O PAPEL DAS INSTITUIÇÕES FINANCEIRAS NA PREVENÇÃO DE GOLPES BANCÁRIOS DIGITAIS: COMPLIANCE E RESPONSABILIDADE PELO DANO AO CONSUMIDOR

Débora Rafaela Coêlho Pereira[1]

RESUMO: A expansão dos serviços bancários digitais trouxe praticidade e rapidez para os consumidores, mas também abriu espaço para o aumento de golpes financeiros realizados por meio de recursos tecnológicos. Este trabalho tem como objetivo analisar o papel das instituições financeiras na prevenção dessas fraudes, com foco nas práticas de compliance e na responsabilidade civil perante os consumidores lesados. Ao longo da elaboração, recorreu-se a pesquisa bibliográfica e documental, com leitura de legislação (LGPD, CDC e Marco Civil da Internet), normativos do Banco Central e estudos setoriais, além de exame de decisões do STJ, dentro de uma abordagem qualitativa de caráter dedutivo. O estudo aborda os principais tipos de golpes digitais, como phishing, engenharia social, clonagem de cartões e fraudes via Pix, e discute os impactos econômicos e sociais dessas práticas. Também são exploradas as normas que regem a proteção de dados e a segurança no ambiente bancário digital. A partir da análise da jurisprudência e de dados sobre fraudes no Brasil, conclui-se que as instituições financeiras devem investir em sistemas de segurança eficientes, atuar de forma preventiva e oferecer suporte adequado às vítimas, reforçando a importância da educação digital dos usuários e da atualização constante das regras diante da evolução dos crimes virtuais.

Palavras-Chave: Golpes bancários digitais. Instituições financeiras. Compliance. Responsabilidade civil. Proteção de dados. Direito do consumidor.

ABSTRACT: The expansion of digital banking services has brought convenience and speed but also opened room for technology-enabled fraud. This article analyzes the role of financial institutions in preventing such scams, focusing on compliance practices and civil liability toward harmed consumers. The analysis draws on bibliographic and documentary research, reviewing statutes (Brazil's LGPD, Consumer Defense Code, and Marco Civil), Central Bank rules and industry reports, together with STJ case law, within a qualitative, deductive approach. It presents major fraud typologies (phishing, social engineering, card cloning and Pix-related scams) and discusses their economic and social impacts, as well as the applicable data-protection and security framework. Based on jurisprudence and Brazilian fraud data, it concludes that banks should invest in effective security systems, act preventively and provide adequate support to victims, while strengthening digital literacy and keeping regulation up to date as crimes evolve.

[1]Acadêmica do curso Direito pela UNISOCIESC em Blumenau/SC. E-mail: drafaelacpereira@gmail.com. Artigo apresentado como requisito parcial para a conclusão do curso de Graduação em Direito da Instituição de Ensino Superior (IES) da rede Ânima Educação. 2025.

Keywords: Digital banking fraud. Financial institutions. Compliance. Civil liability. Data protection. Consumer law.

1 INTRODUÇÃO

Nos últimos anos, a digitalização dos serviços bancários tem proporcionado maior praticidade e acessibilidade aos consumidores, ao mesmo tempo em que expôs clientes e instituições financeiras a um aumento expressivo de golpes bancários no ambiente digital. Fraudes como phishing, engenharia social e invasões de contas têm gerado prejuízos significativos, levantando debates sobre a responsabilidade das instituições financeiras na proteção de seus clientes.

Diante desse contexto, surge o questionamento: até que ponto as instituições financeiras são responsáveis e devem ser responsabilizadas pela segurança de seus usuários em transações digitais? O crescimento dessas fraudes tem levado o setor a aprimorar diretrizes de conformidade (compliance) e adotar medidas preventivas mais eficientes, impulsionadas por marcos como o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD) e normas do Banco Central do Brasil.

O presente estudo analisa o papel das instituições financeiras na prevenção de golpes bancários digitais, considerando os mecanismos de compliance adotados e a responsabilidade civil perante consumidores lesados. Além do objetivo central, o texto mapeia as principais modalidades de fraudes, examina a regulamentação aplicável ao setor, observa o entendimento jurisprudencial sobre a responsabilização dos bancos e discute medidas preventivas e de suporte ao consumidor. Para sustentar a análise, adotou-se uma base bibliográfica e documental, com levantamento de legislação, doutrina, normativos do Banco Central e julgados do STJ, em abordagem qualitativa e método dedutivo.

Ao longo do artigo, inicialmente apresenta-se um panorama das fraudes (Capítulo 2); em seguida, discutem-se compliance e segurança cibernética no setor financeiro (Capítulo 3); examina-se a responsabilidade das instituições (Capítulo 4); reúnem-se soluções e boas práticas (Capítulo 5); e, por fim, apresentam-se as considerações finais (Capítulo 6), retomando a pergunta de pesquisa.

2 OS GOLPES BANCÁRIOS DIGITAIS: PANORAMA E TIPIFICAÇÃO

A digitalização dos serviços bancários e a popularização de ferramentas financeiras online trouxeram diversos benefícios para os consumidores e instituições bancárias; em contrapartida, abriram um campo fértil para o desenvolvimento de fraudes. Os golpes bancários digitais são realizados por meio de ataques tecnológicos ou comportamentais, que visam subtrair valores, informações pessoais e dados bancários dos usuários. Este capítulo tem como objetivo discutir os principais tipos de fraudes bancárias digitais, seus impactos econômicos e sociais, e o perfil das vítimas, além de explorar como esses golpes são aplicados e quais as possíveis consequências para os envolvidos.

2.1 PRINCIPAIS GOLPES BANCÁRIOS DIGITAIS

O uso crescente de serviços bancários digitais contribuiu para o aumento de fraudes que exploram vulnerabilidades em sistemas e comportamentos dos consumidores. Entre as fraudes mais recorrentes, destacam-se o phishing, a engenharia social, a clonagem de cartões e os golpes envolvendo o sistema de pagamentos instantâneos, como o Pix.

O phishing é uma das técnicas mais utilizadas por criminosos para obter dados bancários e informações pessoais de forma fraudulenta. Com esse método, o criminoso envia e-mails, mensagens de texto ou até mesmo ligações telefônicas falsas que se passam por uma instituição financeira legítima, solicitando que a vítima forneça informações sensíveis. Essa técnica tem se tornado cada vez mais sofisticada, com e-mails e sites falsificados que imitam com precisão os originais, induzindo os consumidores ao fornecimento de dados sensíveis como senhas e número de cartão de crédito. De acordo com Atheniense (2021), "o phishing é um dos golpes mais comuns devido à facilidade com que os criminosos conseguem criar sites e e-mails falsos, enganando até os usuários mais atentos" (ATHENIENSE, 2021).

Além disso, de acordo com a Serasa, a tentativa de fraude por phishing cresceu 12% no Brasil entre 2023 e 2024. As técnicas de engenharia social, que

costumam ser utilizadas em conjunto com o phishing, tem sido mais eficiente, pois manipulam psicologicamente a vítima a fim de obter suas informações.

A engenharia social consiste na manipulação emocional das vítimas, induzindo-as a revelar dados pessoais ou efetuar transações financeiras. Ela pode ser realizada através de e-mails, ligações ou até mesmo por redes sociais. Os golpistas podem se passar por funcionários de uma instituição financeira ou empresa conhecida, fazendo com que a vítima acredite que está em situação legítima. "A engenharia social explora a confiança humana, que é um dos fatores mais difíceis de serem prevenidos pelas instituições financeiras" (OLIVEIRA SILVA e COSTA, 2021, p. 42).

A introdução do sistema de pagamento instantâneo PIX no Brasil trouxe vantagens em termos de agilidade nas transações financeiras, no entanto, também gerou novas formas de fraudes, como a solicitação de pagamentos falsos e a indução de vítimas a transferirem dinheiro para contas de golpistas, com a promessa de um serviço inexiste, por exemplo. Segundo Lima (2022), "a facilidade e a instantaneidade do PIX, junto com a falta de mecanismos de reversão, tornam este sistema um alvo fácil para fraudes" (LIMA, 2022, p. 118).

Embora a clonagem de cartões de crédito não seja nova, ela se tornou mais frequente no ambiente digital. Os criminosos têm utilizado tecnologias avançadas para copiar os dados de cartões em transações online. Segundo Barros (2021), "a clonagem de cartões digitais é facilitada pela ausência de sistemas adequados de autenticação e verificação nas compras feitas pela internet" (BARROS, 2021, p. 87).

O impacto da clonagem de cartões é significativo, tanto para as vítimas quanto para as instituições financeiras. O consumidor pode ter seu limite de crédito comprometido ou sofrer perdas financeiras diretas, enquanto os bancos e as operadoras de cartões enfrentam custos com reembolso, investigações e perda de confiança do consumidor.

2.2 IMPACTO ECONÔMICO E SOCIAL DAS FRAUDES BANCÁRIAS DIGITAIS

A fraude bancária digital tem impactos econômicos e sociais significativos. Os danos econômicos são consideráveis, não apenas para os consumidores, mas também para as instituições financeiras, que enfrentam custos elevados para

reverter os danos, melhorar a segurança e lidar com ações judiciais. Segundo o estudo “State of Scams in Brazil” (2024), "o impacto das fraudes digitais no sistema financeiro brasileiro gerou uma perda de aproximadamente R$297,7 bilhões em 2024, o que demonstra a gravidade do problema" (GASA, 2024).

Além das perdas econômicas, o efeito social das fraudes em bancos digitais é extremamente prejudicial, pois cria um clima de desconfiança, onde os consumidores começam a se afastar das operações digitais. A falta de segurança nas transações financeiras, seja pela internet ou aplicativos móveis, resulta em uma queda de captação de novos clientes para serviços bancários digitais. Como apontado por Atheniense (2021), "a insegurança nas transações digitais resulta em um efeito cascata que afeta a confiança na economia digital como um todo" (ATHENIENSE, 2021, p. 92).

O efeito social das fraudes em instituições financeiras que operam digitalmente é significativo, pois atinge principalmente indivíduos vulneráveis, como os mais velhos ou consumidores com pouca experiência em tecnologia. Esses grupos costumam ser mais propensos a serem vítimas de fraudes, visto que detêm menos meios para se proteger contra tais delitos. As fraudes acabam promovendo um aumento na exclusão financeira, comprometendo sua inserção no sistema financeiro. Ademais, as instituições financeiras correm o risco de enfrentar processos judiciais e por vezes, precisam reembolsar os lesados. Esses efeitos impactam diretamente a saúde financeira da instituição e sua capacidade de competitividade no mercado.

2.3 PERFIL DAS VÍTIMAS E COMO OS GOLPES SÃO APLICADOS

O perfil das vítimas de fraudes bancárias digitais é amplo, abrangendo pessoas de diferentes idades e níveis socioeconômicos. Contudo, a faixa etária mais afetada tende a ser as dos usuários mais idosos, que têm menos familiaridade com as tecnologias digitais e com os riscos associados a elas. De acordo com o blog Kaspersky, "a engenharia social é uma técnica de manipulação que explora erros humanos para obter informações privadas, acessos ou coisas de valor” (KASPERSKY, 2025). Além disso, um artigo do Governo Federal destaca que "a engenharia social tem se tornado uma estratégia de manipulação psicológica

comumente usada por criminosos, no contexto de segurança da informação, para induzir as pessoas ao erro e enganá-las através de narrativas convincentes" (GOVERNO FEDERAL, 2025). O Estadão observa que "a dificuldade em reverter as transações e o aumento da confiança nos meios digitais leva os golpistas a agirem com maior rapidez, prejudicando o consumidor de forma irreversível" (ESTADÃO, 2025).

Para mitigar os riscos, faz-se necessário a adoção de medidas preventivas, como utilização de senhas fortes e únicas, manter softwares de segurança atualizados, e manter-se atento a comunicações suspeitas. A educação digital contínua, associada a políticas robustas de segurança e conscientização promovidas pelas instituições financeiras, é fundamental para reduzir o impacto das fraudes bancárias digitais, protegendo tanto os consumidores quanto o sistema financeiro.

3 COMPLIANCE E SEGURANÇA CIBERNÉTICA NO SETOR FINANCEIRO

No Brasil, o sistema financeiro é regulado por um conjunto de normas que asseguram a privacidade dos usuários, a ética nas operações bancárias e a segurança no tratamento de dados. Entre as principais regulamentações estão a Lei do Sigilo Bancário, o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD) e as resoluções e normativas do Banco Central.

A Lei Complementar nº 105/2001 trata especificamente da proteção das informações bancárias, garantindo que dados dos clientes só possam ser acessados com autorização judicial ou nos casos previstos em lei. Conforme explica o Tribunal de Justiça do Distrito Federal, “o sigilo bancário constitui direito fundamental implícito, que advém da inviolabilidade da intimidade [...] e do sigilo de dados” garantido pela Constituição Federal (TJDFT, 2022).

O Marco Civil da Internet, por sua vez, regula o uso da internet no Brasil e estabelece os princípios, como, por exemplo, a proteção da privacidade dos usuários e a segurança dos dados. Segundo a Lei nº 12,965/2014, os registros de conexão só deverão ser fornecidos mediante ordem judicial, o que reforça a concepção da internet segura e responsável.

Já a Lei Geral de Proteção de Dados (Lei nº 13,709/2018) introduziu as regras específicas sobre o tratamento de dados pessoais, requisitando que as instituições financeiras apresentem bases legais para coletar, armazenar e compartilhar essas informações. De acordo com as acadêmicas do Centro Universitário Uninter, Siderly do Carmo Dahle de Almeida e a Tania Aparecida Soares “[,,,] a Lei Geral de Proteção de Dados Pessoais (LGPD), trouxe consigo, a mudança de cultura nas instituições e organizações (pública e privada), agregando no tratamento de dados pessoais, maior responsabilidade. Isso é fato, o que possibilitou rever a forma de processamento e tratamento dos dados, que se considerar seu uso devido ou não, poderá gerar dados há quem as informações cuja titularidade é de direito.” (ALMEIDA; SOARES, 2022).

Ainda, o Banco Central do Brasil, por meio da Resolução nº 4.595/2017, definiu diretrizes para a política de conformidade das instituições financeiras, exigindo controles internos que minimizem riscos e assegurem conduta ética. Segundo o próprio BACEN, a norma “dispõe sobre a política de conformidade (compliance) das instituições financeiras [...] e visa contribuir para a solidez do Sistema Financeiro Nacional” (BRASIL, Banco Central Do, 2017)

O compliance bancário envolve a implementação de políticas e procedimentos que assegurem o cumprimento das normas legais e regulatórias, visando prevenir fraudes e garantir a segurança das transações financeiras. No Brasil, o setor financeiro tem investido significativamente nessa área. Segundo o Valor Econômico, "Bancos destinam bilhões para aprimorar dados, compliance, segurança e experiência do cliente, fortalecendo a luta contra crimes financeiros" (VALOR ECONÔMICO, 2024).

A segurança cibernética é fundamental no setor financeiro devido à sensibilidade dos dados tratados. Instituições financeiras estão adotando medidas robustas para proteger informações confidenciais e prevenir fraudes. De acordo com a ClearSale, "a segurança cibernética desempenha um papel importante no mercado financeiro, ao prevenir os negócios de fraudes e assegurando a continuidade dos negócios" (CLEARSALE, 2023).

Investimentos em tecnologias avançadas, como inteligência artificial, têm sido direcionados para detectar comportamentos suspeitos e prevenir fraudes, minimizando riscos de ataques cibernéticos. A FEBRABAN observa que "os bancos

estão utilizando tecnologias avançadas, como inteligência artificial, para detectar comportamentos suspeitos e prevenir fraudes, minimizando riscos de ataques cibernéticos" (FEBRABAN, 2022).

A conformidade com a segurança cibernética envolve aderir a um conjunto de regras e regulamentos sobre como as organizações devem lidar e proteger dados confidenciais. Segundo a Silverfort, "a conformidade com a segurança cibernética se refere a seguir o conjunto de regras e regulamentos sobre como as organizações devem lidar e proteger dados confidenciais" (SILVERFORT, 2021).

Além disso, a governança de segurança da informação organiza a forma como uma empresa lida com os desafios de cibersegurança, sendo essencial para a proteção de dados sensíveis e a manutenção da confiança dos clientes.

4 RESPONSABILIDADE DAS INSTITUIÇÕES FINANCEIRAS

O sistema jurídico brasileiro estabelece determinadas normas voltadas à proteção dos consumidores e à responsabilidade das instituições financeiras, especialmente no que diz respeito às fraudes bancárias. Considerando este contexto, a responsabilidade civil pode ser abordada sob a ótica objetiva e subjetiva.

A responsabilidade objetiva, prevista no Código de Defesa do Consumidor (CDC), implica que as instituições financeiras devem ser responsabilizadas independentemente de culpa, quando houver falhas nos serviços prestados que resultem em danos aos consumidores. Especificamente o artigo 14 do CDC dispõe que "o fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores" (BRASIL, 1990), o que reforça a necessidade de os bancos adotarem medidas eficazes de segurança, prevenindo fraudes e danos aos clientes.

Já a responsabilidade subjetiva, prevista no Código Civil, exige que se prove a culpa ou dolo da instituição financeira para que haja reparação. O artigo 186 do Código Civil traz que "aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, fica sujeito à reparação" (BRASIL, 2002), demonstrando que, em situações nas quais o banco falhe por

negligência, a responsabilidade pode ser atribuída de forma subjetiva, mas somente com base na comprovação de que existiu uma falha na prestação do serviço.

Em relação à jurisprudência dos tribunais brasileiros, o Superior Tribunal de Justiça (STJ) tem consolidado a tese de que os bancos devem ser responsabilizados pela proteção dos dados de seus clientes e pela prevenção de fraudes bancárias. Em diversas decisões, o STJ reafirma que as instituições financeiras devem estabelecer medidas eficientes com intuito de impedir o acesso não autorizado às contas e dados sensíveis dos clientes, garantindo mais segurança em suas transações financeiras. Cada vez mais tem se destacado que as instituições financeiras são as principais responsáveis pela segurança da operação, e devem promover e adotar mecanismos para prevenir fraudes e danos aos consumidores. A esse respeito, há o entendimento consolidado pelo Supremo Tribunal de Justiça, expresso na Súmula 479 do STJ, que afirma: "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. " (STJ, 2012).

No entanto, apesar da responsabilidade das instituições financeiras, existem algumas excludentes de responsabilidade que podem ser aplicadas, previstas tanto no Código Civil quanto no CDC. A culpa exclusiva da vítima é uma das principais excludentes, sendo quando o consumidor, por sua própria negligência, facilita a ocorrência da fraude. Nesse caso, o banco pode ser isento de responsabilidade, pois não teve como evitar o dano devido à atitude imprudente do cliente. Outra excludente prevista no Código Civil é a força maior, que se refere a eventos imprevisíveis e inevitáveis. O artigo 393 do Código Civil estabelece que "não há obrigação de reparar o dano, quando a ocorrência do fato que o causou se der por motivo de força maior" (BRASIL, 2002). Nesse contexto, se a fraude for resultado de um ataque cibernético altamente sofisticado e imprevisível, o banco pode alegar que a responsabilidade não recai sobre ele, uma vez que a ocorrência foi alheia à sua capacidade de prevenção.

No cenário internacional, a responsabilidade dos bancos em caso de fraudes é tratada de forma semelhante em diversos países, mas com algumas diferenças significativas em relação à abordagem adotada no Brasil. Nos Estados Unidos, por

exemplo, as instituições financeiras também são responsabilizadas pela segurança das transações, mas com foco maior na responsabilidade subjetiva, o que implica que o consumidor precisa provar a falha da instituição para que seja efetuada a reparação do dano. Em países da União Europeia, como a Alemanha, a legislação é mais rigorosa quanto à responsabilidade objetiva dos bancos. A responsabilidade é atribuída automaticamente às instituições financeiras, que são obrigadas a adotar medidas de segurança adequadas para prevenir fraudes e proteger os dados dos consumidores. Dessa forma, enquanto o Brasil opta por um modelo híbrido, que combina a responsabilidade objetiva com a subjetiva, países europeus e norte-americanos possuem sistemas que privilegiam mais a responsabilização direta das instituições, independentemente de quem de fato seria o culpado.

A partir desse contraste, vale detalhar como cada regime constroi a proteção do usuário e a responsabilização das instituições. Nos Estados Unidos, a proteção do usuário se ancora na Electronic Fund Transfer Act (EFTA) e na regulamentação do Consumer Financial Protection Bureau (Regulation E). O ponto crucial é a qualificação de “transferência eletrônica não autorizada”: a norma define a operação como aquela “initiated by a person other than the consumer … and from which the consumer receives no benefit” [iniciada por pessoa diversa do consumidor … e da qual o consumidor não aufere benefício] (ESTADOS UNIDOS, 1978, 15 U.S.C. § 1693a(12); CFPB, 2011, 12 CFR § 1005.2(m)). Em termos práticos, a restituição tende a ser objetiva quando terceiro inicia a transferência, ao passo que, nos golpes em que o próprio consumidor autoriza o envio por indução, o reembolso não é automaticamente exigido e, na prática, costuma depender de demonstração de descumprimento contratual/regulatório pela instituição (CFPB, 2011, 12 CFR § 1005.2(m)).

Na União Europeia, a legislação é mais uniformemente protetiva e preventiva. A PSD2 determina a aplicação de autenticação forte do cliente (SCA) “where the payer … initiates an electronic payment transaction” [quando o pagador … inicia uma transação de pagamento eletrônica], reforçando barreiras ex-ante contra fraude (UNIÃO EUROPEIA, 2015, art. 97). Em 2024, o Regulamento (UE) 2024/886 incorporou a verificação do beneficiário (verification of the payee – VoP) no próprio texto legal, exigindo que o prestador do pagador “shall offer the payer a service

ensuring verification of the payee" [deverá oferecer ao pagador um serviço que assegure a verificação do beneficiário] antes da autorização, com alerta explícito quando houver divergência entre nome e IBAN, medida que previne erro direcionado e gera prova de aviso ao usuário (UNIÃO EUROPEIA, 2024). Em síntese, o eixo europeu combina SCA com VoP obrigatório, padronizando prevenção e melhorando a qualidade da prova de diligência exigida pelos bancos.

Esse contraste ajuda a compreender o lugar do Brasil. Aqui, o sistema combina responsabilidade objetiva (CDC, art. 14) com a orientação de que fraudes integradas ao risco do negócio configura fortuito interno. Conforme mencionado anteriormente, "as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno …" (Súmula 479/STJ), sem prejuízo de excludentes como culpa exclusiva e força maior. Ao observar experiências estrangeiras, vê-se que VoP obrigatório e critérios técnicos padronizados para prevenção e prova, tendem a reduzir litigiosidade e alinhar incentivos, permitindo que a atuação diligente dos bancos seja demonstrável e, por consequência, valorizada na solução de conflitos.

5 SOLUÇÕES E MELHORES PRÁTICAS

A constante evolução digital do setor bancário brasileiro tem desafiado às instituições financeiras a garantir a segurança de dados e transações em um ambiente cada vez mais vulnerável a fraudes e ataques cibernéticos. Como forma de enfrentar esse cenário, os bancos têm buscado implementar estratégias de mitigação de riscos, que envolvem desde investimentos em cibersegurança até a capacitação dos usuários quanto ao uso seguro dos serviços digitais.

Com base no artigo "Evolução digital do setor bancário e cibersegurança: desafios de segurança no setor financeiro e regulação", de Rodrigo Jheison Pontes Santos, publicado em 2024 pela Universidade Federal do Paraná (UFPR), é possível verificar algumas estratégias de mitigação de riscos pelas instituições financeiras, além da a importância da educação financeira e digital para os consumidores, verifica-se a necessidade das parcerias público-privadas no combate a fraudes bancárias e propostas de aprimoramento da legislação e regulamentação bancária.

Rodrigo menciona em seu artigo que “o ritmo de crescimento desses investimentos não tem acompanhado a escalada dos ataques cibernéticos” (SANTOS, Rodrigo Jheison Pontes, 2024), trazendo à tona a necessidade da regulação estatal na busca de promover um ambiente financeiro digital mais seguro e confiável.

Nesse contexto, a educação financeira e digital surge como ferramenta crucial para a prevenção de fraudes. É notório que muitos usuários não possuem conhecimento básico sobre como identificar as tentativas de fraude, o que demonstra a carência de programas de orientação ao consumidor, promovidos tanto por instituições financeiras quanto pelo poder público. É indispensável políticas voltadas à alfabetização digital, isso não apenas reduziria os riscos, como também fortaleceria a confiança no sistema financeiro.

Em contrapartida, existe a necessidade de manter e aprimorar as legislações e regulamentações bancárias, para que a proteção do consumidor se mantenha atualizada frente à inovação tecnológica. Se faz necessário incentivar investimentos mínimos obrigatórios em segurança digital por parte das instituições financeiras, assim como mecanismos mais ágeis de responsabilização e ressarcimento de consumidores lesados por falhas imputadas aos seus sistemas.

De modo complementar, recomenda-se a adoção da verificação do beneficiário (verification of the payee — VoP) no fluxo de transferências, especialmente no Pix, como camada de prevenção antes da autorização. Em termos práticos, o aplicativo do banco confere automaticamente se o nome ou a razão social do recebedor batem com o CPF, CNPJ ou chave pix informados e apresenta ao usuário um retorno objetivo, declarando se as informações prestadas conferem, quase conferem ou não conferem, exigindo confirmação adicional sempre que houver divergência.

Para o banco, o VoP reduz erro de digitação e conta-mula, gera prova de que o usuário foi notificado em relação a divergência e decidiu ou não prosseguir com a transação, além de alinhar a diligência com padrões internacionais de pagamentos instantâneos que tornam obrigatório oferecer esse serviço antes da autorização e notificar quando houver desacordo entre nome e conta. A implementação é tecnicamente viável com integração ao DICT (Diretório de Identificadores de Contas Transacionais), sem perda de fluidez para a maioria das transações.

Além disso, recomenda-se instituir um prazo claro para o tratamento de fraudes por indução (authorized push payment – APP), isto é, situações em que o próprio cliente autoriza a transferência porque foi enganado, diretamente no aplicativo do banco. Na prática, esse prazo inicia com triagem imediata, em que o motor de risco cruza indícios combinados, por exemplo, primeiro pagamento para aquele recebedor, um valor fora do padrão do cliente ou até mesmo um dispositivo recém-vinculado, para decidir, se necessário, o bloqueio cautelar na instituição do recebedor por até 72 horas, já prevista no ecossistema do Pix. Necessário que exista uma comunicação clara e eficiente, com uma resposta inicial em até 48 horas e, havendo elementos, aciona o MED (Mecanismo Especial de Devolução), procedimento padronizado do Pix para viabilizar a recuperação de valores em suspeita de fraude, com cooperação entre as instituições envolvidas. Sendo o caso elegível, o banco concede crédito provisório para amparar o consumidor enquanto a apuração se conclui, visando a resolução em até 5 dias úteis; a referência para prazos curtos e compartilhamento de responsabilidades entre as pontas encontra paralelo em boas práticas internacionais sobre APP. Com isso, o arranjo ganha tempo para o antifraude atuar antes da liquidação definitiva, e oferece previsibilidade ao consumidor, reduzindo a litigiosidade sem sacrificar a fluidez das transações.

6 CONCLUSÃO

Respondendo de forma direta ao problema que orientou esta pesquisa — até que ponto as instituições financeiras são responsáveis pela segurança dos usuários em transações digitais —, os achados indicam que, à luz do Código de Defesa do Consumidor e do entendimento consolidado do STJ, as instituições respondem objetivamente pelos danos decorrentes de fortuito interno. Isso exige a adoção de programas de compliance e de controles antifraude compatíveis com o risco do empreendimento, com prevenção, detecção e resposta ágeis, além de canais eficazes de suporte e ressarcimento às vítimas.

Ao longo do presente trabalho, buscamos abordar e identificar a principal finalidade do papel das instituições financeiras na prevenção de golpes bancários digitais, com ênfase nas práticas de compliance e na responsabilização civil perante

os consumidores lesados pelas fraudes digitais. A partir da abordagem interdisciplinar entre o direito do consumidor, o direito digital e a regulação bancária atribuída pelo Banco Central, buscou-se compreender os deveres impostos às instituições financeiras diante do crescente cenário de crimes cibernéticos.

A pesquisa demonstrou que os golpes digitais, sobretudo aqueles relacionados à engenharia social, ao phishing, à clonagem de cartões, às fraudes no sistema Pix e à manipulação de dados sensíveis, têm se tornado cada vez mais sofisticados e inovadores, demonstrando que há um desafio contínuo para o sistema financeiro nacional. Esses crimes acabam afetando não apenas a esfera patrimonial dos consumidores, mas também abalam a confiança no uso das plataformas digitais bancárias e intensificam a exclusão financeira de parcelas mais vulneráveis da população.

No que se refere à esfera judicial, constatou-se que o ordenamento brasileiro, por meio do Código de Defesa do Consumidor (CDC), detém uma estrutura protetiva robusta ao imputar responsabilidade objetiva às instituições financeiras, com fundamento na teoria do risco do empreendimento. A falha na prestação do serviço, a ausência de mecanismos eficazes de segurança e a demora na resposta às fraudes configuram, em regra, elementos aptos a ensejar a reparação por danos materiais e morais.

Além disso, marcos regulatórios como o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e as normativas do Banco Central do Brasil reforçam a necessidade de as instituições adotarem políticas eficazes de governança, proteção de dados, monitoramento de transações suspeitas e educação do consumidor. Nesse contexto, o compliance se apresenta como instrumento essencial para garantir a aderência a essas exigências legais e normativas, mitigando riscos operacionais e promovendo a integridade institucional.

Todavia, apesar de todo o normativo existente, evidencia-se, na prática, uma lacuna entre o que está previsto em lei e a efetiva aplicação de medidas preventivas pelas instituições financeiras. O volume crescente de ações judiciais envolvendo fraudes bancárias revela a persistência de falhas nos sistemas de segurança e no

atendimento às vítimas, sinalizando a necessidade de maior comprometimento por parte dos agentes financeiros.

Nessa linha, mostra-se essencial avançar de um enfoque apenas reparatório para um desenho integrado de prevenção e resposta. Em termos práticos, a experiência recente indica boa efetividade da verificação do beneficiário antes da autorização da transferência, conferindo se o nome do recebedor corresponde ao identificador informado e alertando o usuário quando houver divergência. Esse cuidado, simples e objetivo, reduz erros de direcionamento, desencoraja o uso de contas de passagem e fortalece a prova de diligência do atendimento, uma vez que a mensagem exibida e a confirmação do cliente ficam registradas de forma auditável.

Por fim, a eficácia de qualquer arranjo técnico depende de educação financeira e digital contínua. Campanhas permanentes, linguagem acessível e orientação prática no próprio canal de atendimento aumentam a capacidade do usuário de reconhecer tentativas de golpe e acionar os caminhos corretos de suporte. Nesse esforço, a UniSociesc mantém atendimento jurídico gratuito à comunidade por meio do Núcleo de Práticas Jurídicas (NPJ), espaço apropriado para educação digital do consumidor, acolhimento a vítimas de golpes e encaminhamento de medidas de ressarcimento A aproximação entre instituições financeiras, poder público e universidade contribui para transformar recomendações deste trabalho em benefícios concretos para a comunidade, sem perder de vista a melhoria contínua de processos internos e a formação de uma cultura de segurança.

Dessa forma, conclui-se que o enfrentamento dos golpes bancários digitais exige mais do que a responsabilização posterior: requer atuação preventiva imediata e eficiente, pautada por investimentos contínuos em tecnologia, programas de integridade e treinamentos específicos voltados à detecção e à prevenção de fraudes. Também é fundamental estimular uma cultura de educação digital entre os consumidores, especialmente os mais vulneráveis, ao lado de atendimento célere e mecanismos de ressarcimento capazes de restabelecer a confiança no sistema financeiro.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. **LGPD e compliance bancário.** Revista Científica PCI, 2022. Disponível em: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/. Acesso em: 20 abr. 2025.

ATHENIENSE, A. **Fraudes bancárias: o impacto econômico das ameaças digitais.** São Paulo: Editora do Direito, 2021.

BARROS, F. L. **A segurança das transações digitais no Brasil: uma análise sobre a clonagem de cartões.** São Paulo: Editora Econômica, 2021.

BRASIL. Banco Central do Brasil. **Resolução nº 4.595/2017. Dispõe sobre a política de conformidade (compliance) das instituições financeiras.** Brasília, 2017. Disponível em: https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50427/Res_4595_v1_O.pdf. Acesso em: 20 abr. 2025.

BRASIL. Banco Central do Brasil. **O que é e como funciona o bloqueio cautelar do Pix?** Brasília, 2025a. Disponível em: https://www.bcb.gov.br/meubc/faqs/p/o-que-e-e-como-funciona-o-bloqueio-cautelar. Acesso em: 12 nov. 2025.

BRASIL. Banco Central do Brasil. **BC aprimora o Mecanismo Especial de Devolução do Pix (MED).** Brasília, 2025b. Disponível em: https://www.bcb.gov.br/detalhenoticia/20817/nota. Acesso em: 12 nov. 2025.

BRASIL. Governo Federal. **Engenharia social: como aspectos psicológicos podem se relacionar com golpes e fraudes.** Disponível em: https://www.gov.br/investidor/pt-br/penso-logo-invisto/engenharia-social-como-aspectos-psicologicos-podem-se-relacionar-com-golpes-e-fraudes-1. Acesso em: 22 mar. 2025.

BRASIL. Superior Tribunal de Justiça. **Súmula n. 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.** Brasília, DF, 2015. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Jurisprudencia/Sumulas/Sumula-479.aspx. Acesso em: 20 abr. 2025.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT). **O sigilo dos dados bancários e as particularidades para o acesso de informações protegidas.** Disponível em:

https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/direito-constitucional/o-sigilo-dos-dados-bancarios-e-as-particularidades-para-o-acesso-de-informacoes-protegidas. Acesso em: 20 abr. 2025.

CLEARSALE. **Segurança cibernética no setor financeiro: como proteger seu negócio.** Disponível em: https://br.clear.sale/blog/seguranca-cibernetica-no-setor-financeiro-como-proteger-seu-negocio?. Acesso em: 22 mar. 2025.

ESTADÃO. **Fraudes no cartão de crédito.** Disponível em: https://economia.estadao.com.br/noticias/geral,como-proteger-se-de-fraudes-com-cartoes-de-credito. Acesso em: 22 mar. 2025.

ESTADOS UNIDOS. Consumer Financial Protection Bureau. **Electronic Fund Transfers (EFTA/Regulation E) — FAQs.** Washington, D.C., 2025. Disponível em: https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/. Acesso em: 12 out. 2025.

ESTADOS UNIDOS. **Electronic Code of Federal Regulations (eCFR). 12 CFR § 1005.2 — Definitions (Regulation E), alínea (m) (Unauthorized electronic fund transfer).** Washington, D.C.: Office of the Federal Register/CFPB, 2011 (atual.). Disponível em: https://www.ecfr.gov/current/title-12/chapter-X/part-1005/subpart-A/section-1005.2. Acesso em: 12 out. 2025.

ESTADOS UNIDOS. **Electronic Fund Transfer Act (EFTA). 15 U.S.C. § 1693a(12) — Definitions (unauthorized electronic fund transfer).** Washington, D.C.: U.S. Congress, 1978 (com alterações). Disponível em: https://www.law.cornell.edu/uscode/text/15/1693a. Acesso em: 12 out. 2025.

GASA. **1 in 3 Brazilians targeted by scammers in 2024: State of Scam Report.** 2024. Disponível em: https://www.gasa.org/post/1-in-3-brazilians-targeted-by-scammers-in-2024-state-of-scam-report. Acesso em: 22 mar. 2025.

KASPERSKY. **O que é engenharia social? Definição.** Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering. Acesso em: 22 mar. 2025.

LIMA, P. T. **Fraudes bancárias digitais e o sistema de pagamentos no Brasil.** São Paulo: Editora Digital, 2022.

OLIVEIRA SILVA, R.; COSTA, A. **Fraudes bancárias digitais e o papel das instituições financeiras na prevenção.** Revista Jurídica, v. 35, n. 2, 2021. Disponível em: https://www.revistajuridica.com.br. Acesso em: 20 abr. 2025.

REINO UNIDO. Payment Systems Regulator. **PS24/7 — Faster Payments APP scams reimbursement requirement: confirming the maximum level of reimbursement.** Londres, 2024. Disponível em: https://www.psr.org.uk/media/e30pwlly/ps24-7-app-scams-maximum-level-of-reimbursement-policy-statement-oct-2024.pdf. Acesso em: 12 nov. 2025.

SANTOS, Rodrigo Jheison Pontes. **Evolução digital do setor bancário e cibersegurança: desafios de segurança no setor financeiro e regulação.** 2024. TCC – Universidade Federal do Paraná, Curitiba. Disponível em: https://acervodigital.ufpr.br/xmlui/handle/1884/94374. Acesso em: 20 abr. 2025.

SILVERFORT. **O que é conformidade com a segurança cibernética?** Disponível em: https://www.silverfort.com/pt/glossary/cyber-security-compliance/. Acesso em: 22 mar. 2025.

UNIÃO EUROPEIA. **Diretiva (UE) 2015/2366 (PSD2), de 25 de novembro de 2015. Art. 97 (Strong Customer Authentication).** Jornal Oficial da União Europeia, 23 dez. 2015. Disponível em: https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng. Acesso em: 12 out. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/886, de 13 de março de 2024 (transferências a crédito imediatas em euros).** Seção “Verification of the payee in the case of credit transfers”, p. 12. Jornal Oficial da União Europeia, L 2024/886, 19 mar. 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/886/oj/eng/pdf. Acesso em: 12 out. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/886, de 13 de março de 2024 — transferências a crédito imediatas em euros (verificação do beneficiário).** Bruxelas: Parlamento Europeu/Conselho, 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/886/oj/eng. Acesso em: 12 nov. 2025.

VALOR ECONÔMICO. **Bancos destinam bilhões para aprimorar dados, compliance, segurança e experiência do cliente.** Disponível em: https://valor.globo.com/patrocinado/dino/noticia/2024/06/18/setor-financeiro-investe-bilhoes-em-compliance-em-2024.ghtml?. Acesso em: 22 mar. 2025.