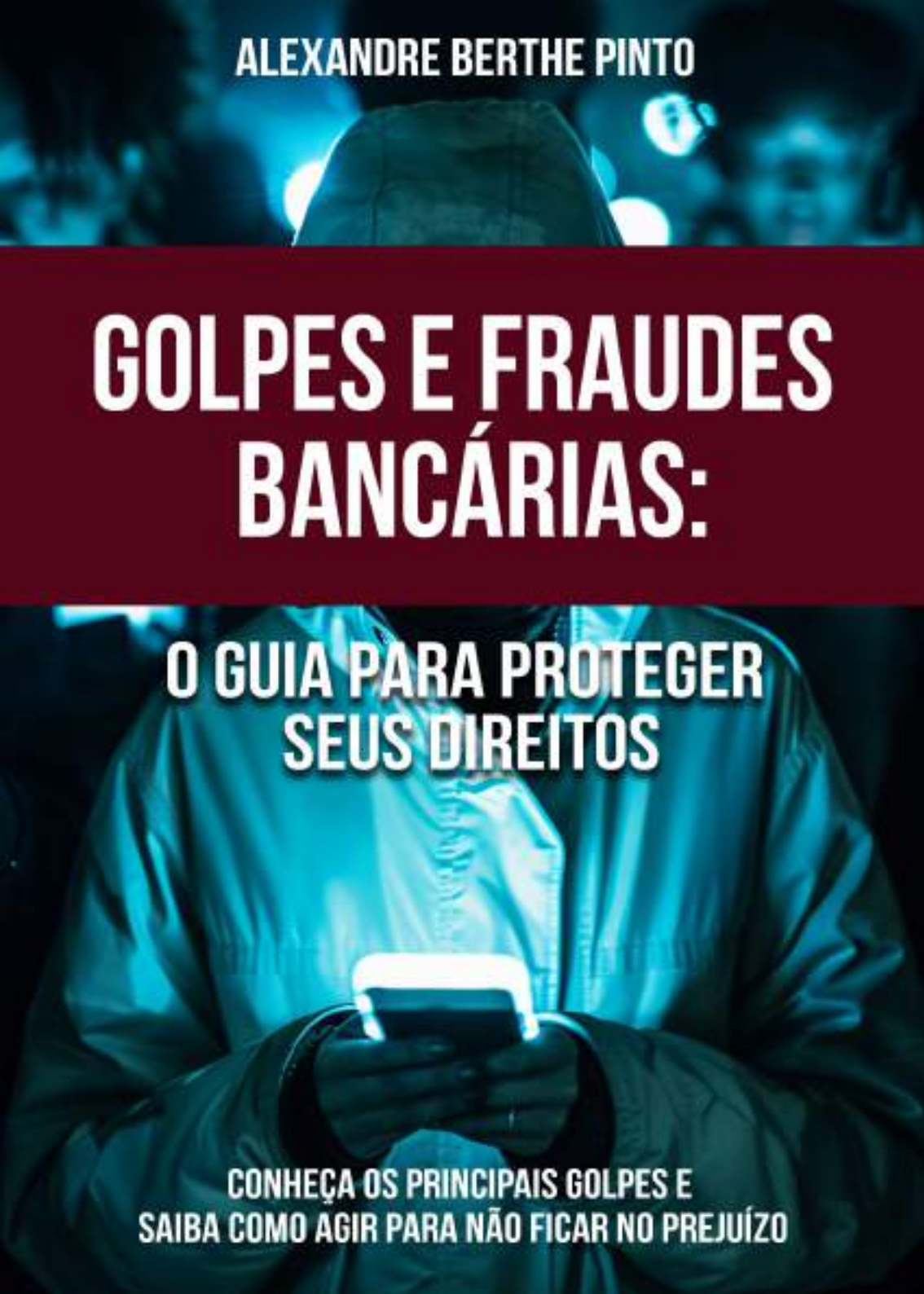
ALEXANDRE BERTHE PINTO

GOLPES E FRAUDES BANCÁRIAS:

O GUIA PARA PROTEGER SEUS DIREITOS



CONHEÇA OS PRINCIPAIS GOLPES E
SAIBA COMO AGIR PARA NÃO FICAR NO PREJUÍZO

Diagramação: LivroEbook Diagramação e Design

1ª edição 2025.

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Pinto, Alexandre Berthe
Golpes e Fraudes Bancárias - Volume I.
Alexandre Berthe Pinto - São Paulo, SP, 2025.
139 pags.

ISBN 978-65-83181-55-8.

1. Fraudes e Golpes Bancários 2. Direito do Consumidor Vítima de Fraude 3. Responsabilidade do Banco 4. Fraude Bancária

CDD-342.5981

Índices para catálogo sistemático:

1. Direito do Consumidor

AGRADECIMENTO

O presente manual é o resultado da compilação de mais de 20 anos de experiência advogando na área de golpes e fraudes financeiras. Foi criado com o intuito de informar todos os leitores sobre uma situação que, infelizmente, é crescente no nosso país.

Deixo aqui meus sinceros agradecimentos à minha esposa, meus dois filhos (dogs), à minha família e uma dedicação especial ao meu pai, que não está mais aqui, mas sempre torceu por mim.

Desejo que todos tenham uma ótima leitura e, se em algum momento o conteúdo aqui apresentado conseguir amenizar o prejuízo de algum leitor, ficarei feliz, pois o objetivo foi alcançado.

Muito obrigado, boa leitura e muito cuidado com os golpes e fraudes financeiras, pois diariamente há um novo golpe ou uma forma diferente de abordagem.

SUMÁRIO

INTRODUÇÃO

1

O presente e-book visa trazer conhecimento sobre casos de golpes e fraudes financeiras, abordando as eventuais possibilidades de ressarcimento e oferecendo algumas dicas e sugestões práticas.

E, é importante o alerta, pois, há um aumento significativo no número de vítimas de golpes e fraudes bancárias; fenômeno preocupante que continua crescendo com o avanço da tecnologia e da digitalização dos serviços financeiros, e violência urbana.

O objetivo é de informar e orientar os consumidores a entenderem seus direitos e as medidas que podem ser tomadas em casos de fraudes.

1.1 POR QUE QUALQUER PESSOA PODE CAIR EM UM GOLPE?

Engana-se quem pensa que apenas pessoas desatentas caem em golpes. **Qualquer um pode ser vítima**, independentemente de idade ou conhecimento tecnológico.

Os golpistas usam **manipulação psicológica** e técnicas que exploram momentos de **distração, confiança ou pressa**. E, com conhecimentos sólidos em informática, sabem como configurar e alterar senhas, e como aproveitar de falhas naturais em um **mundo digital.**

Além disso, o **uso de dados vazados** ou expostos em redes sociais permite que os criminosos personalizem os golpes, tornando-os ainda mais difíceis de identificar. E, o avanço da Inte-

ligência Artificial, colocará os golpes no novo patamar. Portanto, **cair em um golpe não é sinal apenas de descuido, mas a certeza de que as fraudes estão cada vez mais complexas e bem elaboradas.**

1.2 A EVOLUÇÃO DAS FRAUDES COM A TECNOLOGIA

O avanço da tecnologia tornou as fraudes bancárias **mais sofisticadas e difíceis de identificar**. O que antes se limitava à clonagem de cartões evoluiu para golpes digitais como phishing, clonagem de WhatsApp, quebra de senhas, instalação de programas maliciosos e fraudes via Pix.

Além disso, a **violência urbana** contribui para o aumento dos golpes, especialmente após **furtos e roubos de celulares**, quando os criminosos acessam contas bancárias e causam enormes prejuízos.

O fato é que, **a tecnologia facilitou a vida, mas também abriu espaço para golpes mais complexos e perigosos.**

1.3 O PAPEL DO JUDICIÁRIO NA PROTEÇÃO DAS VÍTIMAS

Com o aumento das fraudes bancárias, o **Judiciário** tem um papel essencial na análise da responsabilidade da vítima e ou do banco no caso concreto. Portanto, os tribunais avaliam não apenas a ação dos golpistas, mas também a **responsabilidade das instituições financeiras** em garantir a segurança das transações.

E, os bancos possuem **responsabilidade objetiva**, o que significa que podem ser responsabilizados por falhas na prestação de serviços, mesmo sem culpa direta. No entanto, o judiciário também analisa se houve **culpa do consumidor** para o efeito danoso.

Portanto, o judiciário analisa cada caso individualmente, considerando o **tipo de golpe**, o **comportamento da vítima** e as **medidas de segurança adotadas pelo banco**. E, em muitos casos, as decisões são favoráveis aos consumidores, mas também existem situações em que a justiça entende que a responsabilidade é da própria vítima.

O judiciário busca apurar, em cada situação concreta, qual foi a responsabilidade do banco e do consumidor.

1.4 CONCEITO DE FRAUDE BANCÁRIA

No conceito amplo, **fraude** e **golpe** muitas vezes se confundem, já que ambos envolvem práticas ilegais para obter vantagens financeiras à custa da vítima. A fraude bancária pode ocorrer tanto no ambiente **digital** quanto no **físico**, abrangendo desde **clonagem de cartões** e **phishing** até manipulações mais elaboradas, como o uso de **documentos falsos** e adulteração de **maquininhas de cartão.**

A **violência urbana** também contribui diretamente para o aumento dessas fraudes, especialmente em casos de **roubo e furto de celulares**, afinal, como a maioria dos smartphones pos-

sui acesso direto a **aplicativos bancários**, os criminosos conseguem rapidamente realizar transações e transferências, aumentando os prejuízos das vítimas.

E, as **fraudes eletrônicas** tornaram-se cada vez mais sofisticadas, explorando tanto **falhas de segurança** quanto o próprio comportamento do usuário, ou seja, há um universo amplo de situações e fatos que refletem em uma situação de fraude ou golpe bancários, desde uma situação simplista de um falso boleto premiado até casos complexos de adulteração de maquininhas de cartão.

1.5 LEGISLAÇÃO APLICÁVEL

A proteção contra fraudes bancárias no Brasil é respaldada por diversas leis que garantem os direitos dos consumidores. Mas, devemos destacar principalmente o **Código de Defesa do Consumidor (CDC)**, que responsabiliza as instituições financeiras por falhas na prestação de serviços, mesmo sem culpa direta, o **Código Civil**, a **Lei Geral de Proteção de Dados (LGPD)** e normas do **Banco Central**, com alguns destaques, exemplificativos.

1.5.1 CÓDIGO DE DEFESA DO CONSUMIDOR (CDC)

- **Art. 6º, VI:** Garante ao consumidor o direito à reparação de danos patrimoniais e morais.

- **Art. 14:** Responsabiliza o fornecedor de serviços por danos causados por defeitos na prestação, independentemente de culpa.
- **Art. 14 , § 3º , II:** Afasta a responsabilidade da instituição financeira, quando há culpa exclusiva da vítima.

1.5.2 CÓDIGO CIVIL (C.C)

- **Art. 927:** Estabelece que quem causar dano a outrem, ainda que sem intenção, deve repará-lo.
- **Art. 186:** Define como ato ilícito qualquer ação ou omissão que cause prejuízo a outro.
- **Art. 945:** Trata da **culpa concorrente**, reduzindo a indenização quando o próprio prejudicado tiver contribuído para o dano.

> "Se a vítima tiver concorrido culposamente para o evento danoso, a sua indenização será fixada tendo-se em conta a gravidade de sua

1.5.3 CULPA EM CONFRONTO COM A DO AUTOR DO DANO "LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

- **Art. 42:** Determina que o controlador é responsável por danos causados pelo uso inadequado de dados

- **Art. 46:** Exige que as instituições adotem medidas de segurança para proteger os dados pessoais dos clientes.

1.5.4 REGRAS DE SEGURANÇA DO PIX E ABERTURA DE CONTAS (BANCO CENTRAL)

- **Limites:** Limite de valores em razão do horário e prazo para validar sua alteração, aplicação em conjunto com regras de cada banco.
- **Bloqueios preventivos:** Transações suspeitas podem ser bloqueadas para análise.
- **Mecanismo Especial de Devolução (MED):** Permite a devolução de valores em caso de fraude, desde que o banco seja acionado rapidamente.
- **Validação de Documentos Para Abertura de Conta:** Obrigação da instituição financeira validar corretamente os dados apresentados quando da abertura da conta.

1.5.5 TÉCNICAS DE COMPLIANCE E SEGURANÇA INTERNA:

- Bancos devem adotar práticas de **compliance**, como monitoramento de transações suspeitas, autenticação em duas etapas e sistemas de alerta em tempo real, validação cadastral e termos e regras próprias

para realizar o monitoramento, validações e bloqueios preventivos de transações.

1.5.6 SÚMULA 479 DO STJ:

- Aplicação na grande maioria dos casos em que há culpa da instituição financeira. Isso significa que o banco pode ser responsabilizado mesmo que a fraude tenha sido praticada por terceiros, se houver falha na segurança do serviço.

> "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias"

Assim, sob o ponto de vista jurídico, há vasta quantidade de normas aplicáveis tanto para responsabilizar os bancos, afastar a responsabilidade das instituições e decretar a culpa concorrente.

1.6 RESPONSABILIDADE CIVIL DOS BANCOS

Os bancos possuem **responsabilidade objetiva** na prestação de serviços, o que significa que podem ser responsabilizados por fraudes e falhas de segurança, mesmo sem culpa direta. Essa responsabilidade está prevista no **Código de Defesa do Consumidor (Art. 14)** e na **Súmula 479 do STJ**, que reforça o dever das instituições financeiras de proteger os clientes contra fraudes.

Como **as instituições exercem uma atividade econômica de risco**, assumem o risco da própria atividade, possuindo, por consequência, a obrigação de oferecer segurança nas transações financeiras, monitorar movimentações atípicas e implementar medidas de proteção. O **risco da atividade** implica que eventuais prejuízos decorrentes de fraudes, **mesmo praticadas por terceiros**, podem ser atribuídos ao banco se houver falhas no serviço.

No entanto, a responsabilização dos bancos pode ser afastada quando houver **culpa exclusiva da vítima**, conforme disposto no **Art. 14, §3º do Código de Defesa do Consumidor**. Nestes casos, o banco pode demonstrar que cumpriu todas as medidas de segurança, mas que o prejuízo decorreu da **negligência do próprio cliente**.

Além disso, o **Art. 945 do Código Civil** trata da **culpa concorrente**, que pode reduzir a responsabilidade do banco quando a vítima também contribui para o dano. Por exemplo, casos em que o consumidor compartilha dados bancários sem verificar a autenticidade da fonte.

Já, em casos de **fraude eletrônica** ou **roubo de celular** com acesso a aplicativos bancários, os bancos são frequentemente responsabilizados por não adotarem medidas preventivas adequadas para, por exemplo, bloquear, ainda que preventivamente, transações atípicas, sequências e que é diversa do padrão do perfil de movimentação da vítima.

Assim, ainda que exista o risco da atividade econômica, se demonstrada a culpa da vítima, a decisão judicial afasta a responsabilidade do banco no evento danoso.

1.7 DIREITOS DOS CONSUMIDORES EM CASOS DE FRAUDE

O consumidor vítima de fraude bancária tem direito ao **ressarcimento dos valores subtraídos**, conforme o **Código de Defesa do Consumidor (Art. 14)**. Em alguns casos, pode também obter **indenização por danos morais**, especialmente quando a fraude causa **transtornos significativos**, como bloqueio de contas essenciais, perda do tempo útil para solucionar o problema, negativação cadastral e outras.

Se a fraude resultar em **negativação indevida** ou **cobranças abusivas**, o consumidor pode solicitar **liminarmente** a **suspensão imediata** dessas medidas. Caso o banco se recuse a resolver o problema na via administrativa, o consumidor pode recorrer ao **Procon**, **Banco Central** ou **Consumidor.gov.br**. **Se mesmo assim não houver solução, o caminho judicial será a alternativa restante** para garantir a reparação dos danos.

Portanto, o consumidor tem direito ao ressarcimento financeiro e, em determinadas situações, pode pleitear danos morais e a suspensão de cobranças ou negativação indevida. E, **quando as tentativas administrativas falham, o judiciário passa a ser o único meio de defesa dos direitos do consumidor.**

1.8 FRAUDE ELETRÔNICA: UM DESAFIO MODERNO

As **fraudes eletrônicas** se tornaram um dos maiores desafios da era digital. Com a popularização de ferramentas como o **Pix**, **aplicativos bancários** e **carteiras digitais**, os golpistas encontraram novas formas de aplicar golpes rápidos e difíceis de reverter, **que causam prejuízos financeiros enormes em pouquíssimo tempo**.

O acesso facilitado a **dados pessoais** e o aumento de **vazamentos de informações** na internet também impulsionaram fraudes mais sofisticadas, como phishing, clonagem de WhatsApp e roubo de identidade digital. Além disso, a **violência urbana** agravou o cenário, especialmente com **roubos de celulares**, que permitem o acesso direto a contas bancárias.

Para enfrentar esse desafio, os bancos precisam investir em **tecnologias de segurança**, como autenticação em duas etapas, limites para transações rápidas e monitoramento constante de movimentações suspeitas, com validações biométricas seguras e bloqueio preventivos efetivos. No entanto, a **responsabilidade também recai sobre o consumidor**, que deve adotar práticas seguras no uso de dispositivos e na proteção de dados pessoais.

As fraudes eletrônicas exigem atenção redobrada tanto das instituições financeiras quanto dos consumidores, tornando a segurança digital uma prioridade indispensável.

OS 20 PRINCIPAIS GOLPES E FRAUDES BANCÁRIAS

2

Ao longo de **mais de duas décadas e de advocacia e analisando milhares de causos**, observei que os golpes são os mais variados possíveis, golpes antigos, como ***"Golpe Do Bilhete Premiado"***, ainda faz suas vítimas, outros, como ***"Golpe do Motoboy"***, sofrem "aprimoramentos".

Além **disso, os golpistas possuem uma criatividade** sem limite, portanto, **diariamente um golpe novo é criado**, mas vamos destacar os 21 principais golpes. E, fazer uma análise explicativa relevante sobre cada um deles.

2.1 GOLPE DA MAQUININHA ADULTERADA OU GOLPE DO VISOR ADULTERADO

Como Funciona:

Nesse tipo de golpe, **as vítimas relatam que o visor da maquininha exibe o valor correto da compra**, como ocorreu em qualquer maquininha. Porém, **somente após a digitação da senha**, a máquina apresenta, por exemplo, uma mensagem de erro de conexão, levando o golpista a solicitar que a transação seja repetida. O que a vítima não sabe é que a maquininha foi **adulterada**: não existe erro algum, e cada tentativa está, na verdade, **autorizando múltiplas compras** de valores elevados.

Atualmente, este é considerado um dos **golpes mais sofisticados**, pois a vítima **não tem como identificar visualmente** se a

maquininha foi adulterada ou não, **tornando a fraude praticamente imperceptível** no momento da transação.

Fatos Analisados pelo Judiciário

- **Houve falha na segurança do banco ou da operadora da maquininha?** O judiciário avalia se a instituição financeira ou a operadora deveriam ter detectado transações fora do padrão.
- **A vítima conferiu o valor antes de digitar a senha?** Ainda que o visor mostrasse o valor correto, o juiz analisa se havia alguma possibilidade de a vítima perceber a fraude.
- **Existem provas da fraude?** Gravações de câmeras de segurança, testemunhas ou registros bancários atípicos podem ser usados pela vítima. Em alguns casos, é possível observar o golpista fingir que está procurando um sinal de rede de celular, por exemplo.

Como São as Decisões Judiciais

- **Decisões Favoráveis ao Consumidor**

  O banco ou a operadora são responsabilizados quando:

  - **A adulteração era imperceptível** e a vítima foi induzida ao erro de difícil ou imperceptível verificação prévia.

- O banco ou a operadora **não detectaram movimentações atípicas**, como múltiplas compras sucessivas com valores elevados e não realizaram bloqueios preventivos ou outra forma de validação, por exemplo, confirmação via SMS.
- A maquininha estava vinculada a **contas fraudulentas**, o que deveria ter sido identificado na análise cadastral.

- **Decisões Desfavoráveis ao Consumidor**

  O consumidor perde a ação quando:

  - É comprovado que a vítima **não conferiu o valor** antes de digitar a senha, apesar de ter essa possibilidade e que não existiu alteração no visor.
  - O banco demonstra que a transação foi realizada de forma **regular**, sem qualquer falha de segurança.
  - **Não há provas suficientes** da adulteração, como registros visuais ou movimentações anormais.
  - O valor das transações realizadas **estava dentro do perfil e padrão de movimentação da vítima**, não sendo considerado atípico ou suspeito pelo banco.

Comentário: Atualmente, pode-se entender como sendo um dos golpes mais perfeitos que existe, pois, **é praticamente impossível antes da digitação da senha, a vítima saber se a maquininha é adulterada ou não.**

2.2 GOLPE DO FRETE

Como Funciona:

Neste golpe, a vítima recebe uma **entrega inesperada ou aguardada**, como alimentos, presentes, documentos ou até exames médicos. No momento da entrega, o suposto entregador informa que é necessário pagar um **valor simbólico de frete**, geralmente em torno de **R$10,00**. O detalhe é que o golpista **não aceita Pix ou dinheiro**, exigindo o pagamento via **cartão**.

O problema ocorre no momento da transação: a maquininha utilizada é **adulterada**. O visor exibe o valor correto do frete, mas, após a digitação da senha, a máquina registra **valores muito superiores** ou múltiplas transações. Em alguns casos, o entregador simula um **erro de conexão**, pedindo que a vítima repita a operação, aumentando ainda mais o prejuízo.

Este é considerado um dos golpes mais perfeitos e difíceis de identificar, pois a vítima acredita estar apenas pagando um frete de baixo valor, sem suspeitar que a maquininha foi manipulada.

Informações privilegiadas que vazam, como: data de aniversário, realização de exames, pedido de assistência técnica, compra de delivery e outros, tornam o golpe ainda mais **realista**.

Fatos Analisados pelo Judiciário

- **Houve falha na segurança do banco ou da operadora da maquininha?** O judiciário avalia se o banco deveria ter detectado movimentações atípicas.
- **A vítima conferiu o valor no visor antes de digitar a senha?** Mesmo que o valor estivesse correto, o juiz considera se havia sinais visíveis de fraude, quando há possibilidade de perícia (o que dificilmente ocorre).
- **Existem provas da adulteração?** Registros de transações, movimentações suspeitas ou relatos consistentes podem ser usados como evidência.

Como São as Decisões Judiciais

- **Decisões Favoráveis ao Consumidor**

  O banco ou a operadora são responsabilizados quando:

  » A **adulteração da maquininha era imperceptível**, e a vítima foi induzida ao erro de forma sofisticada, o que está ocorrendo atualmente na maioria dos casos.

- O banco **não detectou movimentações atípicas**, como cobranças elevadas logo após transações simples.
- A maquininha estava vinculada a **contas fraudulentas**, sem verificação adequada pela operadora. É uma análise extrema, que pode existir em casos pontuais.

- **Decisões Desfavoráveis ao Consumidor**

  O consumidor perde a ação quando:

  - É comprovado que a vítima **não conferiu o valor** no visor ou não tomou precauções básicas.
  - As transações realizadas estavam **dentro do perfil de movimentação da vítima** e não foram sequenciais.
  - O banco demonstra que **adotou todas as medidas de segurança**, situação que é analisada com muito detalhes em cada caso.

2.3 GOLPE DA FALSA CENTRAL TELEFÔNICA

Como Funciona:

Neste golpe, o criminoso liga para a vítima se passando por um **funcionário da agência ou do setor de segurança**, alegando que houve uma **movimentação suspeita** na conta ou que o cartão foi **clonado**. Para "resolver" o problema, o golpista orienta a

vítima a ligar para a **central de atendimento** – mas o número fornecido é, na verdade, de uma **central falsa** controlada pelos criminosos OU há simulação de passagem da ligação para o atendente.

Durante a ligação, a vítima é instruída a fornecer **dados pessoais**, **senhas** ou **códigos de autenticação**. Em muitos relatos, os golpistas demonstram conhecimento de **dados sensíveis**, como número da conta, CPF e histórico de transações, que deverá ser debatido na ação para também investigar a possibilidade de **vazamento de informações** que deveriam estar sob a guarda do banco.

Outra tática envolve convencer a vítima de que, para **retomar o acesso à conta**, ela precisa realizar operações de "desbloqueio", fornecendo **códigos de verificação** enviados via SMS ou pelo aplicativo bancário. Esses códigos permitem que os golpistas **habilitem outros dispositivos** vinculados à conta da vítima, facilitando o acesso para realizar transferências, saques e até **contratar empréstimos**.

Em alguns casos, o golpista ainda envia um **motoboy** para coletar o cartão da vítima, supostamente para análise, mas com o objetivo de utilizá-lo para realizar compras e saques.

Podemos dizer que o Golpe da Falsa Central sofre alterações e até mesmo a mesclagem com outros tipos de golpes.

Fatos Analisados pelo Judiciário

- **Houve falha na segurança do banco?** O judiciário avalia se o banco deveria ter identificado movimen-

tações, se solicitou alguma confirmação de validação das transações, se realizou bloqueio preventivo, se as transações foram realizadas com aparelhos cadastrados recentemente e outros.

- **A vítima foi induzida ao erro de forma convincente?** Se o golpe foi sofisticado a ponto de enganar um consumidor cauteloso, isso pode pesar a favor da vítima, é uma análise que muitas vezes está relacionada com o vazamento de dados.
- **O banco adotou medidas preventivas adequadas?** Avalia-se se a instituição implementou sistemas de segurança como alertas de transações ou bloqueios automáticos.
- **Houve vazamento de dados bancários?** O conhecimento de **informações sensíveis** por parte dos golpistas pode indicar falha do banco na proteção dos dados da vítima, em violação à **Lei Geral de Proteção de Dados (LGPD)**.
- **Bloqueio Preventivo?** O juiz analisa se o banco poderia ter evitado a fraude com procedimentos de segurança mais rígidos, por exemplo, ligação, validação biométrica e outras.

Como São as Decisões Judiciais

- **Decisões Favoráveis ao Consumidor**

  O banco é responsabilizado quando:

  - **Falhou em identificar movimentações atípicas** após o golpe, como grandes saques, transferências incomuns ou empréstimos não usuais.
  - A vítima foi **induzida ao erro de forma sofisticada**, sem que houvesse negligência de sua parte, especialmente em razão de vazamento de dados sensíveis.
  - O banco não ofereceu sistemas de **autenticação adequados** ou falhou na comunicação de medidas de segurança.
  - O **uso de dados sensíveis** pelos golpistas indica possível **vazamento de informações** sob a responsabilidade da instituição financeira.

- **Decisões Desfavoráveis ao Consumidor**

  O consumidor perde a ação quando:

  - **Forneceu voluntariamente informações sigilosas**, como senhas, códigos de autenticação ou dados pessoais, mesmo após alertas de segurança do banco.

- O banco comprova que **adotou todas as medidas de segurança disponíveis** e que a transação seguiu os procedimentos corretos e respeitou o perfil da vítima.
- O comportamento da vítima foi considerado **negligente**, como não desconfiar de ligações pedindo informações sensíveis ou realizar operações sem confirmar a veracidade da ligação, ou seja, se o golpe poderia ser evitável facilmente.
- Não há indícios de que o banco tenha sido responsável pelo **vazamento de dados**, e os golpistas utilizaram informações obtidas por outros meios e contaram com a participação da vítima.

Comentário: É um golpe frequente, e, atualmente a análise da culpa concorrente merece **atenção**.

2.4 GOLPE DO FALSO INVESTIMENTO

Como Funciona

Neste golpe, os criminosos se passam por **consultores financeiros**, **corretores** ou **representantes de instituições renomadas**, oferecendo oportunidades de **investimentos com altos retornos** em curto prazo. As ofertas geralmente envolvem **criptomoedas**, **fundos de investimentos falsos** ou **ações**. Para convencer a vítima, os golpistas utilizam **sites falsos**, **documen-**

tos adulterados e até **aplicativos** que simulam plataformas legítimas. Há relatos também de grupos criados em aplicativos de mensagens, porém, é uma armação da própria fraude.

Após o primeiro depósito, a vítima pode até visualizar **lucros falsos** na plataforma, incentivando-a a investir ainda mais. Há relatos inclusive de que alguns resgates ocorrem. No entanto, ao tentar resgatar o valor maior, descobre que foi vítima de um golpe.

É um golpe extremamente complexo e obter o ressarcimento é difícil, moroso e, quando isso ocorre, há uma relação comprovada de falha gravíssima na conta utilizada para recebimento dos "aportes", por conseguinte, aí sim com a possibilidade de responsabilização do banco.

Fatos Analisados pelo Judiciário

- **A "corretora" envolvida era legítima?** O judiciário verifica se a fraude foi facilitada por falhas de segurança ou supervisão de instituições financeiras reais e devidamente registrada.
- **O banco que recebeu o valor seguiu as normas do Banco Central?** O juiz analisa se o banco que **abriu a conta utilizada pelos golpistas** descumpriu regras básicas de cadastro, como exigências de documentação e validação de identidade, o que pode caracterizar responsabilidade da instituição.

- **O banco permitiu movimentações suspeitas?** Avalia-se se a instituição financeira responsável pela abertura da conta deveria ter identificado **transações atípicas** para conta recém-aberta, aplicando bloqueios preventivo.

- **A vítima tomou precauções razoáveis?** O judiciário também considera se o consumidor verificou a **legitimidade da empresa** antes de investir, como o registro na **CVM (Comissão de Valores Mobiliários)**.

Como São as Decisões Judiciais

- **Decisões Favoráveis ao Consumidor**

  O banco que realizou abertura da conta, pode ser responsabilizado quando:

  » O dinheiro foi transferido para **contas fraudulentas** abertas com **graves falhas cadastrais**, em desacordo com as normas do **Banco Central**.

  » O banco não realizou a **devida verificação** de identidade ao abrir contas para os golpistas, facilitando a aplicação do golpe.

  » A instituição falhou em detectar **movimentações atípicas**, como transferências de grandes valores para contas recém-criadas.

- **Decisões Desfavoráveis ao Consumidor**

  O consumidor perde a ação quando:

  - **Investiu sem qualquer verificação mínima**, como confirmar o registro da empresa na CVM ou desconfiar de promessas de **lucros irreais**.
  - O banco demonstra que seguiu todos os **procedimentos legais** para abertura da conta e que não havia indícios claros de fraude.
  - **Culpa concorrente** é aplicada com frequência, reduzindo a responsabilidade do banco quando a vítima agiu com **imprudência** ou **negligência**.

Comentário: Golpe que causa prejuízos elevados, ações são complexas e há necessidade de realizar o levantamento detalhado das contas utilizadas para os "aportes"

2.5 GOLPE DO FALSO LEILÃO

Como Funciona

Neste golpe, os criminosos criam **sites falsos de leilões** que imitam plataformas legítimas, oferecendo **produtos de alto valor** (como carros, imóveis ou eletrônicos). As páginas geralmente apresentam **falsos certificados**, **CNPJ válido** (mas de empresas inexistentes) e até **depoimentos falsificados** de supostos clientes satisfeitos.

Após a arrematação, a vítima é instruída a realizar o pagamento via **transferência bancária**, normalmente para contas em nome de **pessoas físicas ou jurídicas, que na verdade não possui relação alguma com o Leilão verdadeiro**. Depois de efetuado o pagamento, o contato com os golpistas é encerrado, e o produto nunca é entregue.

O envio de carta de arrematação e outros documentos, similares aos usuais em casos análogos, causa uma aparência da licitude.

Ponto de destaque, é que as plataformas falsas sempre atuam de forma a pressionar a eventual arrematação, com contatos frequentes e que foge da normalidade.

Fatos Analisados pelo Judiciário

- **O site era facilmente identificável como falso?** O juiz avalia se havia sinais claros de fraude que poderiam ter sido percebidos pela vítima.
- **O banco realizou o devido controle na abertura da conta?** Verifica-se se a conta utilizada pelos golpistas foi aberta com **falhas cadastrais** ou em desacordo com as normas do **Banco Central**.
- **O banco poderia ter identificado movimentações atípicas?** Analisam-se transações incomuns ou de grande valor que deveriam ter levantado suspeitas.

- **A vítima tomou precauções básicas?** O judiciário considera se a vítima agiu com negligência ou desconfiou de ofertas com **preços irrealistas**.

Como São as Decisões Judiciais

- Decisões Favoráveis ao Consumidor

  Quando há decisão favorável ao consumidor, ela está sempre vinculada à **falha do banco na abertura da conta utilizada pelos golpistas**. Isso ocorre quando:

  » A conta foi aberta com **graves falhas cadastrais**, em descumprimento das normas do **Banco Central**.

  » O banco não detectou **movimentações suspeitas**, como grandes transferências para contas recém-criadas ou sem histórico.

  » A instituição financeira **não adotou procedimentos adequados** para verificar a legitimidade da conta que recebeu os valores.

- Decisões Desfavoráveis ao Consumidor

  O consumidor perde a ação quando:

  » Não tomou **precauções mínimas**, como verificar a **autenticidade do site** ou desconfiar de ofertas com **preços muito abaixo do mercado**.

- A transação foi realizada para uma conta que estava **dentro do padrão de movimentação** ou para contas que não apresentavam irregularidades no momento do cadastro.
- O banco demonstrou que **seguiu todas as normas** para abertura da conta e que não havia sinais claros de fraude.

Culpa concorrente é frequentemente aplicada, reduzindo a responsabilidade do banco quando a vítima agiu com **negligência.**

Comentário: O ressarcimento efetivo atualmente ocorre na minoria dos casos e depende da comprovação da falha do banco na abertura da conta utilizada pelo golpista.

2.6 GOLPE DO FALSO FUNCIONÁRIO

Como Funciona

Este golpe é semelhante ao **Golpe da Falsa Central Telefônica**, mas o grande diferencial está na **abordagem personalizada**. O golpista entra em contato com a vítima se passando por um **funcionário da própria agência**, utilizando o **nome real do gerente** da conta da vítima. Essa personalização faz com que a fraude pareça ainda mais legítima.

Antes da abordagem, os golpistas realizam um **levantamento detalhado dos dados bancários** da vítima, como informações sobre **movimentações financeiras**, **limites de cartões**

e até transações recentes. Em muitos relatos, as vítimas afirmam que os golpistas tinham **acesso a dados sensíveis** que deveriam estar protegidos pelo banco, o que sugere que o golpe **pode** ser precedido por um **vazamento de dados**.

Durante a ligação, o falso funcionário informa que houve uma **atividade suspeita** na conta, como clonagem de cartão ou movimentações não autorizadas. Para resolver o problema, o golpista pede que a vítima forneça **senhas**, **códigos de autenticação** ou até mesmo entregue o **cartão bancário ou habilitação de novos dispositivos**.

Fatos Analisados pelo Judiciário

- **O banco adotou medidas de segurança suficientes?** Avalia-se se o banco poderia ter evitado a fraude com mecanismos mais rígidos, como **autenticação em duas etapas** e **alertas automáticos** de transações suspeitas.
- **A vítima foi induzida ao erro de forma convincente?** Considera-se o grau de sofisticação da abordagem, principalmente quando o golpista utiliza o nome do **gerente real da vítima**.
- **O banco poderia ter identificado movimentações atípicas?** Transações incomuns ou fora do padrão do cliente deveriam acionar alertas.

- **Houve vazamento de dados bancários?** O conhecimento detalhado de **informações sensíveis** pelo golpista pode indicar **falhas na proteção de dados** pelo banco, em violação à **Lei Geral de Proteção de Dados (LGPD)**.

Como São as Decisões Judiciais

- Decisões Favoráveis ao Consumidor

  O banco é responsabilizado quando:

  - **Falhou em identificar movimentações atípicas**, como saques, pagamentos, transferências e alterações cadastrais incomuns.
  - O banco **não implementou medidas de segurança adequadas**, como bloqueios automáticos de transações suspeitas.
  - Há evidências de que o golpe foi facilitado por um **vazamento de dados bancários**, especialmente quando o golpista detinha informações específicas sobre o gerente da vítima, limites de cartões e movimentações recentes.

- Decisões Desfavoráveis ao Consumidor

  O consumidor perde a ação quando:

  - **Forneceu voluntariamente informações confidenciais**, como senhas, códigos de autenticação

ou dados pessoais, mesmo com alertas prévios do banco sobre golpes.

- O banco demonstrou que **adotou todas as medidas de segurança disponíveis** e que as transações ocorreram conforme os procedimentos corretos.
- A movimentação estava **dentro do perfil financeiro da vítima**, não sendo considerada atípica pela instituição.
- **Culpa concorrente** é aplicada quando o judiciário entende que houve **negligência da vítima**, como entregar o cartão a terceiros sem confirmar a autenticidade da solicitação.

2.7 GOLPE DO SETOR DE SEGURANÇA – MÃO FANTASMA

Como Funciona

Neste golpe, o criminoso se passa por um **funcionário do setor de segurança** do banco, informando que houve uma tentativa de fraude na conta da vítima. O golpista orienta a vítima a acessar o **aplicativo bancário** ou o **internet banking** para supostamente "verificar" ou "corrigir" o problema.

O golpe muitas vezes começa **dias antes**, sem que a vítima perceba. Isso ocorre quando a vítima clica em **links suspeitos** recebidos por **e-mail**, **SMS** ou **mensagens em redes sociais**, permitindo a instalação silenciosa de **aplicativos de controle**

remoto no celular ou computador, como **AnyDesk** ou **TeamViewer**. Em alguns casos, o acesso remoto também é facilitado por **vírus** que comprometem o dispositivo da vítima.

Quando o contato telefônico finalmente ocorre, o golpista já tem acesso ao dispositivo. Durante a ligação, a vítima é orientada a **não desligar o celular ou o computador** e a seguir instruções para "resolver o problema". Enquanto isso, os golpistas assumem o **controle remoto** do dispositivo, alterando telas, acessando o aplicativo bancário e realizando **transferências**, **pagamentos** e até **empréstimos**.

Algumas vítimas relatam que perceberam **mudanças nas telas** ou comportamentos estranhos no dispositivo, mas acreditavam que faziam parte do processo de "verificação" orientado pelo falso setor de segurança.

O golpe é utilizado com conhecimento avançado de informática pelos golpistas.

Fatos Analisados pelo Judiciário

- **O banco adotou medidas de segurança para identificar acessos remotos?** Avalia-se se a instituição implementou **bloqueios ou alertas** para acessos não autorizados.
- **A vítima foi induzida de forma sofisticada?** O judiciário considera se o golpe foi convincente, especialmente quando o criminoso utilizou técni-

cas avançadas para simular uma interação legítima com o banco.

- **Houve movimentações atípicas que o banco deveria ter identificado?** Transações elevadas, empréstimos ou movimentações fora do padrão da vítima devem ser analisados.

- **Há indícios de vazamento de dados?** O conhecimento detalhado de **informações bancárias** pode indicar **falhas na proteção de dados** por parte da instituição, violando a **Lei Geral de Proteção de Dados (LGPD)**.

Como São as Decisões Judiciais

- Decisões Favoráveis ao Consumidor

  O banco é responsabilizado quando:

  » **Falhou em identificar movimentações atípicas**, como transferências elevadas ou contratação de empréstimos fora do padrão da vítima.

  » Não ofereceu **mecanismos de segurança adequados** para bloquear acessos remotos suspeitos ou detectar atividades fraudulentas.

  » O golpe envolveu o uso de **dados sensíveis da vítima**, sugerindo possível **vazamento de informações** sob responsabilidade do banco.

- Decisões Desfavoráveis ao Consumidor

  O consumidor perde a ação quando:

  - » **Autorizou voluntariamente o acesso remoto** ao seu dispositivo, mesmo após alertas de segurança do banco.
  - » O banco comprovou que **adotou todas as medidas de segurança disponíveis** e que as transações ocorreram conforme os procedimentos corretos.
  - » A movimentação estava **dentro do perfil financeiro da vítima**, não sendo considerada suspeita pela instituição.
  - » **Culpa concorrente** é aplicada quando o judiciário entende que houve **negligência da vítima**, ao clicar em links suspeitos ou permitir o controle do dispositivo sem confirmar a legitimidade da solicitação.

Comentário: **é fundamental nunca acessar links via SMS ou e-mail suspeitos.**

2.8 GOLPE DA BIOMETRIA FACIAL – FOTO PARA CONFIRMAR ENTREGA

Como Funciona

Neste golpe, o criminoso se passa por um **entregador de encomendas**, funcionário de empresas de logística ou até ser-

viços públicos. No momento da entrega de um produto, brinde ou documento, o golpista solicita que a vítima permita o registro de uma **foto para confirmação de recebimento**, alegando que é um **procedimento padrão de segurança**.

No entanto, a **foto é utilizada para fraudes bancárias**, especialmente em sistemas que utilizam **biometria facial** para autorizar transações, desbloquear contas, alterar dados cadastrais, habilitar dispositivos ou solicitar empréstimos. Após capturar a imagem, os golpistas acessam os **aplicativos bancários** da vítima, **alteram dados cadastrais** e realizam **transferências** ou **contratam empréstimos**. Em muitos casos, a vítima só percebe o golpe ao verificar o **extrato financeiro**, **faturas** ou quando não consegue mais acessar seus **aplicativos bancários** ou **contas online**.

É um golpe evoluído, e o uso da biometria facial, combinado com técnicas de **inteligência artificial** para **falsificação de identidade digital**, tende a se tornar um dos golpes mais comuns nos próximos meses, devido à sofisticação e dificuldade de detecção imediata.

Fatos Analisados pelo Judiciário

- **O banco adotou medidas de segurança suficientes para autenticação biométrica?** Avalia-se se a instituição implementou **mecanismos de verificação eficientes**, além da biometria facial.

- **A vítima foi induzida ao erro de forma sofisticada?** O judiciário considera se o procedimento de "confirmação de entrega" parecia legítimo e inofensivo.
- **Houve movimentações atípicas que o banco deveria ter identificado?** Transações elevadas ou alterações cadastrais fora do padrão da vítima devem ser analisadas.
- **Houve possível vazamento de dados?** Se a fraude envolveu o uso de outros dados bancários, o banco pode ser responsabilizado por falhas na **proteção de informações**, conforme a **Lei Geral de Proteção de Dados (LGPD)**.

Como São as Decisões Judiciais

- Decisões Favoráveis ao Consumidor

  O banco é responsabilizado quando:

  - **Falhou em implementar medidas adicionais de segurança**, permitindo que a biometria facial fosse usada como única forma de autenticação.
  - Não identificou **movimentações atípicas** ou alterações cadastrais suspeitas após o uso fraudulento da biometria.

- A fraude foi facilitada por **vazamento de dados bancários**, além do uso da foto, evidenciando falhas na segurança da instituição.

- Decisões Desfavoráveis ao Consumidor

  O consumidor perde a ação quando:

  - O banco comprovou que **adotou todas as medidas de segurança disponíveis**.
  - A movimentação estava **dentro do padrão financeiro da vítima**, não sendo considerada suspeita pela instituição.
  - O judiciário entende que houve **negligência da vítima** ao permitir o uso da foto sem verificar a legitimidade do entregador ou da empresa.
  - **Culpa concorrente** é aplicada quando a vítima compartilha outras informações pessoais junto com a foto, facilitando a fraude.

Comentário: É um golpe relativamente novo, mas crescente, com prejuízos gigantescos e de complexa análise judicial, pois, será preciso demonstrar que a imagem utilizada da vítima foi obtida através de meios diversos e para outros fins. **O cenário da imagem**, por exemplo, com o fundo de uma portaria, sempre será importante para análise.

2.9 GOLPES APÓS O FURTO DE CELULAR

Como Funciona

Após o **furto de um celular**, os criminosos rapidamente acessam aplicativos bancários e redes sociais para aplicar golpes. O furto geralmente ocorre em locais públicos e movimentados, como transportes coletivos, ruas ou eventos. O número de casos aumentou significativamente devido à crescente **violência urbana** e à **dificuldade de bloquear o aparelho** de forma rápida e eficaz.

Depois do furto, os golpistas normalmente retiram o chip, colocam o celular em **modo avião** ou o desligam, impedindo que a vítima rastreie ou bloqueie o dispositivo remotamente. Em seguida, acessam **e-mails**, **SMS** e **informações salvas no aparelho** para redefinir senhas e invadir **aplicativos bancários**.

Apesar da sofisticação dos sistemas de segurança, muitas instituições financeiras ainda apresentam **falhas**, permitindo transações atípicas sem exigir, por exemplo, a **biometria facial** ou autenticação adicional. Assim, os criminosos conseguem criar uma nova senha, habilitar novos aparelhos sem muita dificuldade técnica, e com isso realizar **transferências via Pix**, **pagamentos** e contratar **empréstimos**, como **CDC (Crédito Direto ao Consumidor)** e **consignados**.

Existem relatos de pessoas que, além de perderem toda a economia de uma vida, enfrentam o impacto financeiro de empréstimos contraídos em seu nome, agravando ainda mais os prejuízos.

Fatos Analisados pelo Judiciário

- **O banco adotou medidas de segurança suficientes para proteger o acesso via celular?** O judiciário avalia se a instituição exigia **autenticação biométrica facial**, bloqueios automáticos após tentativas suspeitas ou validação adicional para transações de alto valor.
- **A vítima notificou o banco rapidamente?** O tempo entre o furto e a comunicação com o banco é analisado para verificar se a vítima tomou as medidas necessárias para bloquear o acesso.
- **O banco permitiu transações atípicas sem verificação adequada?** Movimentações elevadas ou fora do padrão da vítima deveriam acionar **alertas automáticos**. **Vale lembrar que aplicativos bancários possuem sistema de geolocalização, portanto, entender se as transações foram realizadas em locais usuais é importante.**
- **Houve falha na autenticação de dispositivos?** O judiciário verifica se o banco permitiu o acesso a partir de **novos dispositivos ou redefinição de senha** sem exigir etapas de verificação adicionais.

Como São as Decisões Judiciais

- Decisões Favoráveis ao Consumidor

  O banco é responsabilizado quando:

  - **Falhou em identificar movimentações atípicas** ou permitiu transações de alto valor sem exigir autenticação biométrica facial.
  - Não ofereceu **mecanismos de bloqueio eficientes** após o furto, mesmo quando notificado pela vítima.
  - Permitiu o acesso a partir de **dispositivos desconhecidos** ou após alterações cadastrais sensíveis, **sem exigir confirmação adicional.**

- Decisões Desfavoráveis ao Consumidor

  O consumidor perde a ação quando:

  - **Demorou para notificar o banco** sobre o furto, permitindo que os criminosos realizassem diversas transações.
  - O banco comprovou que **adotou todas as medidas de segurança disponíveis**, como autenticação em duas etapas e bloqueios automáticos após tentativas suspeitas.

- A movimentação estava **dentro do perfil financeiro da vítima**, não sendo considerada suspeita pela instituição.
- **Culpa concorrente** é aplicada quando o judiciário entende que houve **negligência da vítima**, como armazenar senhas no celular ou não utilizar medidas básicas de segurança, facilitando o acesso dos criminosos.

Comentário: O uso de aplicativos e a concentração de recursos em um único banco, cujo aplicativo é instalado no celular de uso diário é um risco ao consumidor.

2.10 GOLPES APÓS O ROUBO DE CELULAR

Como Funciona

Diferente do furto, o **roubo de celular** envolve **violência ou ameaça direta**, normalmente com o uso de **armas de fogo** ou **intimidação física**. Após o roubo, os criminosos agem rapidamente para acessar **aplicativos bancários** e realizar **transações financeiras** antes que o dono do aparelho consiga bloquear o dispositivo.

Um fator agravante desse golpe é que, em muitos casos, as vítimas são **coagidas sob ameaça** a fornecer **senhas de desbloqueio** e **acesso direto aos aplicativos bancários**. Sob a ótica inicial, o fornecimento voluntário das senhas poderia afastar a **res-**

ponsabilidade dos bancos, já que as transações foram autorizadas com o uso das credenciais legítimas do cliente. No entanto, o judiciário analisa o contexto mais amplo, considerando se o banco **falhou em implementar medidas de segurança adicionais**, como a exigência de **autenticação biométrica facial** ou a detecção de **movimentações atípicas**.

Após o acesso, os criminosos realizam **transferências via Pix**, **pagamentos** e **empréstimos**, como **CDC (Crédito Direto ao Consumidor)** e **consignados**. O número de casos tem crescido devido à combinação da **violência urbana** com **falhas nos sistemas de segurança bancária**, que não exigem verificações adicionais para operações incomuns.

Existem relatos de vítimas que, além de perderem todas as suas economias, enfrentam o endividamento causado por empréstimos fraudulentos, agravando os prejuízos financeiros e emocionais.

Fatos Analisados pelo Judiciário

- **O banco adotou medidas de segurança suficientes após o roubo?** O judiciário avalia se a instituição exigia **autenticação biométrica facial**, **verificação de dispositivos** e **bloqueios automáticos** para movimentações suspeitas.
- **A vítima notificou o banco imediatamente?** O tempo entre o roubo e a comunicação com o banco é

analisado para verificar se houve tentativa rápida de bloquear o acesso.

- **O banco permitiu transações atípicas sem verificação adicional?** Movimentações elevadas ou fora do padrão da vítima deveriam acionar **alertas automáticos**.

- **O fornecimento da senha sob coação elimina a responsabilidade do banco?** Embora a senha tenha sido fornecida sob ameaça, o banco ainda pode ser responsabilizado se não adotou medidas de **segurança robustas** para proteger o cliente em casos de **movimentações atípicas**.

Como São as Decisões Judiciais

- Decisões Favoráveis ao Consumidor

  O banco é responsabilizado quando:

  - **Falhou em identificar movimentações atípicas**, como transferências elevadas ou empréstimos que não condizem com o perfil da vítima, mesmo que a senha tenha sido fornecida sob coação.

  - **Permitiu o acesso a partir de dispositivos desconhecidos** sem exigir autenticação biométrica ou dupla verificação.

- Não ofereceu **bloqueios imediatos** ou medidas de proteção eficazes, mesmo após a notificação do roubo.
- O golpe foi facilitado por **vazamento de dados bancários**, evidenciando falhas na proteção das informações do cliente.

- Decisões Desfavoráveis ao Consumidor

  O consumidor perde a ação quando:

  - **Demorou para notificar o banco** após o roubo, permitindo que os criminosos realizassem diversas transações.
  - O banco comprovou que **adotou todas as medidas de segurança disponíveis**, como autenticação em duas etapas e bloqueios automáticos após tentativas suspeitas.
  - A movimentação estava **dentro do padrão financeiro da vítima**, não sendo considerada suspeita pela instituição.
  - **Culpa concorrente** é aplicada quando o judiciário entende que houve **negligência da vítima**, como armazenar senhas no celular ou não utilizar medidas básicas de segurança, facilitando o acesso dos criminosos.

Comentário: **O fornecimento da senha em casos de coação, por si só, não exclui a responsabilidade do banco. É aconselhável que a vítima verifique se há algum seguro contratado capaz de amenizar o prejuízo.**

2.11 GOLPE E FRAUDE EM CASO DE SEQUESTRO

Como Funciona

O **sequestro relâmpago** é um crime que envolve o **sequestro da vítima**, com o objetivo de forçá-la a realizar **transações financeiras imediatas**. Durante o sequestro, a vítima é levada a **caixas eletrônicos**, **agências bancárias** ou obrigada a realizar **transferências via Pix**, **pagamentos** e até **contratar empréstimos** como **CDC** e **consignados** diretamente de seus dispositivos móveis, até mesmo em cativeiro.

Com o avanço das tecnologias, muitos bancos utilizam **biometria facial** para autenticar transações. No entanto, criminosos têm explorado essa tecnologia, forçando as vítimas a **liberarem pagamentos via reconhecimento facial**. Em alguns casos, os sequestradores utilizam até **fotos ou vídeos** da vítima para validar o sistema de biometria.

Normalmente, há necessidade de que o advogado realize o levantamento de informações detalhadas, pois, alguns registros de imagens de pessoa já sequestradas, que foram utilizadas para liberação biométrica, por exemplo, indicam um cenário aterrorizante e expressões faciais incomuns. Além disso, entender se as

transações foram precedidas de alterações de limites e/ou realizadas em locais não usuais com base no georreferenciamento pode ser importante.

Fatos Analisados pelo Judiciário

Este tipo de golpe exige uma **análise judicial mais aprofundada**, considerando o contexto de **coação** e a atuação das instituições financeiras. O judiciário analisa:

- **O banco adotou medidas de segurança suficientes para transações forçadas?** Avalia-se se a instituição implementou **autenticação biométrica**, **bloqueios preventivos** e mecanismos de **verificação adicional** para operações atípicas.
- **Houve análise adequada da biometria facial utilizada?** O banco deve ser capaz de identificar se a imagem usada na autenticação foi capturada sob condições suspeitas ou se houve tentativa de **falsificação** com fotos ou vídeos.
- **O banco aplicou bloqueios preventivos e como foi a liberação?** O juiz verifica se houve algum **bloqueio automático** após identificar movimentações suspeitas e se a **liberação** foi feita pelo próprio cliente sob coação.
- **O cliente possui seguro contra fraudes ou sequestros?** O judiciário também avalia se a vítima tinha

algum tipo de **proteção contratual** que poderia cobrir total ou parcialmente os prejuízos.

- **A vítima conseguiu recuperar parte dos valores?** Se houve **recuperação parcial** dos valores com ajuda do banco ou seguradora, isso pode influenciar na decisão judicial.

Como São as Decisões Judiciais

- Decisões Favoráveis ao Consumidor

  O banco é responsabilizado quando:

  - **Falhou em identificar movimentações atípicas**, como transferências elevadas ou empréstimos que não condizem com o perfil da vítima.
  - Permitiu transações usando **biometria facial** sem analisar adequadamente a **imagem utilizada**, ignorando sinais de coação ou falsificação.
  - **Não aplicou bloqueios preventivos** mesmo diante de transações suspeitas, ou **liberou valores** após desbloqueio sob coação evidente.

- Decisões Desfavoráveis ao Consumidor

  O consumidor perde a ação quando:

  - **Forneceu voluntariamente senhas e dados** sob coação, e o banco comprovou que todas as **medidas de segurança foram corretamente seguidas**.

» **Demorou para notificar o banco** ou as autoridades, dificultando o bloqueio de transações ou a recuperação de valores.

» A movimentação estava **dentro do perfil financeiro da vítima**, não sendo considerada suspeita pelas instituições financeiras.

Comentário: É uma situação aterrorizante e, além do abalo emocional, o prejuízo financeiro é gigantesco e, muitas vezes, envolve vários bancos, por isso é sempre aconselhável que a vítima faça uma análise criteriosa com o advogado especialista para entender detalhes das transações.

2.12 GOLPE DA CLONAGEM DE APLICATIVOS DE MENSAGENS E REDES SOCIAIS

Como Funciona

Neste golpe, o criminoso clona o número de WhatsApp da vítima ou invade suas **redes sociais**, assumindo sua identidade para aplicar golpes em amigos, familiares e contatos profissionais. A clonagem ocorre geralmente através de **phishing**, envio de **links maliciosos** ou com o acesso a **dados pessoais** obtidos em vazamentos.

Depois de assumir o controle da conta, o golpista envia mensagens urgentes pedindo **empréstimos**, **transferências via Pix** ou pagamentos para contas fraudulentas. Em muitos casos, o

criminoso utiliza informações pessoais da vítima, como o nome de familiares, locais que frequenta ou até conversas antigas, tornando o golpe mais convincente.

É um golpe antigo, mas que sempre é inovado.

Assim, para a presente análise, considera-se a vítima a pessoa que transferiu valores para o golpista.

E, no caso, como golpes anteriores, haverá necessidade de analisar se o banco cumpriu as normas para abertura da conta utilizada pelo golpista e se há falha de própria vítima.

Comentário: As decisões atuais, não estão sendo favoráveis aos consumidores quando não demonstrada a falha grave do banco, por isso há necessidade da compreensão exata dos fatos ocorridos.

2.13 GOLPE DO BOLETO FALSO

Como Funciona

Neste golpe, o criminoso cria **boletos bancários falsos** que imitam perfeitamente documentos legítimos de empresas, instituições financeiras ou prestadores de serviços. Os golpistas geralmente enviam esses boletos por **e-mail**, **mensagens de texto** ou **aplicativos de mensagens** como o WhatsApp, muitas vezes com logos e informações que aparentam ser autênticas.

Outra variação comum envolve a **adulteração de boletos legítimos**. O golpista intercepta boletos enviados por e-mail ou

altera o campo do **código de barras** para que o pagamento seja direcionado a uma **conta fraudulenta**. Em outros casos, **sites falsos** de geração de boletos ou **QR Codes maliciosos** são usados para enganar consumidores que tentam emitir boletos diretamente nos sites das empresas.

Há também um golpe mais sofisticado, no qual a vítima é contatada por um **suposto funcionário de um banco** com o qual possui um **contrato vigente**, como **financiamento de veículos** ou **empréstimos pessoais**. O golpista, utilizando dados pessoais da vítima, envia um **boleto falso** referente ao pagamento do financiamento. Este tipo de fraude sugere que pode ter havido **vazamento de informações do banco credor**, tornando o caso mais complexo. Quando identificada essa falha de segurança, o **banco credor pode ser responsabilizado** pela exposição indevida dos dados da vítima.

Assim, como há inúmeras variáveis da forma em que o golpe é aplicado, é fundamental que o advogado analise corretamente qual tese jurídica que poderá ser aplicada.

Fatos Analisados pelo Judiciário

- **O banco que recebeu o pagamento adotou medidas de segurança suficientes?** O judiciário avalia se a instituição financeira que recebeu o valor tinha políticas adequadas para identificar **contas fraudulentas** ou movimentações suspeitas. Além do próprio respeito às normais existentes para sua abertura.

- **A instituição emissora do boleto teve alguma falha de segurança?** Caso o boleto tenha sido adulterado ou o golpe tenha ocorrido após contato direto com a vítima, o banco ou empresa credora pode ser responsabilizada por falhas na **proteção de dados** ou na **segurança da emissão**. Portanto, é fundamental entender a tese que será utilizada.

- **Houve vazamento de dados do banco credor?** Em casos relacionados a **financiamentos de veículos ou contratos em andamento**, o judiciário investiga se a fraude foi facilitada pelo **acesso indevido a informações sensíveis** da vítima, o que pode implicar a responsabilidade do banco credor conforme a **Lei Geral de Proteção de Dados (LGPD)**.

- **A vítima teve oportunidade de identificar a fraude?** O judiciário analisa se o consumidor tomou precauções mínimas, como verificar o **nome do beneficiário** e conferir os dados antes de efetuar o pagamento.

Como São as Decisões Judiciais

- Decisões Favoráveis ao Consumidor

  O banco ou a empresa emissora do boleto podem ser responsabilizados quando:

- O valor foi pago para uma **conta fraudulenta aberta com falhas cadastrais**, sem a devida verificação do banco receptor.
- A **instituição financeira falhou em detectar movimentações atípicas** na conta fraudulenta, permitindo que o golpe fosse concluído.
- A fraude ocorreu devido a um **vazamento de informações sensíveis** pelo **banco credor**, facilitando o envio de boletos falsos com dados específicos da vítima.
- O golpe foi facilitado por **falhas na segurança do sistema da empresa emissora do boleto**, permitindo adulterações.
- **Sites ou plataformas** que facilitaram a fraude podem ser responsabilizados se houve falhas na verificação da autenticidade dos boletos gerados.

- Decisões Desfavoráveis ao Consumidor

  O consumidor perde a ação quando:

  - **Não tomou precauções mínimas**, como verificar o **nome do beneficiário** e conferir os dados antes de realizar o pagamento.

- O banco comprovou que **seguiu todas as normas** para a abertura da conta e que **não havia sinais claros de fraude** no momento da transação.
- A transação foi realizada para uma **conta regular**, e o banco não tinha responsabilidade direta sobre a emissão ou adulteração do boleto.
- **Culpa concorrente** pode ser aplicada quando o judiciário entende que a vítima agiu com **negligência**, como utilizar links suspeitos ou QR Codes de procedência duvidosa.

Comentário: **É um golpe que utiliza muitas vezes de arte gráfica na elaboração de boletos falsos, além das mais diversas formas de contato fraudulento, os casos em que há uma interceptação sistêmica para alterar dados são poucos, mas, há relatos de vírus que alteram o boleto, portanto, é necessário muito cuidado ao pagar o boleto e atenção se for ingressar com a ação judicial, pois será preciso entender bem o fato ocorrido.**

2.14 GOLPE DO FALSO EMPRÉSTIMO

Como Funciona

Neste golpe, os criminosos se passam por **instituições financeiras**, **correspondentes bancários** ou **agentes de crédito**, oferecendo **empréstimos com condições atrativas**, como

juros baixos e **liberação rápida**. O contato geralmente ocorre por meio de **anúncios online**, **redes sociais** ou até mesmo **ligações telefônicas e aplicativos de mensagens**, utilizando nomes de **bancos conhecidos** para conferir legitimidade à oferta.

Após o primeiro contato, o golpista solicita que a vítima faça um **pagamento antecipado** para liberar o crédito, sob pretextos como **taxas de cadastro**, **seguros obrigatórios** ou **análise de crédito**. A vítima, acreditando que o valor será reembolsado com a liberação do empréstimo, realiza a transferência. Após o pagamento, o golpista desaparece e o empréstimo nunca é liberado.

Em versões mais sofisticadas do golpe, os criminosos utilizam **sites falsos** que imitam o layout de bancos ou financeiras legítimas, dificultando ainda mais a identificação da fraude.

Fatos Analisados pelo Judiciário

- **O banco que recebeu o valor adotou medidas de segurança suficientes?** O judiciário avalia se a instituição financeira que recebeu o pagamento tinha mecanismos para identificar **contas fraudulentas** abertas com documentação falsa ou movimentações suspeitas.
- **A conta que recebeu o valor foi aberta com falhas?** O banco pode ser responsabilizado se a conta utilizada pelos golpistas foi aberta com **graves falhas cadastrais**, em descumprimento das normas do **Banco Central**.

- **A vítima teve oportunidade de identificar a fraude?** O judiciário considera se a vítima tomou precauções mínimas, como verificar o **registro da instituição financeira** junto ao **Banco Central** ou a procedência do site.

- **Houve vazamento de dados?** Se o golpe foi facilitado pelo acesso prévio a **informações sensíveis** da vítima, a instituição que sofreu o vazamento pode ser responsabilizada, especialmente em violação à **Lei Geral de Proteção de Dados (LGPD)**.

Como São as Decisões Judiciais

- Decisões Favoráveis ao Consumidor

  O banco pode ser responsabilizado quando:

  » O valor foi transferido para uma **conta fraudulenta aberta com falhas cadastrais**, sem a devida verificação por parte do banco.

  » A instituição financeira falhou em detectar **movimentações atípicas** ou **atividades suspeitas** na conta fraudulenta.

  » O golpe foi facilitado por **vazamento de dados pessoais** que permitiram aos golpistas simular ofertas específicas de empréstimos.

- Decisões Desfavoráveis ao Consumidor

  O consumidor perde a ação quando:

  - **Não tomou precauções mínimas**, como verificar o **registro da instituição financeira** ou desconfiar de pedidos de **pagamento antecipado** para liberar crédito.
  - O banco comprovou que **seguiu todas as normas** para a abertura da conta e que **não havia sinais claros de fraude** no momento da transação.
  - O pagamento foi realizado para uma **conta regular**, sem que o banco tivesse meios de identificar a fraude com antecedência.

Comentário: É um golpe que afeta principalmente pessoas que pesquisam por empréstimos sites de buscas ou em redes sociais, e, na grande maioria das vezes, recuperar o valor é extremamente difícil.

2.15 GOLPE COM USO DE DOCUMENTOS FALSOS

Como Funciona

Neste golpe, criminosos utilizam **documentos falsificados** ou **dados pessoais obtidos de forma ilícita** para abrir **contas bancárias**, solicitar **empréstimos**, realizar **compras a crédito** ou contratar serviços em nome da vítima. As informações podem

ser obtidas por meio de **vazamentos de dados**, **phishing**, **furto de documentos físicos** ou até pelo acesso não autorizado a **cadastros públicos** e **bancos de dados privados**.

Com os dados em mãos, os golpistas conseguem criar documentos falsos, que passam despercebidos em processos de verificação simplificados. Isso permite que contas sejam abertas e transações financeiras realizadas sem o conhecimento da vítima, que só descobre o golpe ao receber cobranças inesperadas, ver seu nome negativado ou perceber movimentações estranhas em seu CPF.

É um golpe crescente, até em razão do vazamento de dados cadastrais dos brasileiros .

Fatos Analisados pelo Judiciário

- **O banco adotou medidas de segurança suficientes na abertura da conta?** O judiciário avalia se a instituição financeira realizou a **verificação adequada dos documentos** e seguiu as normas do **Banco Central** para prevenir fraudes na abertura de contas.
- **A instituição teve falhas na análise documental?** Se o banco aceitou documentos claramente falsificados ou não utilizou sistemas de **validação biométrica** ou **análise de autenticidade**, pode ser responsabilizado.
- **A vítima foi impactada por vazamento de dados?** O judiciário pode considerar a responsabilidade de instituições que sofreram **vazamento de informações**

pessoais que facilitaram a fraude, em conformidade com a **Lei Geral de Proteção de Dados (LGPD)**.

- **O banco monitorou adequadamente as movimentações da conta fraudulenta?** Movimentações atípicas ou incompatíveis com o perfil cadastral podem indicar falha na **detecção de atividades suspeitas**.

Como São as Decisões Judiciais

- **Decisões Favoráveis ao Consumidor**

  O banco ou instituição financeira pode ser responsabilizado quando:

  - **Aceitou documentos falsificados** sem realizar a devida verificação, em desacordo com as normas de segurança do **Banco Central**.
  - **Falhou em identificar movimentações atípicas** ou suspeitas na conta aberta com documentos falsos.
  - Ocorreu a negativação cadastral.

- Decisões Desfavoráveis ao Consumidor

  O consumidor perde a ação quando:

  - Quando o banco comprovar que **não existiu uso de documentação falsa** e o consumidor quer usar o judiciário indevidamente.

» Quando comprovado a fraude e o uso de documentação por terceiros, **o êxito do banco ocorre apenas quanto ao eventual pedido de danos morais**, pois, os eventuais débitos serão declarados inexigíveis.

Comentário: **O golpe está sendo aprimorado e aumentando consideravelmente, até em razão do uso da biometria e inteligência artificial para criar "clones" das pessoas. É aconselhável manter um sistema de monitoramento do uso do CPF.**

2.16 GOLPE DO FALSO INTERMEDIÁRIO

Como Funciona

Neste golpe, o criminoso se passa por um **intermediário confiável** em transações comerciais, como na **compra e venda de veículos**, **aluguéis de imóveis** ou **negócios online**. O golpista age como um suposto **facilitador** entre o **comprador e o vendedor**, utilizando informações reais sobre o produto ou serviço, o que torna o golpe ainda mais convincente.

Um dos métodos mais comuns envolve o criminoso monitorando **anúncios legítimos** em plataformas online e cria um **anúncio falso clonado** do mesmo item, com um valor **mais baixo**. Isso atrai outros compradores interessados.

Quando encontra um comprador disposto a fechar o negócio, o falso **intermediário** informa que está vendendo o item

para um **parente**, **amigo próximo** ou **credor**, pedindo para que o comprador **não entre em contato direto com o vendedor** e que o **sigilo da negociação** seja mantido.

Essa solicitação de **sigilo** e o envolvimento de **terceiros** são sinais claros que devem despertar **atenção imediata** dos envolvidos na negociação.

Fatos Analisados pelo Judiciário

- **O banco que recebeu o valor adotou medidas de segurança suficientes?** O judiciário avalia se a instituição financeira realizou a devida verificação da **conta que recebeu o valor**, especialmente em casos de **contas recém-abertas** ou com movimentações suspeitas.
- **A conta fraudulenta foi aberta com falhas cadastrais?** O banco pode ser responsabilizado se a conta usada pelo golpista foi aberta com **documentos falsos** ou sem a devida checagem, em desacordo com as normas do **Banco Central**.

Como São as Decisões Judiciais

- Decisões Favoráveis ao Consumidor

  O banco pode ser responsabilizado quando:

  - A conta que recebeu o pagamento foi aberta com **graves falhas cadastrais**, sem a devida verificação de documentos e identidade.

- A instituição financeira **falhou em identificar movimentações atípicas** ou suspeitas na conta do golpista, como recebimento de valores elevados em contas recém-abertas.
- O banco permitiu a **transferência de valores sem verificar o histórico** da conta ou falhou em aplicar bloqueios preventivos.

- Decisões Desfavoráveis ao Consumidor

  O consumidor perde a ação quando:

  - **Não tomou precauções mínimas** e esperada em uma negociação segura.
  - O banco comprovou que **adotou todas as medidas de segurança disponíveis** para a abertura da conta e que não havia sinais claros de fraude no momento da transação.
  - A movimentação estava **dentro do padrão esperado** para o tipo de transação realizada, não levantando suspeitas automáticas.
  - **Culpa concorrente** pode ser aplicada quando o judiciário entende que a vítima foi **negligente** ao aceitar manter sigilo sobre os detalhes da negociação ou confiar em intermediários sem verificar sua credibilidade.

Comentário: **Como todos os casos de golpes que exige a comprovação de falha do banco que realizou a abertura da conta utilizada pelo golpista, o ressarcimento é complexo e dificilmente ocorre em provas concretas. E, quando ocorre, a culpa concorrente é muito aplicada.**

2.17 GOLPE EM CAIXAS ELETRÔNICOS ALTERADOS QUE PRENDE OU TROCA O CARTÃO

Como Funciona

Neste golpe, criminosos manipulam **caixas eletrônicos** para prender ou trocar o cartão da vítima. O golpe ocorre de diferentes formas:

- **Prender o Cartão:** Os golpistas instalam dispositivos nos caixas eletrônicos que **retêm o cartão** após a inserção. A vítima, acreditando que houve uma falha técnica, se afasta para buscar ajuda, momento em que o criminoso recupera o cartão preso no equipamento.
- **Troca do Cartão:** O golpe também pode ocorrer quando o criminoso observa a vítima durante a transação e, após uma distração, troca o **cartão original** por um **falso**. Muitas vezes, o golpista se passa por um "funcionário" ou oferece ajuda no momento da confusão.

Os criminosos costumam atuar em **locais com menor vigilância**, como caixas eletrônicos em **shoppings**, **supermercados** ou **postos de gasolina**, especialmente nos terminais de **bancos 24 horas**. No entanto, também há registros desse tipo de golpe em **agências bancárias**, onde a sensação de segurança pode fazer a vítima baixar a guarda.

Em ambos os casos, os criminosos conseguem obter a **senha bancária** observando discretamente enquanto a vítima digita, oferecendo "ajuda" durante o processo ou instalando dispositivos eletrônicos. Após o golpe, utilizam o cartão para realizar **saques**, **compras** e **transferências**.

A troca do cartão, portanto, pode ocorrer em razão de diversas situações, sendo necessário ao advogado conseguir identificar corretamente o método utilizado pelo golpista para utilizar a tese jurídica correta.

Fatos Analisados pelo Judiciário

A **localização do golpe** é um fator importante na análise judicial:

- **O golpe ocorreu em caixa eletrônico dentro de uma agência bancária ou em terminais de bancos 24 horas?**
  - » Se o golpe ocorreu dentro de uma **agência bancária**, a responsabilidade do banco tende a ser maior, pois espera-se que o ambiente seja moni-

torado por **vigilância constante** e **câmeras de segurança**.

» Em terminais de **bancos 24 horas** ou locais de acesso público, a responsabilidade pode ser compartilhada com a empresa administradora do caixa eletrônico.

Outros pontos analisados incluem:

- **O banco adotou medidas de segurança suficientes nos caixas eletrônicos?** O judiciário avalia se a instituição financeira ou o operador do terminal realizou a devida **manutenção** e **monitoramento** dos equipamentos para identificar adulterações.
- **Havia câmeras de segurança funcionando?** A presença ou ausência de **câmeras de monitoramento** adequadas pode influenciar na decisão judicial, especialmente em agências bancárias.
- **O banco permitiu movimentações atípicas sem verificação adicional?** Movimentações fora do padrão da vítima, realizadas logo após o golpe, deveriam acionar alertas automáticos.
- **A vítima foi induzida ao erro ou houve negligência?** O judiciário considera se a vítima tomou medidas básicas de segurança, como **não compartilhar**

a senha ou **solicitar ajuda apenas a funcionários identificados**.

Como São as Decisões Judiciais

- Decisões Favoráveis ao Consumidor

  O banco ou a empresa responsável pelo caixa eletrônico podem ser responsabilizados quando:

  - O **caixa eletrônico foi adulterado** e houve falha na **manutenção ou monitoramento** do equipamento.
  - **Falhou em identificar movimentações atípicas**, como saques de grandes valores ou transações incomuns logo após o golpe.
  - **Câmeras de segurança estavam inoperantes** ou não foram usadas de forma eficiente para monitorar atividades suspeitas, especialmente em **agências bancárias**.
  - O banco **não aplicou bloqueios automáticos** após tentativas de uso indevido do cartão ou senhas erradas.
  - Existiu adulteração física no equipamento utilizado.
  - Decisões Desfavoráveis ao Consumidor

O consumidor perde a ação quando:

- **Forneceu voluntariamente informações sigilosas**, como a senha, a terceiros que não eram funcionários do banco, negligenciando a sua própria segurança.
- O banco ou operador do terminal comprovou que **adotou todas as medidas de segurança disponíveis** e que o golpe ocorreu fora do controle da instituição, sem qualquer alteração no equipamento e por negligência da vítima.
- O **uso do cartão** e as transações realizadas estavam **dentro do perfil financeiro da vítima**, dificultando a identificação da fraude.

Comentário: O golpe é muito frequente também em compras realizadas fora do estabelecimento comercial e através de maquininhas portáteis.

2.18 GOLPE DO QR CODE

Como Funciona

Neste golpe, os criminosos utilizam **QR Codes falsificados** para redirecionar a vítima a páginas fraudulentas ou realizar pagamentos indevidos. O golpe pode ocorrer de diversas formas:

- **QR Code adulterado em estabelecimentos físicos:** Os golpistas colam **adesivos com QR Codes falsos**

sobre os códigos legítimos em restaurantes, bares, estacionamentos ou eventos. Quando a vítima escaneia o código para realizar um pagamento, o valor é transferido para uma **conta fraudulenta**.

- **QR Code enviado por e-mail ou redes sociais:** A vítima recebe um **e-mail falso** ou uma **mensagem de WhatsApp** com um QR Code, supostamente para pagamento de boletos, taxas ou serviços. Ao escanear, a vítima realiza uma transação sem perceber que foi direcionada para um ambiente fraudulento.

- **Golpes em transações comerciais online:** Durante negociações em marketplaces ou redes sociais, o golpista envia um **QR Code** para facilitar o pagamento. A vítima, acreditando que o código é legítimo, realiza a transferência para uma conta criminosa.

Fatos Analisados pelo Judiciário

- **O banco que recebeu o valor adotou medidas de segurança suficientes?** O judiciário avalia se a instituição financeira realizou a devida verificação da **conta que recebeu o valor**, especialmente em casos de contas recém-abertas ou movimentações atípicas.

- **O QR Code foi adulterado em local sob responsabilidade de terceiros?** Caso o golpe tenha ocorrido em um estabelecimento comercial ou evento, o **local responsável pelo QR Code original** pode ser envol-

vido na análise de responsabilidade, especialmente se houve falha na vigilância.

- **A vítima teve oportunidade de identificar a fraude?** O judiciário considera se o consumidor tomou medidas básicas de segurança, como **verificar o destinatário** do pagamento após escanear o QR Code ou conferir os dados antes de finalizar a transação.

- **A conta fraudulenta foi aberta com falhas cadastrais?** O banco pode ser responsabilizado se a conta utilizada pelo golpista foi aberta com **documentos falsos** ou sem verificação adequada, em descumprimento das normas do **Banco Central**.

Como São as Decisões Judiciais

- Decisões Favoráveis ao Consumidor

  O banco pode ser responsabilizado quando:

  - O valor foi transferido para uma **conta fraudulenta aberta com falhas cadastrais**, sem a devida verificação de identidade.

  - A instituição financeira **falhou em identificar movimentações atípicas** na conta que recebeu o pagamento.

  - **Estabelecimentos comerciais** podem ser responsabilizados quando não monitoraram ade-

quadamente o ambiente, permitindo a adulteração de QR Codes físicos.

- Decisões Desfavoráveis ao Consumidor

  O consumidor perde a ação quando:

  - **Não tomou precauções mínimas**, como verificar o **nome do beneficiário** após escanear o QR Code ou confirmar a legitimidade do código recebido por mensagem.
  - O banco comprovou que **adotou todas as medidas de segurança disponíveis** e que não havia sinais claros de fraude no momento da transação ou abertura da conta.
  - O golpe ocorreu em um ambiente fora do controle da instituição financeira, como em **transações pessoais** via redes sociais.
  - **Culpa concorrente** pode ser aplicada quando o judiciário entende que a vítima foi **negligente**, como ao escanear QR Codes de fontes desconhecidas sem verificar a autenticidade.

Comentário: **Como há várias formas de aplicação do golpe, é fundamental que o advogado compreenda com detalhes a forma do golpe, evitando com isso o uso inadequado de teses jurídicas superadas.**

2.19 GOLPE DO FALSO SEQUESTRO OU SOLICITAÇÃO DE DINHEIRO POR AMIGOS E FAMILIARES

Como Funciona

Neste golpe, os criminosos entram em contato com a vítima afirmando que um **familiar foi sequestrado** e exigem o pagamento de um resgate imediato. O contato é feito por **telefone**, **mensagens de texto** ou **aplicativos de mensagens** como WhatsApp. Para tornar o golpe mais convincente, os golpistas utilizam **informações pessoais** da vítima ou do suposto sequestrado, obtidas por meio de **vazamentos de dados** ou **pesquisas em redes sociais**.

O golpe é semelhante aplicado através de clonagem de aplicativos de mensagens.

Em alguns casos, os criminosos imitam a voz da suposta vítima ou colocam alguém gritando ao fundo, criando um cenário de desespero. A pressão emocional é intensa, com o objetivo de fazer a vítima agir impulsivamente, realizando **transferências via Pix** ou depósitos para contas fraudulentas.

Outra variação desse golpe ocorre quando os criminosos se passam por **amigos ou familiares** em uma situação de urgência, como acidentes ou problemas financeiros urgentes.

O Avanço da Inteligência Artificial e o Impacto no Golpe
Com o avanço da **inteligência artificial (IA)**, especialmente nas áreas de **clonagem de voz** e **criação de avatares digitais**,

esse tipo de golpe tende a se tornar ainda mais sofisticado. Tecnologias de **deepfake** permitem que golpistas reproduzam **vozes idênticas** às das vítimas ou criem **vídeos falsificados** com imagens realistas de familiares, aumentando a credibilidade da fraude.

A combinação de IA com o acesso a **dados vazados** ou expostos em redes sociais facilita a criação de situações extremamente convincentes. Por isso, a expectativa é que golpes baseados em **simulações de sequestros** ou **pedidos falsos de ajuda** aumentem consideravelmente.

Fatos Analisados pelo Judiciário

- **O banco que recebeu o valor adotou medidas de segurança suficientes?** O judiciário avalia se a instituição financeira realizou a devida verificação da **conta que recebeu o pagamento**, especialmente em casos de contas recém-abertas ou movimentações suspeitas.
- **A conta que recebeu o valor foi aberta com falhas cadastrais?** O banco pode ser responsabilizado se a conta utilizada pelo golpista foi aberta com **documentos falsos** ou sem verificação adequada, em descumprimento das normas do **Banco Central**.

Como São as Decisões Judiciais

- **Decisões Favoráveis ao Consumidor**

  O banco pode ser responsabilizado quando:

  - O valor foi transferido para uma **conta fraudulenta aberta com falhas cadastrais**, sem a devida verificação de identidade.
  - **Empresas de tecnologia** podem ser responsabilizadas quando não adotaram medidas adequadas para prevenir a **clonagem de contas** ou proteger informações sensíveis.

- **Decisões Desfavoráveis ao Consumidor**

  O consumidor perde a ação quando:

  - **Não tomou precauções mínimas**, como tentar entrar em contato com o familiar antes de realizar o pagamento.
  - O banco comprovou que **adotou todas as medidas de segurança disponíveis** e que não havia sinais claros de fraude no momento da transação.
  - O golpe foi realizado utilizando contas legítimas de pessoas conhecidas, mas sem que houvesse falhas evidentes no sistema bancário ou de comunicação.

Comentário: **O efetivo ressarcimento não é tão simples, pois sempre existe uma participação da vítima.**

2.20 GOLPE DO FALSO ADVOGADO

Como Funciona

Neste golpe, criminosos se passam por **advogados** ou **representantes legais**, alegando que a vítima está envolvida em algum **processo judicial**, precisa pagar **taxas** ou quitar **custos processuais** para liberação de valores de uma suposta causa favorável.

O contato é feito por **telefone**, **e-mail** ou **WhatsApp**, utilizando **linguagem técnica** e dados que tornam o golpe extremamente convincente.

Os golpistas frequentemente utilizam **informações reais** sobre processos judiciais em que a vítima está envolvida ou esteve no passado, incluindo **números de processos** e **nomes de advogados contratados**.

O Crescimento do Golpe e o Desafio do Rastreio
Este tipo de golpe tem se tornado cada vez mais comum, levando a **Ordem dos Advogados do Brasil (OAB)** a se manifestar publicamente sobre o problema. A OAB, em conjunto com **autoridades policiais** e **judiciário**, tem trabalhado para identificar o problema.

O acesso a informações públicas em processos muitas vezes dificulta a responsabilização direta de instituições, tornando o rastreio dos criminosos um processo complexo.

Fatos Analisados pelo Judiciário

- **O banco que recebeu o valor adotou medidas de segurança suficientes?** O judiciário avalia se a instituição financeira realizou a devida verificação da **conta que recebeu o pagamento**, especialmente se foi aberta recentemente ou apresenta movimentações suspeitas.

- **A conta que recebeu o valor foi aberta com falhas cadastrais?** O banco pode ser responsabilizado se a conta utilizada pelo golpista foi aberta com **documentos falsos** ou sem a devida verificação, em descumprimento das normas do **Banco Central**.

- **A vítima teve oportunidade de identificar a fraude?** O judiciário considera se a vítima tomou precauções mínimas, como **verificar o registro do advogado na OAB**, entrar em contato com o **escritório de advocacia**, por exemplo.

- **Houve vazamento de dados que facilitou o golpe?** Se o criminoso teve acesso a **informações pessoais** ou **detalhes de processos judiciais** por meio de vazamentos, a responsabilidade pode ser atribuída à instituição que não protegeu adequadamente essas

informações, conforme a **Lei Geral de Proteção de Dados (LGPD)**.

Como São as Decisões Judiciais

- Decisões Favoráveis ao Consumidor

  O banco ou instituições podem ser responsabilizadas quando:

  - O valor foi transferido para uma **conta fraudulenta aberta com falhas cadastrais**, sem a devida verificação de identidade.
  - A instituição financeira **falhou em identificar movimentações atípicas** ou suspeitas na conta do golpista.
  - O golpe foi facilitado por **vazamento de dados pessoais** ou acesso não autorizado a processos judiciais, evidenciando falhas na proteção dessas informações.
  - **Empresas de tecnologia** ou **plataformas judiciais** podem ser responsabilizadas quando não adotaram medidas adequadas para proteger os dados dos usuários ou controlar o acesso a informações sensíveis.

- Decisões Desfavoráveis ao Consumidor

  O consumidor perde a ação quando:

  - **Não tomou precauções mínimas**, como verificar a **autenticidade do advogado** na OAB ou confirmar as informações diretamente nos processos digitais.
  - O banco comprovou que **adotou todas as medidas de segurança disponíveis** e que não havia sinais claros de fraude no momento da transação.
  - A movimentação estava **dentro do perfil esperado**, dificultando a identificação de atividades suspeitas.

Comentário: É um golpe que aumentou consideravelmente, portanto, é fundamental que caso a vítima receba alguma solicitação de valores do advogado que mantenha contato com o próprio advogado por canais oficiais e solicite ajuda de algum familiar.

SEUS DIREITOS COMO VÍTIMA DE FRAUDES BANCÁRIAS

3

3.1 O QUE DIZ O CÓDIGO DE DEFESA DO CONSUMIDOR (CDC)?

O **Código de Defesa do Consumidor (CDC)** protege o consumidor em casos de **fraudes bancárias**, considerando-o a parte mais vulnerável na relação com o banco.

Pelo CDC, os bancos devem garantir **segurança** e **eficiência** na prestação dos serviços. Se ocorrer uma fraude, o banco pode ser responsabilizado, mesmo que o golpe tenha sido cometido por terceiros.

3.2 RESPONSABILIDADE CIVIL DOS BANCOS EM CASOS DE FRAUDE

Os bancos têm **responsabilidade objetiva** em casos de fraudes, ou seja, podem ser responsabilizados **independentemente de culpa** quando há falhas na prestação do serviço, conforme o **Código de Defesa do Consumidor (CDC)**.

Se o banco não comprovar que adotou **medidas de segurança adequadas**, será responsabilizado pelos prejuízos.

No entanto, a responsabilidade pode ser **afastada** se for provada a **culpa exclusiva da vítima** ou de **terceiros**. Já, em casos de **culpa concorrente**, a indenização pode ser reduzida

3.3 QUANDO O BANCO É OBRIGADO A DEVOLVER O DINHEIRO?

O banco deve devolver o dinheiro quando a fraude resulta de **falhas na segurança** ou na **prestação do serviço** e a responsabilidade do banco pode ser:

- **Total**, se não comprovar que adotou todas as **medidas de segurança**.
- **Dividida** com o cliente em casos de **culpa concorrente** (quando ambos contribuíram para o prejuízo).
- **Afastada** se o banco provar que houve **culpa exclusiva da vítima**, como fornecimento voluntário de senhas.

3.4 E SE O BANCO SE RECUSAR A PAGAR?

Se o banco se recusar a devolver o dinheiro após uma fraude, o consumidor pode:

- **Reclamar formalmente ao banco:** Solicitar uma resposta oficial e exigir um **protocolo de atendimento**.
- **Acionar órgãos de defesa do consumidor:** Registrar a reclamação no **Procon** ou no site **Consumidor.gov.br**.
- **Ingressar com ação judicial:** O consumidor pode entrar com uma ação no **Juizado Especial Cível**. Para causas de até **20 salários mínimos**, é possível ingressar **sem advogado**. Acima desse valor ou em casos mais complexos, o acompanhamento de um **advogado** é recomendado.

3.5 RECLAMAÇÃO NO BANCO CENTRAL E PROCON.

Se o banco não resolver o problema, o consumidor pode recorrer a **órgãos de defesa do consumidor** para buscar uma solução:

- **Procon:** O consumidor pode registrar uma reclamação no **Procon** do seu estado. O órgão atua na mediação entre o cliente e o banco, buscando uma **solução administrativa**. Caso o banco não responda adequadamente, o Procon pode aplicar **sanções** à instituição.
- **Banco Central:** Embora o **Banco Central** não resolva disputas individuais, ele monitora o comportamento das instituições financeiras. Reclamações podem resultar em **fiscalizações** e pressionar o banco a cumprir suas obrigações.

Essas ações **podem ajudar** o cliente a resolver o problema **administrativamente** ou servir como prova de que **todas as tentativas administrativas foram esgotadas**, para uma futura ação judicial.

3.6 POSSO USAR O CONSUMIDOR.GOV.BR?

Sim. O **Consumidor.gov.br** é uma plataforma oficial do governo que permite ao consumidor registrar reclamações

diretamente contra instituições financeiras e outros fornecedores de serviços.

Vantagens de usar o Consumidor.gov.br:

- **Resposta rápida:** As empresas possuem prazos para responder à reclamação.
- **Acompanhamento online:** O consumidor pode acompanhar todo o processo pela plataforma.
- **Prova em caso de ação judicial:** Se o problema não for resolvido, a tentativa registrada na plataforma serve como **prova** de que o consumidor **buscou todas as soluções administrativas** antes de recorrer à Justiça.

3.7 COMO SOLICITAR DANOS MORAIS ALÉM DO RESSARCIMENTO

Em casos de fraude bancária, além da devolução do valor perdido, o consumidor pode solicitar **indenização por danos morais** quando houver **prejuízos que vão além do financeiro**. Isso ocorre, por exemplo, nas seguintes situações:

- **Negativação indevida** do nome do consumidor em órgãos de proteção ao crédito.
- **Bloqueio injustificado de contas**, dificultando o acesso a recursos essenciais.

- **Transtornos emocionais**, como estresse, ansiedade ou constrangimento público.
- **Perda do tempo útil**, quando o consumidor precisa despender **tempo excessivo** para resolver o problema, enfrentando burocracias ou negligência do banco.

No entanto, é fundamental destacar que o valor do **dano moral** deve ser analisado com **cuidado para cada caso específico**. O **tipo de golpe**, o **impacto na vida da vítima** e a **conduta do banco** são fatores que influenciam a decisão.

Além disso, as indenizações por danos morais, quando concedidas, geralmente são de **valores moderados** e **não devem alterar o padrão de vida** da vítima.

3.8 CASOS REAIS DE VITÓRIAS NA JUSTIÇA

Existem **inúmeras decisões favoráveis** aos consumidores que foram vítimas de fraudes bancárias. Em muitos casos, a Justiça reconheceu a **responsabilidade dos bancos** por falhas na segurança, permitindo o **ressarcimento integral** dos valores perdidos e, em algumas situações, a concessão de **danos morais**.

No entanto, é importante destacar que cada ação é analisada individualmente, considerando as particularidades do caso concreto.

Fatores como o tipo de golpe, o comportamento da vítima e as medidas de segurança adotadas pelo banco influenciam diretamente o desfecho da ação.

Por isso, é essencial que a vítima consulte um **advogado especializado em golpes e fraudes bancárias**, que poderá avaliar o caso específico e prestar os **esclarecimentos adequados**.

FUI VÍTIMA DE UM GOLPE – O QUE FAZER AGORA

4

Agir rapidamente é fundamental para minimizar os danos e aumentar as chances de recuperar o dinheiro. Este capítulo apresenta um **passo a passo prático** que orienta o que fazer imediatamente após identificar a fraude.

4.1 PASSO 1: BLOQUEIE IMEDIATAMENTE SUAS CONTAS E CARTÕES

Assim que identificar uma movimentação suspeita ou confirmar que foi vítima de um golpe, o primeiro passo é **bloquear imediatamente suas contas e cartões** para evitar novos prejuízos.

Como agir:

- **Solicite o bloqueio total da conta e cartões junto ao banco.** Entre em contato com o banco pelos canais oficiais (aplicativo, site ou telefone) e peça o **bloqueio da conta de forma ampla**, incluindo **transações, cartões, Pix e outros serviços bancários**. Mesmo que isso cause transtornos futuros para a reativação, é a forma mais segura de proteger seu dinheiro.

- **Anote todas as informações do contato.** Registre o **protocolo da ligação**, o **dia e horário do atendimento**, e **tire prints das telas** ou salve e-mails que comprovem que você solicitou o bloqueio. Esses documentos serão fundamentais para futuras ações administrativas ou judiciais.

- **Realize a contestação administrativa.** Se possível, já solicite a **contestação formal** das transações suspeitas durante o atendimento. Esse processo será analisado internamente pelo banco.

- **Atenção aos procedimentos indicados pelo banco.** O funcionário que atende o caso, como **prestador de serviço**, tem a obrigação de fornecer informações claras e completas. Ele pode indicar **outros procedimentos de segurança** ou documentações adicionais necessárias.

Esse passo inicial é fundamental para interromper o golpe e reunir provas que ajudarão na resolução do caso.

4.2 PASSO 2: AVISE O BANCO E EXIJA O PROTOCOLO DE ATENDIMENTO

Após bloquear suas contas e cartões, é fundamental **notificar formalmente o banco** sobre a fraude. Esse contato oficial ajuda a registrar o caso e pode ser decisivo na hora de buscar o ressarcimento.

Como agir:

- **Comunique o banco pelo canal de atendimento oficial.** Utilize o **SAC**, **ouvidoria** ou o chat do aplicativo para registrar a ocorrência da fraude. Informe todos os detalhes: tipo de golpe, valores envolvidos e quando as transações suspeitas ocorreram.

- **Exija o protocolo de atendimento.** Sempre peça o **número do protocolo** da reclamação e guarde essa informação. O protocolo é a **prova oficial** de que você notificou o banco e será essencial em futuras ações administrativas ou judiciais.
- **Reforce a comunicação.** Independentemente do contato inicial, que muitas vezes ocorre em meio ao nervosismo, é recomendável que você **entre em contato novamente.** E, de forma mais calma, reforce o ocorrido, garantindo que todas as informações foram corretamente registradas.
- **Confirme o prazo de resposta.** Pergunte ao atendente qual o prazo para o banco analisar a reclamação. Normalmente, as instituições têm entre **5 a 10 dias úteis** para retornar.
- **Solicite confirmação por escrito.** Se possível, peça para que o banco envie uma **confirmação por e-mail** ou SMS da sua reclamação. Isso ajuda a manter o registro.

4.3 PASSO 3: REGISTRE UM BOLETIM DE OCORRÊNCIA (B.O.)

Registrar um **Boletim de Ocorrência (B.O.)** é uma etapa fundamental após identificar que foi vítima de um golpe. Esse

documento formaliza o crime e pode ser exigido pelo banco, pela **seguradora** ou pelo **Poder Judiciário** em futuras ações.

Como agir:

- **Registre o B.O. online ou presencialmente.** Para golpes simples, como clonagem de cartão ou transferências não autorizadas, o B.O. pode ser feito pela **delegacia virtual**. No entanto, em casos mais graves, como **roubo**, **ameaças**, **furtos qualificados** ou **sequestros**, é altamente recomendável que o registro seja feito **presencialmente** em uma delegacia.

- **Inclua todos os detalhes do golpe.** Descreva o ocorrido com detalhes: como o golpe aconteceu, valores envolvidos, datas e horários das transações suspeitas, e, se possível, **informações sobre contas bancárias**, **números de telefone** ou **endereços de e-mail** usados pelos golpistas.

- **Atualize a polícia com novas informações.** Após o registro inicial do B.O., é aconselhável que a vítima **retorne à delegacia** assim que conseguir **novos dados**, como informações de **contas beneficiárias**, **prints de tela** ou **comprovantes de transações**.

- **Consulte a autoridade sobre a necessidade de representação formal.** Em alguns casos, será necessário que a vítima faça uma **representação formal** para dar continuidade ao processo criminal. As orien-

tações sobre esse procedimento podem ser obtidas diretamente com a **autoridade policial**, que está preparada para fornecer esclarecimentos e orientações adequadas.

- **Entregue o B.O. ao banco e à seguradora.** Após o registro, envie o B.O. ao **banco** para formalizar a contestação das transações e reforçar o pedido de ressarcimento. Se o cliente possuir algum tipo de **seguro bancário ou de cartão**, o B.O. também deve ser entregue à **seguradora**, pois é um documento essencial para a análise e liberação da cobertura.

4.4 PASSO 4: REÚNA TODAS AS PROVAS (PRINTS, E-MAILS, EXTRATOS)

Reunir **provas concretas** é essencial para contestar a fraude junto ao banco, autoridades e, se necessário, na Justiça. Quanto mais **detalhado** for o material coletado, maiores são as chances de recuperar o prejuízo.

Como agir:

- **Salve prints e registros de comunicação.** Capture **telas de conversas** com os golpistas (WhatsApp, SMS, e-mails), **comprovantes de transações** suspeitas e quaisquer mensagens recebidas do banco sobre movimentações.

- **Baixe extratos bancários detalhados.** Solicite ao banco **extratos completos** das movimentações durante o período da fraude, destacando transferências via **Pix**, **TED, Transferências, Empréstimos e outras**.

- **Registre ligações e protocolos de atendimento.** Anote os **protocolos** de todas as ligações feitas ao banco e, se possível, grave ou anote os detalhes das conversas com os atendentes.

- **Guarde documentos relacionados ao golpe.** Se houver **boletos falsos**, **faturas** ou **contratos fraudados**, mantenha cópias desses documentos.

Importante: Caso venha existir uma ação judicial, caberá ao advogado sempre rever os documentos.

1.1. Passo 5: Acompanhe o Retorno do Banco e Esteja Pronto para Agir

Após registrar a fraude e reunir as provas, é fundamental **acompanhar de perto** o retorno do banco. Esse acompanhamento garante que o caso não fique parado e permite que você tome as medidas necessárias caso o banco **não resolva** o problema.

Como agir:

- **Monitore os prazos de resposta.** Bancos geralmente têm entre **5 a 10 dias úteis** para responder às contes-

tações. Se o prazo não for cumprido, entre em contato novamente e exija um posicionamento, se for o caso contate a Ouvidoria.

- **Documente todas as interações.** Continue anotando **protocolos**, **datas**, **horários** e nomes dos atendentes em cada contato com o banco.
- **Esteja preparado para agir se o banco negar o ressarcimento.** Caso o banco **recuse** o reembolso ou ofereça uma resposta insatisfatória, esteja pronto para:
  - » **Acionar órgãos de defesa do consumidor**, como o **Procon** e o site **Consumidor.gov.br**.
  - » **Registrar nova reclamação na ouvidoria** do banco, que é a última instância administrativa interna antes da judicialização.
  - » **Consultar um advogado** especializado em fraudes bancárias para avaliar a possibilidade de **ação judicial**.

4.5 PEDIDOS LIMINARES PARA SUSPENSÃO DE COBRANÇAS E NEGATIVAÇÃO

Quando a fraude resulta em **empréstimos não autorizados**, **compras parceladas** ou **transações futuras**, é fundamental agir rapidamente para evitar **prejuízos contínuos**.

Nestes casos, o consumidor pode entrar com um **pedido liminar** na Justiça para suspender cobranças indevidas e impedir a negativação do nome.

Como agir:

- **Consulte um advogado especializado.** Assim que identificar a fraude, entre em contato com um **advogado especializado em fraudes bancárias** para avaliar a situação. O profissional poderá entrar com uma **ação judicial com pedido liminar** para suspender cobranças imediatas.
- **Objetivo do pedido liminar:**
  - **Suspensão de cobranças** de empréstimos, parcelamentos ou compras não reconhecidas.
  - **Impedir a negativação** do nome em órgãos de proteção ao crédito, como **SPC** e **Serasa**.
  - **Interrupção de descontos automáticos** em folha de pagamento ou conta bancária.
- **A importância da rapidez:** A liminar é uma medida urgente que, quando concedida, pode **bloquear efeitos negativos** da fraude antes mesmo do julgamento do caso. Isso evita que a vítima tenha que arcar com dívidas que não contraiu ou enfrente **constrangimentos** por nome sujo.

Importante: **caberá ao advogado que estiver analisando o caso, sempre prestar esclarecimentos concretos sobre o procedimento.**

4.6 PEDIDOS LIMINARES PARA OBTENÇÃO DE DADOS

Em muitos casos, para fortalecer a ação judicial e identificar os responsáveis pela fraude, é necessário solicitar judicialmente o acesso a **dados sigilosos** relacionados ao golpe. Isso pode ser feito por meio de um **pedido liminar** para obter informações essenciais.

Como agir:

- **Consulte um advogado especializado.** Um **advogado especializado em fraudes bancárias** poderá entrar com uma ação judicial solicitando liminarmente o acesso a dados que podem ser fundamentais para o processo.
- **Quais dados podem ser solicitados?**
  - **Informações sobre contas utilizadas no golpe**, como nome dos beneficiários, CPF/CNPJ e dados bancários.
  - **Registros de acesso sistêmico**, incluindo horários de login, alterações cadastrais e movimentações financeiras.

- » **Dados de geolocalização (GPS)** e identificação da rede utilizada para acessar a conta da vítima.
- » **Histórico de dispositivos conectados**, caso o golpe envolva invasão de aplicativos bancários ou clonagem de celular.

- **Importância da preservação de provas:** O pedido liminar também pode exigir a **preservação dos registros digitais** antes que sejam apagados ou alterados, garantindo que as provas estejam disponíveis para análise durante o processo.
- **Importante:** **caberá ao advogado que estiver analisando o caso, sempre prestar esclarecimentos concretos sobre o procedimento.**

LEVANDO O CASO PARA A JUSTIÇA – COMO FUNCIONA

5

Se o banco **recusar o ressarcimento** ou não oferecer uma solução satisfatória após todas as tentativas administrativas, o próximo passo é recorrer ao **Poder Judiciário**. Este capítulo explica como funciona o processo judicial, desde a decisão de entrar com a ação até o julgamento final.

5.1 QUANDO ENTRAR NA JUSTIÇA É O MELHOR CAMINHO?

Recorrer à Justiça se torna o caminho quando todas as tentativas administrativas para resolver o problema com o banco **não resultam em solução satisfatória**. Isso inclui casos em que o banco:

- **Recusa o ressarcimento** dos valores perdidos na fraude.
- **Oferece respostas insuficientes** ou incompletas durante o processo de contestação.
- **Não cumpre prazos** ou ignora reclamações registradas no **Procon** ou no **Consumidor.gov.br**.

Além disso, a Justiça pode ser necessária para:

- **Obter indenização por danos morais**, especialmente em casos de **negativação indevida**, bloqueio de contas ou prejuízos emocionais.

- **Solicitar liminares** para suspender cobranças indevidas, impedir a negativação do nome ou obter dados necessários para investigar a fraude.

Quando vale a pena entrar com uma ação?

Antes de acionar a Justiça, é fundamental fazer uma **análise ampla** do caso:

- Avalie os **prejuízos materiais** (valores perdidos), os **possíveis danos morais** e o impacto financeiro geral.
- Considere se o caso envolve **falhas claras do banco**, como negligência na proteção de dados ou falta de segurança em transações.
- Examine a situação concreta para identificar se houve **comportamentos graves por parte da vítima** (como fornecimento voluntário de senhas ou descuido com informações pessoais), o que pode **afastar a responsabilidade do banco**.

Para evitar o ingresso de uma **ação temerária** — que pode **aumentar o prejuízo** com custos processuais — é sempre prudente uma **análise consciente**.

Em casos mais complexos, a vítima pode realizar uma consulta prévia com um advogado especializado em golpes e fraudes bancárias para discutir o caso em detalhes e tomar uma decisão mais assertiva.

5.2 JUIZADO ESPECIAL CÍVEL (PEQUENAS CAUSAS)

O **Juizado Especial Cível** é uma alternativa prática para resolver casos de fraudes bancárias, oferecendo um processo mais **rápido** e com **custos reduzidos**. No entanto, é importante avaliar com cautela se essa é a melhor opção para o seu caso.

Avaliação técnica antes de ingressar no Juizado:

Ainda que o Juizado possa ser uma possibilidade, seu **rito simplificado** apresenta algumas limitações importantes. Por exemplo, o Juizado **não permite a produção de provas complexas**, como perícias técnicas detalhadas, que podem ser essenciais em casos de fraudes mais sofisticadas.

Além disso, se a ação for julgada **improcedente**, para recorrer será necessário o **pagamento de custas processuais** e, muitas vezes, a **contratação de um advogado**. Isso pode **aumentar o prejuízo** da vítima caso a ação não tenha o desfecho esperado.

Embora existam ações julgadas favoravelmente ao consumidor no Juizado, muitas outras são **extintas** ou não prosperam, especialmente quando a **complexidade da fraude** exige uma análise mais aprofundada.

É importante destacar que a complexidade de um caso não está necessariamente ligada ao valor do prejuízo, mas sim aos detalhes técnicos da fraude e à necessidade de provas robustas.

Portanto, é fundamental tomar uma **decisão consciente e técnica**, considerando não apenas a possibilidade de **isenção de custas**, mas também as **particularidades do caso concreto**.

A consulta com um advogado especializado em fraudes bancárias pode ajudar a definir a estratégia mais adequada, seja no Juizado Especial ou na Justiça Comum.

5.3 QUANDO PROCURAR A DEFENSORIA PÚBLICA

A **Defensoria Pública** é uma alternativa gratuita para quem não pode arcar com os custos de um advogado particular. Ela oferece assistência jurídica em casos de fraudes bancárias, garantindo que mesmo pessoas com recursos limitados possam buscar seus direitos na Justiça.

Quando recorrer à Defensoria Pública:

- **Baixa renda:** A Defensoria atende pessoas que comprovem não ter condições financeiras de pagar um advogado sem comprometer o sustento próprio ou da família.
- **Casos complexos:** Em situações em que a fraude envolve **valores mais altos** ou **questões técnicas** que exigem uma defesa mais estruturada, a Defensoria pode ser uma excelente opção, especialmente quando o Juizado Especial não é suficiente.

- **Ações na Justiça Comum:** Para casos que fogem da competência do Juizado Especial Cível, como aqueles que exigem **produção de provas complexas**, a Defensoria Pública pode representar o consumidor na **Justiça Comum**.

Como agir:

- **Pesquise as condições e locais de atendimento da Defensoria Pública** na sua cidade ou estado. Cada Defensoria possui **critérios próprios** para definir quem tem direito ao atendimento gratuito e pode variar quanto à documentação exigida.
- **Agende um atendimento** e leve todos os documentos relacionados ao golpe, como **provas da fraude**, **extratos bancários** e **protocolos de atendimento do banco**.
- **Comprove sua renda** conforme as exigências locais. É importante verificar antecipadamente quais documentos são necessários para atender aos critérios da Defensoria.

5.4 O QUE ESPERAR DA AUDIÊNCIA?

Após ingressar com a ação, o processo judicial passa por **audiências** que são etapas fundamentais para resolver o caso.

Essas audiências podem resultar em acordos entre as partes ou no julgamento final da ação.

Tipos de audiências:

- Audiência de Conciliação:

  A primeira audiência geralmente é destinada à **tentativa de acordo** entre o consumidor e o banco. Um conciliador ou mediador facilita o diálogo para que as partes cheguem a um entendimento sem a necessidade de julgamento. Se o acordo for alcançado, o processo é encerrado.

- Audiência de Instrução e Julgamento:

  Se não houver acordo na conciliação, o processo pode seguir para a audiência de instrução, onde as **provas são apresentadas**, as partes e eventuais **testemunhas são ouvidas**, e o juiz analisa todos os elementos do caso antes de emitir a **sentença final**.

Como se preparar:

- **Organize todas as provas:** Leve todos os documentos, extratos bancários, prints de conversas e qualquer outro material que comprove a fraude.

- **Mantenha a calma e clareza:** Explique o caso de forma objetiva, focando nos fatos e apresentando as evidências de maneira clara.

- **Se for representado por advogado, siga suas orientações:** O advogado guiará o processo e poderá intervir quando necessário.

5.5 AUDIÊNCIA DE CONCILIAÇÃO

A **audiência de conciliação** é a primeira tentativa de resolver o caso de forma amigável, sem a necessidade de um julgamento. Nessa etapa, um **conciliador** ou **mediador** atua para facilitar um acordo entre o consumidor e o banco.

O que acontece na audiência de conciliação:

- **Proposta de acordo:** O banco pode oferecer uma **proposta de ressarcimento** ou compensação. O consumidor tem o direito de **aceitar, recusar** ou **negociar** os termos.
- **Decisão imediata:** Se houver acordo, o juiz **homologa** o resultado, e o processo é encerrado. O banco terá um prazo para cumprir o que foi acordado.
- **Sem acordo:** Caso as partes não cheguem a um consenso, o processo segue para a **audiência de instrução e julgamento**, onde o juiz analisará as provas e dará a sentença.

Como se preparar:

- Avalie, antes da audiência, quais seriam os **termos aceitáveis** de acordo.

- Se representado por advogado, discuta com ele as **vantagens e desvantagens** de

5.6 JULGAMENTO E SENTENÇA

Após concluído a fase de argumentações, o processo é direcionado para sentença, que pode ser:

- **Decisão favorável ao consumidor:** O juiz pode determinar o **ressarcimento integral** dos valores, além de **indenização por danos morais**, se for o caso.
- **Decisão desfavorável:** O banco pode ser isento de responsabilidade se o juiz entender que houve **culpa exclusiva da vítima** ou que o banco adotou todas as medidas de segurança adequadas.

Além disso há possibilidade de extinção e/ou de parcial procedência, cabendo ao advogado que assiste o cliente prestar o esclarecimento correto.

5.7 QUANTO TEMPO O PROCESSO LEVA?

O tempo que um processo de fraude bancária leva para ser concluído pode variar de acordo com a **complexidade do caso** e o **ritmo da Justiça**. No entanto, há algumas estimativas gerais:

Prazos médios:

- **Juizado Especial Cível:** O processo costuma levar entre **8 a 12 meses** para a sentença. Caso haja recurso, o julgamento pode levar mais **8 meses** em média.
- **Justiça Comum:** A sentença costuma ser proferida entre **7 a 10 meses**. Se houver recurso, o julgamento pode levar cerca de **12 meses** adicionais.

O andamento do processo pode ser influenciado por diversos fatores, como a **complexidade da fraude**, a **necessidade de produção de provas** e o **volume de processos** no tribunal, por isso, é fundamental que a vítima verifique com o advogado de sua confiança, a simples alteração do local de andamento do processo pode alterar os prazos médios.

COMO EVITAR NOVOS GOLPES – DICAS PRÁTICAS DE PREVENÇÃO

6

Com o aumento das fraudes bancárias e golpes digitais, adotar **medidas preventivas** é fundamental para proteger seu dinheiro e seus dados pessoais. Os golpistas estão cada vez mais sofisticados, utilizando táticas que exploram a **distração**, o **desconhecimento** e até mesmo o **medo** das vítimas.

Neste capítulo, apresentamos **dicas práticas** e simples para ajudar você a se proteger contra os golpes mais comuns. Pequenas mudanças de comportamento e atenção aos detalhes podem fazer a diferença entre manter sua segurança financeira e cair em uma armadilha.

6.1 DESCONFIE DE LIGAÇÕES E MENSAGENS INESPERADAS

Um dos golpes mais comuns envolve **ligações** ou **mensagens** que parecem vir de bancos, instituições financeiras ou até mesmo amigos e familiares. Os golpistas se passam por **funcionários ou pessoas próximas** e utilizam informações pessoais para ganhar a confiança da vítima.

Como identificar e evitar o golpe:

- **Nunca confie em ligações que pedem senhas ou códigos.** Bancos **nunca solicitam informações confidenciais** por telefone, SMS ou e-mail.
- **Cuidado com mensagens de urgência.** Golpistas costumam criar situações de **pressão**, dizendo que sua conta será bloqueada ou que há uma movimen-

tação suspeita. O lado emocional como, ajudar o filho para pagar uma conta, alegação do filho de que está com acesso bloqueado em seu banco e outras situações similares, devem ser consideradas suspeitas.

- **Verifique o número ou e-mail de origem.** Mesmo que o número pareça oficial, prefira **entrar em contato diretamente** com o banco por canais que você já conhece.
- **Evite clicar em links recebidos por mensagens.** Links falsos podem direcionar para sites que roubam seus dados.

Dica extra: Se receber uma ligação suspeita, **desligue imediatamente** e entre em contato com o banco através dos canais oficiais. O mesmo ocorre quando o contato partir de um amigo ou familiares, ou seja, suspenda imediatamente qualquer contato e compartilhe com outros amigos e/ou familiares sobre o ocorrido.

Confirmar a veracidade do contato pode evitar grandes prejuízos.

6.2 NUNCA COMPARTILHE SENHAS OU CÓDIGOS DE SEGURANÇA

Um dos erros mais comuns que facilitam golpes é o **compartilhamento de senhas** ou **códigos de segurança**. Golpistas usam diversas estratégias para convencer a vítima a fornecer

essas informações, se passando por **funcionários de bancos**, **suporte técnico** ou até **familiares em situações de emergência**.

Como se proteger:

- **Bancos nunca pedem senhas ou códigos por telefone, e-mail ou mensagens.** Se alguém solicitar, é golpe.
- **Nunca informe códigos de verificação enviados por SMS.** Esses códigos são usados para validar acessos em dispositivos desconhecidos.
- **Evite anotar senhas em locais de fácil acesso.** Use **gerenciadores de senhas** ou métodos seguros para armazenar suas informações.
- **Crie senhas diferentes para cada serviço.** Não use a mesma senha no banco, e-mail e redes sociais.

Dica: Mesmo em conversas com pessoas próximas, desconfie de pedidos inesperados.

6.3 USE SENHAS FORTES

Crie senhas fortes e únicas. Combine **letras maiúsculas e minúsculas**, **números** e **caracteres especiais**. Evite senhas óbvias, como datas de aniversário ou sequências simples (ex: 123456).

Troque suas senhas periodicamente. Atualizar suas senhas a cada 3 ou 6 meses reduz o risco de acessos indevidos.

- **Evite salvar senhas em dispositivos compartilhados.** Nunca permita que navegadores salvem senhas em computadores públicos ou de terceiros.

6.4 CUIDADO COM PIX E BOLETOS FALSOS

Com a popularização do **Pix** e o uso frequente de **boletos bancários**, os golpistas encontraram novas formas de aplicar fraudes. Transações instantâneas e pagamentos rápidos facilitam a vida dos usuários, mas também aumentam os riscos se não houver atenção.

Como se proteger:

- **Confirme os dados antes de concluir um Pix.** Sempre verifique o **nome do destinatário** e, se possível, faça uma **transferência teste** com um valor pequeno antes de enviar quantias maiores.
- **Evite copiar e colar chaves Pix enviadas por terceiros.** Prefira digitar manualmente ou selecionar contatos já salvos e verificados.
- **Desconfie de boletos enviados por e-mail ou WhatsApp.** Sempre acesse o site oficial da empresa ou

entre em contato com o fornecedor ou familiar antes de pagar.

- **Confira o código de barras do boleto.** Verifique se o **nome do beneficiário** e o **CNPJ** correspondem à empresa correta. Sites de bancos geralmente permitem essa verificação.

Dica extra: Muitos golpes envolvem **boletos falsificados** que simulam cobranças de **financiamentos** ou **serviços conhecidos**. Sempre baixe boletos diretamente do site oficial ou aplicativo da instituição e na dúvida converse sempre com algum familiar próximo.

6.5 PROTEJA SEUS DISPOSITIVOS: CELULAR, COMPUTADOR E REDES WI-FI

A segurança dos seus dados começa com a proteção dos **dispositivos** que você usa diariamente. Golpistas exploram vulnerabilidades em celulares, computadores e redes Wi-Fi para acessar informações bancárias e pessoais.

Como se proteger:

- **Mantenha seus dispositivos atualizados.** Atualizações de sistema e aplicativos corrigem falhas de segurança que podem ser exploradas por hackers.
- **Instale antivírus e firewalls.** Utilize programas de segurança confiáveis para proteger contra **malwares**, **vírus** e **spywares**.

- **Evite usar redes Wi-Fi públicas para transações bancárias.** Redes abertas são menos seguras e facilitam o acesso de golpistas aos seus dados. Prefira redes privadas e protegidas por senha.
- **Habilite bloqueios de tela e biometria.** Utilize **senhas fortes**, **impressão digital** ou **reconhecimento facial** para impedir o acesso não autorizado ao seu celular ou computador.

Dica extra: Caso seu celular seja **roubado** ou **furtado**, entre em contato com o banco e a operadora para **bloquear imediatamente** o acesso a aplicativos financeiros e cartões.

6.6 REVISE SUAS CONTAS BANCÁRIAS REGULARMENTE

Monitorar suas contas bancárias de forma constante é uma das melhores maneiras de identificar rapidamente atividades suspeitas e evitar grandes prejuízos. Pequenas transações não reconhecidas podem ser o primeiro sinal de um golpe.

Como se proteger:

- **Acompanhe extratos e faturas semanalmente.** Verifique todas as movimentações em sua conta e no cartão de crédito, mesmo as de pequenos valores.
- **Ative notificações de transações.** Configure seu banco para enviar **alertas por SMS ou e-mail** sempre que uma movimentação for realizada. Isso

permite identificar imediatamente qualquer operação suspeita.

- **Fique atento a débitos recorrentes desconhecidos.** Golpistas podem inscrever sua conta em **assinaturas fraudulentas** que passam despercebidas se você não revisar os extratos com atenção.
- **Mantenha limites baixos para transações diárias.** Configure **limites reduzidos** para transferências, saques e Pix. Isso impede que grandes quantias sejam movimentadas rapidamente em caso de golpe.
- **Reaja rapidamente a qualquer irregularidade.** Se identificar algo estranho, **comunique o banco imediatamente** para bloquear a transação e iniciar o processo de contestação.
- **Utilize um celular exclusivo para o banco principal.** É aconselhável manter um **celular separado** apenas para o aplicativo do banco principal, guardado em casa com acesso restrito. Isso reduz o risco de fraudes em caso de roubo ou clonagem do celular usado no dia a dia.

6.7 EXPONHA MENOS INFORMAÇÕES PESSOAIS NAS REDES SOCIAIS

Golpistas utilizam as **redes sociais** como uma ferramenta para coletar informações pessoais que facilitam fraudes e golpes.

Detalhes aparentemente inofensivos, como o nome da escola dos filhos, local de trabalho ou viagens planejadas, podem ser usados para criar **estratégias de manipulação**.

Como se proteger:

- **Evite compartilhar informações sensíveis.** Não publique dados como **número de telefone**, **endereços**, **fotos de documentos** ou qualquer informação bancária.
- **Cuidado com fotos que revelem sua rotina.** Golpistas podem usar detalhes de fotos para **clonagem de identidade** ou para aplicar golpes de engenharia social, fingindo conhecer a vítima pessoalmente.
- **Revise as configurações de privacidade.** Limite o acesso às suas publicações, deixando-as visíveis apenas para **amigos confiáveis**.
- **Desconfie de contatos inesperados.** Mesmo que a mensagem venha de alguém conhecido, confirme por outro meio se a pessoa realmente enviou aquela solicitação, especialmente em casos de **pedidos de dinheiro**.

Dica extra: Evite compartilhar informações sobre **movimentações bancárias** ou conquistas financeiras. Golpistas podem usar esse tipo de dado para direcionar golpes específicos.

CONCLUSÃO – VOCÊ NÃO ESTÁ SOZINHO

7

Ser vítima de um golpe bancário pode causar **ansiedade** e **frustração**, mas é importante lembrar que **qualquer pessoa** pode ser enganada. Os golpes estão cada vez mais sofisticados, explorando tanto a **tecnologia** quanto o **fator humano**.

7.1 CAIR EM UM GOLPE NÃO É SINAL DE FRAQUEZA

Cair em um golpe **não é sinal de fraqueza**. Golpistas utilizam técnicas sofisticadas de **manipulação emocional** e **falhas tecnológicas** para enganar até as pessoas mais cautelosas.

O mais importante é **não se culpar**. Concentre-se em agir rapidamente para **minimizar o prejuízo** e buscar seus direitos.

7.2 TRANSFORMANDO O PREJUÍZO EM APRENDIZADO

Embora ser vítima de um golpe cause **prejuízos financeiros** e **emocionais**, a experiência pode se transformar em um **aprendizado valioso**. Compreender como o golpe ocorreu ajuda a identificar **falhas de segurança** e a se proteger contra fraudes futuras.

Além disso, compartilhar sua experiência com amigos e familiares contribui para alertar outras pessoas e fortalecer a rede de proteção contra golpes.

7.3 A JUSTIÇA PODE ESTAR AO SEU LADO: LUTE PELOS SEUS DIREITOS

A Justiça **pode estar ao seu lado** na busca pela recuperação dos valores perdidos em fraudes bancárias. A legislação brasileira, especialmente o **Código de Defesa do Consumidor (CDC)**, oferece base legal para responsabilizar instituições financeiras e garantir o **ressarcimento** e, em alguns casos, **indenização por danos morais**.

No entanto, cada caso deve ser analisado de forma **individual**, considerando a **complexidade da fraude** e o comportamento da vítima.

Mas, lembre-se, a **responsabilidade do banco** pode ser afastada se for comprovada a **culpa exclusiva da vítima**. Por isso, é importante buscar orientação de **advogados especializados** para avaliar as chances de sucesso antes de entrar com uma ação sem o devido conhecimento.

SUGESTÃO PRÁTICA DE DOCUMENTOS E FERRAMENTAS

8

Este capítulo apresenta **sugestões práticas** para auxiliar vítimas de fraudes bancárias na **formalização de reclamações** e na **organização de documentos** necessários para resolver o problema. As orientações incluem modelos para reclamações junto a bancos, boletins de ocorrência e registros em órgãos de defesa do consumidor.

No entanto, é importante lembrar que estas são **sugestões genéricas**. Cada caso de fraude possui **particularidades** que podem exigir estratégias diferentes. Por isso, é sempre aconselhável que a vítima procure a **orientação de profissionais capacitados**, como **advogados especializados em fraudes bancárias**, para garantir que as medidas adotadas sejam as mais adequadas para o seu caso

8.1 COMO REALIZAR A RECLAMAÇÃO JUNTO AO BANCO

Após identificar a fraude, o primeiro passo formal é registrar uma reclamação junto ao banco. Esse procedimento cria um histórico oficial da ocorrência e pode ser essencial para a recuperação dos valores

81.1 O QUE FALAR

- **Descreva o ocorrido de forma objetiva:** Informe o **tipo de golpe**, **data e horário** das transações suspeitas e o **valor** envolvido.

- **Inclua dados relevantes:** Cite o **protocolo de atendimento** (se já houver), e mencione que está solicitando a **contestação formal** das transações.

8.1.2 O QUE DEVE SER EVITADO

- **Evite relatos confusos ou emocionais.** Mantenha o foco nos **fatos objetivos**.
- **Não forneça senhas ou dados desnecessários.** O banco não precisa de informações como **senha de acesso** ou **códigos de segurança** para registrar a reclamação.
- **Evite dar respostas imprecisas.** Se não lembrar de algum detalhe com certeza, **não afirme nem negue**. Diga que **não se recorda** no momento. Isso é fundamental, pois em situações de nervosismo, fornecer informações incorretas pode **prejudicar a análise do banco**.
- **Não aceite respostas vagas.** Caso o atendente não ofereça um prazo ou solução clara, peça para falar com a **ouvidoria**.

8.2 COMO REALIZAR O BOLETIM DE OCORRÊNCIA

Registrar um Boletim de Ocorrência (B.O.) é fundamental para formalizar o crime. O B.O. pode ser feito online ou presencialmente, dependendo do tipo de golpe.

8.2.1 O QUE DEVE CONTER NO BOLETIM DE OCORRÊNCIA

- **Descrição objetiva do golpe:** Informe como a fraude aconteceu, especificando o **tipo de golpe**, **valores envolvidos**, **datas** e **horários** das transações.
- **Dados das contas envolvidas:** Se souber, inclua informações sobre a conta bancária que recebeu o dinheiro (nome do titular, CPF/CNPJ, banco e agência).
- **Providências tomadas:** Mencione que **informou o banco**, bloqueou cartões e reuniu provas da fraude.

8.2.2 O QUE DEVE SER EVITADO E POR QUÊ?

- **Evite informações imprecisas ou suposições.** Se não lembrar de detalhes específicos, como horários exatos ou o nome do golpista, **não invente** ou chute dados. Diga que **não se recorda com precisão**.
- **Não forneça informações desnecessárias.** Concentre-se nos **fatos relevantes**. Detalhes pessoais que não têm relação com o golpe podem confundir a análise policial.
- **Evite conclusões precipitadas.** Não afirme que a culpa é de determinada instituição sem provas con-

cretas. O foco deve estar nos fatos que comprovam a fraude.

Importante: Após o registro, entregue uma cópia do B.O. ao banco e, se tiver seguro bancário, à seguradora. Isso formaliza a fraude e ajuda a acelerar o processo de ressarcimento.

8.3 COMO RECLAMAR NO BANCO CENTRAL

Se o banco não resolver o problema de forma satisfatória após a reclamação formal, o próximo passo é registrar uma queixa no Banco Central. Essa instituição fiscaliza o setor bancário e pode intervir em casos de descumprimento das normas.

8.3.1 O QUE DEVE CONTER

- **Descrição detalhada da fraude:** Explique como o golpe ocorreu, incluindo o **tipo de fraude**, **valores envolvidos** e as **datas** das transações.
- **Histórico de contato com o banco:** Informe o que foi feito até o momento, mencionando os **protocolos de atendimento**, as **respostas recebidas** e o **descumprimento das soluções** oferecidas.
- **Documentos anexados:** Envie **prints**, **extratos bancários**, o **Boletim de Ocorrência** e qualquer outra prova que fortaleça sua reclamação.

8.3.2 O QUE EVITAR

- **Evite reclamações genéricas ou incompletas.** Quanto mais detalhada a reclamação, maiores as chances de um retorno efetivo.
- **Não use linguagem ofensiva ou emocional.** Mantenha o foco nos fatos, evitando desabafos que não contribuem para a análise.
- **Não omita etapas anteriores.** O Banco Central só atua após esgotadas as tentativas com o próprio banco.

8.4 COMO RECLAMAR NO CONSUMIDOR.GOV.BR

O Consumidor.gov.br é uma plataforma oficial que permite ao consumidor registrar reclamações diretamente com bancos e outras instituições financeiras. O site facilita a mediação entre o cliente e a empresa, oferecendo uma solução rápida e eficiente.

8.4.1 O QUE REGISTRAR

- **Relato objetivo da fraude:** Descreva o **tipo de golpe**, os **valores envolvidos**, e o que já foi feito para resolver o problema junto ao banco (incluindo **protocolos** e **respostas recebidas**).

- **Provas anexadas:** Inclua **prints**, **extratos bancários**, o **Boletim de Ocorrência** e qualquer outro documento que comprove a fraude.
- **Pedido direto:** Solicite o **ressarcimento dos valores.** Informe também se deseja o **cancelamento de cobranças** ou a **retirada de registros negativos** do seu nome.

Como registrar: Acesse www.consumidor.gov.br, faça seu cadastro e selecione a instituição com a qual deseja registrar a reclamação.

8.4.2 O QUE EVITAR

- **Evite relatos longos e confusos.** Mantenha a reclamação clara e objetiva, focando nos fatos principais.
- **Não forneça informações pessoais desnecessárias.** Informe apenas os dados relevantes para a análise do caso.
- **Evite acusações sem provas.** Fique atento para não responsabilizar a instituição indevidamente, o que pode prejudicar sua própria reclamação.

8.5 PLANILHA PARA FACILITAR A IDENTIFICAÇÃO DO PREJUÍZO FINANCEIRO

Ter um controle exato sobre o **prejuízo financeiro** é fundamental para fortalecer sua reclamação junto ao banco e, se necessário, na Justiça. Saber com precisão o **valor total perdido** e as **transações específicas** ocorridas na fraude facilitam o processo.

Para que a planilha seja eficiente, é importante incluir informações detalhadas sobre cada transação contestada:

- **Data e horário da operação:** Registre o momento exato em que cada transação foi realizada.
- **Valor total da transação:** Informe o valor exato de cada movimentação.
- **Beneficiário:** Inclua o nome ou identificação da pessoa ou empresa que recebeu o valor.
- **Tipo de transação:** Especifique se foi realizada via **Pix**, **transferência bancária**, **cartão de crédito**, **saque**, **empréstimo** ou outro tipo de movimentação.

8.5.1 ORGANIZAÇÃO DA PLANILHA:

- **Ordem cronológica:** Liste as transações em sequência, da **primeira até a última operação**. Isso facilita a análise do caso pelo banco ou pela Justiça.

8.5.2 FORMATO DA PLANILHA:

- **Uso de programas recomendados:** Utilizar programas como **Excel** ou **Google Sheets** é aconselhável, pois facilita a visualização e o ajuste das informações.
- **Alternativa manual:** Caso o acesso a programas seja difícil, a planilha pode ser feita **manualmente em uma folha**, desde que seja **legível, organizada e correta**.

8.6 DOCUMENTOS OBRIGATÓRIOS E COMO CONSEGUIR

A organização de **documentos comprobatórios** é essencial para fortalecer sua reclamação junto ao banco e, se necessário, na Justiça. Esses documentos ajudam a demonstrar a **ocorrência da fraude**, o **valor do prejuízo** e as **providências adotadas**.

Todos os documentos necessários devem ser **fornecidos pelo banco** mediante solicitação formal.

Sempre peça que os documentos sejam enviados em **formato PDF** ou **impresso em folha sulfite**.

Não aceite extratos fornecidos por caixas eletrônicos, pois o papel térmico utilizado nesses terminais apaga com o tempo e pode prejudicar a comprovação.

Além disso, os **extratos emitidos por terminais gerenciais ou pelo SAC** são mais completos e detalhados. Caso o banco **recuse a apresentação** dos documentos solicitados, registre uma reclamação na **ouvidoria** da instituição. Se ainda assim o problema não for resolvido, leve a reclamação ao **Banco Central** para garantir que seus direitos sejam respeitados.

8.6.1 DOCUMENTOS MÍNIMOS NECESSÁRIOS

Para comprovar a fraude e iniciar o processo de contestação, é fundamental reunir os seguintes **documentos mínimos**:

- **Extratos bancários detalhados** (em PDF ou impressos em folha sulfite).
- **Comprovantes de segunda via** de **transferências**, **pagamentos** e **saques**.
- **Faturas de cartão de crédito** com as transações contestadas.
- **Cópias de contratos de empréstimos** não reconhecidos.

Esses documentos são essenciais para demonstrar o **prejuízo financeiro** e identificar as **movimentações fraudulentas**.

8.7 OS RISCOS DO PROCESSO NO JUIZADO ESPECIAL

O **Juizado Especial Cível** é uma alternativa prática para resolver conflitos de menor valor. No entanto, optar por essa via também envolve **riscos** que precisam ser avaliados com cuidado.

O principal risco está na **limitação do rito** do Juizado, que **não permite a produção de provas complexas**, como perícias detalhadas, o que pode prejudicar casos de fraudes mais sofisticadas.

Além disso, se a ação for julgada **improcedente**, o consumidor poderá ser responsabilizado por **custas processuais** em caso de recurso, o que pode aumentar o prejuízo. E, em muitos casos, processos são **extintos** pela complexidade da fraude, que exige uma análise mais profunda, o que não é permitido no juizado.

Por isso, é fundamental fazer uma **análise consciente e técnica** antes de ingressar com a ação.

Consultar um **advogado especializado em fraudes bancárias** pode ajudar a definir se o Juizado é a melhor opção ou se o caso deve ser levado à Justiça Comum.

IMPORTANTE

9.1 USO CORRETO DAS INFORMAÇÕES

O conteúdo deste e-book tem caráter exclusivamente informativo e visa oferecer uma avaliação educativa sobre golpes e fraudes bancárias.

As informações aqui apresentadas servem **apenas** para orientar e conscientizar o leitor, mas não substituem a orientação de um profissional qualificado, como um advogado especializado em fraudes bancárias.

Cada situação é única e deve ser analisada com o devido acompanhamento técnico e jurídico. O uso inadequado das informações, sem a devida consulta profissional, pode resultar em decisões incorretas.

Os resultados de ações judiciais podem variar de acordo com a complexidade da fraude e as provas apresentadas.

Reforçamos a importância de buscar orientação profissional qualificada para cada situação concreta

CONSULTAS E MENTORIAS ESPECIALIZADAS

10

10.1 A IMPORTÂNCIA DA CONSULTORIA ESPECIALIZADA

Cada fraude bancária possui suas **especificidades**, e o sucesso na recuperação do prejuízo depende da correta **análise do caso concreto**. Consultar um **advogado especializado em fraudes bancárias** ajuda a identificar **estratégias adequadas**, seja na via administrativa ou judicial.

A consultoria especializada pode auxiliar na:

- **Avaliação de riscos** antes de ingressar com uma ação judicial.
- **Orientação sobre documentação** necessária e como obtê-la corretamente.
- **Análise de decisões judiciais anteriores** para definir a melhor abordagem.

10.2 MENTORIA JURÍDICA AVANÇADA PARA ADVOGADOS

A **mentoria jurídica** é um procedimento adequado para **advogados** que buscam uma **análise avançada** de casos de fraudes bancárias. Trata-se de uma **consulta em nível elevado**, voltada para a **discussão técnica** de um caso concreto, com foco em **estratégias jurídicas específicas**.

Durante a mentoria, o profissional especializado pode:

- Realizar uma **análise aprofundada do caso** em conjunto com o advogado.
- Sugerir **estratégias jurídicas** personalizadas, considerando jurisprudências e peculiaridades do caso.
- **Orientar sobre a confecção de peças processuais**, incluindo petições iniciais, recursos e manifestações específicas.

10.3 COMO AGENDAR CONSULTAS E MENTORIAS

As **consultas e mentorias** deverão ser realizadas mediante **agendamento prévio** através dos **canais de atendimento oficiais** disponíveis no site: **www.alexandreberthe.com.br.**

Todos os procedimentos são realizados mediante **remuneração ajustada previamente**, com valores **compatíveis com o mercado**.

AVISO LEGAL

Todo o conteúdo deste e-book é **protegido pelas leis de direitos autorais**, sendo **propriedade intelectual** do advogado **Alexandre Berthe Pinto**. A **divulgação total ou parcial** deste material é **autorizada**, desde que seja realizado o devido **crédito ao autor** e mediante **prévia autorização**.

O material foi elaborado com base em **pesquisas diversas**, incluindo **legislação vigente**, **jurisprudências** e **relatos de casos reais**. No entanto, o conteúdo apresentado **não constitui uma afirmação incontroversa** ou absoluta sobre os temas abordados, podendo variar conforme a **evolução das leis**, **decisões judiciais** e **circunstâncias específicas** de cada caso.

Alexandre Berthe Pinto, é advogado inscrito na OAB/SP há mais de vinte anos, ao longo de sua carreira já teve a oportunidade de ser entrevistado pelos principais meios da imprensa do Brasil, existindo farta documentação sobre seu histórico de atuação nos mais diversos sites de buscas e disponíveis no site do escritório, que leva seu nome.

alexandreberthe.advogado

@alexandreberthe

/alexandre_berthe/

/@duvidajuridica

+55 11 94335-8334 (apenas texto)

11 5093-2572 / 5093-5896

www.alexandreberthe.com.br