Ted Fernandes: Fraudes e dever de segurança dos bancos

Inúmeros são os casos em que hackers acessam os computadores ou telefones celulares de consumidores e, a partir destes dispositivos, efetuam transferências ou Pix para outras contas, causando elevados prejuízos aos correntistas. Casos também existem em que os consumidores são vítimas de engenharia social: são convencidos a fazer transferências, pelos golpistas, por vários meios (a forma clássica é o golpista que se passa por alguém da família, que em tese está numa situação de risco e precisaria de dinheiro urgente), para contas de outros golpistas e/ou intermediários e cúmplices desses golpistas.

Para os dois cenários, as instituições bancárias dispõem de dois mecanismos básicos de segurança para

r e o mecanismo especial de devolução.

O bloqueio cautelar ocorre quando a própria instituição que detém a conta do recebedor suspeita da situação de fraude. Essa medida permite que, no ato do crédito na conta, a instituição efetue um bloqueio preventivo dos recursos por até 72 horas. A opção possibilita que a instituição faça uma análise de fraude mais robusta, aumentando a probabilidade de recuperação dos recursos pelos usuários pagadores vítimas de algum crime [1].

O mecanismo especial de devolução é utilizado nos casos de fundada suspeita de fraude, sejam elas identificadas pelas próprias instituições envolvidas ou quando um usuário faz um Pix, mas logo em seguida se dá conta de que foi vítima de um golpe. Nesse tipo de situação, é preciso registrar um boletim de ocorrência e avisar imediatamente a instituição pelo canal de atendimento oficial, como SAC ou Ouvidoria. No ambiente Pix nos aplicativos dos bancos, há um link direto para o canal a ser utilizado para registrar a reclamação [2].

E se a instituição bancária não cumpre o seu dever de segurança, adotando o bloqueio cautelar ou o mecanismo especial de devolução, viola a norma que se pode extrair do texto do artigo 14 do CDC, além da Súmula 479 do STJ, que prevê que *"as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias"*.

O banco, para não indenizar o consumidor nesses casos, deve provar que as transações bancárias foram regulares; que cumpriu com o seu dever de segurança e bloqueou as movimentações suspeitas. Não o fazendo, deve arcar com o prejuízo, mesmo que as transações tenham sido concluídas com senha e *itoken* , tendo em vista que, por certo, os criminosos invadiram se apoderaram do computador e/ou celular do consumidor, o que viabilizaria tecnicamente as transações. Esta é a interpretação que vem sendo adotada pelo Tribunal de Justiça de São Paulo, em voto da relatoria do Desembargador Vicentini Barroso:

"(…)
Houve, evidentemente, abrupta alteração de perfil da consumidora, com o que os sistemas de segurança da instituição financeira deveriam ter detectado tais movimentações atípicas, com bloqueio correlato e contato com ela para o devido esclarecimento, evitando o ocorrido. Nem se alegue da falta de previsão contratual sobre essa tomada de atitude ou que ainda não havia regulamentação própria do Banco Central a respeito em termos de segurança das operações bancárias, era o mínimo que se haveria de esperar do Banco e nada ocorreu. Inegável, pois, a falha na prestação de serviço, não se verificando, no caso, nenhuma das excludentes do §3º do artigo 14 da Lei 8.078/90. Ainda que tenha havido ação de terceiro, a norma em análise exige culpa exclusiva deste para afastar a responsabilidade da ré, do que não se verificou, não havendo, igualmente, elementos a apontar a culpa concorrente da autora pelos fatos. Os serviços em questão não foram prestados, assim, com a segurança que razoavelmente eram de se esperar pela consumidora, o que caracteriza o defeito na prestação de serviços, na forma do citado artigo 14, §1º. O argumento quanto ao uso de senha pessoal e do itoken para as transações não afasta a responsabilidade dos Bancos. Nem eventual demora na comunicação do ocorrido é suficiente para tanto. É que a falha na prestação de serviços, no presente caso, está no fato de não ter sido feito o bloqueio assim que verificada, na forma acima referida, a atipicidade das operações."
(TJ-SP, 15ª Câmara de Direito Privado, relator Vicentini Barroso, Apelação Cível nº 1015727-50.2022.8.26.0506, julgado em 10 de outubro de 2023).

Especificamente sobre a necessidade de utilização do mecanismo especial de devolução e o dever de segurança da instituição bancária, assim decidiu a 2ª Turma Recursal, do TJ-DF (Tribunal de Justiça do Distrito Federal), em voto relatado pela Magistrada Silvana da Silva Chaves:

"No presente caso, embora o recorrente alegue que a fraude em si foi praticada por terceiros, não é possível caracterizar o ocorrido como fortuito externo a fim de elidir o nexo causal que configura a responsabilidade civil da instituição financeira, conquanto a fraude observada insere-se na categoria de fortuito interno e compõe o risco da atividade bancária. Os documentos juntados com a inicial demonstram o recebimento de ligação do número da central de atendimento do banco, em horário correspondente ao qual foi realizada a transferência (ID 49120272), sendo evidente o fortuito interno e a higidez do nexo causal. 9. A operação bancária objeto da fraude foi realizada de forma única e em valor alto (R$ 4.100,00). Embora a recorrente alegue que tal movimentação não é estranha ao perfil da recorrida, não juntou nenhuma prova a este respeito, ônus que lhe cabia. Diante da movimentação atípica, a instituição financeira recorrente deveria ter tomado todos os cuidados necessários para inviabilizá-la, o que não ocorreu (ID 49120270), pois não tomou as providências previstas nos artigos 39 – B e 41 – B, ambos da Resolução BCB nº 1, de 12 de agosto de 2020 (alterada pela Resolução BCB nº 147, de 28 de setembro de 2021) que permite o bloqueio cautelar das quantias transferidas via PIX, pelo prazo de 72 horas, quando houver suspeita de fraude e o estorno do valores por meio do Mecanismo Especial de Devolução. 10. Recurso conhecido e não provido. Sentença mantida. 11. Condenado o recorrente vencido ao pagamento de custas e de honorários advocatícios, fixados em 10% sobre o valor da condenação, nos termos do art. 55 da Lei 9.099/95. 12. A súmula de julgamento servirá de acórdão, nos termos do artigo 46 da Lei 9.099/95".
(TJDF, 2ª Turma Recursal, relatora: Silvana da Silva Chaves, 07093037420238070016 – (0709303-74.2023.8.07.0016 – Res. 65 CNJ), publicado no DJE : 24/08/2023).

Em acórdão relatado pela ministra Nancy Andrighi, o STJ (Superior Tribunal de Justiça) decidiu que cabe à instituição bancária zelar pela não realização de transações bancárias atípicas, destoantes do perfil do consumidor, evitando fraudes perpetradas por terceiros. Não o fazendo, descumpre o seu dever de segurança e verificada está a falha na prestação do serviço, caracterizando-se o dever de indenizar. Vejamos:

"CONSUMIDOR. PROCESSUAL CIVIL. RECURSO ESPECIAL. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITOS. DEVER DE SEGURANÇA. FRAUDE PERPETRADA POR TERCEIRO. CONTRATAÇÃO DE MÚTUO. MOVIMENTAÇÕES ATÍPICAS E ALHEIAS AO PADRÃO DE CONSUMO. RESPONSABILIDADE OBJETIVA DA INSTITUIÇÃO FINANCEIRA. RECURSO CONHECIDO E PROVIDO.
1. Ação declaratória de inexistência de débitos, ajuizada em 14/8/2020, da qual foi extraído o presente recurso especial, interposto em 21/6/2022 e concluso ao gabinete em 17/2/2023.
2. O propósito recursal consiste em decidir (I) se a instituição financeira responde objetivamente por falha na prestação de serviços bancários, consistente na contratação de empréstimo realizada por estelionatário; e (II) se possui o dever de identificar e impedir movimentações financeiras que destoam do perfil do consumidor.
3. O dever de segurança é noção que abrange tanto a integridade psicofísica do consumidor, quanto sua integridade patrimonial, sendo dever da instituição financeira verificar a regularidade e a idoneidade das transações realizadas pelos consumidores, desenvolvendo mecanismos capazes de dificultar fraudes perpetradas por terceiros, independentemente de qualquer ato dos consumidores.

4. A instituição financeira, ao possibilitar a contratação de serviços de maneira facilitada, por intermédio de redes sociais e aplicativos, tem o dever de desenvolver mecanismos de segurança que identifiquem e obstem movimentações que destoam do perfil do consumidor, notadamente em relação a valores, frequência e objeto.
5. Como consequência, a ausência de procedimentos de verificação e aprovação para transações atípicas e que aparentam ilegalidade corresponde a defeito na prestação de serviço, capaz de gerar a responsabilidade objetiva por parte da instituição financeira.
6. Entendimento em conformidade com Tema Repetitivo 466/STJ e Súmula 479/STJ: "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias.
7. Idêntica lógica se aplica à hipótese em que o falsário, passando-se por funcionário da instituição financeira e após ter instruído o consumidor a aumentar o limite de suas transações, contrata mútuo com o banco e, na mesma data, vale-se do alto montante contratado e dos demais valores em conta corrente para quitar obrigações relacionadas, majoritariamente, a débitos fiscais de ente federativo diverso daquele em que domiciliado o consumidor.
8. Na hipótese, inclusive, verifica-se que o consumidor é pessoa idosa (75 anos – imigrante digital), razão pela qual a imputação de responsabilidade há de ser feita sob as luzes do Estatuto do Idoso e da Convenção Interamericana sobre a Proteção dos Direitos Humanos dos Idosos, considerando a sua peculiar situação de consumidor hipervulnerável.
9. Recurso especial conhecido e provido para declarar a inexigibilidade das transações bancárias não reconhecidas pelos consumidores e condenar o recorrido a restituir o montante previamente existente em conta bancária, devidamente atualizado".
(STJ, REsp 2052228 / DF, relatora ministra NANCY ANDRIGHI, DJe 15/09/2023).

Constata-se que a interpretação dos tribunais estaduais e do STJ, relativa às normas extraídas do texto do Código de Defesa do Consumidor, sobre fraudes bancárias, exige dos bancos que: a) verifiquem a idoneidade das transações bancárias realizadas nas contas dos consumidores, zelando para que elas não sejam concretizadas, se forem suspeitas; b) avaliem se essas transações estão de acordo com o perfil desses consumidores; c) cumpram com o seu dever de segurança, efetivando o bloqueio cautelar para transações suspeitas e/ou disponibilizando o mecanismo especial de devolução. Sempre que não adotarem essas cautelas, os bancos falham ao prestarem os serviços e devem indenizar os consumidores em decorrência de eventuais fraudes perpetradas, seja materialmente e/ou moralmente.

[1] https://www.bcb.gov.br/detalhenoticia/591/noticia

[2]

Op. Cit. *"O banco da vítima, por sua vez, vai usar a infraestrutura do Pix para notificar a instituição que está recebendo a transferência, para que os recursos sejam bloqueados. Após o bloqueio, tanto a instituição do pagador quanto a do possível golpista/fraudador têm até sete dias para fazer uma análise mais robusta do caso para ter certeza de que se trata efetivamente de uma fraude. Caso a fraude se comprove, a instituição de destino da operação devolve os recursos para a do pagador, que deve efetuar o devido crédito na conta do cliente. O MED também poderá ser acionado caso haja um crédito indevido por falha operacional nos sistemas da instituição envolvida. Cabe ressaltar, contudo, que o mecanismo não se aplica nos seguintes casos: usuário fez um Pix por engano, por exemplo, digitando a chave errada; controvérsias comerciais entre usuários; transações com fundada suspeita de fraude em que os recursos forem destinados à conta transacional de um terceiro de boa-fé. Ou seja, o MED não é um mecanismo de chargeback (reversão de pagamento), como o existente nos arranjos de cartões de pagamento.*

Sempre que um recurso for bloqueado ou devolvido, o usuário recebedor será notificado e, caso não se trate de fraude, poderá fazer contato com a instituição para esclarecer o caso".

Meta Fields