.
38. Não tendo o Recorrente demonstrado os pressupostos previstos no artigo 115.º, não pode fazer recair sobre os Autores as perdas resultantes das operações de pagamento não autorizadas.

39. A transferência das perdas para o ordenante pressupõe, designadamente, a demonstração de atuação fraudulenta, incumprimento deliberado das suas obrigações ou negligência grosseira, não podendo qualquer desses pressupostos ser presumido a partir da mera utilização registada do instrumento de pagamento.
40. Deve, consequentemente, ser mantida a decisão recorrida quanto à responsabilidade do Recorrente pelas operações não autorizadas e quanto ao consequente dever de reembolso das quantias indevidamente debitadas.
41. Deve manter-se a condenação do Recorrente no pagamento da quantia de €1.000,00 a título de danos não patrimoniais, por se encontrarem provados danos que, pela sua gravidade, merecem a tutela do direito, nos termos do artigo 496.º do Código Civil.
42. Tais danos, apreciados à luz da natureza, número e valor das operações fraudulentas e das concretas circunstâncias em que ocorreram, ultrapassam manifestamente o limiar dos simples incómodos ou contrariedades quotidianas e merecem tutela nos termos do artigo 496.º do Código Civil.
43. Deve igualmente manter-se a condenação do Recorrente no pagamento dos juros de mora, nos termos do artigo 114.º, n.º 10, do RSP, desde 11.02.2025 até efetivo e integral pagamento.
44. O montante de €1.000,00 fixado pelo Tribunal a quo mostra-se, aliás, moderado e conforme aos critérios de equidade legalmente estabelecidos, inexistindo fundamento para a respetiva revogação.
45. A pretensão recursória relativa aos juros não possui autonomia relativamente à questão principal do dever de reembolso, pelo que, improcedendo a pretendida imputação das perdas aos Autores, deverá igualmente improceder este segmento do recurso.
46. Deve, por fim, manter-se a decisão recorrida quanto às custas, sem prejuízo da condenação do Recorrente nas custas do recurso, em conformidade com o respetivo decaimento.
47. Não existindo fundamento para alteração da decisão de mérito, inexiste igualmente fundamento para modificação da repartição das custas fixada pelo Tribunal a quo, determinada nos termos do artigo 527.º do CPC em função do efetivo vencimento e decaimento das partes."
48. Deverá, por todo o exposto, o recurso interposto pelo Banco Comercial Português, S.A. ser julgado integralmente improcedente, quer quanto à impugnação da matéria de facto, quer quanto à matéria de direito.
49. Assim, o recurso interposto pelo Recorrente deve ser julgado totalmente improcedente, mantendo-se integralmente a douta sentença recorrida, com as legais consequências, designadamente quanto a custas."
Foi admitido o recurso, como apelação, com subida imediata, nos próprios autos, e efeito suspensivo.
Remetidos os autos a este tribunal, inscrito o recurso em tabela, foram colhidos os vistos legais, cumprindo apreciar e decidir.
II – QUESTÕES A DECIDIR
O objeto do recurso é delimitado pelas conclusões da alegação, ressalvadas as matérias de conhecimento oficioso pelo tribunal, bem como as questões suscitadas em ampliação do âmbito do recurso a requerimento do recorrido, nos termos do disposto nos artigos 608, nº 2, parte final, *ex vi* artigo 663º, nº

2, 635º, nº 4, 636º e 639º, nº 1, CPC.
Consequentemente, nos presentes autos, inexistindo questões de conhecimento oficioso a apreciar, as questões a decidir são as seguintes:
- Impugnação da decisão sobre a matéria de facto;
- Responsabilidade civil contratual do réu;
- Imputabilidade do evento à conduta do autor, a título de negligência grosseira;
- Indemnização.
III – FUNDAMENTAÇÃO
Impugnação da matéria de facto
A reapreciação da matéria de facto pelo tribunal de recurso implica que o recorrente, nas alegações em que a impugna, cumpra os ónus que o legislador estabeleceu a seu cargo, enunciados no artigo 640º CPC. Desta norma extrai-se incumbir ao recorrente, por forma a cumprir o que tem vindo a designar-se por "*ónus primário de alegação*", e sob pena de rejeição do recurso, a identificação dos concretos pontos de facto que considera incorretamente julgados (640º, nº 1, alínea a), CPC), dos concretos meios probatórios que impunham decisão diversa (640º, nº 1, alínea b), CPC) e a indicação da decisão que deve ser proferida quanto aos factos impugnados (640º, nº 1, alínea c), CPC).
Já o designado "*ónus secundário*" reporta-se à especificação dos meios de prova que implicariam, na perspetiva do recorrente, diversa decisão da matéria de facto, gerando o seu incumprimento a rejeição do recurso apenas se ficar gravemente dificultado o exercício de contraditório ou o exame pelo tribunal de recurso – Acórdão do Supremo Tribunal de Justiça de 21-03-2019, proferido no processo 3683/16.6T8CBR.C1.S2, disponível em www.dgsi.pt
Assim, na exigência do cumprimento dos ónus de impugnação previstos no citado artigo 640º, "*os aspetos de ordem formal (…) devem ser modelados em função dos princípios da proporcionalidade e da razoabilidade*" – Acórdão do Supremo Tribunal de Justiça de 21-03-2019 (proferido no processo nº 3683/16.6T8CBR.C1.S2, disponível em www.dgsi.pt).
Acresce que nesse âmbito haverá ainda que ponderar o AUJ do STJ de 17-10-2023 (acórdão nº 12/2023 de 14 de novembro, publicado no Diário da República nº 220/2023, Série I de 2023-11-14) que uniformizou a seguinte jurisprudência: "*Nos termos da alínea c), do n.º 1 do artigo 640.º do Código de Processo Civil, o Recorrente que impugna a decisão sobre a matéria de facto não está vinculado a indicar nas conclusões a decisão alternativa pretendida, desde que a mesma resulte, de forma inequívoca, das alegações*." Aplicando tal entendimento, o Supremo Tribunal de Justiça em acórdão de 08-02-2024, (proferido no processo n.º 7146/20.7T8PRT.P1.S1, disponível em www.dgsi.pt) considerou que "*a rejeição do recurso respeitante à impugnação da decisão da matéria de facto apenas deve verificar-se quando falte nas conclusões a referência à impugnação da decisão sobre a matéria de facto, através da referência aos «concretos pontos de facto» que se considerem incorretamente julgados (alínea a) do n.º 1 do artigo 640.º), sendo de admitir que as restantes exigências (alíneas b) e c) do n.º 1 do artigo. 640.º), em articulação com o respetivo n.º 2, sejam cumpridas no corpo das alegações*".

Dado que a recorrente cumpriu os ónus supra enunciados, nada obsta à apreciação da impugnação, cuja procedência dependerá "*existência de erro de apreciação relativamente a concretos pontos de facto impugnados*" – como se refere no Acórdão do Tribunal da Relação de Guimarães de 19-12-2023[1].
Embora o recorrente defenda terem sido apurados factos que, por si, determinariam diversa decisão (com a sua absolvição do pedido), impugnou a matéria de facto, defendendo que os factos não provados sob as alíneas C) e D) da decisão recorrida devem transitar para os factos provados, tendo por base os meios de prova que indicou.
A tais factos foi conferida a seguinte redação:
"***C. Na sequência do identificado em 11., o Autor recebeu através da App do Réu um novo código, que inseriu na página para onde remetia o link identificado em 7. e que permitiu que terceiros o colocassem na Aplicação de carteira da Apple, possibilitando a associação do seu cartão.***
D. As transações identificadas em 15. foram efetuadas com recurso a autenticação forte, através do serviço 3D secure associado ao telemóvel do A., com envio de notificação para a App, tendo os códigos de autorização sido validados e autenticados pelo Autor em cada uma das transações por si efetuadas."
Tal factualidade não apurada foi motivada nos seguintes termos pelo tribunal recorrido:
"***Quanto aos factos C., não foi produzida prova que o sustente. Por outro lado, a prova produzida infirma o facto D.***
Vejamos.
Em primeiro lugar, apesar de a testemunha CC afirmar que método de adesão do cartão à Apple Pay implementado pelo Réu exigia que, após o envio do código por sms, fosse também retirado um código da aplicação do banco e inserido na carteira da Apple, a verdade é que apenas o refere de forma genérica, não tendo, quando questionado, confirmado que foi o que efetivamente sucedeu no caso concreto. Esclarece apenas que teria que ter sido, porque o processo, de acordo com os registos do sistema, foi efetuado na sua integralidade. Concretamente, afirmou que "tem que existir".
No entanto, sucede que esclareceu também que, até dezembro de 2024, o sistema de adesão à Apple Pay assentava apenas no envio da sms, pelo que seria possível, apenas com aquele código, introduzir o cartão na carteira da Apple.
Ora, atendendo à prova produzida pelo Réu, apenas testemunhal, sem que tenha sido junto qualquer registo das operações efetivamente efetuadas e validadas para que o cartão bancário do Autor ficasse associado à Apple Pay de terceiros, não pode o Tribunal concluir que aquele processo foi de facto implementado.
Em primeiro lugar, porque até dois meses antes, bastava a sms, pelo que permanece a dúvida se o sistema poderia continuar a permitir aquela forma de validação algum tempo depois da transição.
A acrescer, não resulta dos autos qualquer prova de que foi gerado um segundo código na aplicação do banco, nem de que forma o mesmo poderia ter sido transmitido aos terceiros que enviaram a mensagem ao Autor. Com efeito,

de toda a documentação junta, incluindo interpelações dos Autores ao Banco e mensagens recebidas pelo Autor do serviço do Réu, aponta noutro sentido – que o sistema do Réu terá permitido a adesão apenas com o envio do código de ativação remetido por sms.
A acrescer, a mensagem com o envio do código de ativação da Apple Pay foi remetida às 18h08m e a mensagem de confirmação da adesão às 18h09m. Do curto espaço de tempo entre o envio do código e da confirmação da adesão é possível concluir, com segurança, que mais nenhum passo foi efetuado ou solicitado, tendo no exato momento em que o Autor forneceu aquele código de ativação, o mesmo sido inserido no dispositivo Apple dos terceiros, ativando aquele serviço.
Por tudo o que se expôs, foi considerado como não provado o facto C.
Por fim, a testemunha CC confirmou expressamente que, por a adesão à Apple Pay ser considerada como autenticação forte, o banco não efetua qualquer controlo das operações efetuadas por esse método. Ademais, também não foi produzida qualquer prova documental que corroborasse a utilização daquele método na realização das operações fraudulentas identificadas nos factos provados.
Em face do exposto, dado como não provado o facto D."
O recorrente sustenta a impugnação, desde logo, no depoimento de CC. Desde já se adianta que, após audição integral de tal depoimento, não pode concluir-se que o tribunal recorrido tenha incorrido em erro na sua valoração.
Efetivamente, sendo funcionário do réu, na área na área da fraude de cartões, prestou um depoimento pormenorizado, caraterizando a aplicação *apple pay* como uma *wallet* ou forma de pagamento digital, salientando o seu funcionamento autónomo do banco. Porém, segundo explicou, existe a necessidade de associar um cartão (bancário) para que sejam feitos os pagamentos a partir daquela aplicação. Mais referiu que a adesão ao *apple pay* envolve vários passos, que visam torná-la segura. Descrevendo esses passos, referiu que a adesão é iniciada com dados do cartão, após o que é recebido um código, por sms, enviado para o telemóvel do cliente (referente ao contacto telefónico registado do banco). Esse código é colocado na *App* do banco que, por sua vez, vai gerar um segundo código, que será introduzido na *wallet.*
Reportando-se ao caso, referiu que o cliente terá fornecido os dados do seu cartão e recebido no seu telemóvel um primeiro código, introduzindo-o na *app* do banco, que gerou um segundo código que vai ser introduzido de volta na *wallet.*
O certo é que embora refira existir registo destes passos, não os concretizou em quaisquer elementos objetivos, designadamente no que se reporta à introdução pelo cliente deste segundo código. Confrontado com a alegação dos autores de que não possuem *iphone,* pelo que nunca poderiam ter serviço *apple pay,* declarou que "ao que tudo indica" terão sido terceiros que, na posse desse equipamento, iniciaram o processo de adesão, através do conhecimento dos dados do cartão que foram introduzidos no site falso da netflix (aparentemente não o verdadeiro, mas algo que o aparentava). Introduzidos os dados do cartão, os terceiros tiveram possibilidade de iniciar

o processo de adesão.
Na sua perspetiva, o sistema cumpriu com a exigência de todas as autenticações fortes. Simplesmente todas as autenticações fortes estavam do lado dos terceiros, que conseguiram a adesão. Estavam na posse do equipamento e terão recebido toda a informação para que fossem feitas as "validações fortes". E quando estas ocorrem, o banco não contacta o cliente, nem procura qualquer certificação.
No caso dos autos, as dezanove transações tiveram validação forte, pelo que o banco não tinha capacidade para cancelar o pagamento. Referiu ainda que o banco tem registo do envio para o telemóvel do cliente de um código (o primeiro) e da sua colocação colocado na *app* do próprio banco. Porém, reconheceu que não conseguem saber de que forma o último código foi transmitido a terceiros, admitindo que possa ter sido introduzido num equipamento que estava na mão de terceiro. Certo é que este passo não é confirmado pelo banco, admitindo que as dezanove transações possam ter sido validadas por um equipamento que não aquele para onde foi enviado o primeiro código, dado que o banco não tem capacidade para verificar que estas transações estão a ser validadas por outro equipamento.
Referiu ainda que até dezembro de 2024, o método de validação (para adesão ao *apple pay*) era diferente, assentava apenas numa única SMS. Como esse procedimento não era considerado uma validação forte, foi necessário reformular o sistema e passou a ser o que a testemunha descreveu. Do seu depoimento extrai-se que, desde então, pagamentos efetuados pelo *apple pay* não são verificados pelo sistema, porque lhes passou a estar associada um sistema de validação forte.
Ora, a valoração deste depoimento efetuada pelo tribunal recorrido merece concordância dado que se mostra insuficiente para o apuramento da matéria incluída nas alíneas C) e D) dos factos não provados. O depoente nunca afirmou que o "novo código" mencionado na alínea C) tenha sido efetivamente recebido pelo autor, e por ele introduzido. E o seu depoimento não se mostrou suportado em quaisquer elementos objetivos, designadamente documentais ou periciais, suscetíveis de fundamentar a factualidade em causa. Aliás, estando em causa operações informáticas, geram registos num sistema do qual o único titular é o banco. E o certo é que tais registos não constam dos autos porque o réu não procedeu à sua junção ou disponibilização.
E os "elementos técnicos" indicados pelo recorrente que alega constarem da contestação também não provam tal realidade. Efetivamente, ainda que do artigo 12º da contestação conste um registo bancário das operações em discussão com a menção de que foram aprovadas, não comprova que tal aprovação tenha sido efetuada pelo autor. Assim como não comprovam que tenha sido por sua ação que o novo (segundo) código tenha sido por ele introduzido, ou sequer que a adesão ao *apple pay*, à data, implicasse efetivamente tal ação (inserção de um novo, segundo, código).
Consequentemente, não estando documental ou pericialmente demonstrados os procedimentos exigidos pelo banco réu para a concreta operação em causa, também do apuramento de que na data inexistiu qualquer avaria (facto provado 20) não pode extrair-se que as transações tenham sido

efetuadas com "autenticação forte".
Merece, por isso, concordância a afirmação do tribunal recorrido de que o sistema do réu do réu poderá ter permitido a adesão apenas com o envio do código de ativação remetido por SMS, como aliás, sucedia, segundo a testemunha já referida, até data muito próxima da ocorrência dos factos (dezembro de 2024).
Sufraga-se, pois, a decisão do tribunal recorrido quanto ao não apuramento dos factos enunciados em C) e D), improcedendo a impugnação.
<u>Factos Provados</u>
Em face da decisão que antecede, os factos que devem considerar-se apurados são os consignados na decisão recorrida:
1. O Réu é uma instituição bancária que se apresenta sob a denominação comercial Banco Comercial Português, S.A.
2. Os Autores são clientes da Ré desde 1991, sendo titulares de uma conta bancária à ordem.
3. O Autor AA indicou, como meio preferencial de comunicação à distância com a Ré, os números ... e ..., bem como o endereço de correio eletrónico ....
4. As Condições Gerais de Constas de Depósito à Ordem do Réu, preveem, no capítulo D "*Condições Gerais de Utilização dos Meios de Comunicação à Distância"*, cláusula segunda:
"1. Os meios de comunicação à distância para acesso do Cliente ao Banco estão sujeitos a riscos de fraude, nomeadamente de "phishing", bem como, de consulta e realização de operações fraudulentas por terceiros não autorizados na conta do Cliente.
2. O phishing é uma fraude que consiste em substituir a identidade do Banco ou de qualquer outra entidade fidedigna, cuja finalidade é a obtenção de informações confidenciais do Cliente, nomeadamente dados bancários, dados pessoais ou códigos de acesso. Os ataques de "phishing" podem produzir-se através de mensagens de correio eletrónico, de serviços de mensagens curtas (SMS) ou chamadas telefónicas nas quais se pode imitar e substituir a identidade do Banco ou de qualquer outra entidade fidedigna.
Essas mensagens de correio eletrónico ou SMS podem conter um ficheiro anexo que efetua a instalação de software malicioso (malware) no equipamento do Cliente ou reencaminhar para uma página web fraudulenta, que reproduz ou copia o aspeto da página original do Banco, e na qual é solicitado ao Cliente a introdução de dados pessoais e/ou códigos e credenciais de acesso, como por exemplo, o seu Código de Utilizador, algumas ou todas as posições do seu Código Multicanal, o Código de Autenticação, o seu número de telemóvel ou os dados dos seus cartões de pagamento.
3. O Cliente deve estar atento, ser precavido e ter em conta que tanto a mensagem de correio eletrónico ou SMS, como a página web fraudulenta, podem ser muito complexas e sofisticadas. O Cliente tem de desconfiar e suspeitar, nomeadamente:
a) do tom de urgência de mensagens que o ameacem com a suspensão do acesso à conta, dos códigos de acesso ou do cartão de pagamento se não fornecer os seus dados imediatamente;
b) da curiosidade criada pela mensagem a qual oferece um serviço ou produto muito desejado;

c) do pedido de confirmação dos seus dados pessoais via correio eletrónico ou SMS, designadamente remetendo-o para o preenchimento on-line de formulários de informações pessoais e códigos de acesso;
d) de erros ortográficos/gramaticais, traduções incompletas, erros no endereço do emissor (@domínio) e outros erros patentes na mensagem ou na página web fraudulenta, ou outros elementos que sugiram a origem diversa ou suspeita dos mesmos;
e) de mensagens de correio eletrónico ou SMS com links ou ficheiros em anexo;
f) da indicação de que, para simular/cancelar operações, deve fornecer Código(s) de Autenticação que o Banco lhe enviou por SMS ou gerados via Token."
5. Consta do Capítulo D, cláusula décima, das Condições Gerais de Constas de Depósito à Ordem supra referidas que:
1. O Banco poderá inibir e bloquear temporária ou definitivamente, o(s) acesso(s) aos meios de comunicação à distância pelo Cliente e/ou de alguma das suas facilidades ou serviços, por motivos objetivamente fundamentados que se relacionem com:
a) Por razões de segurança, nomeadamente se o Banco for informado ou tiver conhecimento de que ocorreu quebra de confidencialidade do(s) códigos e credenciais de segurança personalizadas do Cliente indicados na cláusula 6.ª (Convenção sobre prova), designadamente em caso de extravio, furto ou roubo ou apropriação abusiva dos mesmos, ou suspeita de utilização não autorizada ou fraudulenta, ou de perda ou extravio, furto ou roubo ou falsificação de Cartão de pagamento de que o Cliente seja Titular;
b) A suspeita de utilização não autorizada ou fraudulenta, ou de qualquer irregularidade de que possa resultar um prejuízo sério para o Banco, para o Cliente ou para o Sistema de Pagamentos, nomeadamente quando tal lhe seja solicitado pela entidade gestora do Sistema de Pagamentos por motivos de segurança ou de utilização abusiva, indevida ou não autorizada;
c) Se o Cliente realizar transações ilegais de qualquer natureza;
d) Se o presente Contrato cessar, por qualquer forma, os seus efeitos;
e) Se for declarada falência, insolvência, ou declaração judicial de acompanhamento de maior do Cliente, se o saldo da(s) conta(s) do Cliente se mostrar indisponível na sequência de ordem judicial de penhora, arrolamento, arresto, ou qualquer outra forma de apreensão judicial, ou outras ordens de bloqueio ou análogas decretadas por autoridades judiciais, judiciárias ou de supervisão."
6. A 10.02.2025, pelas 17h43m, o Autor AA recebeu no seu telemóvel, no qual utiliza o número ..., uma mensagem de remetente identificado como "netflix", que o informava da rejeição do pagamento da mensalidade do serviço, sendo-lhe exigido o pagamento imediato sob pena de suspensão do serviço a partir de 12.02.2025.
7. Na mensagem supra referida constava o seguinte link para regularização do pagamento em dívida: https://renovaperfil.com.
8. Convicto da veracidade e autenticidade da mensagem recebida, o Autor acedeu ao link aí disponibilizado, que o dirigiu a uma página web que reproduzia de forma fidedigna a aparência do site oficial da Netflix, com o

propósito de aceder ao pagamento da alegada mensalidade em situação de incumprimento.
9. Nesta sequência, pelas 18h08m do mesmo dia, o Autor inseriu os dados do seu cartão bancário no link supra identificado.
10. De seguida, ainda às 18h08m, o Autor recebeu um código de ativação à Apple Pay.
11. O Autor inseriu na página web para onde o link supra referido o remeteu o código de ativação da Apple Pay.
*12. Pelas 18h09 do dia 10.02.2025, um minuto após a inserção dos dados do cartão bancário e respetivo código de autenticação no referido link, o Autor recebeu nova mensagem SMS, com o seguinte teor: "O seu cartão **…51 está pronto para usar Apple Pay. Pode utilizar sempre que vir o símbolo contactless ou a marca Apple Pay".*
13. O Autor presumiu que a mensagem supra identificada correspondia à confirmação da operação de pagamento da mensalidade do serviço netflix.
14. O Autor não é possuidor de qualquer equipamento da marca Apple.
15. A 11.02.2025 o Autor verificou que terceiros associaram o cartão referido em 9. à Apple Pay a um equipamento que não lhe pertence e realizaram movimentos bancários num total de 19 transações comerciais, no montante global de € 30.654,66, sem a sua autorização.
16. As transações supra referidas correspondem a compras para aquisição de cripto moeda coinbase a uma empresa sedeada na Irlanda do Norte e ainda em compras online na loja IKEA em França.
17. Os Autores nunca efetuaram operações bancárias eletrónicas nos montantes supra referidos ou transações ou aquisições relacionadas com criptoativos.
18. Na sequência do supra descrito, os Autores contactaram a linha de reclamações e movimentos não autorizados junto do seu Banco a 11.02.2025, e endereçaram ao seu gestor de conta um email a informar do sucedido.
19. Como consequência do supra descrito, o Autor sofreu ansiedade, desgosto e de um sentimento de injustiça que o abalou.
20. No dia 10.02.2025 o serviço prestado pelo Réu não foi afetado por qualquer avaria técnica ou deficiência que pudesse originar em falha de segurança.
<u>E são os seguintes os factos não provados</u>:
a. A. Como consequência do *supra* descrito, o Autor teve dificuldades em dormir.
B. Como consequência do *supra* descrito, a Autora sofreu ansiedade e desgosto e de um sentimento de injustiça que a abalou.
C. Na sequência do identificado em 11., o Autor recebeu através da App do Réu um novo código, que inseriu na página para onde remetia o *link* identificado em 7. e que permitiu que terceiros o colocassem na Aplicação de carteira da Apple, possibilitando a associação do seu cartão.
D. As transações identificadas em 15. foram efetuadas com recurso a autenticação forte, através do serviço 3D secure associado ao telemóvel do A., com envio de notificação para a App, tendo os códigos de autorização sido validados e autenticados pelo Autor em cada uma das transações por si efetuadas.
*****

FUNDAMENTAÇÃO DE DIREITO

1. Os autores demandam o réu pretendendo ser ressarcidos de um prejuízo (patrimonial e não patrimonial) que sofreram por este ter omitido as diligências adequadas à garantia da máxima segurança dos valores depositados na conta à ordem de que aí são titulares, consentindo na realização de operações bancárias que não autorizaram.

Invocam, pois, os autores o regime da responsabilidade civil contratual, negocial ou obrigacional, emergente da violação de um direito de crédito ou obrigação em sentido técnico (com assento, entre nós, nos artigos 798º e seguintes do Código Civil).

E assentam a sua pretensão indemnizatória na violação pelo réu das obrigações decorrentes do contrato de abertura de conta bancária (ou contrato de conta bancária) celebrado entre ambos – pontos 2., 4. e 5. da factualidade provada.

Este contrato estabelece os termos da relação duradoura entre cliente (autores) e banco (réu), estando habitualmente associado a outras convenções específicas, como os contratos de depósito bancário, de *homebanking*, de cartão de crédito ou de débito, de mútuo, a convenção de cheque, etc. Nas palavras de Miguel Pestana de Vasconcelos[2], *"É um negócio extremamente amplo e complexo, donde emerge a relação bancária geral. Ele mantém-se independentemente de quantos negócios forem depois concluídos entre as partes, desde o início da relação, que funda, ao momento em que ela se extingue. Aí se integram também os contratos de conta corrente, de depósito e, pelo menos, de alguns serviços de pagamento".* E *"consiste num contrato organizatório, complexo, com produção de efeitos imediatos, direitos e obrigações para as partes, correspondentes a tipos de prestação de serviços. Mas, mais para além, é composto por elementos normativos, ou seja, prevê logo o regime de contratos que as partes podem vir a celebrar entre elas. A sua correta qualificação é a de contrato-quadro, visando-se destacar o carácter amplo e complexo do conjunto da relação bancária com o cliente".*

Ora, no caso em apreço, e muito embora tal não decorra expressamente da factualidade provada, é possível depreender que entre autores e réu (Banco) foram celebrados, além do contrato de abertura de conta bancária:

- Um contrato de depósito bancário (pois os autores mantinham fundos na sua conta);

- Um contrato de utilização de cartão de débito (referido no ponto 9. da factualidade provada);

- Um contrato de utilização de serviços de *homebanking* (pois foi por essa via que o evento lesivo ocorreu).

2. O depósito em dinheiro em instituição bancária, ou contrato de depósito bancário, integra-se na categoria geral dos contratos de crédito, decompondo-se essencialmente em duas relações jurídicas: por um lado, o cliente/depositante transfere a propriedade do dinheiro para o banco/ depositário, o qual fica assim legitimado a dele dispor; por outro lado, o banco constitui-se na obrigação de reembolsar o cliente de tal quantia, e respetiva remuneração (juros), nas condições entre ambos ajustadas.

Assim recortada tal relação jurídica complexa, tem sido doutrinal e

jurisprudencialmente caracterizada juridicamente como um depósito irregular ou mútuo de dinheiro, assumindo a natureza de usura se vence juros – cfr. Sá Carneiro[3]e Pinto Coelho[4], e os Acórdãos do S.T.J. de 23-07-85[5] e de 21-05-96[6], da Relação de Lisboa de 07-10-99[7] e de 30-05-2023[8], e da Relação do Porto de 01-07-2026[9]. Todavia, como concorrem em tal figura circunstâncias especiais, não lhe é aplicável o regime jurídico do mútuo ou da usura – cfr. Acórdãos do S.T.J. de 16-05-69[10], e da Relação de Coimbra de 13-12-88[11].
Mas o contrato de depósito bancário não se confunde com o contrato de abertura de conta, pois este constitui um negócio jurídico que estabelece e enquadra, de forma geral, a relação bancária complexa entre o banqueiro e o cliente, com características próprias e irredutíveis, e função autónoma – cfr. os Acórdãos do S.T.J. de 07-10-2010[12] e de 27-02-2014[13], e o já citado Acórdão da Relação do Porto de 01-07-2026.
3. Já o contrato de utilização de cartão de débito habilita a instituição bancária a emitir e disponibilizar ao cliente um meio de pagamento (cartão), simultaneamente físico e eletrónico, que lhe permite, através do emprego de terminais eletrónicos, aceder direta e imediatamente à sua conta bancária, operando a mobilização dos seus fundos monetários, quer pelo levantamento de numerário, quer pelo pagamento direto das aquisições de bens ou serviços, sem que seja necessário recorrer a qualquer outro meio – cfr. o Acórdão do S.T.J. de 23-11-1999[14].
4. Por seu turno, o contrato de *homebanking*, banco internético, *e-banking*, banco *online* ou banca eletrónica, constitui o serviço pelo qual, mediante a aceitação de determinados condicionalismos, o banco disponibiliza aos clientes a utilização de *"toda uma panóplia de operações bancárias, online, relativamente às contas de que sejam titulares, utilizando para o efeito canais telemáticos que conjugam os meios informáticos com os meios de comunicação à distância (canais de telecomunicação), por meio de uma página segura do banco"*, na definição do Acórdão do S.T.J. de 18-12-2013[15]. Este serviço "*confere ao cliente a possibilidade de efetuar consultas de saldos e de realizar operações bancárias, maxime pagamentos e transferências, relativamente às contas de que seja titular e que possa movimentar livremente, utilizando para o efeito o telefone (serviço telefónico) ou a internet (serviço online)"*, nas palavras de Carolina França Barreira[16].
5. Foi no âmbito destes contratos que se verificou o evento lesivo, como decorre da factualidade provada.
Sendo aqui convocável o regime do D.L. nº 91/2018, de 12-11 (Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica)[17], importa referir que os contratos de utilização de cartão de débito e de *homebanking* constituem contratos-quadro, na aceção do seu artigo 2º, al. i): "um contrato de prestação de serviços de pagamento que rege a execução futura de operações de pagamento individuais e sucessivas e que pode enunciar as obrigações e condições para a abertura de uma conta de pagamento". Desta forma, e como refere Carolina França Barreira[18], *"cada vez que o cliente emite uma ordem de pagamento a favor de terceiro através do sistema*

***informático posto à disposição pelo banco, é celebrado um novo contrato de execução do contrato de homebanking"*, existindo *"tantos acordos de vontade quantos os contratos celebrados, não se cingindo a simples atos de execução de um contrato anterior"* (embora por ele enquadrados).**

6. A mera leitura do diploma preambular do diploma legal citado permite divisar que, como seria expectável, a segurança dos pagamentos eletrónicos e a proteção dos utilizadores constituiu uma das principais preocupações do legislador (nacional e comunitário).

Logo nesse preâmbulo se menciona a *"exigência de uma autenticação forte do cliente, prevendo que sejam adotadas as medidas de segurança suficientes para proteger a confidencialidade e integridade das credenciais de segurança personalizadas dos utilizadores de serviços de pagamento"*. Não admira, pois, que no artigo 70º, nº 1, do D.L. nº 91/2018, de 12-11, se imponha aos prestadores de serviços de pagamento a implementação de "um quadro com medidas de mitigação e mecanismos de controlo adequados para gerir os riscos operacionais e de segurança, relacionados com os serviços de pagamento por si prestados".

Daí que o prestador de serviços de pagamento, como o aqui réu, esteja legalmente vinculado a um conjunto de obrigações ou deveres associados à emissão e utilização de um instrumento de pagamento, previstas no artigo 111º do D.L. nº 91/2018, de 12-11:

- "Assegurar que as credenciais de segurança personalizadas do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento" (nº 1, al. a);

- Não enviar instrumentos de pagamento não solicitados ou necessário para substituição de anterior (nº 1, al. b);

- Assegurar "a disponibilidade, a todo o momento, de meios adequados para permitir ao utilizador de serviços de pagamento proceder à comunicação" da perda, furto, roubo, apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento, ou solicitar o desbloqueio do instrumento de pagamento (nº 1, al. c);

- "Facultar ao utilizador do serviço de pagamento, a pedido deste, os meios necessários para fazer prova, durante 18 meses após a comunicação" da perda, furto, roubo, apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento, de que efetuou essa comunicação ou solicitou o desbloqueio do instrumento de pagamento (nº 1, al. d);

- "Impedir qualquer utilização do instrumento de pagamento logo que a comunicação" da perda, furto, roubo, apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento seja efetuada (nº 1, al. e).

Mas o próprio utilizador de serviços de pagamento, como o aqui autor, também se encontra legalmente vinculado por um conjunto de obrigações ou deveres, enunciados no artigo 110º do D.L. nº 91/2018, de 12-11. Desde logo, deve "utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização", preservando ainda a segurança das credenciais de segurança personalizadas do seu instrumento de pagamento (nº 1, al. a), e 2). Mas só lhe é exigível a adoção de "todas as <u>medidas razoáveis</u>", como expressamente se preceitua no referido nº 2 (sublinhado

nosso).
Deve ainda o utilizador de serviços de pagamento "comunicar, logo que tenha conhecimento dos factos e sem atraso injustificado, ao prestador de serviços de pagamento ou à entidade designada por este último, a perda, o furto, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento" (nº 1, al. b).
Estes deveres das partes dos contratos bancários decorrem diretamente da lei, embora habitualmente se encontrem também plasmados no clausulado dos contratos das contas bancárias, como no presente caso – pontos 4. e 5. da factualidade provada.
7. Como se pode observar, o legislador (nacional e comunitário) consagrou uma divisão de riscos entre o prestador e o utilizador de serviços de pagamento (como se refere no já citado Acórdão da Relação de Lisboa de 30-05-2023):
- O cliente/utilizador, onerado – em medida razoável - com deveres de cuidado na conservação da segurança e na utilização prudente do instrumento de pagamento, apenas será responsável pelo risco de incumprimento desses deveres se agir fraudulentamente, ou com dolo ou negligência grosseira;
- O Banco/prestador de serviço, dono e beneficiário económico do sistema de pagamentos, onerado com especiais deveres de configuração, manutenção, operacionalidade, disponibilização e segurança informática desse sistema, responderá pelo respetivo risco nas restantes hipóteses, ou seja, sempre que não se verifique fraude, dolo ou negligência grosseira do cliente/utilizador.
E o ónus da prova, quer da existência de consentimento (autorização do cliente) para a operação, quer da existência de fraude, dolo ou negligência grosseira do cliente/utilizador, recai sobre o Banco/prestador de serviço de pagamento.
É o que resulta do disposto nos artigos 112º a 115º do D.L. nº 91/2018, de 12-11. A este propósito, veja-se o decidido, entre outros, nos Acórdãos do S.T.J. de 23-01-2024[19] e de 12-12-2023[20], neste se referindo que *"as perdas resultantes de operações de pagamento não realizadas e não autorizadas pelo utilizador/titular do serviço homebanking, mas por terceiros, nos termos do art. 796 nº1 do CCivil e do art. 115 do DL 91/2018 correm por conta do banco, exceto se forem devidas a atuação fraudulenta daquele ou a atuação grosseira do mesmo por incumprimento deliberado das obrigações que lhe estavam impostas, devendo o prestador do serviço demonstrar a existência de fraude, de dolo ou de negligência grosseira".*
8. Ora, um dos principais riscos da atividade de prestação de serviços de pagamento, a que o aqui réu se dedicava, traduz-se na possibilidade de serem efetuadas operações de pagamento não consentidas. É que, muito embora qualquer operação de pagamento apenas se considere autorizada se o ordenante consentir na sua execução, em regra antes da respetiva concretização – artigo 103º, nº 1, 2 e 5 do D.L. nº 91/2018, de 12-11, são frequentes as situações de fraude, ou seja, as situações em que o prestador de serviço de pagamento acaba por executar a operação de pagamento sem o consentimento do ordenante (o seu cliente), por ação (ilícita) de terceiro.

É exatamente essa a situação que se discute nos presentes autos, dado que se provou que o réu executou diversas operações de pagamento, ao abrigo dos contratos bancários estabelecidos com o autor, que não foram por este autorizadas/consentidas, embora tenham sido solicitadas, por terceiro, com utilização do instrumento de pagamento disponibilizado e respetivas credenciais de segurança – pontos 6. a 16. da factualidade provada.
Apurando-se ainda que o autor de imediato (no próprio dia 11-02-2025) comunicou o sucedido ao réu e lhe solicitou o reembolso dos montantes das operações (nos termos do disposto no artigo 112º, nº 1, do D.L. nº 91/2018, de 12-11), o que este lhe negou, recai sobre o aqui réu o ónus de provar:
- Que as operações foram consentidas ou autorizadas pelo autor, ou pelo menos autenticadas (artigo 113º, nº 1 e 3, do D.L. nº 91/2018, de 12-11);
- Que as operações não foram afetadas por avaria técnica ou qualquer outra deficiência do serviço (artigo 113º, nº 1, do D.L. nº 91/2018, de 12-11);
- Que o autor agiu com fraude, dolo ou negligência grosseira (artigo 113º, nº 3 e 4, do D.L. nº 91/2018, de 12-11).
Caso o réu cumpra esse ónus probatório, o autor será considerado responsável pelo sucedido, não tendo direito ao reembolso e indemnização, improcedendo a ação. Se, ao invés, o réu não cumprir o ónus de prova a que se encontra sujeito, deverá reembolsar o autor dos montantes das operações em questão, acrescidos dos "juros moratórios, contados dia a dia desde a data em que o utilizador de serviços de pagamento tenha negado que autorizou a operação de pagamento executada, até à data do reembolso efetivo da mesma, calculados à taxa legal, fixada nos termos do Código Civil, acrescida de 10 pontos percentuais, sem prejuízo do direito à indemnização suplementar a que haja lugar" – artigo 114º, nº 1 e 10, D.L. nº 91/2018, de 12-11.
9. Assim, analisando a matéria de facto provada, constata-se que as operações de pagamento em questão foram objeto de autenticação, embora por terceiro, sem a vontade do autor, utilizando o seu instrumento de pagamento - cartão bancário. Cartão bancário que esse(s) terceiro(s), de forma ilícita (porque sem o conhecimento e autorização do autor), adicionaram a uma carteira Apple Pay, utilizando para o efeito os dados do cartão e um código de ativação que o autor inseriu numa página web que reproduzia de forma fidedigna a aparência do site oficial da Netflix. O autor agiu desse modo por ter sido enganado pela mensagem SMS que recebeu de remetente identificado como "netflix", que o informava da rejeição do pagamento da mensalidade do serviço, sendo-lhe exigido o pagamento imediato, sob pena de suspensão do serviço dois dias depois. Mensagem da qual constava um *link* para regularização do pagamento alegadamente em dívida (https://renovaperfil.com), que o remetia para a referida página web. O autor foi vítima, pois, de uma fraude informática, mais concretamente um esquema de *phishing*. Esta expressão tem sido utilizada na doutrina e jurisprudência, e também na prática quotidiana, para designar uma técnica fraudulenta pela qual o agente, habitualmente através do envio em massa de mensagens por correio eletrónico ou SMS, se faz passar por uma entidade legítima (banco, operador de pagamentos, administração pública, prestador de serviços, etc.) para, enganando o destinatário, dele obter credenciais,

códigos de autenticação, dados bancários, ou induzi-lo à realização de operações de pagamento. A este propósito, cfr. Miguel Pestana de Vasconcelos[21] e Carolina França Barreira[22], e os Acórdãos do S.T.J. de 18-12-2013[23] e de 17-06-2025[24].

Do exposto resulta, portanto, que as operações de pagamento em questão não foram autorizadas pelo autor. Porém, foram autenticadas no sistema informático do réu em consequência de ação do autor, que – enganado - acedeu à página web fraudulenta e aí inseriu os dados do cartão bancário disponibilizado pelo réu e o código de ativação que recebeu, assim permitindo a associação do referido instrumento de pagamento à carteira Apple Pay, gerida ilicitamente por terceiro.

Provou-se ainda que nessa data, o serviço prestado pelo réu não foi afetado por qualquer avaria técnica ou deficiência que pudesse originar em falha de segurança (ponto 20. da factualidade provada).

Mas como resulta do artigo 113º, nº 3, do D.L. nº 91/2018, de 12-11, não tendo o autor autorizado as operações de pagamento em questão, a mera "utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento (…) não é necessariamente suficiente, por si só, para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta, ou que não cumpriu, com dolo ou negligência grosseira", as suas obrigações.

10. Assim sendo, o réu terá ainda de demonstrar em concreto que o autor agiu com fraude, dolo ou negligência grosseira, como se disse.

Ora, o réu não alegou que o autor tenha agido de forma fraudulenta ou dolosa ao realizar os atos anteriormente descritos. Afirma o réu que o autor foi negligente, caracterizando essa negligência de grosseira.

Segundo o considerando 72 da Diretiva Serviços de pagamento revista, ou DSP 2[25], *"para avaliar a eventual negligência ou negligência grosseira cometida pelo utilizador dos serviços de pagamento, deverão ser tidas em conta todas as circunstâncias. Os elementos de prova e o grau da alegada negligência deverão ser avaliados nos termos do direito nacional. Todavia, embora o conceito de negligência implique uma violação do dever de diligência, a negligência grosseira deverá significar mais do que mera negligência, envolvendo uma conduta que revela um grau significativo de imprudência; por exemplo, conservar as credenciais utilizadas para autorizar uma operação de pagamento juntamente com o instrumento de pagamento, num formato que seja aberto e facilmente detetável por terceiros"* (sublinhado nosso). Já Miguel Pestana de Vasconcelos[26] afirma que *"a negligência grosseira deve ser devidamente separada da diligência ordinária ou culpa leve. Não basta a falta de cuidado que um bom pai de família, que aqui significa simplesmente um utilizador cuidadoso, desses instrumentos tivesse adotado, dentro das circunstâncias do caso concreto. Vai para lá dessa medida. Implica um nível de falta de cuidado quase escandaloso, de um desleixo inadmissível seja para quem for (p. ex., deixar o seu nome de utilizador ou palavra passe à vista ou num local de acesso a terceiros fora do seu círculo familiar ou de confiança próxima). A porta para a imputação de perdas ao utilizador por esta via é, assim, bastante apertada".*

Deste modo, devendo a culpa do agente ser avaliada em abstrato, "pela diligência de um bom pai de família, em face das circunstâncias de cada caso" (artigo 487º, nº 2, *ex vi* artigo 799º, nº 2, do Código Civil), e em medida razoável (artigo 110º, nº 2, do D.L. nº 91/2018, de 12-11), a negligência grosseira traduz-se na *"inobservância da diligência mínima adotada até pelos homens medianamente negligentes"*, na expressão do Acórdão do S.T.J. de 17-06-2025[27]. Verifica-se, pois, *"quando a pessoa não observa os deveres de cuidado de modo tal que só uma pessoa muito descuidada não o teria feito, ou seja, quando adote um comportamento bastante reprovável e injustificado, à luz dos normais critérios do senso comum aferidos a partir dos de uma pessoa normal numa sociedade espácio-temporalmente delimitada"*, segundo o Acórdão da Relação do Porto de 25-05-2026[28]. Ou, como refere Maria Raquel Guimarães[29], *"um comportamento que um utilizador médio, razoavelmente informado e esclarecido, não adotaria"*.

Deve, assim, apurar-se, *"no caso concreto, se a conduta do utilizador é censurável tendo em conta a aparência fidedigna ou não da mensagem de correio eletrónico (e a ingenuidade manifestada pelo utilizador), assim como o cumprimento pelo banco das obrigações de informação e esclarecimento dos clientes impostas pela lei"*, como propõe Carolina França Barreira[30].

Ora, na situação em apreço, o Banco réu não provou que tenha cumprido minimamente as suas obrigações de informação e esclarecimento quanto ao risco de *phishing*, não bastando para o efeito a mera inclusão dos deveres do cliente nas condições gerais da conta.

Além disso, o esquema de *phishing* de que o réu foi vítima - simulando um contacto do prestador de serviços de *streaming*[31] Netflix, incluindo uma página web que reproduzia de forma fidedigna a aparência do site oficial, recorrendo ainda à inclusão do instrumento de pagamento numa carteira Apple Pay - revela-se bastante credível e engenhoso, capaz de enganar um grande número de utilizadores comuns. O autor entendeu que a ação que lhe estava a ser pedida consistia apenas num método de pagamento, existindo diversas plataformas de pagamento digitais, como a Apple Pay, a Google Pay, o Paypal, etc. Trata-se, portanto, de um engano comum, sobretudo não se tendo apurado que o réu tenha advertido suficientemente o autor para essa forma de ludibriar.

Assim sendo, cremos que a conduta do autor, embora negligente, não se reveste da culpa gravíssima em que se traduz a negligência grosseira. Neste sentido, observe-se o afirmado por Maria Raquel Guimarães[32], citando os Acórdãos da Relação de Lisboa de 15-03-2016[33] e de 10-07-2019[34], da Relação de Coimbra de 15-01-2019[35], e da Relação do Porto de 27-06-2022[36]: *"Como tem vindo a ser defendido pelos nossos tribunais superiores, não se pode qualificar a conduta de quem fornece credenciais de segurança em resultado de uma prática fraudulenta como gravemente negligente quando "essas práticas fraudulentas são levadas a cabo porque um grande número de pessoas é ludibriado através delas e não apenas as extremamente descuidadas ou incautas; e para uma conduta poder ser qualificada como grosseiramente negligente ela não pode ser suscetível de ser*

levada a cabo por um número significativo dos homens médios”.
Por conseguinte, entendemos que o réu não demonstrou, como lhe incumbia, que o autor tenha agido com fraude, dolo ou sequer negligência grosseira. O que bastaria para responsabilizar o réu pelos eventos lesivos em discussão nos autos, como decidido pelo tribunal recorrido.
11. Mas a responsabilidade do réu apresenta ainda outro fundamento. Estando em causa franquear o acesso à conta de pagamento do autor através da internet e a realização de operações, através de terminal remoto, passíveis de envolver risco de fraude no pagamento, o Banco réu tinha a obrigação de submeter o acesso a autenticação forte – artigo 104º, nº 1, als. a) e c), do D.L. nº 91/2018, de 12-11. Traduzindo-se o conceito de autenticação no “procedimento que permite ao prestador de serviços de pagamento verificar a identidade de um utilizador de serviços de pagamento ou a validade da utilização de um instrumento de pagamento específico, incluindo a utilização das credenciais de segurança personalizadas do utilizador”, a “autenticação forte do cliente” consiste numa “autenticação baseada na utilização de dois ou mais elementos pertencentes às categorias conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é), os quais são independentes, na medida em que a violação de um deles não compromete a fiabilidade dos outros, e que é concebida de modo a proteger a confidencialidade dos dados de autenticação” – artigo 2º, als. c) e d), do referido diploma legal.
Assim, os prestadores de serviços de pagamento, como o aqui réu, passaram a estar obrigados a aplicar a autenticação forte do cliente a partir de 14 de setembro de 2019, data em que entrou em vigor o Regulamento Delegado (UE) 2018/389, da Comissão, de 27 de novembro de 2017. Contudo, no comércio eletrónico baseado em cartão (*e-commerce*), a aplicação obrigatória da SCA (*Strong Customer Authentication*, ou autenticação forte) foi adiada devido às dificuldades de implementação nos diversos mercados europeus. A Autoridade Bancária Europeia (EBA) fixou como prazo final para a migração completa o dia 31 de dezembro de 2020, que foi seguido em Portugal pelo Banco de Portugal[37].
Desta forma, o Banco réu, no presente caso, tinha desde logo o ónus de provar ter submetido o acesso (inicial, para inclusão do cartão bancário na carteira Apple Pay) à conta do autor a autenticação forte.
Ora, não resulta da factualidade provada essa autenticação forte, dado que se apurou que o acesso inicial à conta do autor, para inclusão do seu cartão bancário na carteira Apple Pay, foi franqueado pelo sistema informático do réu apenas com base nos dados do cartão (ponto 9.) e num código de ativação que recebeu (pontos 10. e 11.). Sucede que a mera exigência simultânea dos dados do cartão e de um código recebido por SMS não basta para que se verifique uma autenticação forte, dado que, como decorre do Guia sobre a autenticação forte do cliente do Banco de Portugal[38], os detalhes impressos no cartão bancário não são considerados elementos válidos para esse efeito (autenticação forte).
É certo que o réu alegou ter ainda enviado ao réu, através da sua *app*, um

segundo código, mas esta factualidade resultou não apurada (al. C).
Assim, não tendo o réu demonstrado, como lhe incumbia, ter submetido o referido acesso à conta bancária do autor a autenticação forte, aplica-se a previsão do artigo 115º, nº 5, do D.L. nº 91/2018, de 12-11: "Se o prestador de serviços de pagamento do ordenante não exigir a autenticação forte do ordenante, este não deve suportar quaisquer perdas relativas a operação de pagamento não autorizada, salvo se tiver agido fraudulentamente".
Não bastaria ao réu, portanto, ter demonstrado a negligência grosseira do autor (no que não teve sucesso, repita-se). Teria de alegar e provar a sua atuação fraudulenta, que não provou e nem sequer alegou.
Justifica-se, pois, plenamente a responsabilização do réu pelo evento lesivo em apreço nos autos.
12. E não assiste razão ao réu quando afirma que a sua responsabilização é objetiva, pois é, ao invés, culposa – culpa essa que se presume (artigo 799º, nº 1, CC), mas que até se provou no caso em apreço, como se disse.
Também não assiste razão ao réu quando sustenta a não aplicabilidade no caso do regime do D.L. nº 91/2018, de 12-11, uma vez que, muito embora a recolha dos dados de acesso à conta bancária do autor tenha ocorrido em plataforma externa, as transações, e o próprio acesso, efetivaram-se pela utilização da plataforma digital do Banco – cfr. artigo 3º do referido diploma legal. Foi utilizado um meio de pagamento disponibilizado pelo réu, e as operações de pagamento foram efetuadas necessariamente (também) por acesso ao seu sistema informático.
13. Conclui-se, assim, que o réu é responsável pela indemnização do prejuízo causado ao seu cliente, neste caso o autor, como decidido pela primeira instância.
14. Estando o réu obrigado a indemnizar o autor, deverá "reconstruir a situação que existiria, se não se tivesse verificado o evento que obriga à reparação" (artigo 562º do CC).
A trave mestra da reparação do dano ao nível do direito civil é, pois, o princípio da reposição ou reconstituição natural, o qual se traduz na obrigação de reconstituir a situação anterior à lesão, ou seja, o dever de repor as coisas na situação em que estariam caso o evento lesivo se não tivesse produzido. Tal princípio só será de afastar em qualquer das hipóteses previstas no artigo 566º, nº 1 do CC: impossibilidade da reconstituição natural; insuficiência da reconstituição natural para reparar integralmente os danos; e excessiva onerosidade da reconstituição natural para o devedor.
Ora, no caso em apreço, quer pela aplicação do princípio da reposição ou reconstituição natural, quer pelo recurso subsidiário à indemnização em dinheiro[39], mas sobretudo por força da norma especial do artigo 114º, nº 1 e 10, do D.L. nº 91/2018, de 12-11, o autor tem direito:
- Ao reembolso dos montantes das operações em questão (€ 30.654,66);
- Aos respetivos juros moratórios, contados desde o dia 11-02-2025 e até à data do efetivo reembolso, calculados à taxa de 14% ao ano;
- À indemnização suplementar a que haja lugar.
15. Estando afirmada a responsabilidade civil do réu e o inerente direito à indemnização do autor, esta deve ressarcir não apenas os danos patrimoniais

sofridos pelo lesado, como também os danos não patrimoniais produzidos, desde que, pela sua gravidade, mereçam a tutela do direito (artigo 496º, n.º 1, CC).
Os danos não patrimoniais são os insuscetíveis de avaliação pecuniária, reportando-se a valores de ordem espiritual, ideal ou moral. Não devem ser confundidos com os danos patrimoniais indiretos, os quais se traduzem nos prejuízos patrimoniais sofridos pelo lesado por força da verificação de danos não patrimoniais (por exemplo, um desgosto que reflexamente provoca uma diminuição da capacidade de ganho).
A problemática que tem rodeado a questão da ressarcibilidade dos danos não patrimoniais é extensa, mas o certo é que a orientação doutrinal e jurisprudencial dominante, à qual aderimos, se tem pronunciado no sentido da admissão de tal reparação, não como sendo uma indemnização em sentido estrito, mas sim como uma compensação. *"Mais vale proporcionar à vítima essa satisfação do que deixá-la sem qualquer amparo"*, como elucidativamente afirma Almeida Costa[40]. E que se aplica também no domínio da responsabilidade civil contratual, como tem vindo a ser doutrinalmente defendido e decidido entre nós – cfr., entre muitos outros, os Acórdãos do S.T.J. de 25-06-2009[41] e de 04-05-2010[42], e a posição de Maria Gabriela Páris Fernandes[43].
A lei - artigo 496º, n.º 1, CC - deposita nas mãos do tribunal o encargo de apreciar, no caso concreto, e de acordo com padrões objetivos, se o dano não patrimonial se mostra ou não digno de proteção jurídica. Na hipótese afirmativa, o montante da indemnização será fixado de forma equitativa pelo tribunal, tendo em atenção, em qualquer caso, o grau de culpabilidade do agente, a situação económica deste último e do lesado, e as restantes circunstâncias relevantes (artigos 496º, n.º 3, 1ª parte, e 494º, CC).
Ora, a primeira instância afirmou, e bem, a verificação deste dano, que decorre da factualidade provada (ponto 19.) e se reveste de suficiente gravidade para merecer tutela jurídica. Qualquer pessoa sofreria danos desta natureza na situação em que o autor se viu envolvido, de forma indiscutível.
No que respeita ao quantitativo da indemnização, importa recordar que a jurisprudência vem entendendo que o juízo equitativo da primeira instância é sindicável pelos tribunais superiores, desde logo pelo Tribunal da Relação. Mas não de forma ampla, pois não lhe é permitido substituir livremente o juízo da primeira instância como se constituísse um novo decisor originário. O tribunal de recurso deve, assim, implementar um controle limitado ao erro manifesto ou ao juízo desprovido de razoabilidade. Ou seja, o Tribunal da Relação só deve alterar decisões tomadas segundo o "prudente arbítrio" do julgador de primeira instância quando se verifique erro ostensivo, manifesta desproporção, contrariedade a padrões jurisprudenciais consolidados, ou violação de critérios legais/normativos. Não deve, pois, operar um verdadeiro segundo julgamento equitativo, mas apenas "corrigir" o julgamento equitativo da primeira instância se este padecer de erro manifesto ou de desrazoabilidade ou desadequação.
Neste sentido, atente-se no afirmado nos Acórdãos do S.T.J. de 14-12-2017[44]

e de 19-09-2019[45]: *"o julgamento de acordo com a equidade envolve um juízo de justiça concreta e não um juízo de justiça normativa, razão por que a determinação do quantum indemnizatório não traduz, em rigor, a resolução de uma questão de direito.*
Neste contexto, a intervenção do Supremo Tribunal de Justiça deve reservar-se à formulação de um juízo crítico de proporcionalidade dos montantes decididos em face da gravidade objetiva e subjetiva dos prejuízos sofridos.
A sua apreciação cingir-se-á, por conseguinte, ao controle dos pressupostos normativos do recurso à equidade e dos limites dentro dos quais deve situar-se o juízo equitativo, nomeadamente os princípios da proporcionalidade e da igualdade conducentes à razoabilidade do valor encontrado".
Ainda no sentido propugnado, afirma-se no Acórdão do Tribunal da Relação de Coimbra de 22-09-2021[46]: *"perante decisões recorridas fundadas na equidade, justifica-se um critério de revogação apenas das soluções que excedam manifestamente determinada margem de liberdade decisória, sendo então de verificar o padrão de equidade aplicado em concreto, pelo que, a situar-se a indemnização no quadro de um exercício razoável do juízo de equidade, não será adequada a revogação".*
Assim, não se verificando qualquer desrazoabilidade, desproporcionalidade ou exagero no valor fixado (€ 1.000), não se justifica alterar o decidido em primeira instância. Neste sentido, observe-se que em situações análogas à destes autos, o S.T.J., no seu Acórdão de 14-12-2016[47], fixou a indemnização por danos não patrimoniais em € 7.500, e a Relação de Guimarães, por Acórdão de 30-05-2013[48], em € 20.000.
16. Quanto à condenação em custas, o juízo da primeira instância também se revela adequado e proporcional.
17. Concluindo, deve manter-se o decidido em primeira instância, improcedendo o recurso.
As custas do recurso serão suportadas pelo réu/recorrente - cfr. artigo 527º, nº 1 e 2, do CPC.
*****
IV – DECISÃO
Pelo exposto, acordam os juízes desta 2ª Secção Cível em julgar improcedente a apelação, mantendo a decisão recorrida.
Custas do recurso pelo réu/recorrente - cfr. artigo 527º, nº 1 e 2, do CPC.
D.N.

Lisboa, 22 de outubro de 2026
Rute Sobral (relatora)
João Severino (1º adjunto)
António Moreira (2ª adjunto)
(Assinatura eletrónica)

---

1. Proferido no processo nº 1526/22.0T8VRL.G1, disponível em www.dgsi.pt
2. A responsabilidade do banco por operações de pagamento não autorizadas no online banking decorrente do novo regime de serviços de pagamento (RSP II), *in* Julgar nº 42, 2020, p. 192.
3. "Revista dos Tribunais", ano 87, p. 93.
4. R.L.J., 81, p. 226.
5. B.M.J. nº 349, p. 529.
6. B.M.J. nº 457, p. 343.

7. C.J., 1999, t. IV, p. 118.
8. Proferido no processo nº 5693/22.5T8LSB.L1-7, disponível em *www.dgsi.pt*.
9. Proferido no processo nº 39042/23.0YIPRT.P1, disponível em *www.dgsi.pt*.
10. B.M.J. nº 187, p. 145.
11. C.J., 1988, t. V, p. 81.
12. Proferido no processo nº 283/05.0TBCHV.S1, disponível em *www.dgsi.pt*.
13. Proferido no processo nº 244/1999.E1.S1, disponível em *www.dgsi.pt*.
14. Proferido no processo nº 99A796, disponível em *www.dgsi.pt*.
15. Proferido no processo nº 6479/09.8TBBRG.G1.S1, disponível em *www.dgsi.pt*.
16. Home banking: A Repartição dos prejuízos decorrentes de fraude informática, *in* Revista Electrónica de Direito, outubro de 2015 – nº 3, p. 16 (disponível em *https://cij.up.pt/download-file/1342*).
17. Que procedeu à transposição para a ordem jurídica interna da Diretiva (UE) nº 2015/2366, do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno (segunda Diretiva de Serviços de Pagamento).
18. Obra citada, pp. 15 e 16.
19. Proferido no processo nº 379/21.0T8FAR.E1.S1, disponível em *www.dgsi.pt*.
20. Proferido no processo nº 9240720.5T8LSB.L1.S1, disponível em *www.dgsi.pt*.
21. Obra citada, p. 194.
22. Obra citada, p. 26.
23. Já citado.
24. Proferido no processo nº 25239/19.1T8LSB.L1.S1, disponível em *www.dgsi.pt*.
25. Diretiva (UE) 2015/2366, do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, já anteriormente mencionada.
26. Obra citada, p. 202.
27. Já citado.
28. Proferido no processo nº 4136/23.1T8AVR.P1, disponível em *www.dgsi.pt*.
29. «Na minha conta ou na tua?» Revisitação do regime aplicável às operações de pagamento fraudulentas à luz da nova Proposta de um Regulamento relativo aos serviços de pagamento no mercado interno, de 28 de junho de 2023», *in* A Revista, 4 (2023), p. 84
30. Obra citada, pp. 57 e 58.
31. Tecnologia que permite transmitir e consumir conteúdos digitais, incluindo filmes e séries, através da internet.
32. Obra e local citados.
33. Proferido no processo nº 1063/12.1TVLSB.L1-1, disponível em *www.dgsi.pt*.
34. Proferido no processo nº 2406/17.7T8BCL.G1, disponível em *www.dgsi.pt*.
35. Proferido no processo nº 5600/11.0TBLRA.C1, disponível em *www.dgsi.pt*.
36. Proferido no processo nº 2598/16.2T8VNG.P1, disponível em *www.dgsi.pt*.
37. Informação do Banco de Portugal constante de *https://www.bportugal.pt/sites/default/files/anexos/documentos-relacionados/3._ponto_de_situacao_da_autenticacao_forte_do_cliente_e_comunicacao_comum_e_segura.pdf*
38. Disponível em *https://www.apb.pt/content/files/guia_autenticacao_forte.pdf*
39. Que apresenta como medida a diferença entre a situação real em que se encontra o património do lesado e a situação hipotética atual em que o mesmo se encontraria caso tal evento lesivo não tivesse ocorrido - teoria da diferença, consagrada legalmente no artigo 566º, n.º 2 do CC.
40. "Direito das Obrigações", 5ª ed., p. 483.
41. Proferido no processo nº 08S4117, disponível em *www.dgsi.pt*.
42. Proferido no processo nº 1194/07.0TBBNV.L1.S1, disponível em *www.dgsi.pt*.
43. Comentário ao Código Civil. Direito das Obrigações. Das Obrigações em Geral, coord. José Brandão Proença, Universidade Católica Editora, 2018, pp. 348-364
44. Processo nº 589/13.4TBFLG.P1, disponível em *www.dgsi.pt*.
45. Processo nº 2706/17.6T8BRG.G1.S1, disponível em *www.dgsi.pt*.
46. Processo nº 2426/17.1T8LRA.C1, disponível em *www.dgsi.pt*.
47. Proferido no processo nº 1063/12.1TVLSB.L1.S1, disponível em *www.dgsi.pt*.
48. Proferido no processo nº 6479/09.8TBBRG.G1, disponível em *www.dgsi.pt*.