

Fraudes digitais e responsabilidade das instituições financeiras: dever de segurança, engenharia social e transações via Pix

Digital fraud and the liability of financial institutions: duty of security, social engineering and Pix transactions

Igor de Abreu Januário

João Guilherme Echeverria Peralta

Vitor Hugo Esteves

RESUMO

O artigo investiga a responsabilidade civil das instituições financeiras e de pagamento por fraudes digitais no Brasil, com ênfase em engenharia social, falsa central de atendimento, acesso remoto indevido, contas-laranja e transferências via Pix. O problema consiste em definir quando a autenticação formal da operação afasta o defeito do serviço e quando a fraude permanece integrada ao risco do empreendimento. A pesquisa adota abordagem qualitativa, exploratória e dedutiva, apoiada em fontes normativas, regulatórias, jurisprudenciais e documentais disponíveis até 2 de setembro de 2026. O estudo articula o art. 14 do Código de Defesa do Consumidor, as Súmulas 297 e 479 e o Tema Repetitivo 466 do Superior Tribunal de Justiça, a Lei nº 12.865/2013, a Lei Geral de Proteção de Dados Pessoais e a regulação do Banco Central sobre segurança do Pix, bloqueio cautelar e Mecanismo Especial de Devolução. São contrastados precedentes que reconhecem a responsabilidade diante de operações incompatíveis com o perfil do cliente e decisão que a afasta quando não demonstrados defeito e nexo causal. Sustenta-se que a responsabilidade objetiva não equivale a seguro integral, mas impõe às instituições o ônus de comprovar governança de risco efetiva, monitoramento comportamental, diligência na abertura e supervisão de contas recebedoras, resposta tempestiva e rastreabilidade. A contribuição original consiste em propor uma matriz probatória de seis eixos para avaliação do defeito, do nexo causal e das excludentes.

Palavras-chave: Fraudes digitais. Responsabilidade civil. Instituições financeiras. Engenharia social. Pix.

ABSTRACT

This article examines the civil liability of financial institutions and payment institutions for digital fraud in Brazil, focusing on social engineering, fake call centers, unauthorized remote access, mule accounts and Pix transfers. The central issue is when formal transaction authentication excludes defective service and when fraud remains within the enterprise risk. The research follows a qualitative, exploratory and deductive approach based on statutory, regulatory, case-law and documentary sources available through September 2, 2026. It connects Article 14 of the Consumer Protection Code, Precedents 297 and 479 and Repetitive Theme 466 of the Superior Court of Justice, Law No. 12,865/2013, the Brazilian General Data Protection Law and Central Bank rules governing Pix security, precautionary blocking and the Special Refund Mechanism. Contrasting decisions are examined: those imposing liability where transactions departed from the customer's profile and a decision excluding liability where defect and causation were not established. The article argues that strict liability is not comprehensive insurance, but requires institutions to prove effective risk governance, behavioral monitoring, diligence in opening and supervising receiving accounts, timely incident response and traceability. Its original contribution is a six-axis evidentiary framework for assessing service defect, causation and defenses.

Keywords: Digital fraud. Civil liability. Financial institutions. Social engineering. Pix.

1 INTRODUÇÃO

A digitalização dos serviços financeiros alterou a infraestrutura econômica brasileira. Aplicativos bancários, instituições de pagamento e o Pix reduziram custos, ampliaram a disponibilidade temporal dos serviços e tornaram instantâneas operações antes sujeitas a etapas presenciais. Essa transformação produziu ganhos de inclusão e eficiência, mas também ampliou a superfície de ataque. A fraude contemporânea não depende apenas de violação técnica do sistema: combina dados pessoais, manipulação psicológica, falsificação de identidade, controle remoto de dispositivos, abertura de contas instrumentais e dispersão imediata dos recursos.

A engenharia social explora confiança, urgência e assimetria informacional. O fraudador pode conhecer nome, banco, parte do número do cartão, transações recentes ou outras informações capazes de tornar crível a abordagem. Em seguida, induz a vítima a fornecer credenciais, instalar programa, aumentar limites, contratar crédito ou transferir

valores para uma suposta conta segura. Embora a vítima participe materialmente da operação, a aparência de regularidade não resolve a questão jurídica. É necessário verificar se a instituição detectou sinais incompatíveis com o perfil transacional, se o destinatário apresentava marcações de fraude, se houve mudança de dispositivo e se a resposta posterior foi tempestiva.

O problema adquiriu especial relevância com a instantaneidade do Pix. Uma transferência legítima e uma transferência induzida por fraude podem percorrer a mesma infraestrutura e utilizar credenciais válidas. A diferença emerge do contexto: valor, horário, sequência, dispositivo, geolocalização, contratação prévia de empréstimo, destinatário inédito e comportamento da conta recebedora. A segurança, portanto, não se esgota na autenticação; envolve prevenção, detecção, contenção, rastreio, recuperação e produção de evidência auditável.

A pergunta central é: em que medida instituições financeiras e de pagamento devem responder pelos prejuízos sofridos em fraudes digitais, inclusive quando o consumidor fornece dados ou confirma operações sob influência de engenharia social? A hipótese é que a autenticação formal não elimina o defeito quando a cadeia operacional contém anomalias objetivamente detectáveis por controles proporcionais ao risco. Em sentido inverso, a responsabilidade pode ser afastada quando a instituição demonstra funcionamento adequado do serviço e culpa exclusiva do consumidor ou de terceiro, sem falha concorrente de segurança, monitoramento ou resposta.

O objetivo geral é sistematizar critérios jurídicos, regulatórios e técnicos para imputação da responsabilidade. Os objetivos específicos são: aprofundar o regime do defeito do serviço; distinguir fortuito interno e externo; delimitar culpa exclusiva e concorrente; examinar o dever de segurança à luz da LGPD e da regulação financeira; analisar o papel das contas-laranja e das instituições recebedoras; contrastar precedentes recentes; e desenvolver uma matriz probatória aplicável a litígios de fraude digital.

A relevância prática decorre da insuficiência de soluções binárias. A máxima de que toda fraude gera responsabilidade ignora nexo causal e excludentes. A afirmação de que senha válida exclui responsabilidade ignora o risco do empreendimento e os deveres de monitoramento. O artigo procura superar essa oposição por meio de análise contextual, na qual tecnologia, comportamento, regulação e prova são integrados.

2 METODOLOGIA

A pesquisa é qualitativa, exploratória e dedutiva. Parte-se do regime geral de responsabilidade por defeito do serviço para avaliar sua aplicação ao ecossistema financeiro digital. O corpus normativo compreende o Código de Defesa do Consumidor, o Código Civil, a Lei nº 12.865/2013, a Lei nº 13.709/2018 e atos do Banco Central relativos ao Pix e ao gerenciamento de riscos.

A dimensão jurisprudencial utiliza precedentes qualificados e decisões recentes do Superior Tribunal de Justiça, além do Tema 352 da Turma Nacional de Uniformização. O método de estudo de casos contrastantes permite identificar fatores que aproximam ou afastam a imputação: incompatibilidade com o perfil, cadeia de operações, atuação da vítima, qualidade da autenticação, diligência da conta recebedora e reação após a comunicação.

A dimensão documental incorpora informações públicas do Banco Central sobre segurança do Pix, marcações de fraude, bloqueio cautelar e MED 2.0, bem como dados de percepção sobre golpes. Esses indicadores são usados para contextualização, não para estimar uma taxa universal de fraude. Contestações registradas no MED, ocorrências policiais, reclamações administrativas e pesquisas de opinião possuem universos e metodologias diferentes.

O recorte temporal encerra-se em 2 de setembro de 2026. A pesquisa não acessa modelos proprietários de prevenção nem bases sigilosas das instituições. Por isso, as conclusões sobre eficácia dos controles são normativas e probatórias: indicam o que deve ser demonstrado em cada caso, sem afirmar que determinada tecnologia elimina integralmente o risco.

3 FRAUDES DIGITAIS NO ECOSSISTEMA FINANCEIRO

3.1 Engenharia social e falsa central de atendimento

Engenharia social é o conjunto de técnicas de manipulação destinado a obter comportamento útil ao agente. Seu objeto imediato pode ser uma senha, um código de autenticação, a instalação de aplicativo ou a própria ordem de pagamento. No golpe da falsa central, o criminoso imita a linguagem institucional, simula número telefônico, menciona dados pessoais e produz uma narrativa de urgência. A vítima é levada a agir não por liberalidade econômica, mas para supostamente evitar dano.

A confirmação da operação não deve ser confundida, sem exame adicional, com consentimento plenamente informado. No plano contratual, a manifestação foi contaminada por erro provocado. No plano da responsabilidade civil, porém, a invalidade subjetiva da vontade não basta para imputar o prejuízo à instituição. É indispensável demonstrar defeito do serviço e nexo causal, considerados os riscos razoavelmente previsíveis e a capacidade de prevenção.

A análise deve distinguir a autoria física da ordem e a regularidade sistêmica do processamento. Mesmo quando o dispositivo e a senha são legítimos, o sistema pode validar uma sequência anômala: elevação de limite, empréstimo, destinatário inédito e esvaziamento da conta. A legitimidade de cada etapa isolada não torna regular o conjunto.

3.2 Phishing, malware, SIM swap e acesso remoto

O phishing utiliza mensagens e páginas falsas para capturar credenciais. Malware e aplicativos de acesso remoto permitem visualizar telas, interceptar códigos ou comandar o dispositivo. O SIM swap transfere indevidamente a linha telefônica e pode comprometer fatores de autenticação baseados em SMS. Esses vetores demonstram que a segurança deve ser multicanal e resistente ao comprometimento de uma camada.

Controles eficientes combinam vínculo do dispositivo, biometria, análise de IP e localização, reputação do destinatário, velocidade das operações e autenticação reforçada baseada em risco. A autenticação multifator reduz a probabilidade de acesso indevido, mas não substitui monitoramento transacional: em engenharia social, o próprio usuário pode cumprir os fatores sob indução.

3.3 Contas-laranja, identidades sintéticas e dispersão

A fraude depende de infraestrutura receptora. Contas-laranja são abertas ou disponibilizadas para receber e transferir produto ilícito. Podem pertencer a pessoa cooptada, identidade furtada ou identidade sintética formada por combinação de dados reais e fictícios. A dispersão por contas sucessivas reduz a chance de recuperação e converte a diligência cadastral em componente central do dever de segurança.

A instituição do pagador observa a anomalia na saída; a recebedora controla abertura, atualização e padrão de entrada e saída da conta beneficiária. Responsabilidades não são

automaticamente idênticas, mas podem coexistir quando falhas distintas contribuem para o dano. A análise deve reconstruir a cadeia e individualizar a conduta de cada participante, evitando tanto a solidariedade presumida sem base causal quanto a fragmentação artificial que inviabiliza a tutela.

A velocidade de dispersão exige interoperabilidade das marcações de fraude, bloqueio tempestivo e preservação dos registros. Conta recém-aberta, múltiplos créditos de origens não relacionadas, retirada imediata e incompatibilidade com renda declarada são sinais que justificam escrutínio reforçado. A omissão sistemática diante desses sinais pode configurar defeito autônomo.

4 FUNDAMENTOS DA RESPONSABILIDADE CIVIL

4.1 Relação de consumo e responsabilidade objetiva

O art. 14 do Código de Defesa do Consumidor estabelece responsabilidade objetiva do fornecedor por danos causados por defeitos relativos à prestação do serviço. A Súmula 297 do STJ consolida a aplicação do CDC às instituições financeiras. A objetividade dispensa a prova de culpa, mas não elimina os elementos estruturais: dano, defeito e nexo causal.

O serviço é defeituoso quando não oferece a segurança legitimamente esperada, considerados modo de fornecimento, resultado, riscos e época. Em serviços financeiros digitais, a expectativa de segurança não é abstrata. Ela se concretiza em autenticação proporcional, monitoramento de anomalias, limites, diligência cadastral, resposta a incidentes e mecanismos de recuperação.

O fornecedor pode afastar a responsabilidade provando inexistência do defeito ou culpa exclusiva do consumidor ou de terceiro. Trata-se de ônus de demonstração compatível com a assimetria informacional: logs, parâmetros, alertas e trilhas de auditoria permanecem sob domínio da instituição. A inversão ou distribuição dinâmica do ônus probatório não significa presumir toda narrativa do consumidor, mas exigir de cada parte a prova que está em melhores condições de produzir.

4.2 Risco do empreendimento e fortuito interno

O Tema Repetitivo 466 e a Súmula 479 do STJ estabelecem que fraudes e delitos praticados por terceiros no âmbito de operações bancárias configuram fortuito interno e atraem responsabilidade objetiva. O fundamento é o risco do empreendimento: quem organiza

e explora atividade que administra patrimônio e identidade em escala deve internalizar riscos inerentes ao modelo.

Fortuito interno não se confunde com qualquer evento cronologicamente ligado à conta. É o risco conectado à organização, ao funcionamento ou à utilidade econômica do serviço. O fortuito externo é estranho à esfera de risco controlável e rompe o nexo. A qualificação depende de análise funcional, não apenas da autoria do terceiro.

A atuação criminosa não constitui, por si, causa exclusiva. Fraudes são previsíveis em ambiente financeiro, ainda que o caso individual não seja antecipável. A excludente exige demonstrar que os controles adequados atuaram e que o resultado decorreu de circunstância efetivamente externa. Assim, a Súmula 479 não cria garantia absoluta, mas impede que a simples presença do fraudador desloque automaticamente o risco ao consumidor.

4.3 Defeito do serviço e segurança comportamental

A avaliação do defeito deve superar a segurança credencial, centrada em senha ou token, e incorporar segurança comportamental. Modelos comportamentais identificam desvios em relação ao histórico: valor, horário, frequência, local, dispositivo, destinatário e sequência. Quanto maior a anomalia agregada, maior a justificativa para confirmação adicional ou bloqueio.

A instituição não está obrigada a bloquear toda operação fora do padrão. Tal política comprometeria autonomia, inclusão e disponibilidade dos recursos. O dever é calibrar respostas proporcionais: alertas claros, autenticação reforçada, janela de retenção, contato por canal conhecido ou limitação temporária. A razoabilidade do controle deve considerar custo, impacto e gravidade do risco.

O defeito também pode surgir depois da transferência. Atendimento que demora injustificadamente, não aciona o MED, não comunica a recebedora ou não preserva registros pode ampliar o dano. A causalidade deve separar o golpe inicial do agravamento evitável, atribuindo reparação apenas à parcela ligada à falha institucional demonstrada.

4.4 Culpa exclusiva, culpa concorrente e autonomia da vítima

A culpa exclusiva do consumidor rompe o nexo quando sua conduta é causa suficiente do dano e não há defeito concorrente. A entrega de senha ou a confirmação da transferência é relevante, mas não conclusiva. Devem ser examinados clareza dos alertas, aparência de

legitimidade, dados utilizados pelo fraudador, vulnerabilidade da vítima e anomalias que o sistema poderia detectar.

A culpa concorrente pressupõe contribuição causal de ambos. O art. 945 do Código Civil permite ajustar a indenização à gravidade comparativa, mas não autoriza redução moralizante fundada em imprudência abstrata. É necessário indicar qual comportamento evitável do consumidor contribuiu para qual parcela do resultado e quais controles institucionais falharam.

Em fraudes sofisticadas, a noção de autonomia deve ser aplicada com cautela. O agente manipula a vítima para converter medidas de proteção em atos de perda. A hipervulnerabilidade digital pode decorrer de idade, deficiência, baixa alfabetização digital ou contexto de urgência. Essa condição não elimina deveres de cautela, mas eleva o padrão de transparência e confirmação esperado do fornecedor.

5 DEVER DE SEGURANÇA, LGPD E GOVERNANÇA DE DADOS

A LGPD introduz princípios de segurança, prevenção e responsabilização, impondo medidas técnicas e administrativas aptas a proteger dados pessoais. Fraudes de falsa central frequentemente utilizam informações que aumentam a credibilidade do contato. A ocorrência do golpe não prova vazamento pela instituição, mas torna relevante esclarecer origem, acesso, compartilhamento e proteção dos dados utilizados.

A responsabilidade por incidente de dados e a responsabilidade pelo processamento financeiro são juridicamente relacionadas, porém distintas. Pode existir fraude sem incidente atribuível ao banco; pode existir incidente sem transferência; e podem coexistir falhas de dados e transacionais. A decisão deve identificar o nexo próprio de cada falha, evitando presunções automáticas.

O tratamento de dados para prevenção à fraude possui finalidade legítima, mas permanece sujeito a necessidade, adequação, segurança e prestação de contas. Modelos antifraude não devem operar como caixa-preta imune ao controle. A instituição pode preservar segredos comerciais sem deixar de demonstrar categorias de dados, parâmetros de risco, alertas produzidos e resultado aplicado ao caso.

A governança adequada inclui segregação de acesso, retenção proporcional, auditoria de modelos, revisão humana em situações críticas, registro de decisões e canais de contestação. Também deve mitigar falsos positivos e vieses que afetem grupos específicos.

Segurança e proteção de dados não são objetivos opostos: controles bem desenhados minimizam tanto a fraude quanto a coleta excessiva.

6 REGULAÇÃO DO PIX E MECANISMOS DE PREVENÇÃO E RECUPERAÇÃO

6.1 Arquitetura de segurança e deveres dos participantes

A Lei nº 12.865/2013 inclui segurança, confiabilidade, proteção dos interesses econômicos e transparência entre os princípios dos arranjos e das instituições de pagamento. O dever alcança bancos e participantes não bancários. A natureza tecnológica da entidade não reduz a expectativa de processamento seguro.

A arquitetura do Pix combina autenticação, criptografia, rastreabilidade, Diretório de Identificadores de Contas Transacionais, marcações de fraude, limites, bloqueio cautelar e MED. O desenho sistêmico depende de implementação individual. Cada participante deve manter gerenciamento de risco capaz de identificar transações atípicas ou incompatíveis com o perfil do cliente.

A rastreabilidade do Pix não implica recuperação automática. Valores podem ser transferidos, sacados ou convertidos. Por isso, prevenção e resposta devem atuar em segundos ou minutos. A qualidade dos dados cadastrais e das marcações de fraude influencia todo o ecossistema.

6.2 Bloqueio cautelar e MED

O bloqueio cautelar permite retenção temporária quando a instituição recebedora identifica suspeita. O MED organiza a tentativa de devolução em hipóteses de fraude e falha operacional. Não é instrumento comum para arrependimento, erro de chave ou desacordo comercial. A devolução depende de análise, saldo disponível e tempestividade.

O MED não substitui a responsabilidade civil. Sua abertura demonstra reação, mas não prova que os controles anteriores eram adequados; sua frustração não significa, isoladamente, defeito. O mecanismo é parte da cadeia probatória: tempo de comunicação, notificações, valores bloqueados, justificativas e movimentações subsequentes.

O MED 2.0 amplia o rastreio para além da primeira conta recebedora e prioriza caminhos de bloqueio. A evolução responde à fragmentação do produto da fraude. Juridicamente, reforça a compreensão de que o dever de segurança abrange a cadeia de dispersão e exige cooperação entre prestadores.

A efetividade do MED 2.0 deve ser avaliada por taxa e tempo de recuperação, reincidência de contas, precisão das marcações e tratamento de contestações legítimas. O número bruto de procedimentos não mede, sozinho, sucesso regulatório.

6.3 Contas recebedoras e know your customer

A diligência na abertura e manutenção de contas deve verificar identidade, consistência documental e risco. O dever não termina no onboarding: comportamento superveniente pode revelar uso incompatível. Monitoramento contínuo é especialmente relevante em contas que recebem valores de diversas vítimas e os dispersam imediatamente.

A responsabilização da instituição recebedora exige individualização. A mera recepção de valor fraudado não basta; deve haver defeito relevante na abertura, supervisão, marcação, bloqueio ou resposta. A prova pode incluir data de abertura, renda declarada, volume, destinatários, alertas e histórico de reclamações.

A cooperação entre participantes não afasta a proteção de dados. Compartilhamento deve possuir base legal, finalidade antifraude, controles de acesso e registro. A governança do ecossistema depende de informação de qualidade e de mecanismos para corrigir marcações indevidas.

7 ANÁLISE JURISPRUDENCIAL CONTRASTANTE

7.1 Transações incompatíveis com o perfil e falsa central

Em 2023, o STJ reafirmou que bancos devem identificar e impedir movimentações incompatíveis com o histórico do cliente. A facilidade digital de contratação é acompanhada do dever de desenvolver mecanismos capazes de detectar operações anômalas. O precedente também destacou a hipervulnerabilidade de consumidores idosos e rejeitou inferência de culpa exclusiva baseada em suposição sobre entrega de senha.

Em outubro de 2025, a Terceira Turma julgou os REsp 2.222.059 e 2.229.519, relativos à falsa central. Em um dos casos, quatorze transações foram feitas em um único dia, em contraste com histórico de poucas movimentações, além de empréstimo e pagamento atípicos. A responsabilização decorreu da falha em identificar transações suspeitas e da ausência de prova de culpa exclusiva.

O núcleo decisório está no perfil transacional e na segurança esperada. A sentença de responsabilidade não foi uma sanção por a fraude ter ocorrido, mas consequência de sinais

objetivos não tratados. O uso de credenciais legítimas perdeu força diante da cadeia de anomalias.

7.2 Golpe da “mão fantasma” e culpa concorrente

No REsp 2.220.333, a vítima instalou aplicativo de acesso remoto após orientação de falso funcionário; em seguida houve empréstimo e operações incompatíveis com o perfil. O STJ afastou a redução por culpa concorrente porque a falha de segurança foi determinante e a vítima não assumiu conscientemente o risco.

O precedente não declara irrelevante toda conduta do consumidor. Ele exige relação causal qualificada. A instalação do aplicativo integra a narrativa da fraude, mas não absolve sistema que valida empréstimo e transferências manifestamente anômalos. A culpa concorrente não pode funcionar como atalho para dividir prejuízos sem reconstrução técnica.

7.3 Tema 352 da TNU

O Tema 352 da TNU sistematiza a responsabilidade objetiva em fraudes via Pix por engenharia social e admite seu afastamento quando demonstrada inexistência de falha ou culpa exclusiva. A entrega induzida de dados pode ser considerada para culpa concorrente, com especial atenção à hipervulnerabilidade e às falhas de prevenção e bloqueio.

A aparente tensão com a orientação restritiva do STJ pode ser resolvida pelo nexo causal. A entrega de credenciais é elemento, não presunção absoluta. Quando o serviço contribui decisivamente, não há base para redução automática; quando controles adequados são provados e a conduta externa explica integralmente o dano, a responsabilidade pode ser afastada.

7.4 REsp 2.209.868: limite à responsabilização automática

Em julho de 2026, o STJ divulgou decisão no REsp 2.209.868 afastando a responsabilidade em golpe da falsa central. As transferências via Pix não destoavam do histórico e a operação de maior valor foi realizada presencialmente pela cliente, sem relato da ligação aos funcionários. Mantidas as premissas do tribunal de origem, não havia defeito nem nexo causal.

O caso é relevante porque explicita que a Súmula 479 não dispensa demonstração do fortuito interno. A fraude de engenharia social não basta para responsabilizar; é preciso vincular o dano a falha do serviço. A decisão oferece contraponto metodológico aos casos de 2025 e confirma que o perfil transacional, o canal e a conduta posterior são determinantes.

A comparação indica que a jurisprudência caminha para um teste contextual. Operações anômalas, empréstimos instantâneos, múltiplas transferências e falhas de bloqueio aproximam a responsabilidade. Operações compatíveis, presença física, alertas adequados e ausência de falha comprovada favorecem a excludente.

8 MATRIZ PROBATÓRIA DE SEIS EIXOS

8.1 Identidade, dispositivo e acesso

Devem ser examinados dispositivo cadastrado, IP, geolocalização disponível, troca de telefone ou e-mail, redefinição de senha, recuperação de acesso, biometria, token, SIM swap e sinais de acesso remoto. O objetivo é verificar se a autenticação formal corresponde ao contexto habitual.

8.2 Perfil e sequência transacional

Valor, horário, frequência, destinatário, canal e intervalo devem ser comparados ao histórico. A análise deve ser agregada: contratação de crédito, elevação de limite e transferência para favorecido inédito podem produzir risco que não aparece em cada etapa isolada.

8.3 Conta recebedora e cadeia de dispersão

É necessário reconstruir abertura, titularidade, marcações, padrão de créditos, saídas subsequentes e reclamações anteriores. A instituição recebedora deve explicar controles de onboarding e monitoramento, sem que a mera condição de recebedora gere responsabilidade automática.

8.4 Controles preventivos e decisão

A instituição deve demonstrar parâmetros de risco aplicados, alertas, confirmações, limites, bloqueios e motivos da autorização. Não se exige divulgação de código-fonte, mas prova auditável de funcionamento. A ausência de documentação enfraquece a alegação de serviço adequado.

8.5 Resposta e mitigação

Devem ser registrados horário da comunicação, abertura do MED, bloqueio cautelar, contato com a recebedora, preservação de logs e orientação ao consumidor. A demora pode constituir causa concorrente de agravamento.

8.6 Conduta, vulnerabilidade e causalidade

Compartilhamento consciente de senha, desconsideração de alertas inequívocos, instalação de programa e confirmação do beneficiário são relevantes. Sua força depende da sofisticação do golpe, da clareza do aviso e das falhas institucionais. A conclusão deve apontar causalidade, não censura abstrata.

9 ÔNUS DA PROVA E PROCESSO

O consumidor normalmente possui extratos, comunicações e narrativa do contato, mas não tem acesso a logs, regras antifraude e histórico da conta recebedora. A instituição concentra evidência técnica. O art. 6º, VIII, do CDC e a distribuição dinâmica prevista no CPC permitem adequar o ônus à capacidade probatória.

A inversão não dispensa o autor de individualizar operações, dano e cronologia. Também não autoriza condenação baseada em alegações genéricas. Uma instrução adequada exige preservação e apresentação de dados com cadeia de custódia: identificação do dispositivo, alterações cadastrais, autenticação, alertas, gravações, MED e movimentação da conta destinatária.

A prova pericial pode ser necessária quando houver disputa sobre acesso remoto, biometria, logs ou detecção de anomalias. O perito deve avaliar não apenas se a senha estava

correta, mas se os controles eram compatíveis com o risco e se reagiram à sequência observada. Segredos comerciais podem ser protegidos por sigilo processual e acesso restrito.

A tutela de urgência pode buscar bloqueio e preservação de dados. Como o produto da fraude se dissipa rapidamente, demora processual reduz efetividade. Ordens devem ser proporcionais, delimitadas e compatíveis com o funcionamento do arranjo.

10 LIMITES, RISCOS REGULATÓRIOS E RECOMENDAÇÕES

Segurança excessiva pode produzir indisponibilidade, discriminação algorítmica e exclusão financeira. Modelos baseados em histórico penalizam usuários com pouca movimentação ou mudanças legítimas. Por isso, bloqueios devem ser acompanhados de canais céleres de confirmação e revisão.

Instituições devem adotar governança integrada entre fraude, segurança cibernética, proteção de dados, atendimento e prevenção à lavagem de dinheiro. A fragmentação interna transforma sinais disponíveis em respostas tardias. Indicadores devem medir perdas evitadas, tempo de detecção, recuperação, falsos positivos e reincidência de contas.

É recomendável aplicar autenticação adaptativa, monitoramento comportamental e confirmação reforçada em operações de alto risco; supervisionar continuamente contas recebedoras; preservar trilhas auditáveis; integrar canais de atendimento ao MED; testar planos de resposta; e comunicar alertas de forma específica, sem mensagens genéricas que o usuário aprende a ignorar.

Aos reguladores, recomenda-se aperfeiçoar transparência estatística, interoperabilidade das marcações e supervisão das contas de passagem. A avaliação do MED 2.0 deve publicar métricas comparáveis e esclarecer limitações. A inovação regulatória deve preservar competição sem reduzir padrões de segurança.

Ao Judiciário, recomenda-se utilizar a matriz de seis eixos, individualizar a atuação de cada instituição e evitar presunções absolutas. A senha válida não encerra o caso; tampouco a vulnerabilidade elimina o nexo. A fundamentação deve indicar quais anomalias existiam, qual controle era exigível e como a falha contribuiu para o dano.

Aos consumidores, recomenda-se confirmar contatos em canal oficial independente, recusar instalação de aplicativos, desconfiar de “conta segura”, conferir beneficiário e comunicar imediatamente a fraude. Tais deveres reduzem risco, mas não transferem ao consumidor a administração profissional do sistema.

11 CONCLUSÃO

A responsabilidade civil por fraudes digitais deve ser construída na interseção entre direito do consumidor, regulação financeira, proteção de dados e prova tecnológica. O art. 14 do CDC, o Tema 466 e a Súmula 479 estabelecem o ponto de partida: fraudes inseridas nas operações bancárias integram o risco da atividade, e o fornecedor responde objetivamente pelo serviço defeituoso.

Essa orientação não converte instituições em seguradoras universais. A responsabilidade exige defeito e nexo. O REsp 2.209.868 demonstra que, sem transações incompatíveis ou outra falha provada, a engenharia social pode permanecer externa ao serviço. Em contraste, os casos de 2025 mostram que empréstimos, alterações e transferências anômalas autorizadas sem contenção revelam defeito.

A hipótese foi confirmada. A autenticação é necessária, mas não suficiente. Quando a cadeia operacional produz sinais objetivos detectáveis, a instituição deve demonstrar monitoramento, decisão proporcional e resposta tempestiva. A culpa exclusiva ou concorrente requer contribuição causal concreta e não pode ser inferida apenas da participação material da vítima.

O dever de segurança distribui-se pelo ecossistema. A instituição pagadora monitora a saída; a recebedora responde por diligência cadastral, supervisão e bloqueio; o arranjo fornece mecanismos de rastreabilidade e devolução; o regulador define padrões; e o consumidor mantém deveres razoáveis de cautela. A imputação deve individualizar cada falha.

A matriz de seis eixos oferece contribuição aplicada: identidade e acesso; perfil transacional; conta recebedora e dispersão; controles preventivos; resposta; e conduta da vítima. Seu uso desloca a decisão de fórmulas abstratas para evidência verificável, preservando simultaneamente confiança, autonomia e inovação no sistema financeiro digital.

Pesquisas futuras devem avaliar dados do MED 2.0, qualidade das marcações, tempo de recuperação e impacto distributivo dos modelos antifraude. A maturidade jurídica dependerá de métricas transparentes e de capacidade institucional para transformar a prevenção em prova auditável.

REFERÊNCIAS

BANCO CENTRAL DO BRASIL. BC aperfeiçoa mecanismos de segurança do Pix. Brasília, 2024. Disponível em: <https://www.bcb.gov.br/detalhenoticia/20231/noticia>. Acesso em: 2 set. 2026.

BANCO CENTRAL DO BRASIL. BC aprimora o Mecanismo Especial de Devolução do Pix. Brasília, 28 ago. 2025. Disponível em: <https://www.bcb.gov.br/detalhenoticia/20817/nota>. Acesso em: 2 set. 2026.

BANCO CENTRAL DO BRASIL. Estatísticas de fraude no Pix (MED). Portal de Dados Abertos. Disponível em: <https://dadosabertos.bcb.gov.br/sl/dataset/pix/resource/7eb5efdd-d4dd-47da-a74a-d93ce68ea185>. Acesso em: 2 set. 2026.

BANCO CENTRAL DO BRASIL. Mecanismo Especial de Devolução (MED 2.0). Brasília, 2025. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/pix/MED/MED_2-0_Circuito_Pix-Dia_1.pdf. Acesso em: 2 set. 2026.

BANCO CENTRAL DO BRASIL. Segurança no Pix. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/pix-seguranca>. Acesso em: 2 set. 2026.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Diário Oficial da União, Brasília, 12 set. 1990.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil. Diário Oficial da União, Brasília, 11 jan. 2002.

BRASIL. Lei nº 12.865, de 9 de outubro de 2013. Dispõe sobre arranjos e instituições de pagamento. Diário Oficial da União, Brasília, 10 out. 2013.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, 15 ago. 2018.

CONSELHO DA JUSTIÇA FEDERAL. TNU fixa tese sobre responsabilidade das instituições financeiras em fraudes via Pix. Tema 352, processo nº 1054560-45.2021.4.01.3500/GO. Brasília, 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. Súmula nº 297. O Código de Defesa do Consumidor é aplicável às instituições financeiras. Diário da Justiça, Brasília, 12 set. 2004.

SUPERIOR TRIBUNAL DE JUSTIÇA. Súmula nº 479. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Diário da Justiça Eletrônico, Brasília, 1º ago. 2012.

SUPERIOR TRIBUNAL DE JUSTIÇA. REsp 1.199.782/PR. Tema Repetitivo 466. Rel. Min. Luis Felipe Salomão, Segunda Seção, julgado em 24 ago. 2011.

SUPERIOR TRIBUNAL DE JUSTIÇA. Para evitar fraudes, banco tem o dever de identificar e impedir transações que destoam do perfil do cliente. Brasília, 30 out. 2023.

SUPERIOR TRIBUNAL DE JUSTIÇA. Bancos e instituições de pagamento devem indenizar clientes por falhas que viabilizam golpe da falsa central. REsp 2.222.059 e REsp 2.229.519. Brasília, 21 out. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. Falha de segurança do banco afasta alegação de culpa concorrente do consumidor em caso de golpe. REsp 2.220.333. Brasília, 13 nov. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. Sem transações incompatíveis com perfil de cliente, banco não responde por golpe da falsa central. REsp 2.209.868. Brasília, 15 jul. 2026.