jurisprudência.pt

Tribunal da Relação do Porto
Processo nº 3783/24.9T8AVR.P1

Relator: JOSÉ MANUEL CORREIA
Sessão: 12 Fevereiro 2026
Número: RP202602123783/24.9T8AVR.P1
Votação: UNANIMIDADE
Meio Processual: APELAÇÃO
Decisão: REVOGADA

SERVIÇO DE HOMEBANKING

ÓNUS DA PROVA DE QUE HOUVE NEGLIGÊNCIA GROSSEIRA DO UTILIZADOR

FORNECIMENTO DE DADOS PESSOAIS E CONFIDENCIAIS DE ACESSO

Sumário

I - O serviço de homebanking disponibilizado pelo banco ao cliente tem por objeto, além do mais, a possibilidade de movimentação de fundos para a titularidade de terceiros, pelo que constitui um serviço de pagamento que, enquanto tal, está sujeito ao Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RJSPM) - D.L. 91/2018, de 12/11, que transpôs para a ordem jurídica nacional a Diretiva (EU) n.º 2015/2366, do Parlamento Europeu e do Conselho de 25-11-2025.
II - Tendo havido operação de pagamento não autorizada pelo titular da conta, cabe ao banco, para se desonerar de qualquer obrigação de reembolso dos fundos movimentados, o ónus da prova de que houve negligência grosseira do utilizador do serviço de pagamento no seu manuseio (art. 113.º, n.º 4 do RJSPME).
III - Há negligência grosseira do utilizador do serviço, tendo este, por isso, de suportar a perda resultante da operação de pagamento não autorizada (art.º 115.º, n.º 4 do RJSPME), quando, apesar de utilizador habitual dos canais digitais disponibilizados pelo banco, proporcionou a terceiro desconhecido, por duas vezes e em ocasiões distintas, quatro dados pessoais e confidenciais de acesso àqueles canais e de autenticação de operações, designadamente: o

número do contrato de adesão; o código secreto (PIN) de 6 dígitos; o código de autorização enviado por SMS; e as três posições aleatórias do cartão matriz.

Texto Integral

Processo n.º 3783/24.9T8AVR.P1 - Recurso de apelação
Tribunal recorrido: Tribunal Judicial da Comarca de Aveiro - Juízo Local Cível de Santa Maria da Feira, Juiz 1

***

- Sumário
.....
.....
.....

***

- Acordam na 3.ª Secção do Tribunal da Relação do Porto,

I.- Relatório

- **AA** instaurou a presente ação declarativa de condenação, sob a forma de processo comum, contra **Novo Banco, S.A.**, pedindo que, pela sua procedência, fosse o Réu condenado:
i.- no reembolso das quantias que foram objeto das duas operações bancárias não autorizadas descritas na petição inicial, no valor global de €8.450,00,

acrescido de juros de mora vencidos e vincendos, à taxa legal, até integral pagamento;
ii.- no valor adequado e proporcional que se apurar em liquidação de sentença relativo aos danos não patrimoniais, acrescido de juros vencidos e vincendos, à taxa legal, até integral pagamento.
Para tanto, e em suma, alegou, valendo-nos do que, a propósito, consta da sentença recorrida, que 'no dia 05-11-2021, foi vítima de fraude bancária por *phishing*, pela qual um indivíduo desconhecido, fazendo-se passar por funcionário do *Novo Banco*, com acesso aos seus dados bancários e histórico, o contactou e o levou a fornecer um código de segurança recebido por SMS, supostamente para cancelar uma transferência de valor avultado'.
Acrescentou que 'tinha fundadas certezas de que o interlocutor era funcionário do Réu, dada a informação que este possuía e o remetente da mensagem que recebera era do Novo Banco', sendo que depois de fornecer o referido código 'verificou que 7.050,00€ foram retirados da conta à ordem e 1.400,00€ da sua conta poupança', valores estes cujo reembolso foi declinado pela sociedade Ré.
*

Citada, contestou a Ré, batendo-se pela improcedência da ação.
Em síntese, alegou que 'os prejuízos sofridos pelo Autor decorreram da sua atuação gravemente negligente, na certeza de que: o número de telemóvel pelo qual foi contactado não lhe pertence nem é por si gerido; os seus funcionários não solicitam credenciais por telefone; o o Autor é utilizador frequente dos canais digitais (com mais de 300 logins), pelo que conhecia e aceitou as condições gerais de funcionamento do serviço de *homebanking*; as operações foram realizadas com autenticação forte do cliente, envolvendo o número de adesão, o PIN de 6 dígitos, as posições do cartão matriz e os códigos de validação por SMS/notificação *push,* sendo estes elementos pessoais e intransmissíveis.'
Acrescentou que 'a SMS recebida pelo Autor incluía o alerta «*Não divulgue este código a terceiros, nem através de chamadas telefónicas. Ativar autorizações*", sendo que o Autor o forneceu e a operação não se destinava a cancelar, mas sim a ativar autorizações, assim facultando as suas credenciais de segurança a terceiros, contrariando as recomendações de segurança amplamente divulgadas pelo Banco e pelas autoridades.'
*

Findos os articulados, foi proferido **despacho** a convidar o Autor a substituir por pedido líquido o pedido genérico que, com respeito aos danos não

patrimoniais, formulara na petição inicial, na sequência do que o mesmo liquidou tal pedido em € 3.000,00.
*

Fixado em **€ 11.540,00** o **valor da causa** e prosseguindo os autos com a realização da **audiência de julgamento**, foi proferida, a final, **sentença** julgando a ação parcialmente procedente e, consequentemente.
i.- condenando a Ré no pagamento ao Autor da quantia de € 8.450,00, acrescida de juros de mora, vencidos e vincendos, à taxa de 4%, calculados desde 06-11-2021 até efetivo pagamento;
ii.- absolvendo a Ré do pagamento da quantia de € 3.000,00 peticionada pelo Autor a título de danos não patrimoniais.
*

Inconformada com esta decisão, dela veio a Ré interpor o presente **recurso**, pugnando pela sua revogação e pela sua absolvição do pedido.
Para o efeito, formulou as seguintes **conclusões**:

A.- Vem o presente recurso interposto da sentença proferida pelo Tribunal a quo, recaindo sobre matéria de direito.
B.- Por Sentença proferida em 20 de julho de 2025, o Tribunal a quo julgou a presente acção parcialmente procedente, tendo entendido para este efeito que a atuação do Recorrido não consubstancia um ato de negligência grosseira e, em consequência, condenou o Recorrente no pagamento ao Recorrido da quantia de € 8.450,00 (oito mil quatrocentos e cinquenta euros).
C.- O Recorrente não se pode conformar com o teor da Sentença proferida, uma vez que o Tribunal a quo faz uma errada interpretação e aplicação da matéria de direito.
D.- Nos termos do Decreto-Lei n.º 91/2018, de 12 de Novembro, o Recorrente deve suportar a perda resultante da operação em causa se a sua conduta for classificada como negligência grosseira, recaindo sobre o Banco Recorrido o ónus de demonstrar tal circunstância.
E.- Não obstante a definição empregue pelo Tribunal a quo, sempre se dirá que o conceito de negligência se traduz na grave omissão das cautelas necessárias para evitar a realização do facto antijurídico, quando não foi observado, de forma pouco habitual, o cuidado exigido, ou que resultaria evidente para qualquer pessoa – cfr. Acórdão do Tribunal da Relação do Porto de 14-07-2020, proferido no âmbito do processo n.º 22158/17.0T8PRT.P1.
F.- Apreciando a matéria de facto dada como provada nos termos do direito aplicável, deveria o Tribunal ter classificado a atuação do Recorrido como

negligência grosseira.
G.- Perscrutados os factos provados sob os n.ºs 6 a 21, ficou cabalmente demonstrado que:
i.- O Recorrido era um utilizador habitual dos canais digitais, com mais de 300 acessos autenticados;
ii.- Em dois momentos distintos, o Recorrido disponibilizou a um terceiro desconhecido 4 dados pessoais e confidencias de acesso aos canais digitais e autenticação de operações: (i) n.º de contrato de adesão; (ii) código secreto (PIN) de 6 dígitos; (iii) código de autorização enviado por SMS; (iv) as três posições aleatórias do cartão matriz necessárias à autenticação de operações;
iii.- O que permitiu ao terceiro desconhecido realizar as transferências que resultaram numa perda total de € 7.050,00 (sete mil e cinquenta euros);
iv.- O Recorrente disponibilizou, ao longo dos anos, diversos alertas de segurança e avisos sobre práticas fraudulentas, inclusivamente na SMS recebida pelo Recorrido, de onde constava expressamente a indicação de que o código não deveria ser partilhado com terceiros.
H.- Isto posto, o Recorrido não só facultou, em dois momentos distintos, todas as credenciais necessárias para a concretização das operações fraudulentas, como também ignorou todos os alertas de segurança e avisos disponibilizados pelo Recorrente, tanto ao longo dos anos, como no momento exato da ocorrência.
I.- Desta forma, contrariamente ao juízo formulado pelo Tribunal a quo, é forçoso concluir que o Recorrido incumpriu, de forma desleixada, grave e manifesta, o dever de cuidado a que se encontrava adstrito, omitindo as cautelas mínimas que lhe eram exigíveis para evitar o resultado lesivo.
J.- Pelo que deveria o Tribunal a quo ter determinado que a conduta do Autor se subsume ao conceito de negligência grosseira.
K.- Veja-se, neste sentido, a conclusão explanada no ponto VII. do sumário do Acórdão do Tribunal da Relação de Lisboa de 12-07-2018, proferido no âmbito do Processo n.º 2256/17.0T8LSB.L1-7, bem como o entendimento sustentado por CAROLINA FRANÇA BARREIRA, em repartição dos prejuízos decorrentes de fraude informática, cit., p. 79.
L.- Acresce, por outro lado, que o ónus probatório que recai sobre o prestador de serviços ao abrigo do disposto nos artigos 110.º e 113.º, n.º 1 do D.L. 91/2018 não pode ser interpretado de forma excessiva ou impossível de cumprir.
M.- Demonstrado que o sistema funcionou com normalidade, sem avarias ou interferências externas, e que as operações foram devidamente autenticadas com as credenciais disponibilizadas pelo cliente, não pode o Recorrente ser responsabilizado pelos atos fraudulentos que tenham tido origem no

equipamento do utilizador, sobre o qual não tem qualquer domínio.
N.- Aliás, a interpretação razoável e equilibrada deste regime legal impõe que corra por conta do utilizador a responsabilidade pelas operações, quando executadas por via do acesso que terceiros hajam tido aos seus dispositivos (computadores, telemóveis, tablets).
O.- O entendimento contrário - de responsabilidade automática do banco, mesmo perante indícios de negligência grosseira do utilizador do serviço -, criaria um incentivo à fraude e desvirtuaria o equilíbrio contratual e legal subjacente à prestação de serviços de pagamento.
P.- Crê-se, assim, que a interpretação do regime do risco e da responsabilidade no caso em apreço não pode deixar de passar pela ponderação da factualidade que se deixou expressa, não podendo o ónus da prova que recai sobre o Recorrente ser de cumprimento diabólico ou impossível, no sentido de lhe ser exigível que prove, com toda a solidez, o que se passou ao nível do acesso de terceiros ao equipamento do seu cliente.
Q.- Por isto, ficou demonstrado, por um lado, a regularidade da atuação do Recorrente e a inexistência de avarias ou falhas na prestação do serviço e, por outro, que qualquer eventual atuação fraudulenta ocorreu por parte do utilizador, ora Recorrido.
R.- Como resulta dos factos provados, se as operações são devidamente validadas, à primeira tentativa, com as credenciais de segurança pessoais e intransmissíveis do cliente, o banco não tem como saber (nem pode assumir, porque isso não é o normal) que tais credenciais chegaram ao poder de terceiros, seja por que via for, sendo que in casu, o Recorrido admitiu que prestou todas essas informações a terceiros – factos provados 8 a 11 da sentença.
S.- O banco não tem acesso ao dispositivo dos seus clientes, pelo que a obrigação de apresentar elementos que demonstrem a negligência grosseira por parte do utilizador, a qual decorre do art.º 113.º, n.º 4 do D.L. 91/2018, de 12 de Novembro, não se pode tornar num ónus de cumprimento diabólico ou impossível.
T.- Uma cabal e razoável interpretação do preceito, coerente com a distribuição do risco de utilização destes canais por ambas as partes – porque ambas deles beneficiam -, impõe que corra por conta do utilizador a responsabilidade pelas operações quando executadas por via do acesso que terceiros hajam tido aos seus dispositivos (computadores, telemóveis, tablets).
U.- O entendimento contrário levaria a que os bancos fossem sempre, sem exceção, responsabilizados por operações não reconhecidas, o que não só não é coerente com a mitigação do risco que deve estar subjacente à utilização destes meios, como se prestaria a situações fraudulentas em que os clientes,

conluiados com os beneficiários das operações que alegariam desconhecer, poderiam simplesmente reclamar de transferências executadas a favor destes, obrigando os bancos a reembolsá-los em qualquer situação.
V.- Crê-se, assim, que a interpretação do regime do risco e da responsabilidade no caso em apreço não pode deixar de passar pela ponderação da factualidade que se deixou expressa, não podendo o ónus da prova que recai sobre o Recorrente ser de cumprimento diabólico ou impossível, no sentido de lhe ser exigível que prove, com toda a solidez, o que se passou ao nível do acesso de terceiros ao equipamento do seu cliente.
W.- Face a todo o exposto, demonstrada ficou, por um lado, a regularidade da atuação do Recorrente e a inexistência de avarias ou falhas na prestação do serviço e, por outro, que qualquer eventual atuação fraudulenta ocorreu por parte do utilizador, ora Recorrido.
X.- Face ao exposto, a douta Sentença proferida pelo Tribunal "a quo" violou o disposto nos artigos 110.º a 114.º do D.L. 91/2018, de 12 de Novembro, incorrendo em erro de julgamento quanto à interpretação e aplicação do direito ao concluir que o Recorrido não atuou com negligência grosseira, quando a sua conduta, tal como apurada nos autos, consubstancia inequivocamente esse grau de culpa.
*

Respondeu o **Autor** ao recurso, batendo-se por que lhe fosse negado provimento, concluindo do seguinte modo:

1.- Veio o Réu, NOVO BANCO, SA., não se conformando com o sentido da douta sentença proferida nestes autos, dela interpor recurso, reconhecendo "a boa valoração da matéria de facto", a qual não coloca em crise nem ataca, cingindo as suas alegações à concretização do conceito de "negligência grosseira" e à sua materialização, convenientemente forçada, na conduta do Autor, de forma a tentar alterar o sentido da decisão.
2.- Não lhe assistindo, pois, qualquer razão!
3.- Desde logo, vejamos, que a sentença em crise deu como provados os factos 8., 10., 16., e 18., relevantes para esta contra-argumentação:
(…)
4.- E deu como não provado que:
(…)
5.- Ou seja, atentando apenas a estes factos provados e não provados pelo Tribunal a quo, não se poderá valorar a alegada mas inexistente desleixada, grave e incauta que, segundo o Recorrente, levaria à sua caracterização da conduta da Recorrida como negligência grosseira.

6.- Os factos provados 8. a 16. traduzem o cerne do esquema criado por terceira pessoa de identidade não concretamente apurada, senão vejamos: na posse dos dados de acesso à conta do Autor, o terceiro consegue, por telefone, confrontar o Autor com diversas informações pessoais e que se encontram no seu portal levando-o a acreditar que se trata, efetivamente, de um legítimo funcionário da Ré; o terceiro apresenta-se como um funcionário do banco, indica o departamento e o discurso é assertivo; sob o pretexto de que tem que proceder ao bloqueio de uma operação fraudulenta, esta terceira pessoa antecipa desde logo ao Autor que receberá uns códigos por mensagem de telemóvel e que deverá dizê-lo para validar o cancelamento; o recebimento de códigos SMS "caem" na conversa por mensagem SMS "legítima" e conhecida pelo Autor no seu telemóvel, ou seja, no histórico de conversa fidedigna já detida com a Recorrente.
7.- Relativamente ao facto não provado A, muito bem andou o Tribunal a quo a decidir como decidiu, fundamentando nos termos seguintes: "A Ré alega e a testemunha BB diz que esta operação também foi efetuada através da inserção de 3 números correspondentes a coordenadas do cartão matriz. Contudo, nesta parte, pese embora também não se adira integralmente à versão do Autor (que disse que nunca usou o cartão matriz), a verdade é que além do depoimento da testemunha, o doc. 3 que se destina a mostrar a configuração da ativação das notificações push apenas refere a existência de SMS para o número de telemóvel …93 e nada refere quanto à utilização dos números do cartão matriz. Assim, para esta operação, deu-se como provado que o Autor disse esse código obtido através de SMS Token, mas não forneceu, para o efeito, quaisquer posições do cartão matriz, assim se fundamentando, igualmente, o facto não provado em A."
8.- Quanto ao facto não provado B, entendeu, e bem, o Tribunal a quo, dar como não provado "porquanto, pese embora a Ré diga que as SMS referiam expressamente as operações que visavam autorizar, tal alegação não encontra arrimo na prova junta aos autos. Aliás, mesmo a referência a "ativar autorizações" que vem escrita nas mensagens recebidas pelo Autor não indica o que é que se visa ativar. Autorizações de quê? E, por outro lado, as mensagens serão, segundo até a versão da Ré, padronizadas, porquanto pese embora tenham tido finalidades diferentes, as mensagens recebidas pelo Autor são iguais em redação, apenas diferindo no código."
9.- Cristalinamente se constata que a sentença recorrida faz uma análise minuciosa e tecnicamente louvável dos factos que conduziram aos prejuízos reclamados nestes autos, e, assente na prova produzida e pela aplicação acertada do Direito que ao caso cabe, conduziu ao sentido decisório contrário à tese do Banco Réu.

10.- Como é consabido, para afastar a sua responsabilidade, o prestador de serviços tem de demonstrar que a operação de pagamento foi autorizada pelo ordenante, que este agiu fraudulentamente ou sem cumprir, com dolo ou negligência grosseira, as obrigações a que se encontra vinculado, previstas no artigo 110.º deste diploma legal, cfr. artigo 113.º, n.º 4 do RSP.
11.- Deste modo, cabia à Ré instituição bancária, provar que a operação de pagamento foi devidamente autenticada e, uma vez feita esta prova, compete-lhe ainda provar, no caso concreto, a contribuição do cliente para os prejuízos ocorridos e o grau de culpa subjacente ao seu comportamento, demonstrando, concretamente, que este agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações decorrentes do artigo 110.º, cfr. artigo 113.º, n.ºs 3 e 4 do RSP.
12.- O que, in casu, não ocorreu, como muito bem constatou a 1.ª Instância, quando concluiu que "a conduta do Autor, analisada à luz do circunstancialismo que o envolve, não consubstancia essa violação grosseira e inaceitável dos deveres de diligência".
13.- Afinal, o Recorrido, enquanto utilizador do serviço eletrónico, forneceu informações confidenciais àquele que ele julgava ser o seu banco, sendo que, o terceiro que se fez passar, fraudulentamente, pelo Recorrente só o consegue fazer em virtude quer da vulnerabilidade no acesso ao "canal emissor" de mensagens utilizado na comunicação entre o Banco e o Cliente, aqui Recorrente e Recorrido, quer da vulnerabilidade da página do prestador do serviço de homebanking.
14.- O Recorrido limitou-se a atuar perante uma chamada que tudo indicava ser proveniente do Banco Recorrente, após confirmação de dados bancários daquele a que só este teria acesso –confirmando os últimos movimentos bancários da conta bancária - dando um código que chegou pelo mesmo canal emissor do qual já tinha recebido outros SMS´s todos eles fidedignos e validados quanto à fonte emissora, nunca tendo desconfiado tratar-se de outro emitente que não o seu banco.
15.- No sentido da sentença da 1ª Instância, também já decidiu o Tribunal ad quem, vejamos, pois, o Acórdão do Tribunal da Relação do Porto, proferido no âmbito do processo n.º 659/22.8T8PNF.P1, em que foi relator Rodrigues Pires, quando diz: "IV - Não age de forma grosseiramente negligente o utilizador de conta bancária que, no âmbito do homebanking, fornece os seus dados confidenciais na sequência do recebimento de um SMS, que tudo indicava ser proveniente da respetiva entidade bancária, pelo mesmo canal emissor através do qual já tinha recebido outros SMS´s todos fidedignos, a que acresce o facto de a página web a que depois acede aparentar ser a dessa entidade bancária, por se mostrar idêntica à sua página oficial."

16.- In casu, o Tribunal recorrido ponderou e bem constatou que “Na hora em que julga estar a ser contactado por um funcionário da Ré, não se consegue, igualmente, sindicar o exercício intelectual que associe de forma clara e direta o acesso, anterior – quão anterior? – a essa hiperligação com o contacto telefónico que está a ser alvo no momento. Ademais, pode sempre ocorrer que a pessoa nunca represente que tenha acedido a um link fraudulento porque práticas há em que estes links têm grandes semelhanças com os sítios oficiais e, no caso dos autos, não podemos dizer que não se trata de uma dessas possibilidades.”
17.- E ainda, decidiu, e bem, o Tribunal a quo, que: “…o Autor, a braços com o contacto telefónico que julga ser da Ré, não atua de forma esclarecida, atua num contexto de pressão, em que alguém, de forma bastante credível (até pelo discurso) lhe diz que tem que cancelar aquelas operações. E, pese embora as advertências da Ré, cfr. factos provados 34 e 35, a ocasião dos autos não se dá – como é normal – num contexto em que o Autor acaba de ler os avisos e depois é confrontado com a tentativa de phishing, é uma realidade naturalística, que se dá em poucos minutos. (…) A pessoa comum e medianamente diligente não faz, confrontada com aquela situação, uma ponderação correta. É negligente sim, porque segue as instruções de alguém ao telefone, mas não é grosseiramente negligente porque mesmo uma pessoa dotada de diligência média, confrontada com este nível de sofisticação e manipulação, seria facilmente levada a agir da mesma forma.”
18.ª Os comportamentos adotados pelo Autor, embora manifestamente lamentáveis no desfecho que originaram, revelam uma atuação baseada na boa-fé e num quadro subjetivo de ilusão cuidadosamente construído por terceiros, fornecendo esse contexto psicológico à atuação do Autor.
19.- Em suma, a responsabilidade do Recorrente, proclamada na sentença em crise, corresponde à verdade dos factos, à correta aplicação da legislação e à melhor interpretação do Direito, como se extrai da abundante fundamentação de facto e de Direito e sustentação doutrinal e jurisprudencial daquela decisão.
*

O **recurso** foi admitido como **apelação**, com subida imediata, nos próprios autos e com efeito meramente devolutivo e assim recebido nesta Relação, que o considerou corretamente admitido e com o efeito legalmente previsto..
*

Colhidos os vistos legais, cumpre apreciar e decidir.
***

II.- Das questões a decidir

O âmbito dos recursos, tal como resulta das disposições conjugadas dos art.ºs 635.º, n.º 4, 639.º, n.ºs 1 e 2 e 641.º, n.º 2, al. b) do Código de Processo Civil (doravante, CPC), é delimitado pelas conclusões das alegações do recorrente. Isto, com ressalva das questões de conhecimento oficioso que ainda não tenham sido conhecidas com trânsito em julgado ou das que se prendem com a qualificação jurídica dos factos (cfr., a este propósito, o disposto nos art.ºs 608.º, n.º 2, 663.º, n.º 2 e 5.º, n.º 3 do CPC).
Neste pressuposto, a **questão** que, neste recurso, importa **apreciar** e **decidir** é a seguinte:
.- da responsabilidade da Ré/Apelante enquanto instituição bancária pelo reembolso ao Autor/Apelado dos valores pecuniários alvo de movimentação não autorizada por terceiro da sua conta bancária através do sistema *homebanking*.
***

III.- Da Fundamentação

III.I.- Na sentença proferida em 1.ª Instância e alvo deste recurso foram considerados **provados** os seguintes **factos**:
1.- O Autor é titular de duas contas bancárias, uma com o n.º ...29 e outra com n.º ...34, ambas domiciliadas no Novo Banco, aqui sociedade Ré, que, por seu turno, é uma instituição de crédito.
2.- O Autor aderiu aos canais diretos do Banco, tais como *NBnet, NB smart app, NBapp Tablet* e o *NBdireto*, por via dos quais lhe é permitido beneficiar do acesso a serviços bancários disponibilizados pela Ré através da internet.
3.- No documento intitulado "*Canais Diretos – Condições Gerais*", consta, além do mais, as seguintes cláusulas: «*9.6. Em caso de perda, extravio, falsificação, roubo, furto ou apropriação abusiva dos Códigos de Segurança é o Cliente responsável, até ao montante máximo de 150,00 EUR, pelas transações efetuadas até ao limite do saldo disponível da Conta D/O, considerando os valores das linhas de crédito associadas, bem como das contas poupança de transferência automática associadas".*
"9.7. Havendo negligência grave do Cliente, é este responsável pelas transações efetuadas até ao limite do saldo disponível da Conta D/O, considerando os valores das linhas de crédito associadas, bem como as contas poupança de transferência automática associadas ainda que superiores a

150,00 EUR, dependendo das circunstâncias da perda, extravio, falsificação, roubo, furto ou apropriação abusiva dos Códigos de Segurança.».
4.- Ao número de adesão ao serviço de *homebanking* do Autor encontrava-se associado o seu número de telemóvel ...93.
5.- Para acesso aos canais digitais da Ré, a Ré entregou ao Autor diversos códigos e coordenadas de segurança, pessoais e intransmissíveis, entre os quais, um PIN numérico composto por 6 dígitos e um cartão matriz.
6.- O Autor é utilizador dos canais digitais disponibilizados pela Ré, tendo efetuado, entre o *site* Novobanco online (*corresponde ao acesso via web)* e a *app Novobanco (corresponde ao acesso via smartphone)* mais de 300 logins.
7.- Em data não concretamente apurada, o Autor acedeu a uma hiperligação maliciosa, cujo teor se desconhece, e onde inseriu as suas credenciais de acesso aos canais digitais, designadamente, o número de adesão e o código PIN de 6 dígitos.
8.- No dia 05-11-2021, cerca das 12 horas e 44 minutos, o Autor recebeu uma chamada telefónica proveniente do número ...41, em que o interlocutor era um indivíduo do sexo masculino, que se identificou como responsável do departamento de *phishing* da sociedade Ré.
9.- O n.º de telemóvel ...41 a partir do qual foi efetuado o contacto telefónico não pertence à Ré nem figura, em lado algum, como sendo o respetivo número oficial.
10.- No decurso do mesmo contacto telefónico, o interlocutor procedeu previamente à confirmação de todos os dados pessoais do Autor, e confirmou o histórico de transações realizadas pelo mesmo.
11.- O terceiro, cuja identidade se desconhece, acedeu à conta bancária do Autor através do acesso ao *Novobanco online* no dia 05-11-2021, às 12 horas e 46 minutos, através da inserção correta do n.º de adesão ...36 que pertence ao Autor e o respetivo código secreto (PIN) de 6 dígitos.
12.- Por não se tratar de um primeiro acesso e por não terem decorrido mais de 90 dias desde a última vez que foi pedida autenticação forte, foi aplicada a isenção no acesso à aplicação.
13.- Após, o interlocutor disse ao Autor que existia um alerta para transferência de um valor avultado para o qual deveria confirmar a autorização da operação, tendo o Autor respondido que não tinha conhecimento dessa operação bancária e que não a autorizava.
14.- Foi-lhe perguntado se era habitual fazer transações bancárias de elevado valor, ao que o Autor respondeu que não, mas que excecionalmente, vinha realizando algumas transferências para pagamento de serviços contratados para o seu casamento.
15.- Face à posição assumida pelo Autor, o interlocutor disse-lhe que iriam

cancelar a referida transferência, porém, por questões de segurança iria ter de cancelar o cartão matriz e iria enviar um novo para a morada do Autor, com novos códigos de acesso aos canais diretos.
16.- Para aquela finalidade, o interlocutor disse ao Autor que este iria receber uma SMS para validar a operação de cancelamento da transferência.
17.- Pelas 12:51 horas, foi executada a operação ativação de autorizações por "*notificação push*" (com o n.º de pedido ...61), que permite substituir a disponibilização de códigos de autenticação enviados por SMS pela disponibilização desses mesmos códigos utilizando as notificações aplicacionais dos smartphones, habitualmente designadas "*push notifications*".
18.- Para o efeito, o Autor recebeu, na conversação com a sociedade Ré, um SMS (designado por SMS Token) com o seguinte teor: «*ATENCAO: Não divulgue este código a terceiros, nem através de chamadas telefónicas. Ativar autorizações. Codigo SMS ...64.».*
19.- O Autor recebeu no seu telemóvel pessoal o SMS com o código e disse-o, ainda no decurso da chamada telefónica, ao interlocutor.
20.- Pelas 12:51 horas, foi executada a operação ativação deixar cartão matriz em casa (com o n.º de pedido ...16), funcionalidade esta que permite aos clientes, num só telemóvel, prescindir a seu pedido, da utilização do elemento adicional de segurança que o cartão matriz assegura, substituindo-o por PIN ou biometria, associado a um dispositivo móvel.
21.- Esta operação «ativação deixar cartão matriz em casa» foi realizada através da inserção de 3 (três) posições aleatórias do cartão matriz que o Autor disse ao interlocutor.
22.- Pelas 12:52 horas, foi executada uma operação de transferência interna imediata (com o n.º de pedido ...68) debitada à conta à ordem n.º ...29 e creditada no IBAN ...23, no montante de 7.050,00€ (sete mil e cinquenta euros).
23.- Pelas 12h53, foi executada uma operação de mobilização da aplicação poupança (com o n.º de pedido ...99), debitada à conta ...34 a qual foi creditada na conta destino ...23, no montante de 1.400,00€ (mil e quatrocentos euros).
24.- As transferências referidas em 22 e 23 foram realizadas através do método «*one time password push notification*» enviada para o equipamento autorizado (a que se refere o facto 17) e inserção do código PIN.
25.- Após, pelas 12:54 horas acedendo novamente à *app NovoBanco* através do seu dispositivo móvel, o Autor recebeu, na conversação com a sociedade Ré, um SMS (designado por SMS Token) com o seguinte teor: «*ATENCAO: Não divulgue este código a terceiros, nem através de chamadas telefónicas. Ativar autorizações. Codigo SMS ...68.*»

26.- Após este procedimento, o Autor consultou a conta bancária n.º ...29 e verificou que o seu saldo era de 4,83€, tendo sido retirados da sua conta a quantia de 7.050,00€.
27.- Nessa sequência, confrontado com a ausência desse capital na sua conta bancária, o Autor deslocou-se à agência do Novo Banco em ... onde lhe foi confirmada a realização das transferências de 7.050,00€ e de 1.400,00€, tendo o Autor solicitado o cancelamento dessas transferências.
28.- Autor pediu o cancelamento dos canais diretos online e dos seus cartões.
29.- No mesmo dia 05-11-2021, o Autor apresentou queixa-crime contra desconhecidos.
30.- O Autor apresentou, em 07-11-2021, reclamação junto da Ré, a qual, em 03-12-2021, respondeu declinando a sua responsabilidade.
31.- O Autor apresentou comunicação junto do Banco de Portugal, tendo esta entidade respondido que não detetaram indícios de infração por parte da sociedade Ré.
32.- No dia 05-11-2021 não ocorreram quaisquer deficiências de serviço ou avarias técnicas nos serviços informáticos disponibilizados pela Ré.
33.- A Ré, desde data não concretamente apurada, mas seguramente já em novembro de 2021, disponibiliza diversos alertas de segurança aos utilizadores.
34.- Os alertas disponibilizados pela Ré correspondem às seguintes imagens consoante a plataforma utilizada pelo utilizador:

35.- A Ré publica diversos alertas e recomendações de segurança, em diversos módulos, no seu sítio internet, disponível em https://www.novobanco.pt/seguranca e em https://www.novobanco.pt/seguranca/alertas-fraude.
36.- À data dos factos descritos em 8), o Autor tinha a festa do seu casamento marcada para o dia 22-04-2022.
37.- Os 8.450,00€ retirados da sua conta tinham como destino o pagamento de despesas com o casamento.
38.- O Autor teve de pedir dinheiro a familiares, amigos e à noiva para fazer face às despesas de casamento.
39.- Esta circunstância causou-lhe ansiedade e angústia, humilhação, vergonha, noites de insónia e desgaste físico.

***

III.I.- Na mesma sentença, **não** foram julgados **provados** os seguintes **factos**:
a.- A operação «ativação de autorização por "notificação push"» foi realizada através da inserção de 3 (três) posições aleatórias do cartão matriz que o Autor disse ao interlocutor.
b.- A SMS remetida para o telemóvel do A. - a que se referia a operação de ativação de autorizações por notificações «*push*» - identificava cabalmente a operação a que se destinava o código nela contido.

***

III.III.- Do objeto do recurso

- Da responsabilidade da Ré/Apelante pelo reembolso ao Autor/Apelado dos valores pecuniários alvo de movimentação não autorizada por terceiro da sua conta bancária
Está em causa no recurso a questão de saber se deve a Apelada ser responsabilizada por operações de movimentação não autorizada de fundos por terceiro de conta bancária do Apelado com recurso ao serviço de *homebanking* por ela proporcionado.
Na sentença recorrida, foi reconhecida tal responsabilidade com fundamento na circunstância de a Apelada não ter demonstrado, tal como lhe competia, a **negligência grosseira** do Apelado na não observância das regras de cuidado e de segurança a que se vinculara quando aderiu àquele serviço.
É precisamente contra esta posição seguida na decisão recorrida que se insurge a Apelada no recurso. Segundo a mesma, as operações bancárias dos autos ficaram a dever-se ao incumprimento, "de forma desleixada, grave e manifesta do dever de cuidado a que [o Apelante] se encontrava adstrito, omitindo as cautelas mínimas que lhe eram exigíveis para evitar o resultado lesivo" e, portanto, a negligência grosseira.
Vejamos.

O Apelado, como resulta da factualidade apurada (v. facto provado n.º 1), é titular de duas contas bancárias, uma com o n.º ...29 e outra com n.º ...34, ambas domiciliadas, enquanto instituição de crédito, na sociedade Apelante Novo Banco, S.A..
Entre ambos foi, por conseguinte, tendo presentes os cânones de

interpretação da declaração negocial previstos nos art.ºs 236.º e 238.º do Código Civil, celebrado um **contrato de abertura de conta**. Ou seja, "um acordo entre uma instituição bancária e um cliente através do qual se constitui, disciplina e baliza a respetiva relação jurídica bancária" e "associado [ao qual] aparece o depósito bancário" (D.L. n.º 430/1991, de 02/11), que representa como que "um pressuposto *sine qua non* [daquela], já que nenhuma conta poderá ser aberta sem quaisquer fundo" (v. Engrácia Antunes, in Direito dos Contratos Comerciais, Coimbra, p. 483 e Acórdão da Relação de Coimbra de 11-02-2020, proferido no processo 8592/17.9T8CBR.C1, relatado por Isaías Pádua, disponível na internet, no sítio com o endereço www.dgsi.pt).

O **contrato de abertura de conta** constitui um negócio jurídico "amplo e complexo, donde emerge a relação bancária geral", sendo que, "não sendo legalmente típico, é, de forma clara, socialmente típico", constituindo um verdadeiro "contrato-quadro" no que ao universo da relação que se estabelece entre o banco e o cliente diz respeito, prevendo "logo o regime de contratos que as partes podem vir a celebrar entre elas" (v. Miguel Pestana de Vasconcelos, in A Responsabilidade Do Banco Por Operações De Pagamento Não Autorizadas No *Online Banking* Decorrente Do Novo Regime de Serviços de Pagamento (RSP II), in Revista Julgar, n.º 42, 2020, p. 192 e 193).

Um dos contratos usualmente associado a esse contrato-quadro é o do ***homebanking***.

Isto é, o contrato "mediante o qual o cliente adere a um serviço prestado pelo banco, que consiste na possibilidade de manter relações via *internet*, de forma a ceder informações sobre produtos e serviços do banco; obter informações e realizar operações bancárias sobre contas de que [o cliente seja] titular e realizar pagamentos, cobranças e operações de compra, venda, subscrição ou resgate sobre produtos ou serviços disponibilizados pelo banco" (v. Acórdão do STJ de 23-01-2024, proferido no processo 379/21.0T8FAR.E1.S1, relatado por Nelson Borges Carneiro, disponível no mesmo local).

E foi exatamente um tal tipo de acordo o que foi feito entre Apelado e Apelante, na certeza de que, como resulta do facto provado n.º 2, o primeiro aderiu aos canais diretos do segundo, tais como *NBnet, NB smart app, NBapp Tablet* e o *NBdireto*, por via dos quais lhe é permitido beneficiar do acesso a serviços bancários disponibilizados pelo mesmo *online*.

Objeto do serviço de ***homebanking*** é, além do mais, a possibilidade de movimentação de fundos para a titularidade de terceiros. Constitui o mesmo, por conseguinte, um verdadeiro **serviço de pagamento**, que, enquanto tal, está sujeito ao **Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RJSPME)**, aprovado pelo D.L. 91/2018, de 12/11, que transpôs

para a ordem jurídica nacional a Diretiva (UE) n.º 2015/2366 do Parlamento Europeu e do Conselho de 25-11-2025.
À luz de tal diploma legal, quem, como o Apelado, utiliza um serviço de pagamento a título de ordenante, de beneficiário ou em ambas as qualidades, figura na relação de ***homebanking*** como o **utilizador de serviços de pagamento** (alínea eee) do art.º 2.º).
Nessa qualidade, sobre ele recaem, em geral e aquando da utilização dos serviços de pagamento, os **deveres** de, por um lado, utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização, as quais têm de ser objetivas, não discriminatórias e proporcionais (alínea a) do n.º 1 do art.º 110.º); por outro lado, 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 (alínea b) do mesmo normativo).
No que ao primeiro dever respeita, este passa, não só pela utilização do instrumento de pagamento nos moldes ali consignados, mas, também, por que o utilizador tome todas as medidas razoáveis, em especial logo que receba um instrumento de pagamento, para preservar a segurança das suas credenciais de segurança personalizadas (v. n.º 2 do preceito).
A Apelante, por seu turno, enquanto **instituição de crédito** e **de pagamento** com sede em Portugal, pode prestar serviços de pagamento tais como, no que ao caso importa, execução de operações de pagamento, incluindo a transferência de fundos depositados numa conta de pagamento aberta junto do prestador de serviços de pagamento do utilizador (v. art.ºs 4.º, alínea c) e 11.º, n.º 1, alíneas a) e b)).
Enquanto **prestador de serviços de pagamento** sobre si recaem, na relação com o cliente, **deveres** como, reportando-nos ao que ao caso importa: (i) 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 (alínea a) do n.º 1 do art.º 111.º); (ii) garantir a disponibilidade, a todo o momento, de meios adequados para permitir ao utilizador de serviços de pagamento proceder à comunicação de utilizações não autorizadas de tais serviços (alínea c)); (iii) impedir qualquer utilização do instrumento de pagamento logo que tal comunicação tenha sido efetuada (alínea e)).
Qualquer operação de pagamento ou conjunto de operações de pagamento pressupõem inequivocamente o **consentimento** do ordenante (n.º 1 do art.º 103.º); não sendo prestado tal consentimento, a operação será havida por **não autorizada** (n.º 3 do art.º 103.º).

Neste último tipo de casos de operações de pagamento, isto é, das **não autorizadas**, que correspondem precisamente ao caso dos autos, fixa o diploma legal em apreço um regime especialmente exigente para o prestador de serviços de pagamento.
Assim, recai sobre o mesmo o **ónus da prova** da **autenticação** e dos **termos de execução da operação de pagamento**. A utilização do instrumento de pagamento pelo cliente não basta, por si só, para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu fraudulentamente ou que não cumpriu, com dolo ou negligência grosseira, um ou mais dos seus deveres acima transcritos (n.º 3 do art.º 113.º).
Consequentemente, cabe ao prestador de serviços de pagamento, **provar** que a operação de pagamento foi **autenticada**, devidamente **registada** e **contabilizada** e que **não foi afetada por avaria técnica ou qualquer outra deficiência do serviço por ele prestado** (v. n.º 1 do art.º 113.º). E em tais situações, sobre o mesmo recai, ainda, o dever de apresentar elementos que demonstrem a existência de **fraude, de dolo ou de negligência grosseira da parte do utilizador de serviços de pagamento** (n.º 4 do art.º 113.º).

Trata-se aqui de regime que, considerando a natureza dos serviços em causa, é perfeitamente compreensível.
Sobre o prestador dos serviços de pagamento recai a obrigação de "assegurar a qualidade e segurança do sistema que permita movimentar a conta apenas a quem tem legitimidade, depositando, levantando ou transferindo fundos. O risco de funcionamento deficiente ou inseguro do sistema de prestação de serviços de pagamento ou transferência localiza-se, portanto, na esfera do seu prestador, a quem incumbe a responsabilidade por operações não autorizadas pelo cliente nem devidas a causa imputável ao cliente" (v. Calvão da Silva, in Direito Bancário, Coimbra, 2002, p. 348).
Outrossim, "o prestador de serviços é quem está em melhores condições, do que qualquer outro (incluindo o consumidor), para trazer a factualidade demonstrativa do modo como as coisas se passaram", na certeza de que o "funcionamento do 'sistema informático' homebanking é [pertença] da sua esfera de risco" (v. Acórdão da Relação de Lisboa de 11-04-2019, proferido no processo n.º 18/18.7T8TVD.L1.6, relatado por Adeodato Brotas, disponível no local já referenciado).
Justifica-se, por isso, que sobre o mesmo recaia, como no regime em apreço se faz recair, não só o **risco** pelo funcionamento indevido do serviço de pagamento que proporciona ao seu cliente, como que sobre si recaia, em caso de movimentações não autorizadas, o **ónus da prova** de que, pese embora

essa movimentação indevida, o serviço funcionou correta e adequadamente e que na sua origem tenha havido fraude, dolo ou negligência grosseira do utilizador.
Isto, com as seguintes consequências.
Se não cumprido o ónus pelo prestador de serviços de pagamento, sobre este recairá a obrigação de reembolsar imediatamente o ordenante da operação de pagamento não autorizada, após ter tido conhecimento da operação ou de esta lhe ter sido comunicada e, em todo o caso, o mais tardar até ao final do primeiro dia útil seguinte àquele conhecimento ou comunicação (art.º 114.º, n.º 1)).
Se cumprido o ónus, o ordenante da operação pode ser obrigado a suportar as perdas relativas às operações de pagamento não autorizadas resultantes da utilização abusiva de um instrumento de pagamento, perdas essas que, se devidas a negligência grosseira do mesmo, ascenderão ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, independentemente do valor (art.º 115.º, n.ºs 1 e 5).

A responsabilidade ou irresponsabilidade do prestador do serviço de pagamento pelo reembolso ao cliente dos fundos movimentados sem autorização deste pressupõe, como se viu, e respetivamente, a não demonstração ou a demonstração, no que ao caso importa, da **negligência grosseira** do ordenante da operação.
Sobre o que deve ser entendido por negligência grosseira há que considerar, desde logo, como salientado pela Apelante no seu recurso, o considerando n.º 72 da Diretiva (UE) 2015/2366 acima referenciada.
Segundo tal considerando, "*[p]ara 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 vigilância, 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* ".
Significando mais do que negligência, a negligência grosseira pressuposta no regime normativo em consideração é aquela que tem subjacente uma "falta grave e indesculpável, consistente na omissão dos deveres a que se está adstrito, que só uma pessoa especialmente desleixada, descuidada e incauta

deixaria de observar" (v. Acórdão do STJ de 13-12-2007, proferido no processo P. 0753655, relatado por Sousa Peixoto, disponível no mesmo local).
Noutra perspetiva, "a *negligência grosseira* constitui uma negligência qualificada, uma grau exasperado de negligência (…), uma *negligência temerária* (…), podendo consistir na falta das precauções exigidas pela mais elementar prudência ou das aconselhadas pela previsão mais elementar que devem ser observadas nos actos correntes da vida, ou de uma conduta de manifesta irreflexão ou ligeireza". No fundo, "a negligência grosseira constitui a **grave omissão das cautelas necessárias para evitar a realização do facto anti-jurídico**, quando não foi observado, de forma pouco habitual, o cuidado exigido, ou que, no caso concreto, resultaria evidente para qualquer pessoa" (v. Acórdão da Relação do Porto de 14-07-2020, proferido no processo n.º JTRP000, relatado por Fernando Baptista de Oliveira, disponível no mesmo local).
Como comportamentos grosseiramente negligentes para os fins aqui em consideração, tem a **doutrina** adiantado exemplos como o caso do "utilizador que é constantemente alertado para os indícios de fraude, de maneira a estar, naturalmente, consciente de que os pedidos feitos nestas páginas falsas não são legítimos", ou o caso de resposta "a um pedido incomum na página clonada, por exemplo com indicação de todas as combinações do cartão matriz", casos estes reveladores de "enorme descuido e desatenção do titular do IP" (v. Raquel Sofia Ribeiro Lima, in A Responsabilidade pela utilização abusiva *on line* de instrumentos de pagamento eletrónico na jurisprudência portuguesa, Revista Eletrónica de Direito, Outubro de 2016, n.º 3, p. 48).
Ou, ainda, o caso "do utilizador que não se limita a inserir as credenciais de segurança que habitualmente lhe são solicitadas pelo seu Banco, mas, antes, divulga a quase totalidade das combinações do cartão matriz ou outras informações que o [prestador do serviço de pagamento] não tenha por hábito solicitar aquando da confirmação da ordem de pagamento, nomeadamente a marca, modelo e número de telemóvel, desde que de tal facto se tenha dado conhecimento ao utilizador" (v. Bruno da Silva Palhão, in Operações não autorizadas e repartição dos prejuízos: o *homebanking* na jurisprudência do RSP, Lisboa, abril de 2018, p. 44, consultável em https://repositorio.ucp.pt/).
Na **jurisprudência**, já foram reputados grosseiramente negligentes comportamentos como os seguintes:
.- em que o utilizador do serviço clicou no *link* malicioso e "forneceu a terceiros códigos de segurança e coordenadas do cartão matriz, com base nos quais outrem conseguiu aceder e usar a sua conta bancária", tendo o prestador do serviço de pagamento (o Banco) emitido "alertas com medidas de segurança, para que os clientes [prevenissem] a ocorrência de práticas

fraudulentas e, para além disso, na mensagem em que o Banco enviou o código para autorização da operação, estar contido um alerta no sentido de que tal código não [devia] ser divulgado a terceiros (v. acórdão da Relação de Guimarães de 02-10-2025, proferido no processo 237/23.4T8VRM.G1, relatado por Alexandra Rolim Mendes);
.- em que o utilizador "que, tendo acesso aos canais digitais há cerca de 4 anos, face a uma actuação fraudulenta de phishing, é reencaminhado para um site distinto do da Ré, fornece os dados de acesso ao homebanking e, assim, permite a movimentação de produtos poupança para a conta à ordem e, posteriormente, autentica as compras, após ter recebido uma notificação *push* na *app MBway*, a solicitar autorização para a concretização das mesmas, autorização essa que foi concedida, permitindo a conclusão, com sucesso, das transações" (v. acórdão da Relação do Porto de 21-11-2024, proferido no processo n.º 434/23.2T8PFR.P1, relatado por Álvaro Monteiro);
.- em que o utilizador "transmitiu as credenciais de autenticação ao pai, que as disponibilizou *online* em *site* e por meio não apurado, incluindo os números das coordenadas do cartão matriz e que foi através do uso dessas credenciais de acesso que um sujeito cuja identificação não foi possível apurar actuou" (v. acórdão da Relação do Porto de 14-07-2020, proferido no processo n.º 22158/17.0T8PRT.P1, relatado por Fernando Baptista Oliveira);
.- em que o utilizador "fornece todo o conteúdo do cartão matriz perante uma solicitação numa página idêntica à do Banco", "divulga na internet a totalidade das combinações de algarismos que compõem o seu cartão matriz – apesar dos vários avisos e alertas de segurança que constam do cartão matriz, da carta que a Ré enviou à Autora com o cartão, do site da Ré na internet e da página de login do sistema" (v. acórdão da Relação de Guimarães de 09-06-2020, proferido no processo n.º 51/18.9T8PRG.G1, relatado por Maria Cristina Cerdeira);
.- em que o utilizador, apesar de utilizar com frequência o sistema *homebanking*, "não se limita a inserir as credenciais de segurança que habitualmente lhe são solicitadas pelo seu banco (2 posições de coordenadas, que respeita ao cartão matriz, aviso que o banco disponibilizava no seu site e que constava aposto no cartão matriz), mas que, ao invés, divulga 50% das 72 coordenadas do cartão matriz" (v. acórdão da Relação de Lisboa de 13-10-2022, proferido no processo 344/21.8T8AGH.L1.2, relatado por Carlos Castelo Branco);
.- em que o utilizador revela "a terceiros, na *internet*, os seus códigos pessoais de acesso ao serviço e que, após intromissão destes terceiros visando uma saída (transferência) de numerário para uma conta diferente, alertou eletronicamente para o efeito o Autor e este confirmou/validou pessoa e

expressamente a operação, procedendo à introdução das coordenadas do cartão matriz que lhe foram novamente solicitados, como primeiro elementos de confirmação da operação e, seguidamente, introduzindo também o código *sms token* que lhe foi remetido pela Ré para o seu telemóvel para autenticação desta operação concreta, para a conta de destino indicada (v. acórdão da Relação de Coimbra de 10-07-2024, proferido no processo n.º 3606/20.8CBR.C1, relatado por Rui Moura).

No caso, resulta da factualidade apurada que no dia 05-11-2021, pelas 12h46, um terceiro de identidade desconhecida acedeu à conta bancária de que o Apelado era titular no banco da Apelante por intermédio do sistema *homebanking* deste (v. facto provado n.º 11).
Fê-lo através da inserção correta do n.º de adesão do contrato pertencente ao Apelado e do respetivo código secreto (PIN) de seis dígitos (v. o mesmo facto provado n.º 11), sendo que, uma vez no sistema, executou, pelas 12h52, uma transferência imediata de fundos da conta à ordem do Apelado para outra conta no montante de 7.050,00€ (v. facto provado n.º 22) e, pelas 12h53, nova mobilização de fundos da conta poupança do Apelado para outra conta no montante de 1.400,00€ (v. facto provado n.º 23).
Tais transferências consubstanciaram mobilizações não autorizadas dos fundos do Apelado para conta de terceiro e tiveram na sua origem um comportamento do primeiro motivado por engano ou astúcia do segundo, que, mercê desse engano ou astúcia, lhe proporcionou os dados de acesso às suas contas bancárias.
Saber se a Apelante é ou não responsável pelo reembolso ao Apelado dos fundos transferidos dependerá, pois, tendo presente o que acima foi exposto, da inexistência ou existência de negligência grosseira daquele.

O Apelante foi vítima de um ciberataque usualmente conhecido por *spoofing*. Trata-se aqui de uma espécie de fraude, pela qual alguém recorre a uma forma de falsificação de identidade (o *spoof*, que quer dizer imitar, fingir…), com o objetivo de obter informações pessoais.
Pode ser realizado de diversas formas, tais como o envio de *email* fraudulento ou de *sms* falso, ou mesmo realização de chamadas telefónicas falsas, sendo que o objetivo do agente é o de, com o recurso a tais expedientes, criar no destinatário a ilusão de que se trata de interlocutor credível, ao qual, por isso, podem ser facultados com segurança os dados de acesso ao *homebanking* daquele.
Quando contacta por telefone, o agente utiliza um número nacional ou um *spoofing* do número verdadeiro da instituição bancária ou de outra fonte

credível, ocorrendo a personificação por voz de um funcionário que questiona a vítima relativamente a informação privilegiada como dados pessoais. Desse modo, cria confiança ao ponto de solicitar credenciais de acesso ao banco à vítima e de obtê-las desta (v., neste sentido, a página do Centro Nacional de Cibersegurança de Portugal na internet, com o endereço https://www.cncs.gov.pt/pt/).

Com relevo para a questão que nos ocupa, são os seguintes os factos que resultaram provados.
O Autor é utilizador dos canais digitais disponibilizados pela Ré, tendo efetuado, entre o *site* Novobanco online (*corresponde ao acesso via web)* e a *app Novobanco (corresponde ao acesso via smartphone)* mais de 300 logins (facto provado n.º 6).
Em data não concretamente apurada, o Autor acedeu a uma hiperligação maliciosa, cujo teor se desconhece, e onde inseriu as suas credenciais de acesso aos canais digitais, designadamente, o número de adesão e o código PIN de 6 dígitos (facto provado n.º 7).
No dia 05-11-2021, cerca das 12 horas e 44 minutos, o Autor recebeu uma chamada telefónica proveniente do número ...41, em que o interlocutor era um indivíduo do sexo masculino, que se identificou como responsável do departamento de *phishing* da sociedade Ré (facto provado n.º 8).
O n.º de telemóvel ...41 a partir do qual foi efetuado o contacto telefónico não pertence à Ré nem figura, em lado algum, como sendo o respetivo número oficial (facto provado n.º 9).
No decurso do contacto telefónico, o interlocutor procedeu previamente à confirmação de todos os dados pessoais do Autor, e confirmou o histórico de transações realizadas pelo mesmo (facto provado n.º 10).
O terceiro, cuja identidade se desconhece, acedeu à conta bancária do Autor através do acesso ao *Novobanco online* no dia 05-11-2021, às 12 horas e 46 minutos, através da inserção correta do n.º de adesão ...36 que pertence ao Autor e o respetivo código secreto (PIN) de 6 dígitos (facto provado n.º 11).
Após, o interlocutor disse ao Autor que existia um alerta para transferência de um valor avultado para o qual deveria confirmar a autorização da operação, tendo o Autor respondido que não tinha conhecimento dessa operação bancária e que não a autorizava (facto provado n.º 12).
Foi-lhe perguntado se era habitual fazer transações bancárias de elevado valor, ao que o Autor respondeu que não, mas que excecionalmente, vinha realizando algumas transferências para pagamento de serviços contratados para o seu casamento (facto provado n.º 13).
Face à posição assumida pelo Autor, o interlocutor disse-lhe que iriam

cancelar a referida transferência, porém, por questões de segurança iria ter de cancelar o cartão matriz e iria enviar um novo para a morada do Autor, com novos códigos de acesso aos canais diretos (facto provado n.º 14).
Para aquela finalidade, o interlocutor disse ao Autor que este iria receber uma SMS para validar a operação de cancelamento da transferência, sendo que pelas 12:51 horas, foi executada a **operação ativação de autorizações por** "*notificação push*" (com o n.º de pedido ...61), que permite substituir a disponibilização de códigos de autenticação enviados por SMS pela disponibilização desses mesmos códigos utilizando as notificações aplicacionais dos smartphones, habitualmente designadas "*push notifications*" (factos provados n.ºs 15 e 16).
Para o efeito, o Autor recebeu, na conversação com a sociedade Ré, um SMS (designado por SMS Token) com o seguinte teor: «*ATENCAO: Não divulgue este código a terceiros, nem através de chamadas telefónicas. Ativar autorizações. Codigo SMS ...64.» (facto provado n.º 17).*
O Autor recebeu no seu telemóvel pessoal o SMS com o código e disse-o, ainda no decurso da chamada telefónica, ao interlocutor, sendo que pelas 12:51 horas, foi executada a operação **ativação deixar cartão matriz em casa** (com o n.º de pedido ...16), funcionalidade esta que permite aos clientes, num só telemóvel, prescindir a seu pedido, da utilização do elemento adicional de segurança que o cartão matriz assegura, substituindo-o por PIN ou biometria, associado a um dispositivo móvel (factos provados n.ºs 19 e 20).
Esta operação «ativação deixar cartão matriz em casa» foi realizada através da inserção de 3 (três) posições aleatórias do cartão matriz que o Autor disse ao interlocutor (facto provado n.º 21).
Pelas 12:52 horas, foi executada uma operação de transferência interna imediata (com o n.º de pedido ...68) debitada à conta à ordem n.º ...29 e creditada no IBAN ...23, no montante de 7.050,00€ (sete mil e cinquenta euros) e pelas 12h53, foi executada uma operação de mobilização da aplicação poupança (com o n.º de pedido ...99), debitada à conta ...34 a qual foi creditada na conta destino ...23, no montante de 1.400,00€ (mil e quatrocentos euros) (factos provados n.ºs 22 e 23).
Tais transferências foram realizadas através do método «*one time password push notification»* enviada para o equipamento autorizado e inserção do código PIN (facto provado n.º 24).
A Apelada, desde data não concretamente apurada, mas seguramente já em novembro de 2021, disponibiliza diversos alertas de segurança aos utilizadores (facto provado n.º 33), tais como os representados no facto provado n.º 34.
Também publica diversos alertas e recomendações de segurança, em diversos

módulos, no seu sítio internet, disponível em https://www.novobanco.pt/seguranca e em https://www.novobanco.pt/seguranca/alertas-fraude. (facto provado n.º 35).

Ora, tendo presentes todos estes factos, concluímos que o Apelado, apesar de vítima de um ciberataque, agiu com *negligência grosseira*.
Na verdade, o Apelado é utilizador dos canais digitais disponibilizados pela Apelante há vários anos, tendo efetuado, ao longo do tempo, mais de 300 logins. É o mesmo, como tal, não uma pessoa propriamente impreparada para lidar com o sistema, mas, pelo contrário, relativamente experimentada no seu manuseio.
Pese embora esta constatação, o Apelado, numa primeira ocasião, acedeu a uma hiperligação maliciosa, de teor desconhecido, mas na qual inseriu as suas credenciais de acesso como o número de adesão e o código PIN de 6 dígitos.
Ou seja, num contexto de solicitação exterior, que, por si só, mas sobretudo para quem, como o Apelante, tinha experiência no manuseio da aplicação, era apta do ponto de vista do homem médio a fazer desconfiar da sua origem ilícita, o Apelado, violando o dever a que estava adstrito decorrente do citado art.º 110.º, n.ºs 1, al. a) e 2 do D.L. 91/2018, de 12/11, facultou credenciais de segurança essenciais como são o número de adesão e o código PIN.
Numa segunda ocasião, no decurso de uma chamada telefónica em que um terceiro se fez passar por representante da Apelada, este acedeu ao seu sistema de *homebanking* através da inserção correta dos dados que o Apelado previamente lhe disponibilizou, isto é, o número de adesão e o código secreto de 6 dígitos.
Posteriormente, sob o falso pretexto de o Apelado estar a ser vítima de tentativa de transferência não autorizada de fundos da sua conta bancária, o terceiro informou o Apelado de que iria receber uma SMS para validar uma suposta operação de cancelamento da transferência, sendo que, para o efeito, o Apelado recebeu uma SMS com o seguinte teor: «*ATENCAO: Não divulgue este código a terceiros, nem através de chamadas telefónicas. Ativar autorizações. Codigo SMS ...64.*»
O Apelado, contudo, além de o n.º de telemóvel do qual foi efetuado o contacto telefónico não pertencer à Apelante nem figurar em lado algum como sendo o respetivo número oficial, não atentou no facto de o teor do SMS que recebera mencionar que o objetivo da operação era o de "ativar autorizações" e não, portanto, como seria suposto, o de "cancelar transferências" e prontamente disponibilizou o código ao interlocutor.
Com isso, permitiu ao terceiro, munido do código, executar a operação ativação de autorizações por "*notificação push*", que permite substituir a

disponibilização de códigos de autenticação enviados por SMS pela disponibilização desses mesmos códigos utilizando as notificações aplicacionais dos smartphones e, seguidamente, executar a operação ativação deixar cartão matriz em casa, que permite aos clientes, num só telemóvel, prescindir a seu pedido, da utilização do elemento adicional de segurança que o cartão matriz assegura, substituindo-o por PIN ou biometria, associado a um dispositivo móvel.
Isto, de modo a que, pelas 12h52, executasse as mobilizações de fundos não consentidas pelo Apelado, mobilizações essas realizadas do método «*one time password push notification*» enviada para o equipamento autorizado e inserção do código PIN.

Ou seja, tal como referido pela Apelante no seu recurso, o Apelado, apesar de utilizador habitual dos canais digitais disponibilizados por aquela, proporcionou a um terceiro desconhecido, por duas vezes e em ocasiões distintas, quatro dados pessoais e confidenciais de acesso aos canais digitais e autenticação de operações, designadamente: o n.º do contrato de adesão; o código secreto (PIN) de 6 dígitos; o código de autorização enviado por SMS, necessário para a ativação de operações via «notificação push»; e as três posições aleatórias do cartão matriz.
Outrossim, fê-lo, no segundo momento, depois de receber uma sms da qual constava, não só que o código não deveria ser partilhado com terceiros, como uma informação sobre o motivo da operação que deveria fazer contrária à que anteriormente lhe fora transmitida.
E foi exatamente o seu comportamento e não qualquer outro fator, nomeadamente, imputável à Apelada, que permitiu ao terceiro desconhecido realizar as transferências que resultaram no prejuízo de € 8.450,00.
Acresce que a conduta do Apelado contraria todos os alertas e avisos de segurança que a Apelada foi disponibilizando ao longo dos anos e no momento das transferências.
Na origem do prejuízo sofrido pelo Apelado esteve, por conseguinte, não só a violação, pelo mesmo, do dever objetivo de cuidado no manuseio do sistema de *homebanking*, como uma violação que tem subjacente “a omissão das precauções exigidas pela mais elementar prudência ou das aconselhadas pela previsão mais elementar que devem ser observadas nos actos correntes da vida”, reveladora de “irreflexão ou ligeireza” de comportamento.
O mesmo é dizer de negligência grosseira.

Ora, como se viu, a responsabilidade da Apelada pelo reembolso ao Apelado das quantias de que este se viu desapossado pressupunha a não demonstração

de que aquele atuara em termos tais que não podiam ser qualificados como negligência grosseira.
A Apelada, contudo, cumpriu o ónus que sobre si recaía de demonstrar essa mesma negligência grosseira do Apelado, pelo que a este, enquanto ordenante, cabe suportar as perdas resultantes das operações de pagamento de que foi alvo (v. o citado art.º 115.º, n.º 4 do D.L. 91/2018, de 12/11).
Procede, pois, a apelação, com a consequente revogação da sentença recorrida e absolvição da Apelada do pedido em apreço.
*

As custas da apelação serão suportadas pelo Apelado (art.ºs 527.º e 529.º do CPC).
***

IV.- Decisão

Pelo exposto, acordam os Juízes Desembargadores da 3.ª Secção do Tribunal da Relação do Porto em julgar totalmente procedente o recurso e, consequentemente, revogando a sentença recorrida, absolver a Apelante do pedido de condenação no reembolso das quantias que foram objeto das duas operações bancárias não autorizadas descritas na petição inicial, no valor global de € 8.450,00, acrescido de juros de mora vencidos e vincendos, à taxa legal, até integral pagamento.

Custas da apelação pelo Apelado.

Notifique.

***

Porto, 12-02-2026

Relator: José Manuel Monteiro Correia
1.ª Adjunta: Maria Manuela Barroco Esteves Machado
2.ª Adjunta: Isabel Rebelo Ferreira

(assinado eletronicamente)