

Caiu em golpe?

SAIBA QUE PROVA DE FALHA BANCÁRIA É FUNDAMENTAL PARA O RESSARCIMENTO

Mesmo com prejuízo bilionário em fraudes via Pix, tribunais têm isentado bancos em casos sem falha comprovada; advogado alerta para os cuidados e explica o que ainda gera direito à indenização

Com o aumento expressivo das fraudes digitais, que geraram um prejuízo de R\$ 4,9 bilhões em 2024 apenas com golpes via Pix, segundo o Banco Central, o Judiciário tem adotado uma postura mais restritiva em relação à responsabilidade dos bancos. Embora a expectativa do consumidor seja de proteção total, decisões recentes demonstram que, sem comprovação de falha na prestação do serviço, as instituições financeiras podem ser isentas de reembolsar as vítimas.

“Há jurisprudência consolidada em diversos tribunais indicando que os bancos não têm o dever de ressarcir o consumidor quando não há falha na prestação do serviço bancário. Isso ocorre, por exemplo, em golpes nos quais o consumidor age por conta própria ao transferir valores via Pix após ser enganado por meio de contatos telefônicos, mensagens falsas, ou propostas enganosas. Em situações em que o banco não poderia prever ou impedir a operação”, afirma o advogado Stefano Ribeiro Ferri, especialista em Direito do Consumidor.

Ferri cita uma decisão recente obtida por seu escritório no Tribunal de Justiça de São Paulo, na qual a corte reforçou o entendimento da culpa exclusiva da vítima e isentou a instituição financeira. “A Justiça, no entanto, negou o pedido, afirmando que as instituições bancárias não têm a obrigação de tutelar seus clientes em toda e qualquer operação, ainda mais quando realizada pelo próprio titular da conta”, explica.

CDC

Apesar das críticas, essas decisões não ferem o Código de Defesa do Consumidor (CDC), de acordo com o especialista. “Essas decisões não necessariamente contrariam o CDC, mas representam uma interpretação mais restritiva da responsabilidade objetiva prevista no artigo 14. O entendimento majoritário é que a responsabilidade do banco exige falha na segurança ou inadequação do serviço prestado”, informa Ferri.

Na prática, isso significa

que o consumidor deve redobrar os cuidados, pois o ônus da prova tem recaído sobre ele. “Ele deve demonstrar que houve negligência, omissão, falta de segurança ou ausência de mecanismos de controle por parte da instituição financeira. Isso pode incluir, por exemplo, a não detecção de comportamento atípico na conta, falhas de autenticação ou ausência de confirmação em transações de alto valor”.

Essa movimentação dos tribunais, segundo o advogado, busca preservar a estabilidade do sistema financeiro, diante do crescimento alarmante de fraudes. “Essas decisões representam uma tendência de delimitação da responsabilidade dos bancos diante do avanço dos golpes digitais. Em parte, isso visa evitar um efeito sistêmico no setor financeiro, onde as instituições poderiam ser responsabilizadas por atos que ocorrem fora do seu alcance de controle”, diz Ferri.

Contudo, ele alerta que o excesso de proteção aos bancos pode gerar um efeito colateral perigoso. “Esse entendimento pode enfraquecer a confiança do consumidor, que já se vê vulnerável diante de golpes sofisticados. Ao mesmo tempo, o Judiciário busca equilibrar a autonomia do cliente nas operações bancárias digitais com o dever de segurança dos bancos”.

QUANDO O BANCO DEVE INDENIZAR

Há, porém, situações em que o Judiciário reconhece o dever de indenização. Isso ocorre, por exemplo, quando há clonagem de cartão, vazamento de dados, falhas de autenticação, ou ausência de bloqueios preventivos.

“Quando o banco deixa de alertar ou de bloquear operações atípicas e incompatíveis com o histórico do cliente; o golpe envolve fraude sistêmica ou uso indevido da estrutura do banco, como invasão de conta, simulação de páginas do próprio banco ou falha no sistema de autenticação; o consumidor é vulnerável notório (idosos, pessoas com deficiência, analfabetos digitais) e o banco se omite diante disso”, finaliza Ferri.



DICAS PARA NÃO CAIR EM ARMADILHAS DIGITAIS

DESCONFIE DE OFERTAS MUITO VANTAJOSAS OU QUE EXIGEM PAGAMENTOS ANTECIPADOS PARA VAGAS DE EMPREGO

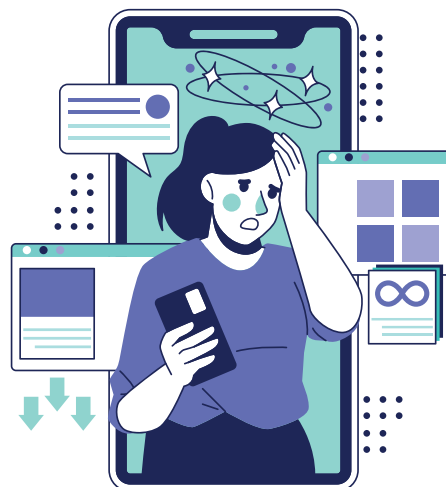
Ofertas de emprego com salários muito acima da média, pouca exigência de qualificação ou que prometem ganhos rápidos e fáceis devem ser vistas com cautela. Golpistas costumam atrair vítimas com essas promessas e, após gerar expectativa, pedem pagamentos antecipados para custos com uniformes, exames médicos ou treinamentos fictícios. Nenhuma empresa séria exige dinheiro do candidato durante o processo seletivo. Sempre pesquise sobre a empresa e verifique sua reputação em sites oficiais.

NUNCA CLIQUE EM LINKS ENVIADOS POR DESCONHECIDOS OU FORA DE CANAIS OFICIAIS

Links recebidos por mensagens de texto, e-mail ou redes sociais podem conter vírus ou direcionar a páginas falsas que imitam sites de bancos, empresas ou instituições públicas. Esses links são usados para roubar dados pessoais e bancários. Sempre verifique a autenticidade da mensagem e acesse sites digitando o endereço diretamente no navegador ou usando aplicativos oficiais.

CONFIRME LIGAÇÕES E MENSAGENS COM A FONTE ORIGINAL (EX: LIGAR PARA O BANCO POR OUTRO NÚMERO)

Criminosos frequentemente se passam por representantes de bancos, operadoras ou órgãos públicos para aplicar golpes. Se receber uma ligação ou mensagem suspeita, desligue e entre em contato com a instituição por canais verificados, como o número que consta no site oficial ou no verso do cartão do banco. Isso garante que você estará falando com um representante legítimo e evita cair em fraudes de engenharia social.



EVITE REPASSAR DADOS PESSOAIS POR TELEFONE OU MENSAGEM, MESMO QUE A PESSOA PAREÇA CONFIÁVEL

Golpistas costumam se passar por familiares, amigos ou funcionários de empresas conhecidas para obter dados sensíveis, como CPF, número do cartão ou senhas. Mesmo que a abordagem pareça legítima, nunca forneça informações pessoais sem confirmar a identidade da pessoa. Se estiver em dúvida, entre em contato por outro meio para verificar a veracidade da solicitação.



ATIVE A AUTENTICAÇÃO EM DOIS FATORES NOS APLICATIVOS BANCÁRIOS

A autenticação em dois fatores adiciona uma camada extra de segurança ao exigir uma segunda verificação (como um código enviado por SMS ou um aplicativo autenticador) além da senha habitual. Mesmo que a senha seja descoberta, esse recurso impede o acesso não autorizado às suas contas, protegendo seu dinheiro e suas informações pessoais.

LIMITE VALORES PARA TRANSAÇÕES VIA PIX, ESPECIALMENTE NO PERÍODO NOTURNO

Reduzir os limites de transferência por Pix, especialmente à noite, é uma forma eficaz de prevenir prejuízos em caso de roubo ou fraude. A maioria dos bancos permite configurar esses limites de forma personalizada. Essa medida pode dificultar que criminosos façam grandes movimentações sem o seu consentimento imediato.

CADASTRE CHAVES PIX APENAS DIRETAMENTE NO APP DO BANCO E JAMAIS POR TERCEIROS

O cadastro de chaves Pix deve ser feito exclusivamente no aplicativo ou site oficial do seu banco. Nunca aceite ajuda de terceiros ou clique em links para realizar esse procedimento. Golpistas utilizam táticas para capturar seus dados e vincular sua chave Pix a contas falsas, dificultando o rastreamento e a recuperação de valores em caso de golpe.