A ATUALIZAÇÃO HERMENÊUTICA DO FORTUITO INTERNO BANCÁRIO EVOLUÇÃO DAS FRAUDES NO SISTEMA BANCÁRIO E O DEVER DE VIGILÂNCIA TECNOLÓGICA À LUZ DO TEMA REPETITIVO 466/STJ

THE HERMENEUTICAL UPDATE OF BANKING INTERNAL FORTUITY EVOLUTION OF FRAUD IN THE BANKING SYSTEM AND THE DUTY OF TECHNOLOGICAL VIGILANCE IN LIGHT OF REPETITIVE THEME 466/STJ

Letícia Zétola Portes – Juíza de Direito do Tribunal de Justiça do Estado do Paraná, integrante da 3ª Turma Recursal dos Juizados Especiais Cíveis do TJPR.
Lattes: http://lattes.cnpq.br/3233785089583725
e-mail: lzpo@tjpr.jus.br

Jéssica Menzyski Markus – Técnica Judiciária do Tribunal de Justiça do Estado do Paraná, especialista em Direito Processual Civil pelo Instituto de Direito Romeu Felipe Bacellar.
Lattes: http://lattes.cnpq.br/3233785089583725
E-mail: jmen@tjpr.jus.br

O estudo propõe uma releitura hermenêutica do fortuito interno bancário diante da transformação tecnológica do sistema financeiro e da sofisticação das fraudes digitais. A partir do Tema Repetitivo 466/STJ e do artigo 14 do Código de Defesa do Consumidor, examina-se a transição do risco físico para o risco informacional, identificando o Know Your Client (KYC) como núcleo técnico do dever jurídico de segurança. O trabalho analisa decisões recentes das Turmas Recursais do TJPR, TJSP e TJDFT, demonstrando que a aplicação contemporânea do Tema 466 exige a aferição da diligência bancária com base em métricas objetivas de compliance e monitoramento comportamental. Conclui-se que a responsabilidade objetiva das instituições financeiras permanece íntegra, mas sua verificação deve acompanhar a realidade tecnológica do serviço, sob pena de anacronismo na tutela do consumidor.

PALAVRAS-CHAVE: Fortuito interno; Responsabilidade bancária; KYC; Fraudes digitais; Hermenêutica jurídica; Tema 466/STJ.

This study proposes a hermeneutic reinterpretation of the banking internal fortuity concept in light of the technological transformation of the financial system and the growing sophistication of digital frauds. Based on the Repetitive Theme 466 of the Brazilian Superior Court of Justice (STJ) and Article 14 of the Consumer Protection Code, it examines the shift from physical to informational risk, identifying Know Your Client (KYC) as the technical core of the legal duty of security. The research analyzes recent decisions from the Small Claims Courts of Paraná, São Paulo, and the Federal District (2023–2025), demonstrating that the contemporary application of Theme 466 requires assessing banking diligence through objective metrics of compliance and behavioral monitoring. It is concluded that the strict liability of financial institutions remains intact, but its assessment must keep pace with the technological reality of banking services, under penalty of rendering consumer protection anachronistic.

KEYWORDS: *Internal fortuity; Banking liability; KYC; Digital fraud; Legal hermeneutics; Theme 466/STJ.*

INTRODUÇÃO

O sistema financeiro brasileiro passou, nas últimas duas décadas, por transformação estrutural decorrente da expansão das plataformas digitais e da universalização do smartphone como meio de acesso aos serviços bancários. A contratação de crédito, as transferências instantâneas e os pagamentos remotos democratizaram o acesso ao serviço, mas ampliaram a superfície de risco, com fraudes cada vez mais recorrentes viabilizadas por engenharia social e por técnicas ilícitas de captura de acesso.

Nesse cenário, a vulnerabilidade do consumidor resulta não apenas da assimetria técnica típica das relações de consumo, mas também do fato de que o serviço bancário passou a operar dentro do dispositivo pessoal do usuário. A situação é mais sensível para idosos, cuja inserção na cultura digital foi acelerada e, muitas vezes, incompleta, o que os expõe a golpes que impactam diretamente sobre benefícios previdenciários.

Diante dessa realidade, impõe-se revisitar a aplicação da responsabilidade objetiva das instituições financeiras fixada pelo Superior Tribunal de Justiça, especialmente à luz da Súmula 479/STJ e do Tema Repetitivo 466/STJ. Esses marcos consolidam que fraudes praticadas por terceiros no âmbito das operações bancárias caracterizam fortuito interno e atraem

a responsabilidade do banco, por decorrerem do risco inerente à atividade. A tese permanece íntegra, mas sua operação prática deve acompanhar a evolução tecnológica do próprio serviço.

A fraude contemporânea se consuma dentro do ambiente digital do próprio banco, mas tem início fora dele, a partir da manipulação direta do correntista. Com os sistemas bancários cada vez mais sofisticados e dotados de múltiplas camadas de autenticação, o fraudador passou a concentrar seus esforços no usuário, visto como o elo vulnerável da cadeia de segurança. Golpes como o da falsa central de atendimento, o encaminhamento para atendimento via WhatsApp, e a contratação fraudulenta de empréstimos consignados com imediata dissipação dos valores ilustram esse novo modelo de fraude híbrida, em que a violação não se dá por invasão do sistema central do banco, mas pela indução do cliente a realizar — ou permitir — operações ilícitas dentro do ambiente legítimo.

Ao contratar serviços bancários, o consumidor parte da premissa de que a segurança é elemento essencial do próprio serviço, e não benefício adicional. Diante da sofisticação crescente das fraudes digitais, um ambiente seguro não é aquele que apenas exige múltiplas validações de acesso, mas aquele capaz de antever o desenrolar da fraude e impedi-la antes de sua consumação, por meio do monitoramento inteligente das transações e da leitura comportamental do perfil individual de cada cliente. A efetividade do dever de segurança, portanto, depende menos da rigidez de autenticações e mais da capacidade preditiva e reativa da instituição financeira, que deve atuar para neutralizar riscos inerentes à atividade que exerce.

A discussão sobre a responsabilidade bancária nas fraudes digitais também tem ocupado espaço relevante no debate institucional dos Juizados Especiais. No Congresso Nacional dos Juizados Especiais, realizado em comemoração aos 30 anos da Lei 9.099/95, destacou-se a importância de fortalecer a proteção do consumidor no ambiente digital e de exigir das instituições financeiras uma compreensão ativa do perfil de seus clientes, como forma de aprimorar a prevenção e a detecção de fraudes. Essa orientação reforça a necessidade de que o dever de segurança bancária seja interpretado à luz das condições tecnológicas atuais e dos princípios fundadores dos Juizados — simplicidade, celeridade e efetividade da tutela jurisdicional.

A relevância deste estudo reside na formulação de parâmetros verificáveis para a aferição da diligência bancária no ambiente digital, compatibilizando a responsabilidade objetiva prevista no artigo 14 do Código de Defesa do Consumidor (CDC) com as novas formas de risco introduzidas pela democratização do sistema financeiro em ambiente digital. A aplicação do Tema 466, portanto, não se limita à reafirmação da culpa objetiva, mas demanda a definição de métricas técnicas e comportamentais que traduzam o dever jurídico de segurança à luz da realidade tecnológica contemporânea.

Metodologicamente, a pesquisa se estrutura a partir da análise dos julgados paradigmáticos do Superior Tribunal de Justiça, especialmente os que originaram o Tema 466, confrontando-os com decisões recentes dos Juizados Especiais do Tribunal de Justiça do Paraná, bem como com o marco regulatório do Banco Central do Brasil relativo à prevenção de fraudes e ao monitoramento de operações financeiras. O objetivo é harmonizar o entendimento consolidado pelo STJ com a dinâmica tecnológica atual, fornecendo subsídios para o aprimoramento da tutela jurisdicional nos casos de fraude bancária, sobretudo quando envolvem consumidores idosos e hipervulneráveis, cujas condições de proteção demandam maior sensibilidade institucional.

1 O TEMA REPETITIVO 466/STJ E A CONSOLIDAÇÃO DO FORTUITO INTERNO BANCÁRIO

A jurisprudência do Superior Tribunal de Justiça consolidou, com o julgamento dos Recursos Especiais 1.197.929/PR e 1.199.782/PR, a compreensão de que as instituições financeiras respondem objetivamente pelos danos decorrentes de fraudes praticadas por terceiros no âmbito de operações bancárias. Esses precedentes, julgados sob o rito dos recursos repetitivos, originaram o Tema 466, que fixou a tese segundo a qual "as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias".

No voto condutor do Ministro Luís Felipe Salomão, observou-se uma reconstrução jurisprudencial que remonta a precedentes anteriores da Corte, nos quais já se firmava a responsabilidade objetiva das instituições financeiras diante de eventos lesivos ocorridos no curso da atividade bancária. O histórico apresentado no voto revela que os casos paradigmáticos que consolidaram essa linha de entendimento envolviam situações mais concretas e materiais, como furto de talonários de cheque, uso de documentos falsos ou contratações presenciais indevidas. Nessas hipóteses, era relativamente simples identificar a conduta omissiva do banco que consistiam na falta de conferência documental, negligência na guarda de valores ou liberação indevida de crédito — o que facilitava a aplicação do conceito de fortuito interno e a consequente responsabilização objetiva.

Contudo, o contexto atual é substancialmente diverso. As fraudes contemporâneas deixaram de explorar falhas estruturais ou administrativas do sistema bancário e passaram a incidir sobre o próprio consumidor, por meio de estratégias de engenharia social. Em vez de falsificar documentos ou invadir sistemas, o fraudador agora se apresenta como se fosse o banco: liga para o cliente, envia mensagens em nome da instituição, cria canais falsos de atendimento e conduz o correntista a executar, pessoalmente, as operações que viabilizam o golpe. Essa inversão de vetor — do ataque ao sistema para o ataque à pessoa — redefine o campo de análise da responsabilidade bancária e desafia a

aplicação tradicional da tese firmada a partir de eventos ocorridos há mais de uma década.

Em razão dessa nova dinâmica, as instituições financeiras têm reiterado, em suas defesas, a alegação de que tais fraudes configuram fortuito externo ou que houve culpa exclusiva do consumidor, por ter fornecido senhas, acessado links fraudulentos ou seguido orientações criminosas. Todavia, essa argumentação ignora que o próprio modelo de negócio bancário mudou: o serviço passou a operar quase integralmente em ambiente digital, em que a interação ocorre por meio de aplicativos, canais remotos e autenticações eletrônicas, todos sob controle tecnológico e informacional do próprio banco.

O ambiente digital traz ganhos inegáveis de agilidade, eficiência e disponibilidade, mas também ampliou o espectro de risco da atividade financeira. A mesma tecnologia que permite transações instantâneas, atendimento contínuo e redução de custos operacionais, expõe o usuário a novas formas de vulnerabilidade, em que o elo humano — o cliente — se torna o principal alvo dos fraudadores. Assim, o risco da atividade não desaparece com a digitalização; apenas se transforma.

Embora o contexto das fraudes tenha se transformado, o núcleo jurídico da tese firmada pelo Superior Tribunal de Justiça permanece intacto. A responsabilidade das instituições financeiras continua a ser objetiva, e o fortuito que decorre das fraudes praticadas no ambiente bancário — ainda que por terceiros — mantém natureza interna, por se inserir no âmbito de previsibilidade e controle da atividade. A digitalização do sistema financeiro não desloca o risco para fora da instituição; ao contrário, amplia sua esfera de deveres.

A hermenêutica jurídica, em sentido gadameriano, recorda que interpretar não é reescrever o texto, mas atualizar o seu sentido no horizonte do presente. A aplicação do Tema 466 às fraudes digitais não representa tentativa de forçar a tese a um novo contexto, mas o exercício de compreensão que preserva sua orientação original diante da mutação tecnológica do serviço bancário. O precedente não é uma moldura estanque, mas um ponto de partida cuja eficácia depende de ser lido à luz das condições em que o risco se manifesta. Reinterpretar é, nesse caso, permanecer fiel à ratio decidendi, evitando o anacronismo de aplicar mecanicamente categorias pensadas para um modelo bancário que já não existe.

O que muda, portanto, não é o fundamento jurídico da responsabilidade, mas a forma de aferi-la. O dever de segurança, que antes se traduzia em vigilância física e verificação documental, passa a exigir inteligência tecnológica, monitoramento preditivo e mecanismos automáticos de resposta. Assim, a leitura contemporânea do Tema 466 impõe que o conceito de fortuito interno acompanhe a transformação digital da própria atividade bancária, reconhecendo que as operações eletrônicas, pela sua instantaneidade e rastreabilidade, pertencem ao domínio técnico do fornecedor do serviço.

Portanto, a sofisticação das fraudes não enfraquece a tese firmada pelo STJ; ao contrário, reforça sua atualidade. A responsabilidade

objetiva e o reconhecimento do fortuito interno constituem hoje, mais do que nunca, os pilares de um sistema financeiro que se pretende confiável, inclusivo e tecnologicamente seguro. Essa constatação conduz à reflexão de que se a modernização das operações bancárias ampliou a conveniência e o alcance dos serviços, também redefiniu a natureza e a escala do risco.

2 A TRANSFORMAÇÃO TECNOLÓGICA DO SISTEMA FINANCEIRO E A NOVA DIMENSÃO DO RISCO

A modernização do sistema financeiro nas últimas duas décadas não apenas alterou o modo de operar das instituições bancárias, mas também transformou a própria natureza do risco envolvido. O que antes se concentrava em estruturas físicas e processos administrativos — cofres, agências, documentos, assinaturas — passou a se manifestar em ambientes digitais integrados, automatizados e permanentemente acessíveis. A atividade bancária se tornou, ao mesmo tempo, mais eficiente e mais exposta.

A democratização do acesso aos serviços financeiros, impulsionada pela popularização dos smartphones, das contas digitais e das transferências instantâneas via PIX, inaugurou um modelo de interação direta e contínua entre o consumidor e o banco. O atendimento passou a ocorrer por múltiplos canais, a qualquer hora e em qualquer lugar, rompendo as antigas barreiras de tempo e espaço que delimitavam o relacionamento bancário. Esse avanço representa um marco de inclusão financeira e de ampliação do acesso ao crédito, mas também resultou na expansão da superfície de ataque das operações, com o surgimento de vulnerabilidades antes inexistentes.

O novo ambiente bancário digital é caracterizado por velocidade, conectividade e automatização, mas também pela ausência de mediação humana — elemento que, no modelo tradicional, funcionava como filtro de segurança. O cliente hoje executa, sozinho, operações complexas de crédito, investimento e transferência, confiando em interfaces simplificadas que tornam o processo rápido, porém menos reflexivo. O design digital elimina etapas de conferência e checagem — como a leitura de contratos ou a verificação atenta de dados sensíveis — e transforma a execução de operações complexas em ações simples: um clique, um toque, um reconhecimento facial. Essa simplificação, embora amplie a acessibilidade e o conforto do usuário, reduz suas defesas cognitivas e facilita a atuação de fraudadores que se apropriam da linguagem e da aparência dos próprios canais bancários para enganar o consumidor.

Nesse contexto, o risco deixa de ser meramente operacional e passa a ser sistêmico, pois decorre da própria forma como o modelo digitalizado de negócios se estrutura. Cada nova camada de conveniência adiciona também uma camada de exposição. A mesma tecnologia que permite transferências instantâneas é a que possibilita a dissipação imediata de valores subtraídos; o mesmo sistema que personaliza ofertas de crédito com base no perfil de consumo

é capaz de ser manipulado por terceiros que dominam a engenharia comportamental.

O resultado é um sistema de alta performance, mas de fragilidade distribuída, em que o elo mais vulnerável — o usuário — se torna o principal vetor de acesso indevido. O consumidor, que antes dependia de intermediação institucional para movimentar sua conta, tornou-se o operador direto de todas as etapas da transação. E, paradoxalmente, essa autonomia reforça a dependência do banco, pois é a instituição quem detém todos os instrumentos técnicos de monitoramento, rastreio e bloqueio de operações suspeitas.

Assim, a transformação tecnológica redefiniu a natureza do dever de segurança e o banco não é mais apenas guardião de valores, mas gestor de riscos informacionais e comportamentais. A proteção esperada pelo consumidor não se limita à integridade do saldo ou à inviolabilidade do sistema, mas à capacidade da instituição de identificar, em tempo real, comportamentos atípicos que revelem a iminência de fraude. Esse novo dever de segurança, que ultrapassa o plano técnico e se projeta como obrigação jurídica de resultado, encontra fundamento direto no artigo 14 do Código de Defesa do Consumidor e se realiza por meio das estruturas de compliance financeiro, voltadas tanto à prevenção quanto à reação frente aos riscos digitais.

3 *COMPLIANCE* FINANCEIRO E O DEVER JURÍDICO DE SEGURANÇA NO CDC

A segurança constitui elemento essencial da prestação de serviços bancários. No regime do artigo 14 do Código de Defesa do Consumidor, o fornecedor responde objetivamente pelos danos decorrentes de defeitos na execução do serviço, o que inclui falhas de prevenção, detecção ou contenção de fraudes. No setor financeiro, esse dever de segurança assume natureza técnica e contínua. A proteção do consumidor não se restringe à integridade dos valores depositados, mas abrange a preservação da confiança no ambiente digital em que o serviço é prestado.

A partir dessa perspectiva, o compliance financeiro não se limita a uma política interna de governança, mas configura o núcleo jurídico do dever de segurança. A instituição bancária, ao operar em ambiente digital, deve adotar sistemas de monitoramento capazes de identificar e reagir a situações atípicas, inclusive quando originadas por condutas de terceiros. A diligência esperada do banco é, portanto, dupla: preventiva e reativa. No plano preventivo, envolve a identificação de riscos antes que se materializem; no plano reativo, impõe a resposta imediata e eficaz quando a fraude ocorre, mediante bloqueio, rastreamento e restituição de valores.

Nesse contexto, ganha relevo o princípio do "Know Your Client" (KYC) — expressão consagrada no sistema financeiro internacional que significa "Conheça o seu cliente". Originalmente voltado ao combate à lavagem de dinheiro e ao financiamento do terrorismo, o KYC evoluiu para uma política mais ampla de conhecimento e rastreabilidade do comportamento do usuário. Seu objetivo é assegurar que o banco compreenda o perfil de

cada cliente, suas movimentações habituais e padrões de uso, permitindo reconhecer, com base em dados objetivos, quando uma transação destoa do comportamento usual.

No ambiente digital, esse conhecimento não é apenas requisito regulatório, mas ferramenta essencial de segurança. Um sistema de compliance tecnicamente adequado deve ser capaz de combinar informações cadastrais estáticas, como identidade e origem dos recursos, com dados dinâmicos de comportamento: horários de acesso, dispositivos utilizados, volume de transferências e histórico de relacionamento. A correlação entre esses fatores possibilita a detecção automática de anomalias e a intervenção tempestiva, antes que o dano se consuma.

As normas do Banco Central do Brasil estruturam o dever jurídico de segurança das instituições financeiras sob uma lógica de prevenção contínua baseada em risco. A Circular nº 3.978/2020 e a Resolução BCB nº 119/2021 estabelecem que os bancos devem implementar políticas, procedimentos e controles internos capazes de identificar, classificar e monitorar clientes e operações de acordo com o risco que representam. Embora editada no contexto da prevenção à lavagem de dinheiro e ao financiamento do terrorismo, essa norma consagra um modelo de compliance comportamental e dinâmico, aplicável também à detecção de fraudes e irregularidades em transações eletrônicas.

Esse conjunto normativo demonstra que o compliance financeiro passou a integrar o núcleo jurídico do dever de segurança bancária. A negligência na utilização efetiva desses mecanismos — seja pela ausência de monitoramento dinâmico, seja pela omissão no bloqueio e devolução de valores — não configura mero erro técnico, mas descumprimento de uma obrigação legal expressa e, portanto, falha na prestação do serviço nos termos do artigo 14 do Código de Defesa do Consumidor.

Desse modo, a aferição da responsabilidade civil das instituições financeiras não pode prescindir da análise da estrutura de compliance e dos mecanismos de KYC efetivamente implementados. A ausência de ferramentas inteligentes de detecção de transações atípicas, de alertas comportamentais e de bloqueios automáticos não revela apenas falha técnica, mas descumprimento de um dever jurídico inerente à própria natureza do serviço bancário digital.

A consolidação dessa compreensão é fundamental para os Juizados Especiais, que enfrentam diariamente litígios envolvendo fraudes digitais. O exame do cumprimento do dever de segurança deve se apoiar em critérios verificáveis: logs de operação, alertas de risco, registros de bloqueio e acionamento do Mecanismo Especial de Devolução (MED). Esses elementos permitem aferir, com objetividade, se o banco atuou de forma diligente ou se a fraude decorreu da omissão em sua governança tecnológica.

Assim, o compliance financeiro, em sua dimensão contemporânea, representa a tradução operacional da responsabilidade objetiva reconhecida pelo Superior Tribunal de Justiça no Tema 466. É, portanto, a ponte entre o dever

jurídico de segurança e a efetividade técnica das ferramentas disponíveis às instituições.

4 *KNOW YOUR CLIENT* (KYC) E A AFERIÇÃO OBJETIVA DA DILIGÊNCIA BANCÁRIA

A diretriz internacional de Know Your Client (KYC) é o eixo central do sistema de prevenção de riscos no setor financeiro. Trata-se de um conjunto de práticas destinadas a conhecer o perfil, o comportamento e as transações de cada cliente, com o objetivo de garantir a integridade das operações. No modelo contemporâneo de banco digital, o KYC não é um procedimento pontual, mas um processo contínuo: o cliente é permanentemente "lido" pelo sistema, que monitora e classifica riscos a partir de dados comportamentais.

No estágio mais avançado do compliance, o KYC se desdobra em duas camadas complementares: o KYC estático, voltado à identificação formal (documentos, dados cadastrais, histórico de relacionamento, origem de recursos), e o KYC dinâmico, que observa o comportamento do cliente em tempo real — como, quando, de onde e em que condições ele realiza suas operações. Essa segunda camada é a que realmente mede a diligência tecnológica do banco, pois é nela que se insere a capacidade de detectar fraudes antes que se consumam.

Do ponto de vista técnico, as instituições financeiras dispõem de ferramentas sofisticadas para análise de risco transacional. Cada cliente possui um perfil comportamental que serve de referência para o sistema: dias e horários usuais de movimentação, localizações habituais de acesso, tipo de dispositivo utilizado, valores médios de transação, destinatários recorrentes e canais preferenciais. Quando uma operação foge desse padrão — por exemplo, quando ocorre à noite, em local ou dispositivo incomum, em valor elevado ou direcionada a contas recém-criadas — o sistema deve emitir alertas de anomalia.

Esses alertas não são opcionais; fazem parte do ciclo de governança de segurança. Uma vez detectado o desvio, o banco deve aplicar regras de bloqueio preventivo, verificação ativa e acionamento do Mecanismo Especial de Devolução (MED). O não funcionamento efetivo dessas etapas configura falha de compliance. É exatamente nesse ponto que se mede a diligência bancária; não apenas pela existência do sistema, mas por sua capacidade de reagir em tempo hábil à fraude em curso.

Transações típicas de fraude apresentam padrões que, sob análise técnica, são facilmente reconhecíveis. Entre os exemplos mais recorrentes estão: saques ou transferências integrais de empréstimos recém-contratados, acessos simultâneos em localidades distintas, alteração repentina de limites seguida de movimentações atípicas, envio de recursos a contas de passagem recém-abertas e sequências de PIX fracionados com destino idêntico em curto intervalo de tempo. São todos comportamentos que um sistema de KYC dinâmico, bem calibrado, deve detectar automaticamente.

Se o banco é capaz de reconhecer padrões de consumo para ofertar crédito ou aumentar

limites, também é capaz — e juridicamente obrigado — a reconhecer esses sinais de irregularidade e agir preventivamente. A omissão diante de indicadores objetivos de risco revela falha na prestação do serviço e vulnera o dever de segurança.

As normas do Banco Central do Brasil reforçam e detalham essa obrigação. A Circular nº 3.978/2020 instituiu um modelo de compliance baseado em risco, impondo às instituições financeiras a adoção de políticas e controles internos para prevenir o uso do sistema financeiro em práticas ilícitas. Posteriormente, a Resolução BCB nº 119/2021 atualizou e aperfeiçoou a Circular, adaptando-a à realidade das operações digitais e ampliando o dever de identificação e verificação. Assim, o banco deve coletar e manter dados capazes de avaliar a capacidade financeira, os padrões de comportamento e a origem dos recursos de cada cliente — tanto pessoas físicas quanto jurídicas.

Essas normas converteram o KYC em verdadeira obrigação jurídica permanente, destinada não apenas à prevenção de lavagem de dinheiro, mas à integridade do sistema financeiro e à segurança das transações digitais. O artigo 18 da Circular, com redação dada pela Resolução, impõe o monitoramento contínuo das operações, exigindo que as instituições avaliem a compatibilidade entre o perfil cadastrado e o comportamento real do cliente, de modo a detectar anomalias antes que causem prejuízo.

Em síntese, o Know Your Client traduz, no plano tecnológico, o dever jurídico de segurança reconhecido pelo Código de Defesa do Consumidor, reafirmado pelo Tema 466 e pormenorizado pelo Banco Central do Brasil. A instituição financeira que conhece o cliente para ampliar crédito ou ofertar produtos deve conhecê-lo, com igual rigor, para protegê-lo. Ignorar alertas e anomalias, quando dispõe de meios tecnológicos para preveni-los, não caracteriza fortuito externo; constitui falha de diligência.

5 JURISPRUDÊNCIA DOS JUIZADOS ESPECIAIS — APLICAÇÃO CONTEMPORÂNEA DO TEMA REPETITIVO 466/STJ SOB A ÓTICA DO KYC

A jurisprudência recente dos Juizados Especiais demonstra que o Tema 466 não apenas mantém plena atualidade, mas vem sendo reinterpretado à luz das novas dinâmicas digitais do risco bancário.

A análise de decisões recentes das Turmas Recursais do TJPR, TJSP e TJDFT, colhidas exemplificativamente, evidencia a transição do fortuito interno clássico — baseado em falhas documentais ou operacionais — para o fortuito interno informacional, em que a falha do serviço decorre da inobservância dos deveres de compliance e de monitoramento comportamental (KYC).

O levantamento não pretende ter caráter estatístico, mas oferecer um panorama contemporâneo e representativo da aplicação prática do Tema 466 nos Juizados Especiais.

Aplicação do Tema 466/STJ e do dever de segurança comportamental		
Categoria de fraude / caso-tipo	**Processo / Tribunal / Data / Turma**	**Resultado / Síntese**
Golpe da falsa central / falso funcionário	0007777-24.2024.8.16.0018 – TJPR – 3ª Turma Recursal – julgado em 15/03/2025	Reconhecida a falha do banco por permitir PIX no crédito e empréstimo fora do perfil. Fortuito interno reconhecido, mas afastada.
	0052081-04.2024.8.16.0182 – TJPR – 1ª Turma Recursal – 20/02/2025	Transações realizadas mediante inserção de senha pessoal pela própria correntista. Não comprovado uso de dados sigilosos nem sistema de convencimento sofisticado. Configurado fortuito externo e culpa exclusiva do consumidor.
	0735541-62.2025.8.07.0016 – TJDFT – 2ª Turma Recursal – 14/08/2025	Configurado fortuito interno, com reconhecimento da hipervulnerabilidade da consumidora e falha no dever de vigilância e resposta.
	4000035-85.2025.8.26.0010 – TJSP – 6ª Turma – 07/10/2025	Configurado fortuito externo e culpa exclusiva da vítima Autora realizou voluntariamente as operações de PIX e contratação de empréstimo, seguindo instruções de estelionatários, sem violação do sigilo bancário. Perfil de movimentações financeiras frequentes e compatíveis com as operações realizadas.
Furto ou roubo de celular	0001928-80.2024.8.16.0209 – TJPR – 2ª Turma Recursal – 16/09/2025	Reconhecida a falha no dever de segurança em transações realizadas após o furto do celular da consumidora, com compras e saques via PIX efetuados fora do padrão de

		consumo. O banco não bloqueou as movimentações nem cancelou as transações, mesmo após comunicação imediata. Declarada a inexistência de débito e configurado fortuito interno, mas afastada a indenização por danos morais
	0741006-52.2025.8.07.0016 – TJDFT – 1ª Turma Recursal – 14/10/2025	Reconhecida a falha no dever de segurança diante de transações realizadas logo após o furto do celular, sem bloqueio efetivo e com inconsistências na gravação do primeiro contato da vítima. O banco manteve cobrança e negativação indevidas mesmo após comunicação imediata. Aplicada a Súmula 479/STJ e configurado
		fortuito interno. Indenização por dano moral fixada em R$ 3.000,00.
	4000037-25.2025.8.26.0020 – TJSP – 6ª Turma Recursal – 09/09/2025	Reconhecida a falha na segurança bancária diante da contratação de empréstimos e transferências via PIX realizadas logo após o furto do celular do consumidor. O banco não comprovou a regularidade das operações nem demonstrou compatibilidade com o perfil do cliente.
Fraudes via PIX	0000602-81.2025.8.16.0102 – TJPR – 1ª Turma Recursal – 19/09/2025	Reconhecida a culpa exclusiva da vítima, que realizou operações após interação com fraudador, utilizando senha pessoal e aplicativo legítimo. Comprovado que o

		objetivamente pelo dano material. O pedido de dano moral foi afastado.
Contratação fraudulenta de empréstimo e serviço (consignado / digital)	0023458-25.2024.8.16.0021 – TJPR – 3ª Turma Recursal – 10/10/2025	Reconhecida a fraude na contratação de empréstimo consignado, realizada enquanto a autora cumpria pena em regime fechado, circunstância que impossibilitava a assinatura do contrato. Fortuito interno reconhecido.
	0001594-68.2023.8.16.0019 – TJPR – 2ª Turma Recursal – 21/10/2025	Reconhecida a inexistência de contratação eletrônica de empréstimo consignado por falta de provas técnicas que confirmassem a adesão do consumidor. O banco não apresentou assinatura, senha, biometria ou logs
		sistema bancário bloqueou tentativas suspeitas e funcionou adequadamente. As transferências e empréstimos estavam compatíveis com o perfil histórico de consumo do cliente. Fortuito externo reconhecido
	0055106-25.2024.8.16.0182 – TJPR – 2ª Turma Recursal – 07/10/2025	Reconhecido o fortuito interno diante de fraude via PIX e demora injustificada na ativação do Mecanismo Especial de Devolução (MED), iniciada cinco dias após a comunicação do consumidor. A instituição financeira não comprovou a inexistência de falha no gerenciamento de riscos, respondendo

		de autenticação, limitando-se a telas sistêmicas genéricas.

A fraude bancária, hoje, assume múltiplas formas. E a jurisprudência recente dos Juizados Especiais demonstra que, independentemente da forma de fraude, o ponto decisivo é a capacidade do banco de reconhecer e bloquear transações atípicas. Quando essa análise comportamental é falha ou inexistente, o evento se insere no âmbito do risco da atividade e, portanto, do fortuito interno.

Assim, o dever de segurança comportamental constitui a atualização técnica do dever de segurança tradicional. O KYC, nesse contexto, deixa de ser apenas instrumento de compliance regulatório e passa a integrar o próprio núcleo da responsabilidade civil bancária.

A multiplicidade de fraudes, portanto, não fragmenta o Tema 466; reafirma sua centralidade. Todas as fraudes, em última análise, testam a mesma estrutura de segurança, que deveria identificar desvios de padrão, bloquear transações suspeitas e proteger o consumidor contra riscos previsíveis.

A amostragem da jurisprudência evidencia que a aplicabilidade plena do Tema 466 depende de uma leitura atualizada das novas modalidades de fraude bancária. Assim, compreender o alcance do Tema 466 na era digital implica reconhecer que a responsabilidade objetiva do banco inclui não apenas reagir ao evento fraudulento, mas prevenir ativamente sua ocorrência por meio de mecanismos eficazes de monitoramento dinâmico do perfil do cliente (KYC) e de inteligência antifraude integrada.

CONSIDERAÇÕES FINAIS

A responsabilidade civil das instituições financeiras por fraudes praticadas em ambiente digital representa, hoje, uma das manifestações mais complexas da teoria do risco do empreendimento. A tese firmada pelo Superior Tribunal de Justiça no Tema Repetitivo 466/STJ permanece plenamente vigente, mas sua aplicação demanda atualização hermenêutica compatível com a realidade tecnológica do sistema financeiro contemporâneo.

O fortuito interno, antes vinculado a falhas documentais ou operacionais, passou a abranger o fortuito informacional, em que a violação decorre de deficiências no monitoramento comportamental e nos mecanismos de prevenção automatizada de fraudes. A leitura moderna do dever de segurança exige que o banco atue não apenas para reagir ao evento lesivo, mas para antecipá-lo — conhecendo o cliente, suas rotinas e seus padrões de operação, a fim de detectar anomalias antes que o dano se consume.

Nesse contexto, o Know Your Client (KYC) deixa de ser mera exigência regulatória e se torna o núcleo técnico do dever jurídico de segurança. A efetividade da proteção do consumidor depende da capacidade da instituição financeira de demonstrar, em juízo, que possui sistemas ativos e eficazes de prevenção, bloqueio e

restituição. A ausência ou ineficiência desses mecanismos revela descumprimento do próprio dever contratual de diligência e atrai a responsabilidade objetiva prevista no artigo 14 do Código de Defesa do Consumidor.

A análise comparada da jurisprudência recente dos Juizados Especiais evidencia que o Tema 466 continua a orientar as decisões, mas sob novas bases fáticas e tecnológicas. O fortuito interno permanece a regra, sobretudo quando o evento se desenvolve dentro do ambiente bancário digital; o fortuito externo, por sua vez, restringe-se a hipóteses alheias ao domínio técnico da instituição, como fraudes consumadas fora do sistema ou mediante canais não oficiais.

Em síntese, o que se observa é que a eficácia contemporânea do Tema 466 depende de sua leitura à luz do KYC dinâmico e do compliance informacional. O dever de segurança deixou de ser uma obrigação genérica de cautela e se tornou um dever tecnológico de vigilância inteligente, intrinsecamente vinculado ao funcionamento do sistema bancário digital.

O risco da atividade financeira, outrora confinado ao espaço físico do cofre e da agência, hoje habita o campo invisível dos dados e da informação. É nesse território que se define, em última instância, a fronteira entre o fortuito e a falha. E é nele que o dever de segurança bancária deve continuar a evoluir.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Superior Tribunal de Justiça. Súmula n. 479, Segunda Seção, julgada em 27 jun. 2012, publicada em 1º ago. 2012.

BRASIL. Superior Tribunal de Justiça. Tema Repetitivo n. 466, Segunda Seção.

BRASIL. Superior Tribunal de Justiça. REsp 1.197.929/PR, Rel. Ministro Luis Felipe Salomão, Segunda Seção, julgado em 24 ago. 2011, publicado em 12 set. 2011.

BRASIL. Superior Tribunal de Justiça. REsp 1.199.782/PR, Rel. Ministro Luis Felipe Salomão, Segunda Seção, julgado em 24 ago. 2011, publicado em 12 set. 2011.

BRASIL. Tribunal de Justiça do Estado do Paraná. 3ª Turma Recursal. Processo n. 0007777-24.2024.8.16.0018, Maringá. Rel. Juiz Fernando Swain Ganem. Julgado em 13 out. 2025.

BRASIL. Tribunal de Justiça do Estado do Paraná. 1ª Turma Recursal. Processo n. 0052081-04.2024.8.16.0182, Curitiba. Rel. Juíza Vanessa Bassani. Julgado em 22 set. 2025.

BRASIL. Tribunal de Justiça do Estado do Paraná. 2ª Turma Recursal. Processo n. 0001928-80.2024.8.16.0209, Francisco Beltrão. Rel. Juiz Irineu Stein Junior. Julgado em 16 set. 2025.

BRASIL. Tribunal de Justiça do Estado do Paraná. 1ª Turma Recursal. Processo n. 0000602-81.2025.8.16.0102, Joaquim Távora. Rel. Juiz Douglas Marcel Peres. Julgado em 22 set. 2025.

BRASIL. Tribunal de Justiça do Estado do Paraná. 2ª Turma Recursal. Processo n. 0055106-25.2024.8.16.0182, Curitiba. Rel. Juiz Helder Luis Henrique Taguchi. Julgado em 7 out. 2025.

BRASIL. Tribunal de Justiça do Estado do Paraná. 3ª Turma Recursal. Processo n. 0023458-25.2024.8.16.0021, Cascavel. Rel. Juiz Fernando Swain Ganem. Julgado em 13 out. 2025.

BRASIL. Tribunal de Justiça do Estado do Paraná. 2ª Turma Recursal. Processo n. 0001594-68.2023.8.16.0019, Ponta Grossa. Rel. Juiz Álvaro Rodrigues Junior. Julgado em 21 out. 2025.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. Segunda Turma Recursal. Processo n. 0735541-62.2025.8.07.0016. Rel. Juíza Marilia de Avila e Silva Sampaio. Julgado em 8 out. 2025.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. Segunda Turma Recursal. Processo n. 0741006-52.2025.8.07.0016. Rel. Juíza Silvana da Silva Chaves. Julgado em 8 out. 2025.

BRASIL. Tribunal de Justiça do Estado de São Paulo. 6ª Turma Recursal Cível. Processo n. 4000035-85.2025.8.26.0010. Rel. Juíza Márcia Rezende Barbosa de Oliveira. Julgado em 7 out. 2025.

BRASIL. Tribunal de Justiça do Estado de São Paulo. 6ª Turma Recursal Cível. Processo n. 4000037-25.2025.8.26.0020. Rel. Juiz Márcio Bonetti. Julgado em 9 set. 2025.