Acórdão do Tribunal da Relação do Porto

Processo:	**13769/23.5T8PRT.P1**
Nº Convencional:	**JTRP000**
Relator:	**RUI MOREIRA**
Descritores:	**CONTA BANCÁRIA** **PAGAMENTO NÃO AUTORIZADO** **PHARMING** **PAGAMENTOS INDEVIDOS EFETUADOS PELO BANCO** **PAGAMENTO POR TRANSFERÊNCIA BANCÁRIA** **PRESTADORA DE SERVIÇOS** **ÓNUS DA PROVA**
Nº do Documento:	**RP2025011413769/23.5T8PRT.P1**
Data do Acordão:	**14-01-2025**
Votação:	**UNANIMIDADE**
Texto Integral:	**S**
Privacidade:	**1**
Meio Processual:	**APELAÇÃO**
Decisão:	**CONFIRMADA**
Indicações Eventuais:	**2. ª SECÇÃO**
Área Temática:	**.**
Sumário:	I - É facto notório a ocorrência de um elevado número de situações do fenómeno designado por *phishing,* e que aparece sob diversos formatos (*blind phishing, clone phishing, smishing, vishing, spear phishing, whaling,* a par de outro, designado por p*harming,* mas todos eles redundando no acesso fraudulento, isto é, através de meios enganosos e sem o conhecimento ou autorização do respectivo titular, à aquisição dos elementos identificativos de um utilizador de um sistema ou aplicação informática, em ordem a permitir ao autor de tal conduta utilizar esse mesmo sistema ou aplicação. A modalidade de *pharming* é mais complexa e difícil de detectar, pois consiste na própria intromissão no sistema do utilizador, para assim conhecer esses elementos ou operar o próprio acesso às aplicações, como se do verdadeiro utente se tratasse. II - O facto de pagamentos bancários terem sido determinados por dispositivo que apresentou o mesmo IP anteriormente usado pela autora, que usou os seus códigos de identificação e ainda mediante o uso do código remetido por SMS para um número de telemóvel da mesma, não determina necessariamente a conclusão de que tenha sido por a autora ter permitido o acesso a esses meios, dolosamente ou por falta de cuidado, que as transacções foram possíveis. III - Tendo-se adquirido a convicção de que nem a autora, nem ninguém com o seu consentimento ou a quem tenha sido facultado o acesso a esses sistema e meios de identificação, ordenou a execução de pagamentos, cumpre admitir que não se logrou apurar quem e por que forma conseguiu levar o banco réu a executar tais transacções. IV - O legislador previu essa situação, dispondo, no nº 3 do art. 113º do DL n.º 91/2018, de 12 de Novembro, que "… a 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, uma ou mais obrigações previstas no artigo 110.º" V - Optou o legislador, no nº 4 dessa norma, por impor ao prestador do serviço o ónus de "… apresentar elementos que demonstrem a existência de fraude, de dolo ou de negligência grosseira da parte do utilizador de serviços de pagamento." VI - O incumprimento de um tal ónus, determina ao prestador de serviço de pagamento o reembolso pelos pagamentos concretizados.
Reclamações:	
Decisão Texto Integral:	PROC. Nº 13769/23.5T8PRT.P1 Tribunal Judicial da Comarca do Porto Juízo Local Cível do Porto - Juiz 5 REL. N.º 927 Juiz Desembargador Rui Moreira Juíza Desembargadora Anabela Dias da Silva Juiz Desembargador Pinto dos Santos

*

ACORDAM NO TRIBUNAL DA RELAÇÃO DO PORTO

1 – RELATÓRIO

A..., Lda. intentou acção em processo comum contra Banco 1..., S.A. pedindo a condenação deste a pagar-lhe a quantia de € 7.992, a título de reembolso do montante retirado por terceiros da conta bancária que mantinha junto do réu, por via de operações não autorizadas por si, mas apesar disso executadas, quantia aquela acrescida de juros vencidos (€ 5.552,80) e vincendos, até integral pagamento.
Alegou que, sendo titular de uma conta bancária junto do banco réu, celebrou com este um contrato de *homebanking*, mediante o qual o banco lhe facultou a possibilidade de realizar operações bancárias online. Aconteceu que, no dia 20/4/2021, ao aceder à conta, o legal representante da Autora constatou que aquela tinha sido acedida de forma fraudulenta, dali tendo sido retirado o montante de € 7.992, sem a sua permissão e contra a sua vontade, por desconhecidos.
A Ré contestou a ação, negando a sua responsabilidade pelo ocorrido e pedindo a improcedência da ação e a sua absolvição do pedido.
Alegou, em suma, que "… a operação só foi realizada porque o utilizador autorizado pela Autora, ou outra pessoa com acesso ao único computador onde se mostrava instalado o certificado digital que permitia acesso à área de empresas do sítio de internet do Banco, utilizou o referido certificado digital, apôs o código de utilizador da Autora, a password (cód. secreto previamente fornecido exclusivamente à Autora) e introduziu, de forma aleatória, duas posições do número fiscal do utilizador, para ser efetuada a respetiva verificação de identidade."
Foi proferido despacho saneador, com fixação do valor da causa e enunciação do objeto do litígio e dos temas da prova.
Realizado o julgamento, foi proferida sentença que concluiu pela procedência da acção, condenado o réu como peticionado.

Dessa decisão vem interposto o presente recurso, que o banco réu termina formulando as seguintes conclusões:
"1) Os factos 20º, 21º e 22º da contestação devem ser julgados provados.
2) Tal é imposto pela ponderação conjugada de:
i. Documento 5 junto com a contestação (comprovativo do acesso à página de homebanking com menção do login e sua hora, bem como do IP (endereço de computador utilizado) e sistema operativo utilizado)
ii. documento 6 junto com a contestação (histórico de acessos realizados à área reservada da Autora no Homebanking do Banco Recorrente, sempre utilizando o mesmo IP)
iii. Depoimento de AA, testemunha que prestou depoimento no dia 27.06.2024, com início às 11:12 e termo às 11:37 a partir das 00:05:37.9 até 00:08:44.5
3) Os factos 23.º, 24.º e 25.º da contestação devem ser julgados provados.
4) Tal é imposto pela ponderação conjugada de:
i. documentos 7, 8 e 9 juntos com a contestação e que consubstanciam os comprovativos documentais retirados dos sistema informático do Banco que demonstram o envio de uma mensagem SMS para o número de telemóvel associado à Autora com o teor nele ínsito,
ii. documento 11 junto com a petição inicial, correspondente a cópia do ecrã do telemóvel do Autor com identificação, entre o mais da mensagem acima referida: "M Banco 1...Emp - Envio Ficheiro – Cta Deb:...466EUR - Tipo:PSM - N. reg:9 - Mont:8.991,00EUR - Data Proc:20/04/2021 - Codigo Autorizacao. ...81"
iii. Depoimento de AA, testemunha que prestou depoimento no dia 27.06.2024, com início às 11:12 e termo às 11:37 a partir das 00:08:44.5 até 00:11:32.6
5) O facto 26º da contestação deve ser julgado provado.
6) Tal é imposto pela ponderação do depoimento de AA, testemunha que prestou depoimento no dia 27.06.2024, com início às 11:12 e termo às 11:37 a partir das 00:11:39.9 até 00:12:26.5
7) O facto 27º da contestação deve ser julgado provado.
8) Tal é imposto pela ponderação conjugada de:

i. documento 11 junto com a petição inicial pela Autora, daí resultando que a mesma recebeu mensagens com códigos secretos referentes a tais operações ordenadas, mas não concretizadas, pela não aposição no sistema dos códigos secretos recebidos por mensagem SMS no telemóvel atribuído pela Autora.
ii. depoimento de AA, testemunha que prestou depoimento no dia 27.06.2024, com início às 11:12 e termo às 11:37 a partir das 00:12:30.9 até 00:12:41.6
9) Os factos 30.º, 31º, 32 e 33º da contestação devem ser julgados provados.
10) Tal é imposto pela ponderação conjugada de: i. Documento 5 junto com a contestação (comprovativo do acesso à página de homebanking com menção do login e sua hora, bem como do IP (endereço de computador utilizado) e sistema operativo utilizado)
ii. documento 6 junto com a contestação (histórico de acessos realizados à área reservada da Autora no Homebanking do Banco Recorrente, sempre utilizando o mesmo IP)
iii. Depoimento de AA, testemunha que prestou depoimento no dia 27.06.2024, com início às 11:12 e termo às 11:37 a partir das 00:05:37.9 até 00:08:44.5, 00:08:44.5 até 00:11:32.6, 00:11:39.9 até 00:12:26.5 e 00:12:30.9 até 00:12:41.6
iv. documentos 7, 8 e 9 juntos com a contestação e que consubstanciam os comprovativos documentais retirados do sistema informático do Banco que demonstram o envio de uma mensagem SMS para o número de telemóvel associado à Autora com o teor nele ínsito, v. documento 11 junto com a petição inicial, correspondente a cópia do ecrã do telemóvel do Autor com identificação, entre o mais da mensagem acima referida: "M Banco 1...Emp - Envio Ficheiro – Cta Deb:...466EUR - Tipo:PSM - N. reg:9 - Mont:8.991,00EUR - Data Proc:20/04/2021 - Codigo Autorizacao: ...81" e daí resultando que a mesma recebeu mensagens com códigos secretos referentes a tais operações ordenadas, mas não concretizadas, pela não aposição no sistema dos códigos secretos recebidos por mensagem SMS no telemóvel atribuído pela Autora.
11) A aposição por representante da Autora de um código secreto enviado por mensagem SMS que objetivamente indicava uma quantia de dinheiro a ser objeto de operação bancária no sistema informático do Banco, ou a sua mera comunicação a terceiros não autorizados, conforma atuação com negligência grosseira que isenta de responsabilidade o Banco Recorrente, porque corresponde a comportamento que nunca por nunca seria adotado pela generalidade dos utilizadores do serviço de pagamento colocados perante as concretas circunstâncias do agente, pois que a diligência e cuidados exigíveis no caso os levariam a abster-se de o adotar e/ou prosseguir.
12) No caso dos autos ocorre uma confluência de condutas culposas na produção dos resultados lesivos sofridos pela Autora, que não pode deixar de ser atendida.
13) Considerando a matéria de facto provada, nunca a responsabilidade do Banco Recorrente deveria ser valorada em mais do que 30% do dano da Autora.
14) A sentença recorrida violou os arts. 570.º, 796º do Cód. Civil e 113.º DL n.º 91/2018, de 12 de Novembro.
TERMOS EM QUE, no provimento do presente do presente recurso deve a sentença recorrida ser revogada e substituída por Acórdão que decrete a absolvição do Banco 1... do pedido."

*

A autora apresentou resposta ao recurso, sustentando a confirmação da sentença recorrida.
O recurso foi admitido como apelação, com subida nos próprios autos e com efeito suspensivo.
Cumpre apreciá-lo.

*

2- FUNDAMENTAÇÃO

O objecto do recurso é circunscrito pelas respectivas conclusões, sem prejuízo da decisão de questões que sejam de conhecimento oficioso - arts. 635º, nº 4 e 639º, nºs 1 e 3 do CPC.
No caso, atentas as conclusões acima reproduzidas, importa decidir:
- Se devem dar-se por provados os factos alegados sob os arts. 20º a 27º e 30º a 33º da contestação;
- Se se verifica uma confluência de condutas culposas na produção dos resultados lesivos sofridos pela Autora, em função da qual a responsabilidade do recorrente deve ser limitada a 30%.

*

Apreciando a matéria controvertida, decidiu o tribunal recorrido nos seguintes termos:
Factos provados:
“1. A Autora é uma sociedade comercial por quotas, que se dedica à importação, exportação, distribuição e comercialização de produtos cosméticos, terapias naturais e acessórios.
2. A Autora é titular de uma conta bancária com o nº ...66, junto do Réu Banco 1..., S.A.
3. Entre a Autora e o Réu foi celebrado um contrato de “homebanking”, o qual assenta na possibilidade conferida pela entidade bancária aos seus clientes, de realizar um conjunto de operações bancárias, online, relativamente às contas bancárias de que estes últimos são titulares, utilizando para o efeito meios informáticos.
4. Indivíduo(s) cuja identidade não se conseguiu apurar obteve(iveram) fraudulentamente as credenciais de acesso ao serviço de homebanking do Banco 1..., S.A. relativos à conta nº ...66, titulada pela Autora, com o intuito de movimentar as quantias monetárias aí depositadas sem permissão da respetiva titular.
5. E, munido(s) dos códigos de autorização e credenciais de acesso ao serviço de homebanking, no dia 20/4/2021, indivíduo(s) desconhecido(s) da Autora ordenou(aram) a realização de nove transferências bancárias para conta cujo respetivo(s) titular(es) a Autora desconhece, cada uma delas no montante de € 999 (novecentos e noventa e nove euros), sendo que uma não chegou a concretizar-se.
6. No dia 20/4/2021, pelas 9h50, a Autora, na pessoa do seu sócio-gerente BB, ao efetuar um pagamento ao Instituto da Segurança Social, constatou que da conta bancária em apreço tinha sido debitada a quantia de € 7.992 (sete mil, novecentos e noventa e dois euros).
7. Estas transferências encontram-se registadas no extrato bancário identificado nos autos como documento 3 apresentado com a petição inicial, que se dá aqui por reproduzido.
8. Ao verificar que tal quantia monetária tinha sido subtraída, o referido BB contactou de imediato os serviços de apoio ao cliente do Réu e o funcionário deste informou-o que “alguém” teria tido acesso ao computador e ao telemóvel do sócio gerente da Autora, acedendo aos dados de confirmação.
9. Após ter sido informada do sucedido, a Autora, na pessoa do seu sócio-gerente BB, constatou que recebeu mensagens no seu telemóvel com um código, conforme documento nº 11 que acompanha a petição inicial, que se dá aqui por reproduzido, mas os valores constantes dessas mensagens em nada correspondem aos valores subtraídos da conta bancária da Autora pelo(s) desconhecido(s).
10. Nesse mesmo dia, pelas 12h42, a Autora, na pessoa do seu funcionário CC, apresentou reclamação junto do apoio ao cliente da plataforma de pagamentos online da PayPall, conforme documento nº 4 apresentado com a petição inicial, que se dá aqui por reproduzido.
11. Pelas 14h12, a Autora, na pessoa do sócio-gerente BB, apresentou queixa-crime, que deu origem ao inquérito nº 251/21.4 PEVFX, o qual correu termos na 7º Secção do Departamento de Investigação e Ação Penal (DIAP) de Loures - Comarca de Lisboa Norte, conforme documentos nºs 5, 6 e 7 da petição inicial, que aqui se dão por reproduzidos.
12. Apresentada a queixa junto dos órgãos de polícia criminal, a Autora, em 22/4/2021, pelas 14h35, apresentou reclamação escrita junto do Réu, conforme documento nº 8 que acompanha a petição inicial, que se dá aqui por reproduzido.
13. O Réu respondeu por carta, em 13/7/2021, conforme documento nº 9 que acompanha a petição inicial, que se dá aqui por reproduzido.
14. Em 14/9/2021, a Autora, por intermédio do sócio gerente BB, apresentou nova reclamação, desta vez junto do Banco de Portugal, que manteve o entendimento perfilhado pelo Réu na sua missiva de 13/7/2021, conforme documento nº 10 que acompanha a petição inicial, que se dá aqui por reproduzido.
15. A Autora jamais forneceu a terceiros ou introduziu os códigos de autorização para efetuar qualquer transferência bancária.
16. O(s) agente(s) dos factos vindos de descrever previu(ram) e quis(eram) proceder às transferências bancárias supra, de modo fraudulento, ciente(s) da origem ilícita das transferências realizadas.
17. A conta bancária em questão foi aberta em 11/7/2013.
18. A Autora, através da sua gerência, e o Banco 1... celebraram contrato de utilização e operações bancárias online, nos termos e condições que decorrem dos documentos nºs 1 a 3 apresentados com a contestação, que se dão por integralmente reproduzidos.
19. As condições contratuais aplicáveis a tal contrato a 20/4/2021 eram as que constam do documento nº 4 apresentado com a contestação, que se dá aqui por reproduzido, remetidas e aceites pela Autora no final do ano de 2020, por assim ter sido acordado e convencionado entre ela e o Réu.

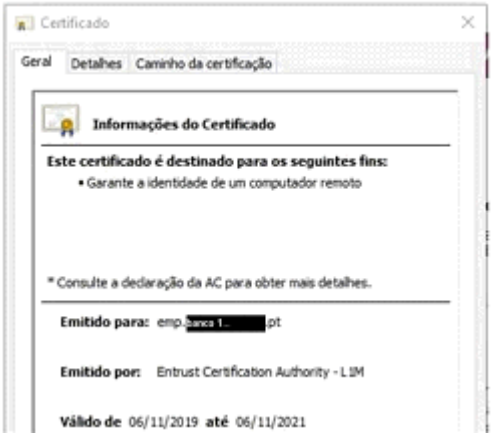
20. Nos termos do documento nº 3 a que se refere o ponto 18) dos factos provados, Autora e Réu acordaram que:
"Pelo presente contrato, o Banco 1... SA, Sociedade Aberta, adiante designado por Banco, disponibiliza ao Cliente que subscreva o contrato de utilização, o acesso a determinados serviços e operações bancárias através da área de empresas do portal banco 1....pt, assim como a possibilidade de contratar produtos ou serviços também oferecidos no mencionado Portal por parte de terceiras entidades alheias ao Banco.
Deste modo, mediante a utilização de equipamento informático e de comunicação adequado, as pessoas singulares indicadas pelo Cliente, adiante designados Utilizadores, poderão aceder ao Banco, através da área de empresas do portal banco 1....pt e efetuar um conjunto de operações, designadamente de consulta e/ou movimentação de contas, de acordo com as competências definidas pelo Cliente.
É da inteira e exclusiva responsabilidade do Cliente quer a definição do perfil dos Utilizadores, os quais poderão ser ou não colaboradores do Cliente, quer a sua seleção, nomeação e cancelamento.
O Cliente expressamente reconhece e aceita que a utilização, pelos Utilizadores, dos serviços disponibilizados pelo Banco, bem como a contratação, pelos mesmos, de operações com o Banco, nos termos do previsto neste contrato será sempre tida, em qualquer caso e para todos os efeitos legais, como uma atuação em nome e por conta do cliente, única contraparte do Banco no presente contrato – cfr. cláusula 1ª;
As operações efetuadas através da área de empresas do portal banco 1....pt ficam sujeitas às presentes Condições Gerais, modelos anexos, tarifário em vigor no preçário do Banco, legislação aplicável e usos bancários em geral - cfr. cláusula 2ª;
O Cliente deverá dispor de equipamento informático e de comunicação com as características adequadas para poder aceder ao Banco através da área de empresas do portal banco 1....pt, sendo da sua responsabilidade a segurança, manutenção e introdução das modificações eventualmente necessárias para assegurar em permanência o acesso, por essa via, ao Banco, de acordo com as inovações e alterações tecnológicas que vierem a ser introduzidas – cfr. cláusula 5ª;
O acesso regular ao Banco efetua-se através da utilização de um código de utilizador, de um código pessoal secreto (password) e, para as transações que envolvam qualquer tipo de alteração ao património financeiro do Cliente, de um certificado digital, ou de qualquer outra forma ou meio alternativo, com condições de segurança equivalentes, que o Banco disponibilize. Os códigos de utilizador, password e certificado digital destinam-se ao uso pessoal e exclusivo dos Utilizadores e apenas permitirão a execução das operações que sejam indicadas no Contrato (Anexos e eventuais Adendas) - cfr. cláusula 6ª;
No processo de recenseamento do Utilizador é solicitada a definição de uma password, é atribuído um código de utilizador e, no caso do Utilizador poder efetuar operações, o download de um certificado digital.
O Utilizador tem a possibilidade de alterar a password e deverá efetuá-lo regularmente - cfr. cláusula 7ª;
As ordens e instruções que o Banco recebe do Cliente através da área de empresas do portal banco 1....pt, corretamente validadas conforme definido pelo presente Contrato, gozarão de plenos efeitos jurídicos, ficando o Banco irrevogavelmente legitimado para cumpri-las e efetuar os débitos e créditos que delas decorram, entendendo-se, em todo o caso, que o Banco atua em cumprimento das ordens e instruções dadas pelo Cliente. O Banco poderá, contudo, reservar a aceitação das instruções mediante prévia confirmação por qualquer outro modo julgado conveniente - cfr. cláusula 18ª;
As ordens transmitidas e autorizadas pelo Cliente serão executadas de acordo com as condições e níveis de serviço aplicáveis ao tipo de produto/serviço solicitado, que estiverem em vigor – cfr. cláusula 19ª;
As partes aceitam a equiparação jurídica do conjunto composto pelo código de utilizador, certificado digital e password dos Utilizadores às assinaturas manuscritas dos mesmos.
Acorda-se igualmente que esta mesma condição é extensível à relação que o Cliente estabelece com fornecedores terceiros através da área de empresas do portal banco 1....pt, sendo que o Banco assina igualmente este contrato em nome e representação daqueles para aceitar, em seu benefício, a presente cláusula - cfr. cláusula 29ª;
O Cliente compromete-se a manter a confidencialidade dos códigos de utilizador, certificados digitais e passwords, bem como a zelar pelo seu bom uso, sendo plenamente responsável por todas as consequências que decorram do seu emprego e utilização. Do mesmo modo, o Cliente obriga-se a exigir dos Utilizadores e a assegurar que estes se obriguem a observar as obrigações constantes desta cláusula - cfr. cláusula 30ª;
Em caso de extravio, furto ou reprodução das chaves de acesso, do código de Utilizador, password, certificado digital, ou em qualquer situação que indicie que terceiros não autorizados tenham acedido ao serviço, bem como sempre que o Cliente verifique o registo na conta de qualquer transação não consentida ou a existência de erros ou

irregularidades na efetivação das operações, deve o Cliente dar de imediato conhecimento do facto ao Banco pelo meio mais expedito, confirmando-o por escrito num prazo não superior a 5 dias - cfr. cláusula 31ª;
Se a ocorrência afetar as passwords, deverá o Cliente alterá-las imediatamente. No caso do Cliente não conseguir modificá-las por qualquer motivo, deverá solicitar ao Banco o seu cancelamento e proceder a novo recenseamento dos Utilizadores cujas passwords foram canceladas - cfr. cláusula 32ª;
O Cliente poderá a todo o tempo ordenar ao Banco que bloqueie o acesso a determinados Utilizadores. Quando da receção da comunicação por telefone, o Banco procederá de imediato, à suspensão do Utilizador, procedendo ao seu cancelamento somente após a receção da comunicação escrita do Cliente - cfr. cláusula 33ª;
O Banco bloqueará o acesso do Cliente, ou de determinados Utilizadores, durante o primeiro dia útil de funcionamento bancário seguinte ao da receção da comunicação escrita prevista nos pontos anteriores, não se responsabilizando por eventuais prejuízos que ocorram até ao momento do bloqueio. A partir desse momento e não se verificando dolo ou negligência pela ocorrência, cessará a responsabilidade do Cliente - cfr. cláusula 34ª;
O Banco poderá proceder à alteração das presentes Condições Gerais, as quais serão previamente comunicadas ao cliente por correio eletrónico, dirigido a todos os utilizadores ativos e recenseados pelo Cliente. Caso não opte pela resolução do Contrato, o Cliente obriga-se a cumprir as novas condições a partir da data da sua entrada em vigor - cfr. cl. 39ª".
21. Face às condições contratuais em vigor em abril de 2021, nos termos do documento nº 4 apresentado com a contestação, que aqui se dá por reproduzido, destaca-se entre o mais que:
"Cláusula 2ª: Riscos associados aos meios de comunicação à distância
1. Os meios de comunicação à distância para acesso do Cliente ao Banco estão sujeitos a riscos de fraude por terceiros, 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, e 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, 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 acesso, como por exemplo, o Código de Utilizador, a Password e/ ou (todas) as posições do Código de Acesso Multicanal, o Código de Autenticação, o número de telemóvel ou os números dos cartões bancários.
3. O Cliente deve estar atento, ser precavido e ter em conta que tanto a(s) 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:
(….)
e) da indicação de que, deve fornecer Código(s) de Autorização que o Banco lhe enviou por SMS ou gerados via Token, para simular operações; 4. O Cliente obriga-se a ler atentamente e dar cumprimento escrupuloso às recomendações e regras de segurança constantes do ANEXO 1 -
RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra e faz parte integrante do presente acordo, bem como, a ir consultar e ler, pelo menos uma vez em cada trimestre do ano civil, os avisos de segurança e os alertas periódicos que o Banco divulga no sítio de Internet www.banco 1....pt, incluindo a descrição das fraudes comuns nesse período para a captura fraudulenta do Código de Utilizador, Password/ Código de Acesso Multicanal e demais credenciais personalizadas de acesso dos Clientes
(….)
7. O Cliente deverá dispor de equipamento informático e de comunicação com as características adequadas para poder aceder ao Banco através dos meios de comunicação à distância, sendo da sua responsabilidade a segurança, manutenção e introdução das modificações eventualmente necessárias para assegurar em permanência o acesso, por essa via, ao Banco, de acordo com as inovações e alterações tecnológicas que vierem a ser introduzidas e o cumprimento rigoroso das regras e recomendações de segurança constantes do ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra, bem como, dos alertas divulgados pelo Banco, em cada momento, no sítio de Internet www.banco 1....pt.

(….)
Cláusula 8.ª: Obrigações e responsabilidades do Cliente
(….)
5. O Cliente obriga-se conhecer e a assegurar o cumprimento escrupuloso das recomendações e regras de segurança constantes do ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra e faz parte integrante do presente acordo, bem como a ir consultar e ler, pelo menos uma vez em cada trimestre do ano civil, os avisos de segurança e os alertas periódicos que o Banco divulga no sítio de Internet www.banco 1....pt, incluindo a descrição de concreto(s) procedimento(s) utilizados nesse período para a captura fraudulenta de credenciais de segurança personalizadas de Clientes.
(….)
7. O Cliente é inteiramente responsável perante o Banco pelos atos dos seus representantes legais e dos seus Utilizadores praticados no acesso e na utilização dos meios de comunicação à distância, segundo o disposto no número um do artigo 800º do Código Civil.
8. Neste âmbito, fica bem entendido que compete exclusivamente ao Cliente selecionar criteriosamente os seus Utilizadores, e instruir e dotar cada Utilizador dos conhecimentos e dos meios adequados para o acesso e utilização dos meios de comunicação à distância do Banco em conformidade às disposições das presentes cláusulas, do(s) Documento(s) “Perfil de Utilizador”, e, se for o caso, do Documento “Regras para Autorização de Operações”, bem como, transmitir-lhe(s) as recomendações e regras de segurança constantes do ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra e faz parte integrante do presente Contrato.
Designadamente, o Cliente obriga-se a:
a) Comunicar a cada Utilizador especificas instruções e informação sobre os riscos de fraude, nomeadamente de “phishing”, alertando-o para a indispensabilidade de ser cuidadoso, atento e precavido e transmitindo-lhe as informações e sinais de alerta expostos no precedente número quatro; e
b) Facultar a cada Utilizador um exemplar do ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra e faz parte integrante do presente acordo, assegurando-se que este o lê atentamente; e
c) Assegurar que cada Utilizador consulta e lê atentamente, pelo menos uma vez em cada trimestre do ano civil, todos os avisos de segurança e alertas periódicos que o Banco divulga no sítio de Internet www.banco 1....pt, incluindo a descrição das fraudes mais comuns em cada momento para a captura fraudulenta de credenciais de acesso personalizadas, para se manter devidamente informado e atualizado sobre as precauções e regras de cuidado a adotar; para tanto, o Cliente deverá instruir cada Utilizador nesse sentido e assegurar o cumprimento periódico dessas instruções; e
(….)
ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA Regras gerais para o acesso/uso de todos os Meios de Comunicação à Distância do Banco
1. O Cliente obriga-se a ler atentamente e dar cumprimento escrupuloso às presentes recomendações e regras de segurança aqui constantes, bem como, a ir consultar e ler, pelo menos uma vez em cada trimestre do ano civil, todos os avisos de segurança e os alertas periódicos que o Banco divulga no sítio de Internet www.banco 1....pt, incluindo a descrição das fraudes perpetradas em cada momento para a captura fraudulenta de credenciais de segurança personalizadas.
2. O Cliente deve estar atento e ser precavido contra tentativas de fraude por terceiros não autorizados. Designadamente, o Cliente tem de suspeitar e de desconfiar de qualquer mensagem, por correio eletrónico ou SMS, que peça uma “ação imediata” ou crie uma sensação de urgência, que contenha erros ortográficos/gramaticais, contenha links e/ou anexos de ficheiros executáveis.
(….)
4. O Cliente deve analisar as mensagens de correio eletrónico que recebe antes de abrir, confirmando sempre a origem e o assunto da mesma e, se continuar com dúvidas, confirme previamente junto da entidade emitente. O Cliente não deve aceitar a execução de programas cujo download se ative sem o ter solicitado.
5. Se em algum momento o Cliente receber um Código de Autenticação para confirmação de uma operação que não tenha solicitado, o Cliente deve abster-se de introduzir ou divulgar esse código e deve de imediato reportar o facto sem demora para o(s) número telefónico ...24 / ...24 / ...24 / ...24 (chamada nacional) ou ...24 / ...24 (chamada internacional) que é um serviço de atendimento permanente – 24 horas/ dia, 365 dias/ano, a fim de dar o alerta e solicitar o respetivo bloqueio/impedimento de uso abusivo ou fraudulento perante o Banco 1....
6. O Cliente não deve nunca facultar o(s) Código(s) de Autenticação a terceiros, sob nenhum pretexto, obrigando-se a fazer uma utilização atenta, prudente, e exclusivamente

pessoal do mesmo, e assumindo todos os riscos e consequências inerentes à sua divulgação indevida.
(….)
Regras Adicionais para o sítio de Internet www.banco 1....pt:
1. Sempre que aceder às suas contas bancárias, através do sítio do Banco 1..., verifique se:
(i) o endereço se inicia por https://emp.banco 1....pt/,
(ii) a barra de endereços se apresenta a verde e (iii) junto ao endereço se encontra um cadeado, seguido de "Banco 1...", conforme:

2. Em caso de dúvida, confirme a origem do certificado digital - efetuando clique sobre o cadeado - e verifique se corresponde, efetivamente, ao Banco 1...:



3. O acesso ao sítio de Internet www.banco 1....pt pode ser realizado através de 2 métodos:
a) identificação do Código de Utilizador, da Password e dois (2) dígitos aleatórios do documento de identificação fiscal (que serão sempre os mesmos até que o login seja efetuado com sucesso);
b) identificação do Código de Utilizador e três (3) dígitos aleatórios do Código de Acesso (Multicanal), que serão sempre os mesmos até que o login seja efetuado com sucesso.
Tudo o que for solicitado para além do referido constitui uma tentativa de fraude que deverá reportar imediatamente e sem demora para o ...24. Para chamadas a partir do estrangeiro, ligue para ...24. Atendimento personalizado, disponível nos dias úteis das 8 horas às 02 horas e nos dias não úteis das 10 horas às 24 horas, hora de Portugal Continental.
4. No acesso ao sítio de Internet www.banco 1....pt o Banco nunca solicita o número de telemóvel nem a instalação de software/programas de segurança.
5. O Banco 1... envia sempre SMS e e-mails sem links.
6. Nunca aceda ao sítio do Banco 1... através de links de mensagens, motores de pesquisa ou, mesmo, através da opção "Favoritos".
Digite sempre o endereço completo www.banco 1....pt para evitar o acesso a páginas fraudulentas e muito idênticas à do sítio do Banco 1..., bem como evitar a instalação de software malicioso no equipamento utilizado para acesso ao sítio do Banco 1....
(….)
9. Deve ler atentamente o conteúdo do SMS recebido com Código de Autenticação, pois os dados da operação são identificados no texto da mensagem. Nunca forneça a terceiros os Códigos de Autenticação recebidos por SMS ou obtidos via token".
22. O Réu divulga na página de internet avisos constantes sobre ataques de phishing.
23. O sistema informático do Réu não foi alvo/objeto de qualquer avaria técnica, ou qualquer outra deficiência do serviço, sendo que os dados informáticos existentes revelam que não houve nenhuma avaria, deficiência nem quebra de serviço, designadamente nenhuma fraude foi perpetrada por terceiro nos equipamentos informáticos do Banco 1....
24. Nos termos acordados entre Banco 1... e Autora, sempre que esta pretendia aceder à área reservada (homebanking – área de empresas onde podia efetuar operações bancárias à distância) tinha de utilizar o seu computador pessoal onde tinha instalado o Certificado Digital previamente fornecido pelo Banco com um código de 15 dígitos disponibilizado pela sucursal à Autora, o código de utilizador da Autora, a password (código secreto previamente fornecido exclusivamente à Autora) e introduzir, de forma

aleatória, duas posições do número fiscal do utilizador, para ser efetuada a respetiva verificação de identidade.
25. Era a Autora quem tinha o exclusivo domínio e posse do seu equipamento informático e telemóvel de forma a dotar o mesmo das medidas necessárias a precaver-se de ataques informáticos de terceiro.

Não provados:
1. Que o funcionário do Réu que atendeu o legal representante da Autora se chamasse BB;
2. Que há vários anos que na página inicial de internet para acesso à área de empresas do Banco 1..., utilizada pela Autora, consta em destaque e bem visível uma caixa de AVISOS DE SEGURANÇA permanentemente atualizados, bem como um separador intitulado SEGURANÇA, onde são divulgados em permanência um conjunto de recomendações e informações relevantes para os Utilizadores do canal internet do Banco;
3. Que, concretamente, já há vários anos prévios a abril de 2021 que com destaque bem visível logo na página inicial de internet de acesso à área de empresas, o Banco 1... divulga sucessivamente AVISOS DE SEGURANÇA, contendo a descrição dos meios e métodos utilizados em cada momento por terceiros mal intencionados para a captura fraudulenta do Código de Utilizador, Password, dados pessoais e outras credenciais de acesso às contas de Clientes, bem como, recomendações e informações pormenorizadas e atualizadas para que os Utilizadores estejam conscientes e prevenidos para evitar tais fraudes;
4. Que existe ainda, já há vários anos prévios a abril de 2021, um separador intitulado SEGURANÇA acessível a partir da página inicial de internet de acesso à área de empresas do Banco utilizada pela Autora, que contém um conjunto de informações e conselhos relevantes para os Utilizadores do canal internet do Banco, incluindo a descrição de concretos procedimentos de segurança e precauções a observar pelos Utilizadores contra práticas fraudulentas de terceiros;
5. Que, ademais, já há vários anos prévios a abril de 2021, que o Banco divulga ainda com frequência alertas específicos de segurança, com regras de cautela a adotar pelos Utilizadores, que vão surgindo em *"pop-ups"* ou "*banners"* ao longo da navegação na página de internet do Banco;
6. Que, além disso, em todos os AVISOS DE SEGURANÇA com destaque bem visível na página inicial de internet de acesso à área de empresas do Banco, consta sempre e repetidamente o alerta aos Utilizadores de que o Banco 1...:
• "NÃO pede a instalação/atualização de software
• NÃO envia SMS com link
• NÃO envia Email com link
• NÃO solicita o Código Multicanal completo (os 7 dígitos)
• NÃO pede o número de telemóvel
• NÃO pede, por telefone ou outro meio, o Código de Autorização enviado por SMS e
• NÃO simula transações com os Clientes".
7. Que considerando o fuso horário GMT (+0:00), as transações a que alude a petição inicial foram registadas com os acessos do utilizador empresas BB, com o Código de Utilizador "NPCP...34", por débito da ...66 e foram efetuadas através do acesso ao site empresas do Banco 1....
8. Que na data de 2021-04-20 às 9:54:31 Hrs foi efetuado um login ao site Empresas, num dispositivo Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/...28 Safari/537.36 Edg/... com Certificado Digital, com o Código de Utilizador, Password e 2 dígitos do NIF do Utilizador no IP ...33;
9. Que da conjugação destes dados com todos os acessos efetuados pela Autora desde fevereiro de 2021 verifica-se que foi para o efeito utilizado o computador da Autora onde se mostrava instalado o certificado digital que permitia acesso à área de empresas;
10. Que às 09:57:37 Hrs foi registado um lote de PSM (Pagamentos de Serviços Multibanco), com nove (9) pagamentos no valor total de € 8.991,00, o que foi solicitado através do acesso à área de empresas acima melhor identificado;
11. Que para confirmar esta operação foi emitido pelo Banco, às 09:56:57 Hrs, um Código de Autorização que foi enviado e recebido para o nr de telemóvel do Utilizador (...07), com o seguinte conteúdo: "M Banco 1...Emp – Envio Ficheiro – Cta Deb:...466EUR - Tipo:PSM - N. reg:9 - Mont:8.991,00EUR – Data Proc:20/04/2021 - Codigo Autorizacao:*****81";
12. Que a operação (transferências em lote para Pagamentos de Serviços Multibanco) só foi efetuada depois de ter sido aposto no sítio reservado (área de empresas) do sítio de internet do Banco o referido código de autorização enviado para o telemóvel fornecido pela Autora, conforme por esta foi recebido;

13. Que este ficheiro PSM continha 9 transações, mas uma delas não foi executada por a referência estar incorreta;
14. Que no mesmo acesso foram identificadas tentativas de registos de transações não concretizadas por não terem sido identificados os Códigos de Autorização (autenticação de transação), a saber:
- às 10:03:36 Hrs foi emitido pelo Banco, a pedido do utilizador, um Código de Autorização para o nr de telemóvel do Utilizador (...07), com o seguinte conteúdo: “M Banco 1...Emp - Envio Ficheiro - Cta Deb:...466EUR - Tipo:PSM - N. reg:9 - Mont:8.492,00EUR - Data Proc:20/04/2021 – Codigo Autorizacao:*****22”;
- às 10:10:16 Hrs foi emitido pelo Banco, a pedido do utilizador, um Código de Autorização para o nr de telemóvel do Utilizador (...07), com o seguinte conteúdo: “M Banco 1...Emp - Envio Ficheiro - Cta Deb:...466EUR - Tipo:PSM - N. reg:8 - Mont:7.493,00EUR - Data Proc:20/04/2021 – Codigo Autorizacao:*****11”;
- às 10:10:17 Hrs foi emitido pelo Banco, a pedido do utilizador, um Código de Autorização para o nr de telemóvel do Utilizador (...07), com o seguinte conteúdo: “M Banco 1...Emp - Envio Ficheiro - Cta Deb:...466EUR - Tipo:PSM - N. reg:8 - Mont:7.493,00EUR - Data Proc:20/04/2021 – Codigo Autorizacao:*****09”;
15. Que a operação só foi realizada porque o utilizador autorizado pela Autora, ou outra pessoa com acesso ao único computador onde se mostrava instalado o certificado digital que permitia acesso à área de empresas do sítio de internet do Banco, utilizou o referido certificado digital, após o código de utilizador da Autora, a password (cód. secreto previamente fornecido exclusivamente à Autora) e introduziu, de forma aleatória, duas posições do número fiscal do utilizador, para ser efetuada a respetiva verificação de identidade;
16. Que após a verificação de identidade, o utilizador autorizado pela Autora, ou terceiro com acesso ao seu computador, onde estava instalado o certificado digital solicitou a realização da operação de PSM acima melhor identificada;
17. Que, posteriormente, o utilizador autorizado pela Autora, ou terceiro com acesso ao telemóvel do número fornecido pela Autora ao Banco 1..., após receber uma mensagem SMS com o seguinte teor “M Banco 1...Emp -Envio Ficheiro - Cta Deb:...466EUR - Tipo:PSM - N. reg:9 - Mont:8.991,00EUR – Data Proc:20/04/2021 - Codigo Autorizacao:*****81”, isto é após receber uma mensagem escrita que identificava expressamente que estava a fornecer um código de autorização para uma operação de pagamento, digitou esse código na área de empresa do sítio de internet do Banco 1... no espaço previsto para a realização da operação, ou forneceu esse código a um terceiro com acesso ao computador da Autora que o digitou na área de empresa do sítio de internet do Banco 1... no espaço previsto para a realização da operação;
18. Que foi a aposição de tal código secreto no sistema informático do Banco 1..., seja pelo utilizador autorizado pela Autora, seja por terceiro com acesso ao computador da Autora, depois do código ter sido divulgado pela Autora a terceiros, que permitiu a realização da transferência/pagamentos alegada na petição inicial;
19. Que a Autora não podia permitir que terceiros acedessem ao seu computador e área de empresas do sítio de internet do Banco 1..., nem podia fornecer os códigos secretos fornecidos pelo Banco a terceiros;
20. Que a Autora tinha ainda a obrigação de proteger o seu equipamento informático de intromissões e ataques de terceiros;
21. Que o utilizador autorizado pela Autora deveria ter lido o conteúdo da concreta mensagem SMS que lhe foi remetida nos termos acima alegados e, caso não quisesse realizar a operação alegada na petição inicial, não podia digitar esse código na área reservada de empresas, ou não podia ter fornecido esse código a terceiros sob pretexto algum;
22. Que decorre dos dados objetivos decorrentes da análise do ocorrido no sistema informático de Banco e da Autora que:
- foi o computador da Autora, com o certificado digital aí instalado, que acedeu à área de empresas e requereu a realização da operação PSM;
- foi digitado pelo utilizador autorizado pela Autora, ou por terceiro a quem este forneceu tal informação, o código secreto e específico enviado para o telemóvel fornecido pela Autora para efeitos de autorização daquela específica operação;
23. Que a Autora permitiu que terceiros acedessem ao seu equipamento informático, divulgando-lhes passwords e códigos de acesso e, por fim, divulgando um código especial e especificamente enviado pelo Banco 1... para o telemóvel pessoal de um seu representante/pessoa autorizada, código este que expressamente referia que se destinava à realização de operação de débito na conta bancária da Autora.

*

Pretende o apelante impugnar a decisão negativa do tribunal, relativamente à

demonstração dos factos descritos sob os itens 7º a 18º, no rol dos factos não provados.
Tendo-se por cumpridos os requisitos processuais referentes à especificação da factualidade a apreciar e ao sentido da decisão pretendida, deve ter-se igualmente por satisfeito o ónus da concretização dos meios de prova que devem justificar a alteração do decidido. Por conseguinte, observado o regime do art. 640º do CPC, apreciar-se-á o recurso nessa parte.
Para esse efeito, porquanto em sede de apreciação da matéria de facto controvertida nos encontramos, é pertinente ter presente o enquadramento legal da relação jurídica em causa, na vertente sob análise, pois que nele se dispõe sobre o ónus da prova em situações deste tipo.
Refere-se, no item 17 dos factos provados, que a conta bancária em questão foi aberta em 11/7/2013, mas afirma-se no item 19 que as condições contratuais aplicáveis a tal contrato foram aplicadas e aceites pela autora no final de 2020.
Deve, então, ter-se por aplicável à situação *sub judice* o regime do DL n.º 91/2018, de 12 de Novembro (Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica), e já não o que antes constava do Decreto-Lei n.º 317/2009, de 30 de Outubro, designadamente do respectivo art. 70º e ss., tanto mais que aquele DL n.º 91/2018 dispôs, no respectivo art. 159º, que o corresponde regime jurídico "… não prejudica a validade dos contratos em vigor relativos aos serviços de pagamento nele regulados, sendo-lhes desde logo aplicáveis as disposições que se mostrem mais favoráveis aos utilizadores de serviços de pagamento.
De todo o modo, cumpre afirmar que, quanto ao que aqui nos ocupa, as soluções prescritas naquele art. 70º são iguais às previstas no art. 113º do DL 91/2018, a saber:
"(Prova de autenticação e execução da operação de pagamento)
1 - Caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, ou alegue que a operação não foi corretamente efetuada, incumbe ao respetivo prestador do serviço de pagamento fornecer prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento.
2 - Se a operação de pagamento tiver sido iniciada através de um prestador do serviço de iniciação do pagamento, recai sobre este último o ónus de provar que, no âmbito da sua esfera de competências, a operação de pagamento foi autenticada e devidamente registada, e não foi afetada por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de pagamento por si prestado.
3 - Caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, a utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento, incluindo o prestador do serviço de iniciação do pagamento, se for caso disso, 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, uma ou mais obrigações previstas no artigo 110.º
4 - Nas situações a que se refere o número anterior, o prestador de serviços de pagamento, incluindo, se for caso disso, o prestador do serviço de iniciação do pagamento, deve apresentar elementos que demonstrem a existência de fraude, de dolo ou de negligência grosseira da parte do utilizador de serviços de pagamento."
Verifica-se, assim, que o regime dispõe sobre a imposição do ónus da prova ao prestador do serviço, quando o utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, além de impor outras soluções, que é relevante destacar.
Antes de mais, perante as definições constantes das als. pp) e qq) do art. 2º do D.L. 91/2018, é possível classificar o banco réu como «Prestador de serviços de pagamento», por referência ao elenco do art. 11º do mesmo diploma (al. pp)).
Assim, perante a circunstância de a autora afirmar, ter reclamado e denunciado não ter sido ela a ordenar as sucessivas transferências de 999,00€ concretizadas por débito na sua conta, no dia 20/4/2021, resulta do art. 113º citado que:
a) cabe ao banco réu fornecer prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento.
b) não é suficiente 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, uma ou mais obrigações a que estava sujeito (art. 110 do diploma) demonstrar a utilização do instrumento de pagamento registada pelo banco;
c) deve o banco apresentar elementos que demonstrem a existência de fraude, de dolo ou de negligência grosseira da parte do utilizador de serviços de pagamento.
No caso, sem impugnar parte da factualidade provada, designadamente a inscrita sob os

pontos 15 e 16 dos factos provados (*A Autora jamais forneceu a terceiros ou introduziu os códigos de autorização para efetuar qualquer transferência bancária e quem ordenou as transferências actuou de modo fraudulento, ciente da sua origem ilícita*) e sob os itens 4 e 5 (4. *Indivíduo(s) cuja identidade não se conseguiu apurar obteve(iveram) fraudulentamente as credenciais de acesso ao serviço de homebanking do Banco 1..., S.A. relativos à conta nº ...66, titulada pela Autora, com o intuito de movimentar as quantias monetárias aí depositadas sem permissão da respetiva titular (5.) E, munido(s) dos códigos de autorização e credenciais de acesso ao serviço de homebanking, no dia 20/4/2021, (…) ordenou(aram) a realização de nove transferências bancárias para conta cujo respetivo(s) titular(es) a Autora desconhece, cada uma delas no montante de € 999 (novecentos e noventa e nove euros), sendo que uma não chegou a concretizar-se*), pretende a apelante que se dê por provado um outro elenco de factos descritos entre os itens 7º e 18º dos factos não provados.
Em suma, pretende que se dê por provado:
Do facto não provado 7º - que as transacções foram registadas com os acessos do utilizador empresas BB, com o Código de Utilizador “NPCP...34”,
Do facto não provado 8º - que na data de 2021-04-20 às 9:54:31 Hrs foi efetuado um login ao site Empresas, num dispositivo Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/...28 Safari/537.36 Edg/... com Certificado Digital, com o Código de Utilizador, Password e 2 dígitos do NIF do Utilizador no IP ...33;
Do facto não provado 9º - que foi, para o efeito, utilizado o computador da Autora onde se mostrava instalado o certificado digital que permitia acesso à área de empresas;
Do facto não provado 10º - que às 09:57:37 Hrs foi registado um lote de PSM (Pagamentos de Serviços Multibanco), com nove (9) pagamentos no valor total de € 8.991,00, o que foi solicitado através do acesso à área de empresas acima melhor identificado;
Do facto não provado 11º - que, para confirmar esta operação, foi emitido pelo Banco, às 09:56:57 Hrs, um Código de Autorização que foi enviado e recebido para o nr de telemóvel do Utilizador (...07), com o seguinte conteúdo: “M Banco 1...Emp – Envio Ficheiro – Cta Deb:...466EUR - Tipo:PSM - N. reg:9 - Mont:8.991,00EUR – Data Proc:20/04/2021 - Codigo Autorizacao:*****81”;
Do facto não provado 12º - que a operação (transferências em lote para Pagamentos de Serviços Multibanco) só foi efetuada depois de ter sido aposto no sítio reservado (área de empresas) do sítio de internet do Banco o referido código de autorização enviado para o telemóvel fornecido pela Autora, conforme por esta foi recebido
Do facto não provado 13º - . que este ficheiro PSM continha 9 transações, mas uma delas não foi executada por a referência estar incorreta;
Do facto não provado 14º - que no mesmo acesso foram identificadas tentativas de registos de transações não concretizadas por não terem sido identificados os Códigos de Autorização (autenticação de transação, descritas nos autos:
Do facto não provado 15º- que a operação só foi realizada porque o utilizador autorizado pela Autora, ou outra pessoa com acesso ao único computador onde se mostrava instalado o certificado digital que permitia acesso à área de empresas do sítio de internet do Banco, utilizou o referido certificado digital, apôs o código de utilizador da Autora, a password (cód. secreto previamente fornecido exclusivamente à Autora) e introduziu, de forma aleatória, duas posições do número fiscal do utilizador, para ser efetuada a respetiva verificação de identidade;
Do facto não provado 16º - que após a verificação de identidade, o utilizador autorizado pela Autora, ou terceiro com acesso ao seu computador, onde estava instalado o certificado digital solicitou a realização da operação de PSM acima melhor identificada;
Do facto não provado 17º - que, posteriormente, o utilizador autorizado pela Autora, ou terceiro com acesso ao telemóvel do número fornecido pela Autora ao Banco 1..., após receber uma mensagem SMS com o seguinte teor “M Banco 1...Emp -Envio Ficheiro - Cta Deb:...466EUR - Tipo:PSM - N. reg:9 - Mont:8.991,00EUR – Data Proc:20/04/2021 - Codigo Autorizacao:*****81”, isto é após receber uma mensagem escrita que identificava expressamente que estava a fornecer um código de autorização para uma operação de pagamento, digitou esse código na área de empresa do sítio de internet do Banco 1... no espaço previsto para a realização da operação, ou forneceu esse código a um terceiro com acesso ao computador da Autora que o digitou na área de empresa do sítio de internet do Banco 1... no espaço previsto para a realização da operação;
Do facto não provado 18º - que foi a aposição de tal código secreto no sistema informático do Banco 1..., seja pelo utilizador autorizado pela Autora, seja por terceiro com acesso ao computador da Autora, depois do código ter sido divulgado pela Autora a terceiros, que permitiu a realização da transferência/pagamentos alegada na petição inicial.

A pretensão da apelante sustenta-se essencialmente na conjugação dos documentos juntos com a contestação, sob os nºs 5 e 6, com os depoimentos de AA, que trabalha no "laboratório" de segurança digital do banco réu e estudou os elementos documentadores das operações que descreveu, cujo depoimento se mostrou isento e esclarecedor,. Esta avaliação foi, de resto, partilhada pelo tribunal recorrido, que o classificou como "coerente e convincente".
Acresce que a genuinidade e veracidade dos documentos referidos não se mostra posta em causa, sendo que a explicação dada por tal testemunha sobre o respectivo conteúdo leva a que tenham de se considerar os elementos que deles constam como reais.
Do documento junto com a contestação sob o nº 5, com a designação "Backoffice - Consulta de Histórico de Contactos" resulta que o utilizador "BB" (sócio-gerente da autora, segundo o ponto 6º dos factos provados), para utilizar o canal Web-Empresas, junto do banco, utilizava um equipamento onde estava instalado o certificado digital com o código NPCP...34. E, bem assim, que às 9:54:31, um equipamento foi usado, onde estava instalado esse certificado, sendo ele descrito pelo browser e sistema usados: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/...28 Safari/537.36 Edg/... com Certificado Digital, com o Código de Utilizador, Password e 2 dígitos do NIF do Utilizador no IP ...33.
Do documento junto a seguir, com o nº 6, consta a descrição de operações realizadas respeitantes ao cliente utilizador desse certificado digital, desde 24/2/2021 e 22/4/2021, onde se inclui a operação de pagamento em causa. O acesso iniciou-se às 9:54:31, tal como referido no documento nº 5 e o dispositivo usado tinha o mesmo IP ...33.
Por sua vez, no documento 7, também com a designação "Backoffice - Consulta de Histórico de Contactos" são descritos, como "Detalhe de Transacções", os elementos da transação em causa, sob o uso do certificado digital NPCP...34, ocorrida às 9:56.57 do dia 20/4/2021, sobre a conta ...66, com o valor de 8.991,00, bem como que, pelo sistema, foi exigido o código de autorização:*****81
Sucessivamente, no documento junto sob o nº 8, relativo à mesma operação, é referido, como resultado um código numérico ...81, o qual, no documento nº 6, é indicado como relativo à operação registada por referência ao mesmo certificado digital NCPC...34, às 09:56:57 hrs. Mais consta o relato de que tal operação foi "Executada".
Explicou AA que o ficheiro que compreendia 9 transações, não mereceu integral execução, pois a identificação da referência relativa a uma delas deu erro. Daí que, apesar de o total das transacções pedidas fosse de pagamento de € 8.991,00, só tenham sido executadas 8, com o valor total de € 7.992.
Por outro lado, que para o telemóvel indicado pela autora para o recebimento dos códigos de confirmação para as suas operações foi remetido aquele código *****81, bem como que foram igualmente emitidos outros códigos, para outras operações, como descrito no item 14 dos factos provados, resulta ainda da reprodução das mensagens recebidas pelo gerente da autora, que constitui o documento 11, junto com a petição inicial.
Acolhendo o teor destes meios de prova, que nada justifica desconsiderar, só pode dar-se por provada a matéria que está descrita nos itens 7, 8, 10, 11, 12, 13, 14.
De resto, como bem salienta o apelante, seria até contraditório dar como não provada a matéria do item 13, quando o tribunal deu por provado o facto essencial ali descrito, respeitante à não execução de uma das 9 transacções ordenadas, ao incluí-lo no item 5 dos factos provados.
Pelo exposto, ao elenco dos factos provados, tem-se por aditada a matéria anteriormente descrita nos itens 7, 8, 10, 11, 12, 13, 14 dos factos não provados, a qual, paralelamente, aí deixará de figurar.
Em resumo, têm-se por provada também a seguinte factualidade, com a numeração sucessiva à do último dos factos que haviam sido dados por provados
26. Considerando o fuso horário GMT (+0:00), as transações a que alude a petição inicial foram registadas com os acessos do utilizador empresas BB, com o Código de Utilizador "NPCP...34", por débito da ...66 e foram efetuadas através do acesso ao site empresas do Banco 1....
27. Na data de 2021-04-20 às 9:54:31 Hrs foi efetuado um login ao site Empresas, num dispositivo Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/...28 Safari/537.36 Edg/... com Certificado Digital, com o Código de Utilizador, Password e 2 dígitos do NIF do Utilizador no IP ...33;
28. Às 09:57:37 Hrs foi registado um lote de PSM (Pagamentos de Serviços Multibanco), com nove (9) pagamentos no valor total de € 8.991,00, o que foi solicitado através do acesso à área de empresas acima melhor identificado;
29. Para confirmar esta operação foi emitido pelo Banco, às 09:56:57 Hrs, um Código de Autorização que foi enviado e recebido para o nr de telemóvel do Utilizador (...07), com o seguinte conteúdo: "M Banco 1...Emp – Envio Ficheiro – Cta Deb:...466EUR - Tipo:PSM -

N. reg:9 - Mont:8.991,00EUR – Data Proc:20/04/2021 - Codigo Autorizacao:*****81";
30. A operação (transferências em lote para Pagamentos de Serviços Multibanco) só foi efetuada depois de ter sido aposto no sítio reservado (área de empresas) do sítio de internet do Banco o referido código de autorização enviado para o telemóvel fornecido pela Autora, conforme por esta foi recebido;
31. Este ficheiro PSM continha 9 transações, mas uma delas não foi executada por a referência estar incorreta;
32. No mesmo acesso foram identificadas tentativas de registos de transações não concretizadas por não terem sido identificados os Códigos de Autorização (autenticação de transação), a saber:
- às 10:03:36 Hrs foi emitido pelo Banco, a pedido do utilizador, um Código de Autorização para o nr de telemóvel do Utilizador (...07), com o seguinte conteúdo: "M Banco 1...Emp - Envio Ficheiro - Cta Deb:...466EUR - Tipo:PSM - N. reg:9 - Mont:8.492,00EUR - Data Proc:20/04/2021 – Codigo Autorizacao:*****22";
- às 10:10:16 Hrs foi emitido pelo Banco, a pedido do utilizador, um Código de Autorização para o nr de telemóvel do Utilizador (...07), com o seguinte conteúdo: "M Banco 1...Emp - Envio Ficheiro - Cta Deb:...466EUR - Tipo:PSM - N. reg:8 - Mont:7.493,00EUR - Data Proc:20/04/2021 – Codigo Autorizacao:*****11";
- às 10:10:17 Hrs foi emitido pelo Banco, a pedido do utilizador, um Código de Autorização para o nr de telemóvel do Utilizador (...07), com o seguinte conteúdo: "M Banco 1...Emp - Envio Ficheiro - Cta Deb:...466EUR - Tipo:PSM - N. reg:8 - Mont:7.493,00EUR - Data Proc:20/04/2021 – Codigo Autorizacao:*****09".
*
Questão diferente é a relativa ao juízo de comprovação da matéria de cariz conclusivo, que o apelante pretende que se obtenha por inferência de toda a restante factualidade dada por provada, designadamente a descrita nos itens 9º e 15º a 18º dos factos não provados.
Pretende, assim, que se dê por adquirido:
· que as transacções foram ordenadas a partir do computador da autora, onde estava instalado o certificado digital NPCP...34;
· que elas só foram possíveis por ter sido usado tal computador, por ali ter sido aposto o código de utilizador da Autora, a password e duas posições do número fiscal do utilizador, o que deu azo à ter-se por verificada a identidade;
· que essas circunstâncias foram necessárias para ser solicitada a operação integrada pelo conjunto das nove transacções;
· que foi na sequência disso que o telemóvel indicado pela autora recebeu uma SMS para que fornecesse o código de autorização para uma operação de pagamento,
· que foi o utilizador autorizado pela autora ou alguém a quem foi facultado o acesso ao telemóvel usado para o efeito que digitou esse código na área de empresa do sítio de internet do Banco 1... no espaço previsto para a realização da operação;
· que foi com a aposição desse código, pela autora ou alguém a quem o facultou ou permitiu que conhecesse, que levou o banco a executar as transferências em causa.
Acontece, porém, que tais conclusões não são consequência necessária da restante factualidade provada, designadamente a relativa ao sistema e concatenação de operações descritos através dos quais se realizam as transacções referidas nestes autos, tanto mais que também se provou que alguém de forma não apurada, obteve o conhecimento dos elementos identificativos que facultavam o acesso ao serviço de homebanking relativo à conta bancária da autora junto do réu (facto 4º, dos provados) e que foi com o uso de tais elementos que logrou aceder efectivamente á conta e determinar as transacções em questão (facto 5º).
Foi, pois, com surpresa, por não ter sido um acto seu, que o gerente da autora detectou a subtracção de valores da conta bancária. Acresce que também se provou que não foi por acção da autora que alguém conheceu ou fez uso dos sucessivos elementos identificativos, nas condições que conduziram a que o banco executasse as operações em causa, que a autora não lhe ordenou. É o que resulta dos factos provados 6º, 8º, 9º a 11º e 15º.
Nestas concretas circunstâncias, a utilização de um dispositivo que apresentava o mesmo IP ...33, por alguém que conseguiu conhecer os códigos de acesso da autora à funcionalidade de homebanking associada à conta bancária mantida junto do banco réu, e que conseguiu mesmo ser o destinatário da SMS que transmitiu o código *****81, cuja aposição na aplicação informática em causa foi necessária para determinar ao banco a execução do conjunto de 8 transacções de 999,00€, não pode ter-se por proveniente de qualquer acção ou omissão da própria autora, da transmissão desses elementos a quem os tenha vindo a usar, ou sequer da facilitação de acesso aos mesmos.
Como se refere na sentença recorrida, é já facto notório o elevado número de situações congéneres, num fenómeno designado por *phishing,* e que aparece sob diversos

formatos (*blind phishing, clone phishing, smishing, vishing, spear phishing, whaling,* modalidades cuja caracterização facilmente se apura mediante qualquer pesquisa e que aqui seria despiciendo reproduzir), a par de outro, designado por p*harming,* mas todos eles redundando no acesso fraudulento, isto é, através de meios enganosos e sem o conhecimento ou autorização do respectivo titular, à aquisição dos elementos identificativos de um utilizador de um sistema ou aplicação informática, em ordem a permitir ao autor de tal conduta utilizar esse mesmo sistema ou aplicação, como aconteceu no caso em apreço.
A modalidade de *pharming* é mais complexa e difícil de detectar, pois consiste na própria intromissão no sistema do utilizador, para assim conhecer esses elementos ou operar o próprio acesso às aplicações, como se do verdadeiro utente se tratasse.
A própria jurisprudência evidencia a recorrência destas acções, como se pode ver quer das citações na sentença recorrida, quer nas alegações do próprio apelante, a que pode acrescentar-se a lista de 41 acórdãos do STJ e das Relações que se pronunciaram sobre a matéria, constante do Ac. de 28/4/2022, proc. nº 17903/19.1T8LSB.L1-8, em dgsi.pt.
Em qualquer caso, servem estas referências para sustentar a afirmação anterior, nos termos da qual o facto de as transacções terem sido determinadas por dispositivo que apresentou o mesmo IP anteriormente usado pela autora, que usou os seus códigos de identificação e ainda mediante o uso do código remetido por SMS não determina necessariamente a conclusão de que tenha sido por a autora ter permitido o acesso a esses meios, dolosamente ou por falta de cuidado, que as transacções foram possíveis.
Diferentemente, tendo-se adquirido a convicção de que nem a autora, nem ninguém com o seu consentimento ou a quem tenha sido facultado o acesso a esses sistema e meios de identificação ordenou a execução das transacções em causa, temos de admitir que não se logrou apurar quem e por que forma conseguiu levar o banco réu a executar tais transacções. De resto, isso nem sequer foi apurado em sede criminal, na sequência da denúncia feita pela autora.
Em qualquer caso, o legislador não deixou de prever essa situação. Nos termos do nº 3 do art. 113º citado supra, logo dispôs que "… a 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, uma ou mais obrigações previstas no artigo 110.º"
Em suma, optou legislador para impor ao prestador do serviço, *in casu*, ao banco, o ónus de "… apresentar elementos que demonstrem a existência de fraude, de dolo ou de negligência grosseira da parte do utilizador de serviços de pagamento." Fixou-o expressamente no nº 4 da norma citada, do DL n.º 91/2018, de 12 de Novembro.
Esta opção surge explicada no Ac. do TRL de 11.04.2019, no proc. 18/18.7T8TVD.L1-6, em dgis.pt: "*Deste normativo [o acórdão referia-se ao artº 70º do DL 242/2012, de 07/1, mas de sentido idêntico às regras citadas, do D.L. 91/2018] resulta que o legislador faz recair sobre o banco a prova de que as operações de pagamento não foram efectuadas por avarias técnicas ou quaisquer outras deficiências, não bastando, para o efeito, socorrer-se do registo da operação de molde a demonstrar que ela foi autorizada pelo ordenante, tendo ainda de demonstrar que o cliente agiu de forma fraudulenta, ou não cumpriu deliberadamente ou por negligência grave algumas das suas obrigações previstas no artº 67º do DL 242/2012.*
A opção pelo afastamento do ónus da prova a cargo do consumidor quanto ao mau funcionamento do sistema informático de homebanking, resulta da circunstância de ser o prestador de serviços de homebanking quem tem maior facilidade em demonstrar a versão factual que lhe aproveita, ou seja, a de que a utilização fraudulenta do serviço de homebanking por parte de terceiros não se deveu ao mau funcionamento do sistema informático.
No fundo, o legislador entendeu que 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. E é assim, porque o funcionamento do "sistema informático" homebanking "pertencente à sua esfera de risco", funcionando como critério suplementar de distribuição do ónus da prova, ou, melhor dizendo, ao "círculo de vida" em que o facto se produz: é a consagração da denominada teoria das esferas de risco, que preconiza uma ligação umbilical entre o ónus da prova e a dicotomia obrigações de meios/obrigações de resultado. (Cf. Hugo Luz dos Santos, "Plaidoyer por uma distribuição dinâmica do ónus de prova…", cit., pág. 21 e segs.)."
No caso, não foi feita, pelo ora apelante, prova que satisfaça uma tal exigência.
Tal como se referiu no Ac. do TRL citado supra (17903/19.1T8LSB.L1-8) "… cabe ao prestador do serviço de transferência, provar não só que a operação de pagamento foi autenticada, devidamente registada e contabilizada, mas também que a operação não foi afectada por avaria técnica ou qualquer outra deficiência. O facto de as ordens serem

provenientes de endereço de correio eletrónico autorizado e validado não é suficiente para provar que a operação de pagamento foi autorizada pelo ordenante, que este tenha agido de forma fraudulenta, ou que não cumpriu as obrigações a que estava obrigado. Não tendo resultado provado, pelo Banco, que existiu atuação fraudulenta pelos utilizadores e aqui autores, ou que estes não cumpriram as obrigações que lhes cabiam, deliberadamente ou com negligência grave, inexiste razão para presumir que a operação, ainda que validada, tenha sido autorizada."
Resta, em suma, afirmar que, da demonstração de toda a factualidade apurada, incluindo aquela que agora foi aditada ao rol dos factos provados, não se pode inferir, sem mais, a demonstração das conclusões fácticas que se encontram enunciadas nos itens 9º e 15º a 18º dos factos não provados. Conclusões estas que também se não mostram fundadas na alegação e prova directa do seu conteúdo, ou de qualquer outra factualidade de onde este pudesse inferir-se
Em conclusão, permanecerão como não provados os factos em questão.

*

A pretensão do recorrente fundava-se na alteração da factualidade que integra a premissa menor da decisão a proferir.
Sustenta que *"… a Autora – deliberada ou inconscientemente – disponibilizou a terceiros:*
1) O acesso, físico ou remoto, ao seu computador onde estava instalado o certificado digital, ou os dados recebidos e enviados pelo mesmo;
2) O acesso, físico ou remoto, ao seu telemóvel, ou os dados recebidos no mesmo.
Em concreto disponibilizou a terceiros o código secreto recebido pela mensagem SMS constante do documento 11 da petição inicial (cfr. art. 24º da contestação) que, após ser aposto no sistema informático do Banco, permitiu realizar a operação em causa. " (pg. 21 das alegações).
Porém, rejeitou-se acima a possibilidade de se admitir uma tal factualidade.
Por consequência, não é possível eximir o banco à responsabilidade de reembolsar a autora pelos valores transferidos, tal como decidido na sentença recorrida. É o que resulta do disposto no nº 1 do art. 114º do D.L. 91/2018.
Acresce que, da factualidade apurada, nem sequer é possível concluir pela formulação de qualquer juízo de censura sobre qualquer conduta da autora, por acção ou por omissão, que permita, sequer a título de negligência, afastar ou mitigar a imputação ao réu da responsabilidade por um tal reembolso.
Inexiste, em suma, qualquer fundamento para que se possa concluir, como chega a ser pedido pelo apelante, que a sua responsabilidade seja reconhecida apenas numa proporção de 20%.
A total carência de factualidade que permita explorar uma tal hipótese torna inútil qualquer desenvolvimento sobre a questão.
Por todo o exposto, na confirmação da decisão recorrida, cabe negar provimento ao presente recurso de apelação.

*

Sumário:
…….
…….
…….

3 - DECISÃO

Pelo exposto, acordam os juízes que constituem este Tribunal em negar provimento ao presente recurso, com o que confirmam integralmente a decisão recorrida,

Custas pelo apelante.

Registe e notifique.

*

Porto, 14 de Janeiro de 2025
Rui Moreira
Anabela Dias da Silva
Pinto dos Santos