FUNDAÇÃO UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL
CAMPUS DE NAVIRAÍ - CPNV
CURSO DE ADMINISTRAÇÃO

EWELLYN FERNANDA MOURA WUST

TRABALHO DE CONCLUSÃO DE CURSO

FRAUDES E GOLPES BANCÁRIOS NO BRASIL: Tipologia e Iniciativas das Instituições Financeiras

Orientador: Prof. Dr. Victor Fraile Sordi

Naviraí-MS

2023

FRAUDES E GOLPES BANCÁRIOS NO BRASIL: Tipologia e Iniciativas das Instituições Financeiras

Ewellyn Fernanda Moura Wust

RESUMO

No contexto bancário brasileiro, a proteção contra golpes e fraudes tem sido uma prioridade, refletida nas iniciativas das principais instituições financeiras. No entanto, ao analisar essas medidas, percebe-se que são vulneráveis diante da crescente sofisticação dos golpes. Este estudo visa identificar os principais tipos de fraudes e golpes bancários praticados no Brasil, adotando uma abordagem exploratória qualitativa. A pesquisa utiliza dados do STJ (2023), analisando 138 processos relacionados a fraudes bancárias. Os resultados revelam diversas táticas, desde fraudes cibernéticas até golpes diretos. As instituições financeiras desempenham um papel crucial na prevenção dessas fraudes, mas é evidente a necessidade de medidas mais abrangentes e adaptáveis. A confiança do cliente é fundamental, e os danos financeiros podem afetar a continuidade do uso de serviços financeiros online. Recomenda-se aprimorar a segurança cibernética, investir em educação financeira e fortalecer a colaboração entre instituições, reguladores e órgãos governamentais. Este estudo contribui para a compreensão das fraudes bancárias no Brasil, destacando a importância contínua de medidas proativas para manter a confiança no sistema financeiro.

Palavras-chave: Fraudes Bancárias; Responsabilidade Civil; Engenharia Social; Medidas de Prevenção; Confiança Bancária.

1 INTRODUÇÃO

A cada ano, à medida que a tecnologia avança, a complexidade dos golpes aplicados aumenta, resultando em danos para um número cada vez maior de pessoas. De acordo com uma pesquisa da Confederação Nacional de Dirigentes Lojistas (CNDL) e do Serviço de Proteção ao Crédito (SPC Brasil), 46% dos internautas brasileiros foram vítimas de algum tipo de golpe financeiro nos 12 meses anteriores ao estudo, o que equivale a mais de 12 milhões de pessoas (BACEN, 2020).

Esses crimes financeiros vêm sendo uma preocupação crescente para as instituições financeiras e seus clientes, uma vez que podem resultar em danos financeiros significativos, perda de dados pessoais sensíveis e outros impactos negativos.

As instituições financeiras desempenham um papel crucial na sociedade, uma vez que são responsáveis pela guarda e movimentação do dinheiro de milhões de pessoas e empresas. Como citado por Rezende (2010, p.77) “apesar dos imensos benefícios e conveniências trazidos pelo uso da internet na prestação de serviços, a vulnerabilidade (...) e a complexidade das relações que lhe são admitidas, possibilitam a perpetração de inúmeras fraudes”.

A importância da confiança nas instituições bancárias se torna evidente na prestação de serviços bancários por meio do 'internet banking', uma vez que as transações, como regra, envolvem movimentação de dinheiro. Conforme apontado por Rezende (2010), as tentativas frequentes de fraudes visando a apropriação indevida ou desvio de numerário dos correntistas indicam que a confiança nas instituições financeiras é fundamental para o funcionamento saudável da economia. No entanto, quando fraudes e golpes ocorrem, essa confiança é abalada, deixando os clientes em situações financeiras precárias e com sérios questionamentos sobre quem deve arcar com as perdas.

Nesse contexto, este trabalho se propõe a identificar os principais tipos de fraudes e golpes bancários praticados no Brasil. Serão examinadas também as medidas que as instituições financeiras têm adotado para proteger seus clientes e garantir a integridade do sistema financeiro.

Por meio de uma análise aprofundada, este trabalho busca contribuir para uma compreensão mais clara das tipologias de fraudes bancárias e o que as instituições têm feito para se proteger e proteger seus correntistas, bem como para o desenvolvimento de políticas e estratégias mais eficazes na prevenção e reparação desses incidentes. A segurança e a confiança no sistema bancário são valores fundamentais que devem ser protegidos e promovidos, e este estudo busca lançar luz sobre como isso pode ser alcançado em um mundo cada vez mais digital e interconectado.

2 REVISÃO DA LITERATURA

À medida que a sociedade se torna cada vez mais dependente da tecnologia da

informação, os golpes que adotam a técnica da engenharia social tendem a crescer de forma contínua, constituindo-se em uma das principais ameaças aos sistemas de segurança da informação (MONTEIRO, 2022, p.48). Essa crescente dependência da tecnologia tem levado a um aumento alarmante nas violações de contas correntes, especialmente quando os correntistas realizam transações por meio da internet (REZENDE, 2010, p.77).

Neste contexto, é fundamental compreender a questão da responsabilidade dos bancos quando se trata dessas violações. À medida que os ataques cibernéticos continuam a evoluir, surge a necessidade de definir claramente as responsabilidades das instituições financeiras e dos consumidores.

> Através dos elementos constitutivos da responsabilidade civil, as excludentes de ilicitude, e até mesmo suas espécies, é possível identificar aquele que deve ser responsabilizado pelos danos causados, que nem sempre, será aquele que praticou diretamente o ilícito (PEREIRA, 2020, p. 118).

As instituições financeiras estão sujeitas ao risco operacional devido às fraudes. Em resposta a esse risco, o Banco Central do Brasil, por meio da Resolução BACEN 3380/2008, exige que os bancos implementem um sistema de gerenciamento de risco operacional para lidar com fraudes e eventos semelhantes. Esse sistema tem o objetivo de identificar, avaliar, monitorar, controlar e reduzir tais riscos operacionais. "A jurisprudência inclusive já vem fazendo recurso de normas do Código de Defesa do Consumidor (CDC) quando se trata de definir a responsabilidade dos bancos em matéria de fraudes eletrônicas" (REINALDO FILHO, 2006, n.p).

Neste sentido, esta revisão irá abordar (a) as principais fraudes e golpes bancários praticados no Brasil e, também, (b) as responsabilidades das instituições financeiras neste contexto.

2.1 As fraudes e golpes bancários no Brasil

Entre as ameaças mais comuns que têm afetado as instituições financeiras e seus clientes, encontram-se os golpes bancários, com diversas técnicas prejudiciais. Neste contexto, destacam-se duas abordagens insidiosas: (1) *Phishing* e (2) *Pharming*. Cada uma dessas táticas tem como alvo a confiança dos usuários, explorando sua falta de conhecimento ou até mesmo seu comportamento ingênuo.

(1) ***Phishing***

Segundo Monteiro (2022, p.16) "*Phishing* trata-se de um tipo de ataque da engenharia social de grande potencial nocivo, sendo provavelmente a forma mais comum dentre todas as modalidades de ataque cibernético".

> A primeira etapa do *phishing* consiste na apropriação de informações de outra pessoa (como nome, informações de conta e senha bancária), para serem utilizadas fraudulentamente nas fases seguintes da trama (transferências de numerários de contas correntes e aplicações financeiras). É um ato de "impersonificação" (numa incorporação para o português do termo inglês impersonation), consistente na apropriação de informações pessoais do cliente do banco com finalidades ilegais. O criminoso se apodera da informação de outra pessoa, sem o conhecimento desta, que é enganada de forma fraudulenta (REINALDO FILHO, 2006, n.p).

(2) ***Pharming***

Monteiro (2022, p.18) afirma que "nesse tipo de golpe, mesmo que o usuário digite em seu navegador o caminho correto do site da instituição financeira, ele é automaticamente redirecionado para outro site fraudulento".

> O *pharming* opera pelo mesmo princípio do *phishing*, ou seja, fazendo os internautas pensarem que estão acessando um site legítimo, quando na verdade não estão. Mas ao contrário do *phishing*, o qual uma pessoa mais atenta pode evitar simplesmente não respondendo ao e-mail fraudulento, o *pharming* é praticamente impossível de ser detectado por um usuário comum da Internet, que não tenha maiores conhecimentos técnicos. Nesse novo tipo de fraude, os agentes criminosos se valem da disseminação de softwares maliciosos que alteram o funcionamento do programa de navegação (browser) da vítima. Quando esta tenta acessar um site de um banco, por exemplo, o navegador infectado a redireciona para o spoof site (o site falso com as mesmas características gráficas do site verdadeiro). No site falseado, então, ocorre a coleta das informações privadas e sensíveis da vítima, tais como números de cartões de crédito, contas bancárias e senhas. (REINALDO FILHO, 2006, n.p).

Desta forma a FEBRABAN (2021) listou alguns dos principais golpes sofridos pelos correntistas:

(a) **Falso Link (*Phishing*):** O *phishing,* ou pescaria digital, é uma fraude eletrônica cometida pelos fraudadores (engenheiros sociais) que visa obter as senhas e dados pessoais do usuário. A forma mais comum de um ataque de *phishing* são as mensagens em e-mails, SMS, aplicativos de mensagens como WhatsApp, redes sociais que induzem o usuário a clicar em links maliciosos. Também existem páginas falsas na internet que induzem a pessoa a revelar as senhas e dados pessoais. Os casos mais comuns de *phishing* são e-mails recebidos de supostos bancos com mensagens que afirmam que a conta do cliente está irregular, ou o cartão ultrapassou o limite, atualização de token ou ainda que existe um novo software de segurança do banco que precisa ser instalado imediatamente pelo usuário.

(b) **Clonagem do WhatsApp:** Os golpistas descobrem o número do celular e o nome da vítima de quem pretendem clonar a conta de WhatsApp. Com essas informações em mãos, os criminosos tentam cadastrar o WhatsApp da vítima nos aparelhos deles. Para concluir a operação, é preciso inserir o código de segurança que o aplicativo envia por SMS sempre que é instalado em um novo dispositivo. Os fraudadores enviam uma mensagem pelo WhatsApp fingindo ser do Serviço de Atendimento ao Cliente de bancos e instituições financeiras ou da empresa em que a vítima tem cadastro. Eles solicitam o código de segurança, que já foi enviado por SMS pelo aplicativo, afirmando se tratar de uma atualização, manutenção ou confirmação de cadastro. Com o código, os bandidos conseguem replicar a conta de WhatsApp em outro celular, tendo acesso a todo o histórico de conversas e contatos. A partir daí, os criminosos enviam mensagens para os contatos, passando-se pela pessoa, pedindo dinheiro emprestado.

(c) **Falso motoboy:** O golpe começa quando o cliente recebe uma ligação do golpista que se passa por funcionário do banco, dizendo que o cartão foi fraudado. O falso funcionário solicita a senha e pede que o cartão seja cortado, mas que o chip não seja danificado. Em seguida, diz que o cartão será retirado na casa do cliente. O outro golpista aparece onde a vítima está e retira o cartão. Mesmo com o cartão cortado, o chip está intacto e os fraudadores podem utilizá-lo para fazer transações e roubar o dinheiro da vítima.

(d) **Falsa Central de Atendimento:** O fraudador entra em contato com a vítima se passando por um falso funcionário do banco ou empresa com a qual ela tem um relacionamento ativo. Informa que sua conta foi invadida, clonada ou outro problema

e, a partir daí, solicita os dados pessoais e financeiros da vítima. Em alguns casos, os golpistas até mesmo pedem para que a vítima ligue para central do banco, no número que aparece atrás do seu cartão, mas o fraudador continua na linha para simular o atendimento da central e pedir os dados da sua conta, dos seus cartões e, principalmente, a senha do correntista.

(e) Golpe da troca de cartão: Golpistas que trabalham como vendedores prestam atenção quando você digita sua senha na máquina de compra e depois trocam o cartão na hora de devolvê-lo. Com seu cartão e senha, fazem compras usando o seu dinheiro. O mesmo pode acontecer com desconhecidos oferecendo ajuda no caixa eletrônico. Eles se aproveitam de alguma dificuldade sua no terminal eletrônico para pegar rapidamente o seu cartão e depois devolver um que não é seu, ao mesmo tempo que espiam sua senha.

Além dos golpes indicados pela FEBRABAN, um tipo de fraude recorrente no setor financeiro, que foi mencionado por Oliveira (2012, p.17), são as "fraudes documentais que trata, por exemplo, de clonagem de cheques, falsa identidade, abertura de conta corrente com documento falso". As fraudes documentais se caracterizam pela adulteração e/ou falsificação de documentos bancários ou de identidade.

> As principais fraudes documentais podem ser separadas em seis grandes grupos: Fraude na Abertura de Conta; Cheques Clonados/Falsificados e Adulterados; Fraude em TEDs, DOCs, Ordens de Pagamento e Bloquetos de Cobrança; Fraude no Crédito Direto ao Consumidor; Fraude no Crédito Consignado e Fraude no Financiamento de Veículos (OLIVEIRA, 2012, p.34)

Ao abordar os desafios impostos pelos crimes cibernéticos, destaca-se a natureza intrínseca desses delitos, os quais dependem exclusivamente do suporte oferecido pelos sistemas informáticos. Nesse contexto, a violação do bem jurídico crucial, os dados, revela-se como uma faceta inescapável dessas práticas delituosas (SILVA, 2023, n.p).

Além disso, conforme ressaltado por Alcântara (2021), o estelionato, que envolve artimanhas fraudulentas para ludibriar a vítima e levá-la a ceder voluntariamente sua propriedade, representa um desafio adicional. As consequências dessas fraudes não se limitam a perdas financeiras substanciais para as instituições bancárias; elas também prejudicam a confiança dos clientes nos sistemas de pagamentos e transações online (REINALDO FILHO,

2006).

Essas considerações sublinham a urgência de estratégias abrangentes por parte das instituições financeiras no enfrentamento de golpes e fraudes. Na seção subsequente, exploraremos mais a fundo a responsabilidade dessas entidades nesse cenário, examinando como as leis e regulamentos, como o Código de Defesa do Consumidor, a Lei do Sigilo Bancário e a Lei Geral de Proteção de Dados, delineiam diretrizes claras. Além disso, será analisado o papel da Estratégia Nacional de Educação Financeira (ENEF) na promoção da conscientização e prevenção. Este exame minucioso é essencial para compreendermos as nuances desse desafio complexo e desenvolvermos abordagens eficazes que fortaleçam a resiliência do setor financeiro diante das ameaças emergentes.

2.2 A responsabilidade das instituições financeiras

As responsabilidades das instituições financeiras no Brasil em relação a golpes e fraudes são delineadas por um conjunto abrangente de leis e regulamentos. O Código de Defesa do Consumidor (Lei nº 8.078/1990) e a Lei nº 7.102/1983, que trata da segurança para estabelecimentos financeiros, estabelecem as bases regulatórias para a conduta dessas instituições (BRASIL, 1990).

A legislação se estende à esfera do sigilo bancário por meio da Lei Complementar nº 105/2001, que impõe regras específicas para a proteção das informações financeiras dos clientes. As instituições financeiras, conforme estipulado, devem implementar medidas de segurança cibernética, tais como criptografia de dados, autenticação de dois fatores e monitoramento de transações suspeitas, visando salvaguardar as informações e os ativos dos clientes (BRASIL, 2001).

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) reforça as responsabilidades das instituições financeiras ao exigir a adoção de medidas específicas para detectar e prevenir fraudes. Essas medidas incluem a implementação de sistemas de detecção de fraude e a análise de transações incomuns, com o objetivo de identificar atividades suspeitas (BRASIL, 2018).

Paralelamente às leis, a Estratégia Nacional de Educação Financeira (ENEF) representa uma iniciativa governamental crucial para promover a educação financeira da população. Embora não seja uma legislação formal, a ENEF insta as instituições financeiras a

desempenhar um papel ativo na educação de seus clientes sobre práticas seguras no uso de serviços financeiros, incluindo a divulgação de informações sobre tipos de golpes comuns e estratégias de prevenção (BACEN, 2010).

Além disso, o Código de Defesa do Consumidor, estabelecido pela Lei nº 8.078/1990, complementa o arcabouço legal ao definir diretrizes gerais para a proteção dos direitos do consumidor no Brasil. Em casos de clientes sendo vítimas de golpes ou fraudes, as instituições financeiras são obrigadas a fornecer canais eficientes de atendimento ao cliente para relatar problemas e obter assistência na resolução dos mesmos (BRASIL, 1990). Este conjunto interligado de regulamentações e iniciativas destaca a complexidade do cenário regulatório e a necessidade de uma abordagem holística na proteção dos consumidores e na prevenção de atividades fraudulentas.

Diante da extensa legislação que regula as responsabilidades das instituições financeiras em relação a golpes e fraudes no Brasil, é evidente que o ambiente jurídico delineia parâmetros claros para a atuação dessas entidades na proteção dos interesses e direitos dos consumidores. A abrangência das leis, como o Código de Defesa do Consumidor, a Lei do Sigilo Bancário, e a Lei Geral de Proteção de Dados, evidencia a complexidade e a constante evolução das demandas relacionadas à segurança financeira.

Além disso, a Estratégia Nacional de Educação Financeira (ENEF) destaca-se como uma importante iniciativa governamental que, embora não imponha obrigações legais, desempenha um papel crucial na promoção da educação financeira da população. Nesse contexto, as instituições financeiras não apenas devem aderir às normas estabelecidas, mas também são incentivadas a desempenhar um papel ativo na educação dos clientes, divulgando informações sobre golpes comuns e práticas seguras. A conjunção dessas regulamentações forma um arcabouço robusto que não apenas delimita as responsabilidades das instituições financeiras, mas também busca construir um ecossistema financeiro mais seguro e esclarecido para todos os envolvidos.

3 METODOLOGIA

Este estudo se propõe a identificar os principais tipos de fraudes e golpes bancários praticados no Brasil. Por meio de uma pesquisa exploratória qualitativa, busca-se compreender essas práticas fraudulentas, observando também o que as instituições financeiras

estão fazendo para mitigar tal fenômeno.

De acordo com Fontelles (2009), uma pesquisa exploratória tem por objetivo primordial permitir que o pesquisador se familiarize com o tema, compreendendo os fatos e fenômenos relacionados ao problema em estudo. Durante a investigação, o pesquisador busca obter informações que não apenas revelam a existência de uma relação, mas, acima de tudo, que ajudem a compreender o seu tipo. No presente trabalho, iremos abordar o assunto sob a metodologia da pesquisa exploratória com viés qualitativo.

Para Godoy (1995) uma pesquisa qualitativa possui alguns aspectos essenciais: (1) preocupação fundamental com o estudo e a análise do mundo empírico em seu ambiente natural; (2) fonte direta de dados e o pesquisador; (3) anotações de dados; (3) descrição; (4) análise e interpretação dos dados coletados.

Utilizou-se os dados disponíveis na base do STJ (2023), "Jurisprudência do STJ", com processos que constem o termo "fraudes bancárias". A busca na base com o termo descrito, foi feita no dia 26/10/2023, obtendo 138 processos.

Os processos judiciais foram analisados quantitativamente e qualitativamente, buscando-se abordar as evidências sobre quais tipos de fraudes ocorreram e de que modo ocorreram para que tais dados pudessem ser categorizados e contabilizados. Na Tabela 1 apresenta-se a disposição quantitativa dos tipos de fraudes disponíveis na amostra.

Tabela 1: Quantitativo de Fraudes na Base do STJ

TIPO GOLPE OU FRAUDE	QUANTIDADE
Fraudes documentais	62
Golpe link falso	31
Golpe da troca de cartão	8
Estelionato	9
Vazamento de dados	4
Golpe do boleto	3

Falso motoboy	3
Não classificados para a pesquisa	18
Total	138

Fonte: STJ (2023).

Os casos foram examinados individualmente a fim de identificar a natureza dos golpes e fraudes presentes na amostra, assim como seu *modus operandi*. Os resultados são apresentados e discutidos na seção seguinte.

4 DISCUSSÃO E ANÁLISE DOS DADOS

Os dados coletados e analisados revelaram oito tipologias de fraudes. Em uma busca posterior, encontrou-se em sites e portais institucionais algumas medidas de segurança para evitar cada um desses oito tipos de golpes. Em complemento, coletou-se nos portais das instituições que compõem a lista das 10 instituições financeiras do país com mais reclamações reguladas como procedentes no Banco Central do Brasil (BSB, 2023), o que essas instituições estão fazendo para mitigar essas fraudes e golpes.

4.1 As principais fraudes e medidas preventivas

Fraudes documentais representam a maioria dos casos identificados, apontando para a exploração da falta de segurança nos processos de autenticação e verificação de identidade. Esses golpes, como a abertura de contas falsas em nome de vítimas, indicam a necessidade de medidas preventivas. O Serasa Experian (2023) destaca a importância de salvaguardar documentos, evitar o compartilhamento de dados pessoais e adotar práticas seguras, como guardar documentos em locais seguros para prevenir roubos.

Outro tipo frequente são os golpes de phishing e ataques de engenharia social, evidenciados pelos casos relacionados à links falsos. O Santander (2023) sugere estratégias de proteção, incluindo a verificação do endereço de e-mail do remetente, a confirmação da camada de segurança do site e a desconfiança de solicitações de dados sigilosos.

Os golpes que envolvem a troca de cartões são uma tática prejudicial, muitas vezes

perpetrada por criminosos disfarçados. O C6BANK (2023) orienta a atenção durante as transações financeiras, recomendando a verificação do valor na maquininha, o próprio uso do cartão na máquina e a cobertura da senha para evitar a visualização por terceiros.

O estelionato, um clássico golpe de engano para obter ganho financeiro, é uma ameaça de complexidade variada. O Banco do Brasil (2023) sugere a busca imediata de contato com a instituição financeira em casos de estelionato, destacando a importância de redefinir senhas e ativar a autenticação de dois fatores.

Os vazamentos de dados, indicados por quatro casos, revelam a sofisticação crescente dos ataques cibernéticos. O G1 (2023) propõe medidas preventivas, como a verificação do endereço do site, o uso de cartão virtual e a criação de senhas fortes.

Embora em menor número, os golpes envolvendo boletos mostram a exploração de vulnerabilidades nos processos de pagamento. O Serasa Premium (2019) aconselha a verificação do código de barras, a confirmação da fonte do boleto e a atenção aos dados, destacando a importância de observar erros de português e a coerência dos valores.

Finalmente, a fraude do falso motoboy destaca-se por sua natureza invasiva, com fraudadores se passando por funcionários de bancos para enganar as vítimas. O Banco do Brasil (2023) alerta sobre a não solicitação do cartão de volta pelos bancos e orienta os clientes a entrarem em contato pelos números oficiais em caso de dúvidas. Este panorama abrangente de fraudes e as estratégias sugeridas para prevenção enfatizam a importância das instituições financeiras em adotar medidas proativas para proteger seus clientes contra uma variedade de ameaças.

Houveram também casos com status “Não Classificados para a Pesquisa” que não puderam ser classificados. Os casos não classificados dizem respeito à falta de informações suficientes nos acórdãos. Alguns acórdãos não apresentavam informações essenciais para a classificação dos casos, como a descrição da conduta fraudulenta.

Esses dados revelam uma variedade de estratégias utilizadas por fraudadores, desde fraudes cibernéticas, como *phishing*, até golpes que envolvem a interação direta com as vítimas (engenharia social), como o golpe do falso motoboy. É evidente que os fraudadores estão constantemente adaptando e inovando suas táticas para explorar as vulnerabilidades nos sistemas de segurança das instituições financeiras e a ingenuidade dos clientes. No Quadro 1,

elenca-se as principais medidas de segurança indicadas para coibir essas fraudes e golpes.

Quadro 1: Tipos de Fraudes e Medidas de Segurança Recomendadas

Tipos de Fraudes	**Medidas de Segurança Recomendadas**
Fraudes Documentais	- Salvaguardar documentos em locais seguros para prevenir roubos. - Evitar o compartilhamento de dados pessoais.
Golpes de Phishing e Links Falsos	- Verificar o endereço de e-mail do remetente. - Confirmar a camada de segurança do site. - Desconfiar de solicitações de dados sigilosos.
Golpes com Troca de Cartões	- Verificar o valor na maquininha durante transações financeiras. - Passe o cartão você mesmo na máquina. - Cobrir a senha para evitar visualização por terceiros.
Estelionato	- Buscar contato imediato com a instituição financeira em casos de estelionato. - Redefinir senhas e ativar autenticação de dois fatores.
Vazamentos de Dados	- Verificar o endereço do site. - Utilizar cartão virtual para transações online. - Criar senhas fortes.
Golpes com Boletos	- Verificar o código de barras e sua consistência. - Confirmar a fonte do boleto. - Observar erros de português e a coerência dos valores. - Prestar atenção aos dados do boleto, como CNPJ e nome do beneficiário.
Fraude do Falso Motoboy	- Não entregar o cartão mesmo se cortado. - Entrar em contato pelos números oficiais em caso

	de dúvidas sobre solicitação de cartão.

Fonte: Elaborado pela autora (2023).

Essa análise dos tipos de golpes e fraudes fornece informações valiosas que podem ser usadas para o desenvolvimento de estratégias mais eficazes de prevenção e educação financeira. Ela também destaca a importância de as instituições financeiras continuarem aprimorando suas medidas de segurança cibernética e de autenticação, bem como de os clientes se tornarem mais conscientes das ameaças e saber como se proteger.

4.2 Iniciativas das instituições brasileiras para proteger os clientes desses golpes

No quadro 2, observa-se a lista com as 10 instituições financeiras brasileiras com mais reclamações reguladas como procedentes pelo Banco Central do Brasil em 2023. Avaliou-se os portais dessas instituições acerca de possíveis materiais ou ações que visassem proteger os seus clientes dos golpes e fraudes supracitados.

Quadro 2: Top 10 Reclamações reguladas procedentes BSB 2023

Posição	Banco	Portais Avaliados	Ações/Materiais
1º	BTG Pactual/Banco PAN	https://ri.bancopan.com.br/ e https://www.btgpactual.com/	1. Cartilha com dicas 2. Manual do usuário
2º	Bradesco	https://banco.bradesco/html/classic/index.shtm	1. Cartilha com dicas de segurança 2. campanha “Olha A Cilada – Antifraude”, que aborda os principais tipos de golpes e fraudes sofridos pelos clientes.
3º	Inter	https://inter.co/	1. Cartilha com dicas de segurança; 2. Adoção do IBM Safer Payments. A solução

			utiliza uma abordagem de computação cognitiva, em que une inteligência artificial e aprendizado de máquina para analisar padrões de comportamento fraudulentos.
4º	PagBank-PagSeguro	https://pagseguro.uol.com.br/	1. Cartilha com dicas de segurança
5º	C6 Bank	https://www.c6bank.com.br/	1. Cartilha com dicas de segurança; 2. Recursos de segurança, permite ocultar saldo de investimentos ao acessar app fora de casa.
6º	Santander	https://www.santander.com.br/	1. Cartilha com dicas de segurança 2. Adoção da nova solução SAS na prevenção a Fraude e de Inteligência Analítica.
7º	Itaú	https://www.itau.com.br/	1. Cartilha com dicas de segurança; 2. Campanha “Itaú e você contra golpes e fraudes” o objetivo é alertar para o fato de que ninguém está livre das tentativas de fraudes bancárias.

8º	Original	https://www.original.com.br/	1. Cartilha com dicas de segurança
9º	Neon	https://neon.com.br/	1. Cartilha com dicas de segurança
10º	Caixa Econômica Federal	https://www.caixa.gov.br/Paginas/home-caixa.aspx	1. Cartilha com dicas de segurança 2. Utiliza o software CPqD Antifraude, solução de monitoramento, prevenção e tratamento de incidentes.

Fonte: Elaborado pela autora com base em BSB (2023).

No cenário brasileiro de instituições financeiras, a proteção dos clientes contra golpes e fraudes tem sido uma prioridade evidente, como refletido nas iniciativas destacadas pelas 10 principais instituições financeiras listadas no Quadro 2. No entanto, ao avaliar os portais dessas instituições em busca de materiais ou ações voltadas para a segurança dos clientes, é possível observar que, apesar dos esforços empreendidos, tais iniciativas ainda se mostram frágeis diante da sofisticação e diversificação dos golpes.

A presença de cartilhas com dicas de segurança é comum entre essas instituições, mas a persistência das reclamações reguladas procedentes indica que a eficácia dessas medidas pode ser limitada. A complexidade dos golpes atuais requer uma abordagem mais abrangente e adaptável, considerando a rápida evolução das táticas utilizadas pelos fraudadores.

Nesse contexto, torna-se crucial reconhecer a importância da educação dos clientes como uma camada adicional de proteção. Além de depender das medidas adotadas pelas instituições, os clientes precisam estar equipados com conhecimentos sólidos sobre práticas seguras e atualizados sobre os riscos emergentes, fortalecendo, assim, a defesa contra ameaças virtuais.

5 CONCLUSÕES

O objetivo primordial deste estudo foi identificar e analisar os principais tipos de

fraudes e golpes bancários praticados no Brasil, bem como avaliar as medidas adotadas pelas instituições financeiras para proteger seus clientes e garantir a integridade do sistema financeiro. No decorrer deste trabalho, alguns resultados significativos foram alcançados.

Os dados coletados revelaram uma ampla diversidade de táticas empregadas por fraudadores. As fraudes vão desde fraudes cibernéticas, como *phishing* e *pharming*, até golpes que envolvem interações diretas com as vítimas, como o golpe do falso motoboy e a troca de cartões.

Os dados evidenciam a importância crucial das instituições financeiras na proteção de seus clientes contra essas ameaças. As instituições financeiras desempenham um papel crítico na manutenção da confiança de seus clientes em seus serviços e na prevenção de fraudes. Os resultados da pesquisa destacaram que as instituições financeiras devem continuar aprimorando e evoluindo suas medidas de segurança para fazer frente às estratégias em constante mudança dos fraudadores.

Cada tipologia de fraude encontrada tem o potencial de minar a confiança dos clientes nas instituições financeiras. Os danos financeiros e a exposição de informações pessoais sensíveis podem deixar os clientes desconfiados e relutantes em continuar a utilizar serviços financeiros online. Portanto, é fundamental que as instituições financeiras não apenas previnam fraudes, mas também ajam prontamente para restaurar a confiança dos clientes e garantir um ambiente seguro.

Os resultados obtidos neste estudo têm implicações significativas. Além de aumentar a compreensão das tipologias de fraudes bancárias, eles destacam a necessidade de aprimorar medidas de segurança cibernética, investir em educação financeira e promover a colaboração entre instituições financeiras, reguladores e órgãos governamentais para combater eficazmente as fraudes bancárias.

No entanto, é importante reconhecer algumas limitações desta pesquisa. A análise se baseou em dados disponíveis na base do STJ e pode não capturar todas as nuances das fraudes bancárias. Além disso, a pesquisa não avaliou a eficácia das medidas de segurança das instituições financeiras, que poderia ser um tópico importante para futuras pesquisas.

Como sugestão para futuras pesquisas, recomenda-se a avaliação da eficácia das medidas de segurança cibernética adotadas pelas instituições financeiras, bem como a análise

de como as leis e regulamentos atuais abordam casos de fraudes bancárias. Além disso, investigar como a colaboração e o compartilhamento de informações entre instituições financeiras, reguladores e órgãos governamentais podem ser aprimorados para uma resposta mais eficaz às ameaças é um tópico de pesquisa promissor.

Em suma, este estudo contribui para uma compreensão mais clara das fraudes bancárias no Brasil e destaca a importância contínua de medidas proativas para proteger os clientes e manter a confiança no sistema financeiro. A segurança e a confiança no sistema bancário são valores fundamentais que devem ser protegidos e promovidos, e este trabalho lançou luz.

REFERÊNCIAS

ALCÂNTARA, Thais Cesário. Fraudes ao auxílio emergencial distinção entre furto mediante fraude e estelionato. 2021.

BACEN, Banco Central do Brasil. Notícia sobre Economia. Disponível em: https://www.bcb.gov.br/detalhenoticia/412/noticia Acesso em: 12/10/ 2023.

BACEN, Banco Central do Brasil. Notícia sobre Economia. Disponível em: https://www.bcb.gov.br/detalhenoticia/13011/nota Acesso em: 14/10/2023

Banco Central do Brasil. Ranking de Instituições Financeiras. Disponível em: https://www3.bcb.gov.br/ranking/. Acesso em: 20 de novembro de 2023.

Banco do Brasil. Como se proteger contra o golpe do falso motoboy. Blog BB, 2023. Disponível em: https://blog.bb.com.br/golpe-do-falso-motoboy-saiba-como-se-proteger/. Acesso em: 21 de novembro de 2023.

Banco do Brasil. Foi vítima de um golpe? Veja como se proteger. Blog BB, 2023. Disponível em: https://blog.bb.com.br/foi-vitima-de-um-golpe-veja-como-se-proteger/: Acesso em: 21 de novembro de 2023.

Brasil. Lei Complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 11 jan. 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm Acesso em: 14/10/2023

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em: 14/10/2023

Brasil. Lei nº 7.102, de 20 de junho de 1983. Dispõe sobre segurança para estabelecimentos financeiros, estabelece normas de segurança e dá outras providências. Diário Oficial [da]

República Federativa do Brasil, Brasília, DF, 21 jun. 1983. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7102.htm Acesso em: 14/10/2023

Brasil. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L8078.htm Acesso em: 14/10/2023

C6Bank. Golpe da Troca de Cartão. 2023. Disponível em: https://www.c6bank.com.br/blog/golpe-da-troca-de-cartao. Acesso em: 19 de novembro de 2023.

C6 Bank. Segurança. 2023. Disponível em: https://www.c6bank.com.br/seguranca/. Acesso em: 23 de novembro de 2023.

FEBRABAN. Pesquisa FEBRABAN de Tecnologia Bancária 2021 disponível em: https://antifraudes.febraban.org.br/#golpe-no%20whatsapp Acesso em: 10 de outubro de 2023.

FONTELLES, Mauro José et al. Metodologia da pesquisa científica: diretrizes para a elaboração de um protocolo de pesquisa. Revista paraense de medicina, v. 23, n. 3, p. 1-8, 2009.

G1 Globo. Vazamento de dados pessoais: veja como se proteger e o que fazer se for vítima. G1 Tecnologia, 2023. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/05/08/vazamento-de-dados-pessoais-veja-como-se-proteger-e-o-que-fazer-se-for-vitima.ghtml: Acesso em: 21 de novembro de 2023.

GODOY, Arlida Schmidt. Introdução à pesquisa qualitativa e suas possibilidades. Revista de administração de empresas, v. 35, p. 57-63, 1995.

GONÇALVES, Carlos Roberto. Direito Civil Brasileiro: responsabilidade civil. 15. ed. São Paulo: Saraiva Educação, 2020.

MONTEIRO, André de Oliveira. A responsabilidade civil das instituições financeiras em casos de golpes contra correntistas. Trabalho de Conclusão de Curso (Bacharelado em Direito)-Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2022.

OLIVEIRA, Rossimar Laura. Gestão de fraudes financeiras externas em bancos. 2012. Tese de Doutorado. Universidade de São Paulo.

PagBank-PagSeguro. Dicas de Segurança Online. 2023. Disponível em: https://pagseguro.uol.com.br/dicas-de-seguranca-online/. Acesso em: 23 de novembro de 2023.

PEREIRA, Claudia Fernanda Aguiar; SILVA, Roberta. As fraudes bancárias e a responsabilidade civil das instituições financeiras. Revista JurisFIB, v. 11, n. 11, 2020.

REINALDO FILHO, Demócrito. A responsabilidade dos bancos pelos prejuízos resultantes do *phishing*. Revista Magister de Direito Empresarial, Concorrencial e do Consumidor, 2006.

REZENDE, Frederico Antonio Oliveira. RESPONSABILIDADE CIVIL DOS BANCOS EM RELAÇÃO ÀS FRAUDES ELETRÔNICAS. FMU DIREITO-Revista Eletrônica (ISSN: 2316-1515), v. 24, n. 33, 2010.

Santander. Links Falsos. 2023. Disponível em: https://www.santander.com.br/blog/links-falsos. Acesso em: 19 de novembro de 2023.

Serasa. Fraude em Documentos. Certificado Digital Serasa, 2023. Disponível em: https://serasa.certificadodigital.com.br/blog/certificado-ssl/fraude-em-documentos/?gclid=CjwKCAiAgeeqBhBAEiwAoDDhn2y4CuGA3TDasw6sx41RtKMb99Bhgmt9hIziO7gWu6t4PAZKrqqIrhoCx5kQAvD_BwE. Acesso em: 19 de novembro de 2023.

Serasa. Boletos Falsos. 2019. Disponível em: https://www.serasa.com.br/premium/blog/boleto-falso/. Acesso em: 19 de novembro de 2023.

SILVA, Lucas. FRAUDE ELETRÔNICA: FURTO OU ESTELIONATO?(DIREITO). Repositório Institucional, v. 1, n. 1, 2023.