

ENTREVISTA — LEO ROSENBAUM, advogado especialista em direito do consumidor

Golpes digitais: quando bancos devem ressarcir vítimas?

Ana Maria Campos

O estelionato já é o principal crime patrimonial do Brasil, com mais de 2,2 milhões de registros em 2025 e média de 258 golpes por hora. Dados do Anuário de Segurança Pública mostram um salto de 429,8% desde 2018, impulsionado pela migração da criminalidade para o ambiente digital. Assim, essas fraudes tornaram-se um dos principais desafios para os consumidores brasileiros. O avanço dessas

fraudes virtuais expõe não apenas a sofisticação dos criminosos, mas também as dificuldades das vítimas para recuperar o dinheiro perdido e responsabilizar os envolvidos. Nesta entrevista, o advogado especialista em direito do consumidor Leo Rosenbaum explica quais são os direitos de quem sofre um golpe, o papel dos bancos e das plataformas digitais e quais medidas devem ser tomadas imediatamente após a fraude. O especialista também analisa como a Justiça tem decidido esses casos e aponta caminhos para fortalecer a proteção dos consumidores.

Divulgação



Quais são os principais direitos da vítima de estelionato virtual e quais medidas ela deve tomar imediatamente após perceber que foi enganada?

A vítima tem direito à proteção do seu patrimônio e à reparação dos danos quando houver falha na prestação do serviço, conforme os arts. 6º, VI, e 14 do Código de Defesa do Consumidor. Na prática, o tempo é o fator mais importante. Ao perceber o golpe, ela deve comunicar imediatamente o banco (pelo app ou pela central oficial, nunca por número recebido do golpista), pedir o bloqueio da operação e, no caso do Pix, o acionamento do Mecanismo Especial de Devolução (MED), criado pelo Banco Central pela Resolução BCB 103/2021. Em seguida: registrar boletim de ocorrência (pode ser feito on-line), comunicar as plataformas envolvidas e preservar todas as provas. Quanto mais rápida e documentada a reação, maiores as chances de recuperar o valor e, se for preciso, de demonstrar em juízo que o banco foi avisado a tempo.

Em casos de transferências via Pix ou outros meios eletrônicos, em quais situações a vítima pode tentar recuperar o dinheiro? Qual a responsabilidade dos bancos e instituições financeiras?

No Pix, a vítima pode solicitar o MED quando houver fraude, golpe ou crime, possibilitando o bloqueio cautelar e a devolução dos valores que ainda estiverem na conta de destino. O limite prático é esse: o mecanismo só alcança o dinheiro que não foi pulverizado. Quando o MED não resolve, entra a responsabilidade da instituição. Os bancos respondem objetivamente, nos termos do art. 14 do CDC e da Súmula 479 do STJ, quando houver falha de segurança ou ausência de mecanismos adequados para identificar operações suspeitas. Nosso Observatório mostra o peso disso na prática: quando a transação não foi

feita nem autorizada pelo cliente (conta invadida, cartão clonado, saque não reconhecido), 93,3% das decisões do TJSP determinam o ressarcimento total ou parcial. Quando a vítima foi induzida a transferir ela mesma o dinheiro (golpe do Pix, falsa central), o índice cai para 57,3%. A responsabilidade, portanto, depende das circunstâncias concretas — e especialmente de quem executou a operação.

A vítima pode ser responsabilizada por ter fornecido dados, senhas ou códigos ao golpista?

O fornecimento de dados ou senhas não elimina automaticamente a responsabilidade da instituição financeira. É necessário verificar como o golpe ocorreu e se houve falha de segurança do fornecedor. A culpa exclusiva do consumidor pode afastar a responsabilidade, conforme o art. 14, § 3º, II, do CDC — e essa é, de longe, a defesa mais usada pelos bancos nesses casos. Mas a Justiça também reconhece situações em que a vítima foi enganada por técnicas sofisticadas de engenharia social e o banco deixou de adotar medidas de segurança adequadas: transferências fora do padrão do cliente, vários Pix em sequência, valores altos de madrugada, empréstimo contratado e sacado em minutos. Nesses casos, o tribunal costuma entender que o golpe só se consumou porque o sistema de monitoramento falhou — e o banco responde.

Como a Justiça costuma avaliar esse tipo de situação?

A análise é feita caso a caso. Os tribunais consideram o comportamento da vítima, o método utilizado pelo fraudador, o perfil das transações, a existência de movimentações atípicas, a rapidez da comunicação ao banco e as providências adotadas pela instituição. O STJ entende que bancos devem possuir mecanismos capazes de detectar operações incompatíveis com o perfil do cliente. Nos dados do TJSP, a lógica aparece

tipo a tipo: conta ou aplicativo invadidos (94,8% de ressarcimento), saque ou compra não reconhecida (90,5%), cartão clonado (90%), falso funcionário ou motoboy (83,7%), empréstimo fraudulento (79,1%) e falsa central de segurança (74,1%). Os golpes em que a própria vítima transfere são os mais disputados: clonagem de WhatsApp (52,3%), boleto falso (50,3%) e Pix induzido (50,2%). Quando há condenação por dano moral, o valor mediano em São Paulo fica em R\$ 5 mil, geralmente somado à devolução integral do que foi desviado.

Quais provas a vítima deve preservar para aumentar as chances de identificar os responsáveis e recuperar os prejuízos?

É fundamental preservar conversas, e-mails, prints, gravações, números de telefone, perfis utilizados pelos golpistas, links, anúncios, comprovantes de Pix ou transferências, chaves Pix, dados das contas destinatárias e documentos enviados pelos criminosos. Também devem ser guardados os protocolos de atendimento, o horário exato de cada contato com o banco e todas as comunicações feitas com bancos e plataformas. Esse registro cumpre duas funções: demonstra a fraude e prova a rapidez da reação da vítima — que é um dos critérios que os tribunais mais levam em conta. Um detalhe que faz diferença: pedir ao banco o extrato com horário e canal de cada operação e a gravação ou protocolo da ligação em que o golpe foi comunicado.

Em que situações plataformas digitais, bancos, operadoras de telefonia e empresas de tecnologia são responsabilizadas por esses golpes?

A responsabilidade depende da existência de falha atribuível ao fornecedor. Bancos podem responder por falhas de segurança, falta de monitoramento de transações suspeitas ou demora em agir após a comunicação da fraude.

A responsabilidade também pode atingir o banco que recebeu o dinheiro, quando a conta foi aberta com documentos falsos ou usada de forma evidentemente irregular. Operadoras de telefonia podem responder por trocas de chip (SIM swap) sem a devida conferência da identidade do titular. Já plataformas e empresas de tecnologia podem ser responsabilizadas por falhas em suas próprias obrigações de segurança ou quando integram a cadeia do serviço e contribuem para o dano, como um marketplace que intermedia o pagamento. Não há, porém, responsabilidade automática pelo simples fato de a fraude ocorrer em determinado ambiente.

A legislação brasileira está preparada para enfrentar a evolução dos golpes digitais, ou são necessárias novos mecanismos?

O Brasil possui instrumentos importantes para combater golpes digitais, como o Código de Defesa do Consumidor, a LGPD, o Marco Civil da Internet, a Lei 14.155/2021, que agravou as penas do estelionato eletrônico, e a regulamentação do Banco Central, com limites noturnos do Pix, MED e exigências de monitoramento de fraudes. O problema, porém, não é a falta de leis, mas a velocidade: os golpes evoluem em semanas, enquanto a resposta institucional leva anos. Três avanços fariam diferença: ampliar o MED para rastrear e bloquear o dinheiro ao longo da cadeia de contas; padronizar o dever de monitoramento das instituições, com critérios objetivos para operações atípicas; e integrar bancos, operadoras e plataformas na troca de informações sobre contas e números usados em golpes. Enquanto isso, a proteção das vítimas depende principalmente da rapidez na reação e da análise de cada caso pelo Judiciário.

Quais medidas o poder público deveria adotar para aumentar a proteção do consumidor?

O poder público deve priorizar a integração entre Banco Central, autoridades policiais, Ministério Público, órgãos de defesa do consumidor, instituições financeiras e plataformas digitais para permitir respostas rápidas aos golpes. Hoje, cada elo reage isoladamente, enquanto o dinheiro é pulverizado em minutos. Três frentes são urgentes: aprimorar os mecanismos de bloqueio e recuperação de valores, ampliando o MED para rastrear o dinheiro ao longo da cadeia de contas; fortalecer a identificação e o fechamento das chamadas “contas laranja” e a investigação dos crimes digitais; e estabelecer critérios mais claros e rigorosos de monitoramento e resposta dos fornecedores aos avisos dos clientes. A necessidade de regras claras fica evidente na divisão da Justiça. O Observatório, que analisou 19.504 decisões do TJSP entre junho de 2025 e agosto de 2026, mostra que, quando a operação não foi feita nem autorizada pelo cliente, 9 em cada 10 decisões determinam o ressarcimento. Quando a vítima é induzida a transferir o dinheiro, o índice cai para 57%, e o caso passa a depender da comprovação de falha do banco. Para o consumidor, a prevenção deve ser acompanhada de mecanismos simples e ágeis de contestação e reparação, evitando que todo o prejuízo recaia sobre a vítima.