Textos para Discussão 222

Núcleo de Estudos e Pesquisas
da Consultoria Legislativa

ARRANJOS DE PAGAMENTOS NO BRASIL: vulnerabilidade de segurança no uso de cartões em terminais POS e a perspectiva regulatória

Cesar van der Laan

SENADO FEDERAL

Textos para Discussão

Núcleo de Estudos e Pesquisas
da Consultoria Legislativa

222

ARRANJOS DE PAGAMENTOS NO BRASIL: vulnerabilidade de segurança no uso de cartões em terminais POS e a perspectiva regulatória

Cesar van der Laan[1]

1 Engenheiro, Doutor em Economia (UFRGS). Consultor Legislativo do Senado Federal na área de Economia (Políticas Macroeconômicas e Sistema Financeiro). E-mail: cesarvdl@senado.leg.br

Brasília, janeiro de 2017

SENADO FEDERAL

DIRETORIA GERAL

Ilana Trombka – Diretora-Geral

SECRETARIA GERAL DA MESA

Luiz Fernando Bandeira de Mello Filho – Secretário Geral

CONSULTORIA LEGISLATIVA

Danilo Augusto Barboza de Aguiar – Consultor-Geral

NÚCLEO DE ESTUDOS E PESQUISAS

Rafael Silveira e Silva – Coordenador

Núcleo de Estudos e Pesquisas
da Consultoria Legislativa

Conforme o Ato da Comissão Diretora nº 14, de 2013, compete ao Núcleo de Estudos e Pesquisas da Consultoria Legislativa elaborar análises e estudos técnicos, promover a publicação de textos para discussão contendo o resultado dos trabalhos, sem prejuízo de outras formas de divulgação, bem como executar e coordenar debates, seminários e eventos técnico-acadêmicos, de forma que todas essas competências, no âmbito do assessoramento legislativo, contribuam para a formulação, implementação e avaliação da legislação e das políticas públicas discutidas no Congresso Nacional.

Contato:
conlegestudos@senado.leg.br

URL: www.senado.leg.br/estudos

ISSN 1983-0645

Como citar este texto:

LAAN, C. R. v.d. **Arranjos de Pagamentos no Brasil: vulnerabilidade de segurança no uso de cartões em terminais POS e a perspectiva regulatória**. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/ Senado, Janeiro/2017 (Texto para Discussão nº 222). Disponível em: www.senado.leg.br/estudos. Acesso em 25 de janeiro de 2017.

ARRANJOS DE PAGAMENTOS NO BRASIL:
VULNERABILIDADE DE SEGURANÇA NO USO DE CARTÕES EM TERMINAIS POS E A PERSPECTIVA REGULATÓRIA

RESUMO

O trabalho destina-se a analisar o risco de segurança em arranjos de pagamentos com cartões, aspecto de relevância social e econômica que vem revelando demandas crescentes à agenda regulatória doméstica. Com base na literatura e em estudos de casos, traça-se um panorama das características de segurança dos terminais de leitura de acesso remoto e da regulação sobre risco e responsabilidade de perdas. Os resultados apontam uma assimetria de segurança entre os distintos meios de acesso, que acentua os riscos de crimes associados ao uso de cartões em terminais *Point-of-Sale* (POS). Identifica-se uma série de vulnerabilidades, com destaque para a fragilidade do acesso baseado somente em senha numérica, já reconhecida e abolida dos terminais ATM. Argumenta-se que o deslocamento do risco do negócio e das perdas associadas para o usuário não induz o investimento necessário para mitigação de riscos e superação do quadro de fragilidade identificado, perpetuando-o. Esse cenário não pode ser desconectado da necessidade de ampliação da regulamentação do setor, desalinhada das diretrizes prudenciais internacionais e da prática em países desenvolvidos. Conclui-se que o combate ao crime financeiro deve ser uma combinação de tecnologia e de medidas preventivas, com destaque para o papel regulatório.

PALAVRAS-CHAVE: cartão bancário, cartão de crédito, arranjos de pagamentos.

SUMÁRIO

1 INTRODUÇÃO

A disseminação de cartões magnéticos consolidou o padrão de pagamento atual para as transações diárias. O uso da moeda em papel é cada vez menor e o talão de cheques não dista da extinção, pois os pagamentos podem ser realizados por meio dos sistemas eletrônicos, que hoje apresentam ampla difusão pela economia real[1].

Se, por um lado, a infraestrutura de terminais POS (conhecidas como "maquininhas"), requerida para utilização de cartões, já alcança a maioria dos estabelecimentos comerciais e prestadores de serviços pelo País – abundando em pontos remotos como táxis e junto a vendedores ambulantes em qualquer hora do dia ou da noite –, por outro a segurança e proteção dos sistemas de pagamentos não tem se mostrado suficiente para inibir condutas criminosas a partir desses terminais.

O nível de segurança dos arranjos de pagamentos[2] é, ainda, questionável, com riscos operacionais relevantes permitindo a perpetração de fraudes financeiras. Vários estudos têm mostrado riscos significativos associados ao atual padrão tecnológico de segurança incorporado aos cartões, como USHR (2014), ECB (2014), BIS (2014a), ACI Worldwide (2014), Serasa (2014), SPC (2013), Schwartz (2014), Hillebrand (2008), FPEG (2007), Cruz (2006), Sanger, Perlroth (2015), dentre outros.

São comuns experiências de pessoas lesadas como vítima de roubo e clonagem de cartão, que, inclusive, levam ao uso efetivo dos cartões para comandar operações comerciais em jurisdições estrangeiras. Independentemente de ser o prejuízo arcado pelo estabelecimento comercial (via *chargeback*[3]), pela instituição financeira (IF)[4] ou

---

1 Os números do Banco Central (BC) espelham essa realidade: atualmente, em torno de 90 milhões de cartões de crédito e mais de 100 milhões de débito estão em uso no País. Em regra, as modalidades estão reunidas num mesmo plástico.

2 A legislação chama o serviço de pagamentos com cartões como "arranjo de pagamento", nos termos da Lei nº 12.865, de 2013. Esquemas, sistemas ou redes de pagamentos, e instrumentos de pagamento de varejo são, também, termos utilizados pela literatura específica, referentes à mesma estrutura de prestação de serviço financeiro. São, aqui, utilizados como sinônimos.

3 *Chargeback* é o estorno ou devolução da transação de venda feita com cartão de débito ou crédito, que pode acontecer em virtude de contestação, pelo não reconhecimento da compra pelo titular do cartão. Assim, o valor da venda não será creditado ao lojista porque a compra foi considerada inválida.

4 Utiliza-se o conceito amplo de instituição financeira, abrangendo bancos e administradoras de cartões. Estas são, de fato, essencialmente instituições financeiras: efetuam intermediação financeira, administrando ativos (créditos a receber dos clientes titulares dos cartões) e passivos (junto a lojistas), e assumindo risco de crédito – independente do adimplemento do consumidor, assumem o compromisso de pagar o lojista. Além disso, os serviços de pagamentos vinculados a cartão de crédito, emitidos por instituições financeiras ou instituições de pagamento, estão sujeitos à regulamentação baixada pelo Conselho Monetário Nacional (CMN) e pelo BC, nos termos dos arts. 4º e 10 da Lei nº 4.595, de 1964, e da Lei nº 12.865, de 2013.

pelo titular do cartão, o fato é que os riscos operacionais não são desprezíveis e atestam a vulnerabilidade intrínseca do dinheiro de plástico. No limite, a ocorrência de um crime de grande vulto pode abalar a própria confiança dos usuários nos sistemas de pagamentos com cartões.

Todavia, esforços sistematizados de avaliação dos riscos de segurança inerentes do setor e da capacidade de mitigação de fraudes por meio de novas tecnologias incorporadas aos sistemas de pagamentos de varejo mostram-se tímidos frente ao crescimento acelerado da atividade financeira. Portanto, faz-se necessário avaliar o assunto, com vistas a subsidiar a política pública imponível.

Esse trabalho busca preencher essa lacuna, estruturado como segue. A segunda seção faz um panorama dos conceitos e da regulamentação doméstica aplicada, além de consolidar diretrizes de regulação prudencial e experiências de países desenvolvidos sobre assunção de riscos em sistemas de pagamentos com cartões. A terceira seção faz um diagnóstico de riscos do setor no País, apontando práticas de mercado e o estado atual da segurança dos sistemas de pagamentos com cartões. A quarta seção justifica a ação preventiva da indústria e do regulador nesse cenário, seguida de considerações finais.

2 ASPECTOS REGULATÓRIOS DE RISCOS DE SEGURANÇA DE SISTEMAS DE PAGAMENTOS COM CARTÕES

O nível de segurança dos sistemas de pagamentos com cartões baseia-se em dois pilares, providos pela autorregulação setorial. Ambos estão restritos à arquitetura básica de tecnologia do sistema operacional e do ambiente eletrônico por onde se desenvolvem as transações.

O primeiro pilar consiste na incorporação da tecnologia do *chip* ao cartão magnético. Seu desenvolvimento permitiu a proteção dos dados do cartão por um sistema de criptografia, em substituição ao padrão tecnológico anterior baseado em tarja magnética. Os cartões armazenam dados de forma mais segura (criptografados) e, pela presença de um microprocessador interno, também possuem maior capacidade de memória, permitindo sua utilização para múltiplas funções. Outra característica dos cartões com *chip* é que dispensam a assinatura do titular do cartão, utilizando-se a senha de acesso para identificar o cliente e comandar as transações.

Dentre as tecnologias disponíveis, destaca-se o predomínio do padrão EMV, desenvolvido como fruto da colaboração dos principais sistemas de pagamento globais (Europay, Mastercard e Visa). Com isso, criou-se uma série de regras que passaram a direcionar o setor quanto às características dos sistemas eletrônicos incorporados aos cartões magnéticos sob o ponto de vista de segurança, o que também permite a própria interoperabilidade dos cartões nos terminais em nível global.

O segundo pilar consiste em diretrizes que se estendem além das características tecnológicas incorporadas aos próprios cartões magnéticos, voltadas para a segurança dos dados que trafegam pelas redes de infraestrutura de comunicação dos sistemas de pagamentos. Destaque para o padrão de segurança PCI, criado pelas bandeiras Visa, Mastercard e American Express. O PCI introduziu o *Payment Card Industry Security Standards* para estabelecer padrões de segurança e coordenar as boas práticas no uso, manuseio e armazenagem de dados de cartões de crédito. O padrão especifica os requisitos de segurança a serem observados pelos membros, estabelecimentos e prestadores de serviços que estejam armazenando, processando ou transmitindo dados dos cartões, de forma a reduzir os riscos de fraudes.

A associação desses dois pilares, restritos à tecnologia, delineia o nível de segurança do sistema operacional e do ambiente eletrônico voltado à proteção dos dados do cartão e das redes de comunicação de dados frente aos riscos de fraudes financeiras[5].

2.1. DIRETRIZES INTERNACIONAIS DE REGULAÇÃO PRUDENCIAL

A ocorrência reiterada de fraudes e roubos perpetrados a partir da captura de dados de cartões para realização de transações não autorizadas mostrou que a autorregulação, voltada apenas a questões tecnológicas dos sistemas de pagamentos, não era suficiente para garantir a segurança das transações. Isso tornou o nível de segurança dos dados dos cartões e dos sistemas de pagamentos objeto não apenas de autorregulação do mercado como também objeto de monitoramento pelos reguladores internacionais.

A tradição da regulação prudencial financeira internacional, formada a partir das regras de Basileia, sugere que a ação do regulador em cada país deve também atentar à segurança dos sistemas de pagamentos e à proteção do cliente bancário. Em nível

[5] Veja em www.pcisecuritystandards.org.

internacional, chama a atenção o fato de que segurança e eficiência de sistemas de pagamentos de varejo constituem preocupação prioritária para bancos centrais e outras autoridades (BIS, 2014a). O tema envolve fraudes e riscos operacionais, com relação estreita com a proteção do cliente bancário, constituindo, portanto, tema de banco central (CPMI, 2014).

Sistemas de pagamentos são vistos pelos bancos centrais como parte vital da infraestrutura financeira e econômica dos países (BIS, 2014a). Sua funcionalidade e eficiência, permitindo execução de transações com segurança e rapidez, oferecem uma contribuição chave ao desempenho econômico geral. Isso é de particular importância para os sistemas considerados "sistemicamente importantes" para o funcionamento do sistema financeiro, como o Sistema de Transferência de Reservas, operado pelo BC, ou as câmaras de compensação e liquidação interfinanceira centralizadas na BM&F. Mas a preocupação também é válida para outros sistemas que são relevantes para o funcionamento da economia real, como é o caso dos principais sistemas de pagamento com cartões[6].

A natureza crítica dos sistemas de pagamentos com cartões relaciona-se com o impacto potencial que podem produzir sobre o funcionamento e a eficiência da economia real, decorrente de qualquer disruptura que possa ocorrer e que paralise as transações diárias. Isso demonstra uma relevância sistêmica para o funcionamento regular da economia. De fato,

> "The increasing importance of card payments and the lack of suitable alternatives make the role of this firm even more crucial for the economy and the risk even more critical than previously. A default by the company would trigger a loss of confidence in crucial payment instruments and have adverse effects on the real economy." (CPMI, 2014).

Sistemas de pagamentos com cartões são, naturalmente, sistemicamente importantes, requerendo nível de segurança e monitoramento apropriados. Diferentemente dos demais sistemas de compensação do sistema financeiro – caracterizados por transações envolvendo poucos agentes bancários –, a exposição a

[6] No Brasil, o BC considera os principais sistemas de liquidação e compensação de transações com cartões como sistemicamente importantes, como Cielo e Redecard, que já estão arrolados dentre os sistemas de vigilância e supervisão pela Autarquia no âmbito do Sistema de Pagamentos Brasileiro (SPB). Vide Comunicado BC nº 25.164, de 2014.

fraudes e roubos acaba sendo muito maior em sistemas de pagamentos que envolvem milhões de estabelecimentos comerciais e prestadores de serviço executando operações a partir de terminais remotos distribuídos amplamente pela economia real.

Isso significa que a regulação deve visar à segurança dos clientes e à confiabilidade dos serviços financeiros prestados, como função essencial de um banco central, especialmente para promover o objetivo de eficiência dos sistemas de pagamentos (CPSS, 2005). Esse papel engloba monitorar os sistemas correntes, avaliá-los em relação ao *benchmark* estabelecido e, quando necessário, exercer o papel de indutor de mudanças. Como órgão regulador, bancos centrais utilizam de sua capacidade técnica e altamente especializada para direcionar o mercado financeiro para um objetivo pré-estabelecido – como o nível de segurança adequado e a mitigação de fragilidades e riscos operacionais dos sistemas – a fim de assegurar o equilíbrio de interesses entre os agentes econômicos e a proteção de um setor fundamental da economia.

Diante da importância da intermediação financeira para a economia e da necessidade de uma infraestrutura de pagamentos funcional que permita rápida e segura transmissão de informações para efetuar movimentações financeiras, é esperado que entidades supervisoras monitorem o funcionamento da infraestrutura de pagamentos em suas jurisdições. É o que acontece na Europa, onde sistemas de pagamento com cartões são monitorados pelo Banco Central Europeu (BCE) desde meados dos anos 1990 (CPMI, 2014). A justificativa consiste em que:

> "retail payment systems and instruments are significant contributors to the broader effectiveness and stability of the financial system, in particular to consumer confidence and to the functioning of commerce. Moreover, efficient and safe use of money as a medium of exchange in retail transactions is an essential function of the currency and a foundation of the trust people have in it. For these reasons, the efficiency and safety of retail payments are of interest to central banks." (CPMI, 2014)

Assim, a resiliência dos sistemas de pagamentos com cartões é prioridade a ser perseguida em cada país europeu. Isso se alinha com o entendimento do Banco de Compensações Internacionais (BIS) que também considera importante que as jurisdições tenham claras suas responsabilidades na supervisão desses sistemas de

pagamentos, e com os princípios básicos estabelecidos[7], ainda em 2001, no âmbito do Comitê de Infraestrutura de Mercado e Pagamentos.

2.2. A REGULAÇÃO NACIONAL

No Brasil, a regulação do setor de cartões é recente, construída a partir da publicação da Lei nº 12.865, de 2013, que incorporou os arranjos e instituições de pagamento às regras do Conselho Monetário Nacional (CMN) e à supervisão do Banco Central do Brasil (BC). Seu art. 7º já inclui a preocupação do legislador quanto ao nível adequado de segurança dos sistemas de pagamento com cartões, nos seguintes termos:

> "Art. 7º Os arranjos de pagamento e as instituições de pagamento observarão os seguintes princípios, conforme parâmetros a serem estabelecidos pelo Banco Central do Brasil, observadas as diretrizes do Conselho Monetário Nacional:
>
> (...)
>
> IV – atendimento às necessidades dos usuários finais, em especial liberdade de escolha, segurança, proteção de seus interesses econômicos, tratamento não discriminatório, *privacidade e proteção de dados pessoais*, transparência e acesso a informações claras e completas sobre as condições de prestação de serviços;
>
> V – confiabilidade, qualidade e *segurança* dos serviços de pagamento." (Lei nº 12.865, de 2013, grifos adicionados)

Daí decorre a observância de regras de gerenciamento de riscos e adoção de estruturas voltadas para controles internos e governança dos arranjos de pagamento. O monitoramento de riscos deve ser permanente para os sistemas que possuam representatividade como instrumento de pagamento na economia real, comando alinhado com as reconhecidas diretrizes prudenciais da Basileia, das quais o Brasil é aderente[8]. Trata-se de procedimento voltado para garantir a segurança dos sistemas de pagamentos por meio dos quais a moeda é movimentada, que faz parte da abordagem internacional de gerenciamento baseado em risco (RBA). Essa é a norma no setor financeiro mundial, que já vem sendo adotada no Brasil desde o final dos anos 1990.

---

[7] Conhecidos como *Core Principles for Systemically Important Payment Systems.*

[8] O CMN também reiterou esse comando, indicando que a regulamentação e a supervisão das instituições e arranjos de pagamento integrantes do SPB devem observar, dentre outros, os objetivos de confiabilidade, qualidade e segurança dos serviços de pagamento (Resolução BC nº 4.282, de 2013).

Com isso, a IF deve estabelecer controles próprios para o gerenciamento dos riscos, consistentes com os riscos das operações que realiza – à luz da tradicional Resolução BC nº 2.554, de 1998. Com a incorporação das instituições que compõem os arranjos de pagamento ao âmbito da regulação e supervisão financeira doméstica, os comandos da Resolução 2.554 também passaram a ser aplicáveis às administradoras de cartões, que passaram a necessitar da autorização do BC para operar no País. A norma estabelece diretrizes mínimas para os controles internos das instituições financeiras. Dentre outras, os controles devem:

- Ser efetivos e consistentes com a natureza, complexidade e risco das operações por ela realizadas (art. 1º);
- Prever a contínua avaliação dos diversos riscos associados às atividades da instituição e assegurar que quaisquer desvios possam ser prontamente corrigidos, inclusive com a realização de testes periódicos de segurança para os sistemas de informações;
- Ser periodicamente revisados e atualizados, incorporando medidas relacionadas a riscos novos ou previamente não abordados (art. 2º);
- Ser objeto de relatório anual contendo as recomendações sobre eventuais deficiências e o estabelecimento de cronograma de saneamento, se for o caso (art. 3º).

Essas regras visam estabelecer um padrão mínimo de monitoramento de riscos, complementar às regras da própria indústria de cartões. Além disso, autorizam o BC a determinar a adoção de controles adicionais caso constate inadequação dos controles das instituições (art.6º), pois falhas graves de controles internos das IFs não podem prevalecer em prejuízo da segurança e confiabilidade das transações eletrônicas no País. Isso implica que movimentações financeiras efetuadas em poucos minutos, que claramente denotem operações irregulares, não podem predominar, nem a omissão das IFs no reconhecimento e aprimoramento de falhas em seus sistemas de controle.

O CMN também já indicou que as IFs devem ter estruturas de gerenciamento do risco operacional que documentem e armazenem as informações referentes às perdas associadas ao risco operacional, inclusive quanto a falhas em sistemas de tecnologia da informação (Resolução BC nº 3.380, de 2006). Além disso, indica que as instituições autorizadas a funcionar pelo BC devem assegurar "a integridade, a confiabilidade, a

segurança e o sigilo das transações realizadas, bem como a *legitimidade* das operações contratadas e dos serviços prestados", nos termos da Resolução BC nº 3.694, de 2009.

Entretanto, a assunção de perdas decorrentes de fraudes e roubos no âmbito do Sistema Financeiro Nacional (SFN) é um aspecto que foi deixado à arbitragem do mercado. Uma modificação em outro comando da Resolução BC nº 3.694, de 2009, passou a permitir o repasse ao cliente bancário do ônus derivado de falhas de segurança dos produtos e serviços financeiros. A redação dada pela Resolução nº 4.283, de 2013, substituiu o comando que prezava a adequação dos produtos e serviços financeiros às necessidades dos clientes por outro que dá margem à atribuição a terceiro do ônus de segurança dos produtos, nos seguintes termos:

> "Art. 1º As instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, na contratação de operações e na prestação de serviços, devem assegurar:
>
> ~~III – a adequação dos produtos e serviços ofertados ou recomendados às necessidades, interesses e objetivos dos seus clientes; (Incluído pela Resolução nº 3.919, de 25/11/2010.)~~
>
> III – a prestação das informações necessárias à livre escolha e à tomada de decisões por parte de clientes e usuários, explicitando, inclusive, direitos e deveres, responsabilidades, custos ou ônus, penalidades e eventuais riscos existentes na execução de operações e na prestação de serviços; (Redação dada pela Resolução nº 4.283, de 4/11/2013)." (Resolução BC nº 3.694, de 2009)

Isso tornou a assunção de responsabilidade por perdas decorrentes de fraudes e roubos, no âmbito dos sistemas de pagamentos, passível de repasse, a critério das IFs, garantido o pressuposto de que o cliente bancário, na prática hipossuficiente, tenha plena capacidade de contornar os riscos para utilizar aos sistemas de pagamentos com cartões. Consolidou-se, assim, uma prática de mercado que não é nova, já existente quando a segurança do uso dos cartões era baseada somente na leitura da tarja magnética, sem contar ainda com a senha de acesso.

Com efeito, a responsabilidade é atribuída geralmente ao cliente diante de transações conduzidas em seu nome mediante interposição de senha de acesso, mesmo que obtida em decorrência de roubo, sequestro ou extorsão. Os contratos de adesão são bem claros nesse sentido: em caso de perda, furto ou roubo do cartão, o titular é responsável pelos prejuízos resultantes desses fatos até a data de cancelamento do

cartão. Decorre que as IFs não assumem, via de regra, a responsabilidade pelo uso não autorizado do cartão enquanto não houver a comunicação da irregularidade pelo titular do cartão[9].

Nesse contexto de responsabilidade por perda, extravio, roubo e eventuais fraudes atribuídas ao próprio titular do cartão, o crime de falsificação de cartões chegou a ser, recentemente, tipificado no Código Penal. O seu art. 298 equipara cartão de crédito ou débito a documento particular para fins de cominação de sanção penal. Na prática, esse enquadramento do cartão bancário como documento particular corrobora a visão construída no País de que a segurança do acesso aos sistemas de pagamentos constitui atribuição do titular do cartão e não dos provedores do serviço.

A regulação também tem sede na legislação consumerista, com o Código de Defesa do Consumidor (CDC) sendo aplicável a serviços financeiros para proteger o cliente bancário. Os benefícios derivados encontram-se tanto na esfera do indivíduo quanto na esfera da organização social, especialmente por incentivar a introdução de produtos e serviços com nível apropriado de segurança.

A natureza jurídica existente entre cliente bancário e IF constitui relação de consumo, com base no § 2º do art. 3º da Lei nº 8.078, de 1990[10]. Isso implica que prevalece, nos contratos bancários, a presunção de vulnerabilidade do cliente bancário (art. 4º, I, do CDC), diante da supremacia das IFs ante os consumidores, no estabelecimento de cláusulas contratuais em benefício de quem elabora os termos de contratação. Nesse caso, as cláusulas devem ser interpretadas restringindo-se o princípio da autonomia da vontade, no sentido de reequilibrar a hipossuficiência do cliente bancário (MIRANDA, 2010)[11]. Também implica a prevalência do princípio da inversão do ônus da prova no processo civil, como direito básico estabelecido pelo CDC (art.6º, VIII). O art. 14 do CDC brasileiro também deve ser observado, que atribui ao

---

[9] Tanto Bradesco como Itaú e Citibank, por exemplo, atribuem responsabilidade exclusiva ao cliente pelo uso do cartão. O mesmo procedimento é adotado pelo BB, que emite o "termo de recebimento e responsabilidade do cartão", quando do desbloqueio do cartão no terminal ATM, atribuindo ao cliente "única, exclusiva e integral responsabilidade pela guarda e uso do cartão".

[10] A jurisprudência também é clara na aplicação do CDC ao SFN. Tanto o STJ quanto o STF já pacificaram a questão da aplicação do CDC ao setor financeiro. Vide súmula STJ 297; Adin STF 2591/DF, de 7.6.2006. Veja também decisão da 3ª Turma do STJ no Agravo 277.191 (RJ 1999/0113374-2), publicado no DJ em 01/08/2000, acerca da responsabilidade das administradoras de cartões devido à falta de segurança dos serviços prestados.

[11] A imposição de responsabilidade total a clientes por perdas decorrentes de fraudes denota o contrato de adesão típico, tal como descreve o art. 54 do CDC: as cláusulas são impostas unilateralmente, sem que o titular possa influir substancialmente em seu conteúdo.

fornecedor a responsabilidade pelos serviços prestados, inclusive quando não fornece a segurança normal esperada. Isso implica a responsabilização objetiva das IFs em face de danos sofridos pelos usuários dos sistemas de pagamentos.

Orientações do Sistema Procon também devem ser observadas pelo setor, para a segurança não só do consumidor como do próprio sistema. Assim, por exemplo, os estabelecimentos credenciados, no ato do pagamento com cartão, devem conferir a assinatura do consumidor, além de solicitar a apresentação de documento pessoal que comprove a titularidade do usuário do cartão. Legislações estaduais e municipais, já existentes em algumas jurisdições, reforçam esse quesito, tornando obrigatória a apresentação de documento público de identificação mediante uso de cartão[12].

Também indicam que a administradora de cartões é obrigada a assumir o uso por terceiros relacionado à perda, furto ou roubo, independente de cláusula nos contratos de adesão atribuindo responsabilidade ao titular pelo uso indevido anterior à comunicação do fato à central de atendimento. Tal cláusula é considerada indevida à luz do art. 14 do CDC, pois a responsabilidade na segurança da prestação do serviço é do fornecedor, que deve adotar cuidados e mecanismos apropriados para efetuar o pagamento de produtos ou serviços com o cartão. Em seus termos, "o consumidor é vulnerável e a fragilidade do sistema permite, por vezes, a utilização indevida do cartão por terceiros"[13].

2.3. PRÁTICAS REGULATÓRIAS SOBRE ASSUNÇÃO DE RISCOS DE SEGURANÇA[14]

Em países desenvolvidos, a preocupação é frequente com a qualidade dos produtos financeiros oferecidos aos clientes. A experiência de jurisdições mais avançadas mostra que medidas preventivas são adotadas tanto pelas IFs quanto pelos reguladores, voltadas para a efetiva segurança dos sistemas de pagamentos com cartões.

No Canadá, o assunto é tratado com prioridade institucional, tanto no âmbito público quanto privado. Bancos e administradoras de cartões possuem sistemas de segurança sofisticados e times de especialistas treinados para monitorar as transações

---

[12] Vide, por exemplo, Lei Estadual RS nº 12.714, de 2007, Lei Estadual SC nº 14.207, de 2007, Lei Estadual PE nº 13.308, de 2007, Lei Estadual GO nº 16.582, de 2009, e Lei Distrital DF nº 4.132, de 2008, que tornam obrigatória, em suas jurisdições, a apresentação de documento de identidade com foto para pagamentos efetuados com cartões.

[13] Fonte: http://www.procon.sp.gov.br/categoria.asp?id=248. Acesso em: 14 dez. 2016.

[14] Esta subseção não tem a pretensão de ser exaustiva, mas tão somente informativa de experiências mais avançadas na regulação de serviços de pagamento de varejo, para eventual aprimoramento regulatório local.

tempestivamente, detectando e prevenindo fraudes. Os sistemas de inteligência das instituições naquela jurisdição podem detectar, automaticamente, atividades fora de padrão numa conta corrente e tomar medidas precaucionais tempestivas, impedindo a ocorrência de um evento fraudulento (CBA, 2013).

Na esfera regulatória, a proteção do cliente bancário canadense foi consolidada em 1992 como resultado de acordo intrassetorial elaborado por grupo de trabalho que envolveu organizações consumeristas, instituições financeiras, lojistas e entes governamentais estaduais e federais, e foi endossada pelos bancos e operadoras dos sistemas de pagamentos naquela jurisdição. Em 2002, uma seção específica referente à responsabilidade de perdas foi adicionada à regulação, estabelecendo diretrizes diante da ocorrência de transações não autorizadas e outros problemas operacionais. As diretrizes atingem não apenas uso de cartão de débito em terminais de autoatendimento ATM e terminais POS nas lojas, mas também terminais remotos de leitura em computadores pessoais. Uma importante diretriz de segurança direcionada ao lojista busca evitar o *shoulder phishing*: os terminais POS devem ser instalados em locais com privacidade suficiente para o cliente digitar a senha com o mínimo risco de captura por terceiros.

Há um critério de responsabilização bem claro associado aos riscos financeiros, incorporado no Código Canadense para Serviços de Cartões de Débito de 2004. A principal diretriz consiste em que o titular do cartão não é responsável por perdas resultantes de circunstâncias que estão fora de seu controle. Assim, não assume perdas derivadas de problemas técnicos e mau funcionamento de sistemas, nem do uso não autorizado do cartão e senha quando o emissor é responsável por prevenir tal uso, por exemplo, após o cartão ter sido declarado perdido ou roubado, cancelado ou expirado.

Sua responsabilidade também é afastada caso reporte que a senha pode ter sido descoberta por terceiro e também diante da ocorrência de uso não autorizado do cartão, mesmo que tenha contribuído inadvertidamente para tanto, desde que coopere em quaisquer investigações subsequentes (CBA, 2004). Assim, o cidadão canadense não assume responsabilidade em caso de *shoulder phishing* em terminais POS, desde que reporte o incidente prontamente (assim que tenha ciência da perda ou descoberta da senha) e coopere na investigação subsequente. O mesmo critério é estabelecido diante de casos de fraude, roubo ou coação por ameaça, força ou intimidação.

Apenas se o titular contribuir de forma negligente para o uso não autorizado dos dados que será responsável pelas perdas resultantes, inclusive se houver acesso a linhas de crédito pela conta corrente ou limite contratado. Esse seria o caso de escrever a senha no cartão ou próximo dele ou de falhar em avisar ao emissor, em prazo razoável, que o cartão foi perdido ou roubado, ou que a senha tenha sido descoberta por terceiro. Mas é de atribuição da IF a prova de que o titular contribuiu para o uso não autorizado do cartão, já na esfera administrativa. O tempo limite para resolução das demandas dos clientes é de dez dias úteis.

Com isso, as principais operadoras Visa, MasterCard e AmEx adotam políticas de *zero liability* naquela jurisdição, diante da ocorrência de aprovação de transações não autorizadas pelos clientes. Nesse caso, clientes estão protegidos quando utilizam cartões bancários, não ficando sujeitos por transações fraudulentas feitas em seus nomes (CBA, 2013). Isso também levou à introdução de medidas de segurança específicas nos sistemas com cartões naquele país.

O estabelecimento de teto diário para saque com cartão ocorre não apenas nos terminais ATM (limitado a mil dólares canadenses), mas também nos terminais POS espalhados pelas lojas (em dois mil dólares canadenses, via de regra). Essa medida mitiga o risco potencial de perdas inerente às transações por acesso remoto, o que mostra a capacidade de soluções administrativas simples em reduzir a atratividade do crime financeiro – minimizando a ocorrência real de crimes nos sistemas de cartões.

Tabela 1. Regulação canadense na responsabilidade do uso de cartão de débito

Responsável	Medida
Estabelecimento comercial.	Segurança para evitar *shoulder phishing* no uso do terminal POS.
Estabelecimento bancário.	Limite diário para saques em terminais ATM ($1,000) e POS ($2,000).
Titular de cartão vítima de roubo, furto, coação, *shoulder phishing*.	Não é responsável pelas perdas.
Titular que contribui para o uso não autorizado (ônus da prova da IF).	Responsável pela totalidade das perdas.

Fonte: *Canadian Bankers Association* (2004).

Nos EUA, a proteção legal do cidadão tem raízes em atos constituídos já nos anos 1970, sendo clara a responsabilidade de titulares e fornecedores de cartões. O *Fair Credit Billing Act* (FCBA), de 1974, que emendou o *Truth in Lending Act* (TILA), de

1968, e o *Electronic Fund Transfer Act* (EFTA), de 1978, estabelecem limites para perdas causadas por transferências eletrônicas não autorizadas, inclusive atribuindo ônus da prova à IF diante de contestação de uma transação financeira. Se há a comunicação da perda ou roubo do cartão antes do uso por terceiro, não há responsabilidade do titular, o que também ocorre diante de roubo de dados sem subtração do cartão magnético, comum em casos de clonagem.

Para o cartão de crédito, o limite máximo para repasse de perda ao titular é de 50 dólares. No caso do cartão de débito, a perda máxima pode chegar a 500 dólares, no caso de notificação acima de 48 horas após a ciência do problema. No limite, pode-se chegar ao repasse de responsabilidade para todos recursos em conta, caso não seja a IF notificada no prazo de 60 dias, mas há informações de que os bancos voluntariamente limitam a perda ao valor de 50 dólares[15].

Tabela 2. Atribuição de perdas ou fraudes com cartões de débito nos EUA

Tempo da Comunicação à IF	Perda Máxima do Titular (USD)
Antes de efetuadas quaisquer cobranças não autorizadas.	0,00
Em até dois dias após a ciência da perda ou roubo.	50,00
Mais do que dois dias úteis após a ciência da perda ou roubo, em até 60 dias corridos após o envio do extrato bancário.	500,00
Acima de 60 dias corridos após o envio do extrato bancário.	Toda quantia subtraída, inclusive aplicações ligadas à conta corrente.

Fonte: *Federal Trade Comission* (2015).

Assim, o critério temporal define a perda máxima atribuída ao cliente norte-americano, mas há exceções a esse critério. Diante de uma circunstância atenuante, como uma viagem prolongada ou doença que impeça o cliente de avisar o emissor do cartão no prazo legal, o período de notificação de 48 horas é estendido. A legislação ainda permite que o contrato particular ou a lei estadual mais benéfica imponha limites mais reduzidos à responsabilidade atribuída ao cliente, prevalecendo o limite inferior.

[15] Além disso, a discussão corrente no âmbito do congresso estadunidense está na unificação da proteção do cartão de crédito ao de débito. Uma primeira medida seria aumentar a proteção do titular de cartão de débito estabelecida pelo EFTA, equalizando-a ao nível aplicável a cartões de crédito, estabelecido pelo TILA. Veja em http://www.pirg.org/consumer/banks/debit/debitcards1.htm

O assunto também faz parte da ação de supervisão pelas entidades reguladoras do sistema financeiro nos EUA. Já em 2001, o *Office of the Comptroller of the Currency*, responsável pela regulação e supervisão dos bancos de âmbito nacional nos EUA, alertou que cabe às IFs o ônus da prova em uma investigação sobre fraudes para mostrar que uma transação foi devidamente autorizada pelo cliente. Isso implica que o banco não pode atribuir, desde já, a responsabilidade por perdas ao cliente, quando este alega fraude:

> "The OCC is concerned that some banks may be rejecting claims of unauthorized transactions solely because the customer's Automated Teller Machine (ATM) card or debit card and personal identification number (PIN) were used in the transaction, and the customer supplied no information indicating that the card or PIN was misappropriated. These facts alone may be insufficient to establish that a transaction was authorized because fraudulent means may have been used to obtain the customer's account number, card, or PIN. For instance, the customer may have been a victim of 'shoulder surfing', a practice used by criminals to obtain account or card numbers or PINs by observing customer transactions. Therefore, banks cannot assume that they have satisfied their duty to investigate simply by concluding that the customer's debit card and PIN were used in the transaction at issue." (OCC, 2001, p.1)

A legislação e a regulação financeira alinham-se com o reconhecimento da própria Casa Branca de que o setor privado possui papel crucial no combate a crimes no âmbito do sistema financeiro que estão sendo conduzidos por meio da incorporação de novas tecnologias. O entendimento é de que segurança de tecnologia e informação bancária é assunto corporativo das IFs e também do regulador.

Isso explica o lançamento, em outubro de 2014, pelo presidente americano, da *Buy Secure Initiative,* para aprimorar a proteção do cliente bancário. Em fevereiro de 2015, novas iniciativas de promoção de segurança de tecnologia também foram divulgadas, em associação com setores da indústria de cartões (veja White House, 2015), com o reconhecimento pelo *Financial Services Roundtable* e pela *Retail Industry Leaders Association* da fragilidade do nível de segurança do acesso bancário baseado apenas em senha numérica. O objetivo das iniciativas é desenvolver e incorporar novos princípios e padrões de tecnologia que minimizem o valor de informações e dos dados de acesso bancário roubados ou perdidos.

Decorre que companhias têm anunciado novas iniciativas de autenticação multifatorial para aumentar o padrão de segurança de acesso. A Intel está lançando uma nova tecnologia de autenticação que não vai se basear em senha, mas em outras ferramentas como biometria. A AmEx está incorporando tecnologia multifatorial de autenticação de clientes e a MasterCard, introduzindo uma combinação de biometria de reconhecimento facial e vocal. Já a Visa está implementando, em 2015, o padrão *token,* substituindo a numeração de cartões magnéticos por códigos gerados aleatoriamente para cada transação (WHITE HOUSE, 2015).

Na Europa, a regulação também possui uma tradição voltada à proteção das transações eletrônicas. Já em 2004, observa-se política pública específica para combater o crime e prevenir fraudes em pagamentos eletrônicos (FPEG, 2007). O terceiro relatório do BCE sobre fraudes contra cartões de pagamento bancário (ECB, 2014) demonstra a relevância do tema para o regulador europeu. A iniciativa regulatória contou com o desenvolvimento, em 2011, de uma série de recomendações para aumentar a segurança dos serviços de pagamento eletrônico de varejo, visando reduzir fraudes e aumentar a confiança do usuário nos sistemas com cartões.

A *EU's Payment Services Directive,* válida em todos países europeus, estabelece a assunção aos consumidores de perda de, no máximo, 150 euros, em caso de ocorrência de transações não autorizadas. O limite é imponível tanto para operações de crédito quanto de débito, efetuadas pela *internet*, telefone ou de forma presencial, desde que o cliente não tenha agido de forma não diligente – o que não inclui eventual falha em manter a senha de acesso em segredo[16].

Da mesma forma, no Reino Unido, já em 2009 a lei britânica limitava a perda máxima atribuída ao titular do cartão em 50 libras para perdas ocorridas até a comunicação à IF, com isenção após esse montante. Mas, na prática, a maioria das companhias estornam os valores totais – a menos que os clientes tenham agido com extrema negligência, cujo ônus da prova é atribuição da IF. A prática naquela jurisdição é o estorno imediato de recursos retirados da conta corrente de forma não autorizada[17].

---

[16] "…consumers' liability will be limited in the same way even if they have 'failed to keep the personalised security features safe from misappropriation of a payment instrument'" (FPEG, 2007, p.15).

[17] Há, ainda, boas experiências regulatórias na Cingapura e México, baseadas no *Singapore's Payment Systems (Oversight) Act33* e no *Transparency and Financial Services Arrangement Act.* Veja BIS (2014a).

3 VULNERABILIDADE DE SEGURANÇA NO MERCADO BRASILEIRO DE CARTÕES

Por ser, em tese, mais segura do que o porte de dinheiro em espécie, a movimentação remota de depósitos bancários passou a ser o meio de pagamento predominante na economia brasileira. A ampla difusão do cartão associa-se, sobretudo, à ideia de segurança que proporciona para realizar as transferências financeiras, cuja credibilidade é essencial para essa modalidade de pagamento.

Todavia, a evolução tecnológica não eliminou a possibilidade de perdas decorrentes de fraudes contra o sistema financeiro, com o nível de segurança dos sistemas de pagamentos com cartões permitindo a subtração de recursos dos usuários. O cartão magnético coloca em risco uma quantidade infinitamente maior de recursos do que o papel-moeda que, no passado, era carregado no bolso (CRUZ, 2006). O padrão de disponibilização simultânea das funções crédito e débito no mesmo plástico significou pôr em risco a totalidade dos créditos vinculados às contas correntes de milhões de clientes bancários – inclusive dos créditos pré-aprovados disponibilizados automaticamente pelos bancos e que podem ser vistos impressos em qualquer extrato bancário[18].

Em relação ao cheque, se a passagem para o cartão magnético permitiu a transferência mais rápida de fundos, eliminou-se a possibilidade de sustação ou contraposição de ordem de pagamento pelo titular para uma emissão ilegítima, especialmente para operações de débito, que geram saída financeira imediata da conta corrente. O sistema não permite ao cliente questionar a licitude da operação, como ocorre no sistema de pagamento baseado no cheque[19] [20]. Isso aponta que a evolução dos meios de pagamento não foi acompanhada pela evolução regulatória. Não existe uma "Lei do Cartão Bancário", nos moldes da Lei do Cheque (Lei nº 7.357, de 1985), para proteger o novo meio de pagamento predominante.

---

[18] O BB, por exemplo, não oferece cartão magnético sem a função de débito, que poderia ser uma forma de mitigar riscos que são repassados ao cliente bancário.

[19] Recentemente, os sistemas passaram a admitir o estorno de operações autorizadas a partir de um terminal POS. Todavia, trata-se de prerrogativa não regulada e pouco conhecida, passível de utilização geralmente quando o cliente ainda se encontra na loja e constata um erro de valor, logo após o comando da operação original.

[20] Na *internet,* que é um ambiente muito suscetível ao uso de dados roubados, o cliente até consegue contestar compras realizadas sem uso direto do cartão. Todavia, alguma parte vai assumir o ônus pelo uso não autorizado dos dados. Caso a fraude tenha sido descoberta após a entrega física do produto ou serviço, o prejuízo foi concretizado, sendo geralmente assumido pelo estabelecimento comercial.

Ao mesmo tempo, a senha de acesso substituiu a assinatura imposta no cheque, cuja conferência era de responsabilidade dos bancos, e hoje é de responsabilidade exclusiva do cliente bancário. O sistema de segurança totalmente baseado na senha permite a execução de transferências instantâneas a partir de qualquer lugar e em qualquer horário do dia ou da noite, em substituição aos prazos de compensação do sistema de pagamento com cheque. Na prática, a passagem do cheque para o cartão magnético acabou atribuindo maior potencial de perdas ao cliente bancário, ainda que tenha sido introduzido com o intuito de reduzir crimes financeiros (CRUZ, 2006).

A tabela resume os riscos e mecanismos mitigadores para cada meio de pagamento:

Tabela 3. Meios de pagamento em varejo, riscos e mitigadores

Meio de pagamento	Emissor	Risco a crime	Perda potencial	Mitigação de risco	Aceitação	Proteção legal
Papel-moeda	Estado	Limitado e gerenciável diretamente pela pessoa.	Quantidade no bolso.	Sistema policial repressivo eficiente.	Curso Forçado.	Política de combate à fraude (ação conjunta do BC e Polícia Federal).
Talão de cheque	Banco (ordem de pagamento criada pelos bancos)	Controlável (associado à adulteração, perda e roubo).	Exposição de todo saldo em conta corrente, e aplicações com baixa automática à conta corrente.	Tempo de compensação permite sustação; IFs ligam para confirmar valores elevados.	Opcional (risco do recebedor) – em desuso.	Lei do Cheque estabelece regras; mecanismos de proteção por contraordem.
Cartão magnético	Banco (ordem de pagamento em substituição ao cheque)	Expressivo.	Limite do cartão de crédito + saldo total em conta corrente e poupança e crédito pré-aprovado.	Compra de seguro.	Opcional, mas na prática é o novo meio de pagamento; padrão no comércio eletrônico.	Não há regulação prevendo mecanismo de contraordem, tanto para compensação a débito quanto a crédito.

Fonte: elaboração própria.

O novo padrão de meio de pagamento também alterou a forma de perpetração do crime financeiro. Na década de 1980, foi corriqueiro o assalto à mão armada diretamente no balcão do caixa do Banco. O problema tornou-se tão grave que levou à edição da Lei de Segurança Bancária (Lei nº 7.102, de 1983). A partir dos anos 1990, a explosão de caixas eletrônicos de autoatendimento bancário passou a ser comum,

levando à introdução de uma série de equipamentos e sistemas de segurança específicos em torno dos terminais bancários. A recente introdução do mecanismo de segurança baseado na inutilização de cédulas manchadas tende a mitigar ainda mais esse risco.

Surgiu o golpe da "saidinha", com quadrilhas especializadas em atacar aposentados e mulheres sozinhas nas redondezas das agências bancárias. A alta incidência de crime de sequestro relâmpago e de captura de senhas nas agências fez com que o tema chegasse a se tornar lei em diversas localidades. A imposição de legislações protetivas do cliente bancário, em nível municipal, levou os bancos a aumentarem os níveis de segurança para reduzir a incidência dessas ameaças[21].

Como efeito colateral, o risco e grande parte da demanda criminosa que circunda o sistema bancário deslocaram-se para as operações efetuadas fora das agências bancárias. Desprovidas de todo o aparato de segurança construído em torno da agência bancária e dos caixas eletrônicos, a ação criminosa desviou o foco de atuação para a ponta mais frágil de acesso ao SFN, que são os terminais POS encontrados em qualquer estabelecimento comercial. A captura de dados de cartões magnéticos a partir desses terminais passou a ser mais usual.

Há evidências indicando maior frequência de captura de senhas nos terminais em estabelecimentos de varejo, o que sugere que as portas de acesso remoto pelos terminais POS são mais vulneráveis do que por terminais ATM. Com efeito, há conceitos pouco eficientes de segurança e de tecnologia da informação (TI) caracterizando especialmente esse meio de acesso, que se associam ao nível único de senha de acesso e às próprias características físicas dos terminais POS, que não os tornam imunes especialmente à espionagem visual. Além disso, terminais POS ainda permitem uso de cartões apenas com a leitura da tarja magnética, tecnologia menos segura do que a baseada em *chip*[22].

Já os bancos trabalham com medidas múltiplas de segurança. Além de níveis complementares de identificação de acesso aos sistemas de pagamentos, os Bancos também impõem medidas administrativas de controle mais eficientes para contrapor a criminalidade nos centros urbanos brasileiros – por exemplo, restringindo horário e

[21] É o caso da cidade de São Paulo, cuja Lei nº 15.429, de 2011, reconhece a magnitude de riscos associados ao SFN como um problema social crônico. Diversos municípios paulistas também já proibiram o uso do celular em agências, pois o próprio sinal sonoro de digitação pode ser alvo de captura por olheiros ou por filmagem com celulares. Curitiba, Belo Horizonte e Salvador têm legislação semelhante. Minas, Rio e Ceará também aprovaram leis estaduais similares.

[22] Uma parcela do estoque de cartões ativos no País ainda não possui tecnologia de *chip.*

valor em espécie disponível para saque em terminais ATM durante a madrugada. Há, de fato, poucos caixas eletrônicos em operação nos grandes centros urbanos durante o período noturno, que é de maior risco.

Com isso, o SFN trabalha, atualmente, com níveis distintos de segurança para a realização de transações financeiras, restando o acesso remoto por terminais POS mais vulnerável a roubo e fraude (tabela 4).

Tabela 4. Assimetria de segurança em canais de acesso bancário

	Terminais ATM	**Terminais POS**
Padrão predominante de senha de acesso.	Senha com sílabas disponibilizadas em conjuntos de três (maior segurança).	Senha numérica, de até 6 dígitos; cada dígito em um botão isolado (menor segurança).
Segunda camada de segurança de acesso.	Perguntas como parte de CPF ou outros dados pessoais.	Não há.
Sistema Biométrico de identificação.	Já comum desde 2014.	Não há.
Medidas de segurança complementares.	Horário reduzido; poucos pontos em operação de madrugada; limite de saque tanto de dia quanto de noite (mais reduzido).	Não há.
Vulnerabilidade a crime.	Maior risco.	Menor risco.

Fonte: elaboração própria.

Terminais POS também são alvo preferencial não apenas pelo menor nível de segurança que apresentam, mas pela magnitude crescente de suas operações. Hoje, a quantidade média mensal de transações com movimentação financeira é maior em terminais POS, em comparação aos acessos pela *internet*, terminais ATM ou nos caixas das agências (FEBRABAN, 2014). Isso torna maior o retorno esperado derivado do crime, pois aumenta a probabilidade de sucesso da tentativa de fraude ou roubo.

Em tese, não há limite de valor para uma transferência eletrônica, a depender apenas dos controles e limites gerenciais impostos pelas IFs – que são frágeis para transferências comandadas a partir de terminais POS em estabelecimentos comerciais. Isso aumenta a vulnerabilidade e o risco intrínseco aos sistemas de pagamentos.

Trata-se de um universo permeado por riscos operacionais. Acaba-se sujeito a fraudes com uso de equipamentos utilizados para capturar os dados dos cartões para

clonagem. De fato, proprietários e funcionários dos estabelecimentos podem não saber que estão utilizando um aparelho adulterado, pois acabam sendo vítimas de falsos técnicos de manutenção dos aparelhos. Tanto o estabelecimento quanto o cliente, nesse caso, não têm capacidade técnica para conferir a autenticidade do terminal POS. Também não têm como conferir se os dados introduzidos para acesso foram corretamente direcionados para a administradora de cartões. Ninguém sabe se, após a digitação de senha no teclado, os dados foram corretamente direcionados para a administradora de cartões ou acabaram interceptados por terceiros.

Na realidade, à medida que o número de pontos de acesso remoto para efetuar operações financeiras cresceu e ultrapassou os limites dos estabelecimentos bancários, as IFs passaram a se defrontar com uma inevitável complexidade: a verificação de que o acesso individual remoto está sendo realmente feito pelo cliente e não por um terceiro. Ao expandir seus serviços com base na incorporação de tecnologias, o SFN optou por abrir mão da confirmação da identidade visual do cliente – como feições, altura e voz –, que fazia parte da tradicional relação gerente-cliente, para se basear em uma identidade numérica de uma chave de acesso remoto (o cartão magnético) aos sistemas de transferências bancárias[23].

O cartão, ao possuir uma função legitimadora, permite que qualquer pessoa imputando dados de terceiros nos sistemas de pagamentos efetue transações de forma ilegítima. Diante de assimetria de informação, o fraudador, que não faz parte da relação contratual original, acaba enganando a IF, que autoriza operações a partir do uso de cartão clonado ou sob qualquer outra circunstância que torne ilegítima a operação por parte de terceiro não autorizado.

Para superar essa fragilidade, o SFN passou a assumir serem intransmissíveis tais dados, como se pudessem ser mantidos sob a guarda e sigilo e utilizados apenas pelo titular do cartão. Todavia, o pressuposto tem se mostrado frágil, pois o risco de subtração do cartão e de sua utilização não autorizada é característico da atividade financeira. Assim como para o uso do cheque, o risco é implícito para o uso do cartão tanto em terminais ATM quanto POS. É o sistema de acesso remoto ao SFN que se baseia em pressupostos frágeis para a identificação correta do cliente.

---

[23] Também se abriu mão da assinatura do cliente, que é uma característica pessoal que é confirmada pela apresentação de documento de identificação, que ainda caracteriza o uso remanescente do cheque, tornando-o mais seguro.

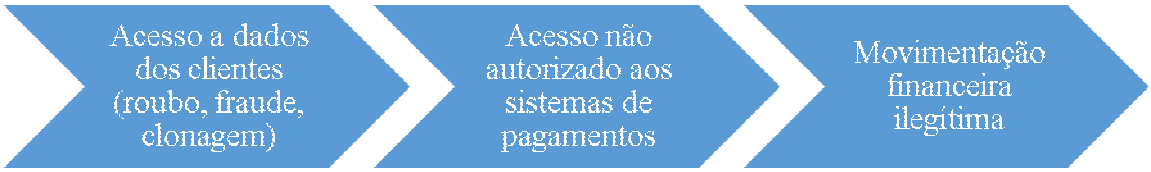
Mesmo que os contratos de adesão de cartões prevejam uso exclusivo por seu titular, os dados dos cartões são passíveis de uso por terceiro, com consentimento ou não. Isso implica que, a partir do momento em que são utilizados por terceiro não autorizado, os cartões perdem a legitimidade como instrumento de pagamento. É o que decorre da cláusula contratual padrão, por meio da qual a IF declara que "o titular do cartão de crédito está investido na condição de único beneficiário possível de sua idoneidade legitimadora" (CRUZ, 2006).

Apesar disso, é comum as IFs não assumirem perdas decorrentes de operações efetuadas por terceiro, validadas por imposição de senha. A justificativa de que "crime acontece" é frágil e eximitória, descarregando no sistema social a responsabilidade pela insegurança dos sistemas de pagamentos bancários. Sob essa visão, ocorreria a figura do caso fortuito externo, constituindo questão de segurança pública e atribuição do Estado, que afastaria a responsabilidade objetiva da IF. Decorre que o prejuízo dos clientes acaba tratado como assunto alheio à responsabilidade das IFs.

Contudo, a problemática real refere-se ao engano produzido em face da entidade financeira. A interceptação de senha, código de segurança e do número do cartão, mesmo que ocorra contra o cliente individualmente, mostra a fragilidade dos sistemas de pagamentos, que é sistêmica, pois não existe sistema de pagamento imune a fraudes (FPEG, 2007). Na verdade, enganar o cliente para obtenção de dados bancários não é suficiente, *per se,* para permitir o acesso aos sistemas de pagamentos e a subtração de recursos, pois isso depende do nível de segurança de acesso dos próprios terminais remotos. Soma-se a isso até mesmo a prática de o lojista não conferir o documento de identificação do cliente, a despeito do que algumas legislações subnacionais impõem.

O prejuízo decorrente do conhecimento indevido de dados de um cartão se perfaz somente quando ocorre o engano da IF. Mesmo que um cartão seja subtraído da posse de seu titular, o que importa é a configuração atual de segurança dos sistemas tornando-o passível de utilização ilícita, prática que ocorre contra a entidade bancária. Apenas nesse momento que ocorrerá a disponibilização equivocada de dinheiro ou a autorização indevida de uma compra mercantil. Somente a identificação tempestiva de tentativa de uso de cartão falso ou de acesso por terceiro não autorizado aos sistemas de pagamentos que evitará a ocorrência de crimes financeiros. É essa fragilidade sistêmica que deve ser combatida, que constitui a segunda etapa na figura seguinte.

Figura 1. Encadeamento de condutas para movimentação ilegítima de recursos de terceiros



Fonte: elaboração própria.

O foco do combate ao crime financeiro não pode se desviar da principal problemática dos sistemas de pagamentos, que é sua vulnerabilidade de acesso a terceiro. Apesar da existência de sistemas de segurança com algoritmos e chaves altamente sofisticadas, quadrilhas conseguem capturar, por meio de aparelhos ou artifícios eletrônicos, dados e informações gravadas nas tarjas magnéticas ou nos *chips*. Com cartões fraudados, realizam compras como se fossem o verdadeiro titular, o que demonstra a fragilidade do acesso dos sistemas de pagamentos.

3.1. MAGNITUDE DE RISCOS E FRAGILIDADES[24]

O reconhecimento da fragilidade do acesso aos sistemas de pagamentos a partir de terminais POS não é inferido apenas pelo contraste com os mecanismos de segurança complementares incorporados em terminais ATM. O próprio custo contabilizado pelo SFN em investimentos de segurança, os alertas de cuidado emitidos pelas IFs especialmente no ambiente virtual e também as próprias proposições legislativas já apresentadas no Congresso Nacional, desde pelo menos 1997, denotam a relevância do assunto no Brasil [25].

As fraudes podem ocorrer devido à perda ou roubo do cartão, à coação direta do titular em assalto ou à interceptação dos dados para uso geralmente em transações não presenciais, especialmente pela *internet* e por telefone. Podem também ocorrer em larga escala devido a vazamentos de dados em um provedor de pagamentos ou armazenador de informações de pagamentos. Todas as formas refletem sistemas de segurança inadequados, apontando que a indústria de cartões continua sujeita a crime, ainda que a

[24] Os fatos e evidências constatadas para traçar um panorama dos crimes no setor tiveram origem em periódicos e portais especializados, inclusive Procon, BC e Idec, método comum de pesquisa utilizado no âmbito jurídico e legislativo. A veracidade e credibilidade dos fatos, que podem ser testados e avaliados quanto à confiabilidade, podem sustentar ações públicas. Alguns casos ilustrativos estão apensados em anexo.

[25] Vide, por exemplo, os projetos de lei PLS nº 148/1997, PLS nº 261/2001, PLC nº 1.547/2007, PLC nº 7.121/2010, PLC nº 137/2011, PL nº 5.196/2013, PLS nº 243/2014 e PLS nº 363/2014.

incorporação dos *chips* nos cartões tenha levado à redução considerável das fraudes (CIELO, 2015).

Há indícios de que a tecnologia de *chip* possa ter reduzido a quantidade de fraudes e roubos de cartões especialmente a partir de terminais POS (LEACH, 2014), pois o padrão prévio baseado apenas na tarja magnética não seria capaz de sustentar níveis toleráveis de fraudes e permitir a continuidade de funcionamento dos sistemas de pagamentos (SCHWARTZ, 2014). Todavia, se houve queda na quantidade de clientes lesados, em termos de montante total não há comprovação de redução consistente de crime – até pelo crescimento do uso de cartões, tornando-os o meio de pagamento predominante. Isso sugere que a capacidade da tecnologia em deter o crime, *per se* e de forma satisfatória, é relativa (CRUZ, 2006)[26].

Na realidade, a dinâmica do crime sugere que as IFs adotam uma ação predominantemente reativa. Novas táticas criminosas surgem continuamente, e bancos são atacados por facções com incorporação de alto nível de tecnologia em seus métodos fraudulentos, por qualquer meio de acesso de informática. Novas tecnologias induzem a uma queda de eventos de crime no curto prazo, mas não garantem a imunidade dos sistemas de pagamento no longo prazo, até porque é esperado que a curva de aprendizagem para burlar um novo padrão tecnológico seja superada pelos fraudadores com métodos tão ou mais sofisticados. Ainda que, num primeiro momento, um novo padrão de segurança constitua uma barreira à forma de perpetração do crime, com o tempo fraudadores aprendem a sobrepujar os mecanismos de segurança.

Daí a consistência da visão de Mierzwinski (2014), segundo o qual comerciantes e consumidores acabam sujeitos a sistemas inseguros de pagamentos com cartões, caracterizados por padrões de segurança em constante mudança para compensar as falhas dos padrões tecnológicos anteriores.

Mesmo em países onde o uso de *chip* é o padrão corrente de tecnologia de segurança, a indústria de cartões não está imune a fraudes e captura de dados quando os clientes utilizam o cartão nos terminais de pagamento (SCHWARTZ, 2014). Na Colômbia, por exemplo, onde desde 2013 é mandatório o padrão de *chips*, autoridades locais reportaram um aumento de 25% nas estatísticas de falsificação de cartões. Nos EUA, que se encontra em processo de transição para tecnologia de *chip-pin*

[26] No País, pesquisa recente indica que mais de 30% dos usuários de cartões já foram vítimas de fraude nos últimos cinco anos (SERASA, 2014).

no lugar do *swipe-sign*, já se admite que a tecnologia não é a panaceia para o setor. Apesar de representar avanço em relação ao padrão baseado na tarja magnética, especialistas em segurança de tecnologia de informação admitem não constituir um sistema imune a fraude[27].

No Brasil, ainda que a vulnerabilidade dos terminais de acessos remotos e a reiteração de crimes contra o SFN constituam um problema social crônico, não há disponibilidade de dados globais acerca dos crimes praticados contra os sistemas de pagamentos bancários. Isso prejudica a apuração da real dimensão do risco de fraudes e roubos associados ao uso indevido de cartões magnéticos e constitui entrave ao combate ao crime financeiro. Ainda que tenham caráter público e sejam úteis para a investigação e para a ação de inteligência policial coercitiva, são basicamente dados privados, mantidos sob a guarda e o sigilo das próprias IFs.

Isso pode ser explicado, em parte, pela assunção direta de danos pelas IFs ou pelos estabelecimentos comerciais. O mero tratamento administrativo – por um lançamento contábil de prejuízo, por exemplo –, impede o conhecimento e tratamento do crime na esfera pública (CRUZ, 2006). Além disso, nenhum banco ou administradora de cartões tem interesse em divulgar dados que possam atestar ou apontar falta de segurança de seus produtos e serviços. A divulgação dos números poderia afugentar clientes e reduzir a adesão tanto de novos consumidores quanto de lojistas. A exposição da fragilidade dos sistemas de pagamentos comprometeria, no limite, a própria liquidez da moeda eletrônica e a disseminação do uso de cartões magnéticos nas transações diárias – daí que a preservação da informação constitui fator essencial para seu funcionamento (PRADO, 2005).

Há racionalidade econômica subjacente às IFs, por vezes, até optarem por suportar o prejuízo e não tornar públicas as ocorrências. Muitas vezes, ocorrem crimes até com auxílio de empregados das IFs, fato que não chega ao conhecimento público para preservar a imagem de segurança e a sensação de baixa fragilidade do SFN. Mas são fatores que acabam reduzindo o mapeamento de riscos em torno do setor.

Muitos casos também não chegam ao conhecimento de órgãos de defesa do consumidor ou do próprio BC porque são resolvidos na esfera da própria IF, principalmente para os clientes de seu maior interesse. Via de regra, bancos ressarcem

[27] Veja em http://money.usnews.com/money/personal-finance/articles/2014/10/28/coming-next-fall-more-chip-and-pin-cards-in-the-us?page=2. Acesso em: 14 dez. 2016.

clientes de renda mais alta no intuito de manter seu fluxo financeiro e aplicações. A comodidade da compra de um seguro contra perdas e roubos em cartões magnéticos também acaba reduzindo o registro de casos na esfera pública. O resultado derivado da análise custo-benefício, diante do custo de reparação, acaba tornando preferencial essa alternativa para muitos clientes. Para os casos que chegam ao registro em delegacias policiais, em órgãos de defesa do consumidor ou no próprio BC, não há uma divulgação sistematizada de dados.

A característica de as fraudes serem impetradas majoritariamente contra contas bancárias intituladas por pessoas físicas também dificulta a mudança do cenário de riscos[28]. Como os valores sob risco são, geralmente, menores do que os valores sob risco de uma pessoa jurídica, o custo intrínseco a litígios judiciais ou mesmo derivado do longo processo de contestação administrativa pode desincentivar, muitas vezes, a busca de reparação, seja pelo tempo despendido ou pelos custos adicionais associados ao acesso ao Judiciário, por exemplo. Associado à desvantagem econômica do cliente bancário médio, isso cria uma barreira natural para a devida reparação, que é, por definição, mais vantajosa para as IFs do que a assunção direta das perdas decorrentes das fraudes e roubos.

3.2. PRINCIPAIS CONSTATAÇÕES DA REALIDADE DE RISCOS DE SEGURANÇA

A ocorrência de fraudes e roubos reiterados sugere que há princípios e pressupostos frágeis relativos aos mecanismos de proteção utilizados nos sistemas de pagamentos. Decorre daí que vários aspectos de natureza tecnológica, administrativa e regulatória não conseguem, por definição, reduzir a vulnerabilidade dos sistemas, como elencado a seguir.

(i) **A realidade nega a hipótese de que o sistema de cartão com *chip* é inviolável**. Trata-se de tecnologia rapidamente aceita como segura, como se a senha constituísse a panaceia de segurança e fosse de desconhecimento até da IF. Apesar de terem aumentado a segurança em transações presenciais (BC, 2015), ocorrências reiteradas mostram que a tecnologia de *chip* não torna o cartão imune a crimes. Cartões com *chip* são passíveis de terem os dados capturados – inclusive senha – e são clonáveis. A própria senha numérica, de seis e até apenas quatro dígitos, é um

[28] Esse fato relaciona-se com o fato de que mais de 95% do volume das operações com cartão de crédito é realizado por pessoa física.

mecanismo reconhecidamente frágil, tanto que os bancos utilizam outros mecanismos complementares de autenticação nos terminais ATM. Impõem vários níveis de acesso como senha silábica – blindada à espionagem visual – e identificação biométrica da impressão digital – que é efetivamente pessoal e intransferível, até que venha a ser burlada. Não existe método de identificação invulnerável e não é sensato basear, exclusivamente, a segurança de um sistema de pagamento em apenas um nível de acesso tecnológico (FPEG, 2007).

(ii) **O cartão, e o mecanismo de senha, não é pessoal nem intransferível,** como imposto nos contratos de adesão. Dados dos cartões, incluindo a senha, são capturáveis, inclusive por filmagem oculta ou mera visualização, daí podendo ser utilizados facilmente por terceiros. Isso se relaciona com a própria configuração de leiaute dos terminais POS e com a falta de privacidade para seu uso no varejo. Isso mostra que o processo de identificação do usuário do cartão precisa ser pessoal e intransferível. O risco corrente de captura de dados precisa ser mitigado para garantir que o usuário dos sistemas seja somente o titular autorizado, o que parece estar mais associado à incorporação de outros mecanismos de segurança, já comum em terminais ATM.

(iii) **Os riscos são gerados pelas IFs, porém, na prática, estão deslocados para o titular do cartão**. As IFs não contestam transações mediante digitação da senha correta, que são autorizadas diante da assunção de que a interposição de senha torna a operação legítima. Para os bancos, se houver interposição de senha e uso de cartão, o titular deverá pagar operações de crédito e débito indevidas, pois aceitou os riscos ao aderir ao contrato de adesão, com as IFs apenas cumprindo sua atribuição contratual de efetuar uma transação mediante imposição da senha. A contrapartida do repasse dos custos de fraude aos clientes é a proteção insuficiente dos sistemas de pagamentos, que se tornam obsoletos e inseguros diante das novas formas de perpetração do crime, no limite reduzindo a confiança e atratividade do negócio[29] [30].

---

[29] No caso de interceptação de dados sem subtração física do cartão do titular que levam à clonagem do cartão, as IFs têm assumido as perdas diretas derivadas de falhas de seus sistemas.

[30] Há casos em que bancos garantem, contratualmente, apenas o ressarcimento de um evento por ano, mas se trata de proteção voluntária que pode ser suprimida ou alterada a qualquer momento, que não substitui a proteção legal. Algumas empresas de cartão se comprometem a não cobrar do titular do cartão compras e saques indevidos feitos por criminosos, estornando lançamentos nas 48 horas anteriores à comunicação do sinistro. Mas o prazo para esse estorno pode não ser suficiente, pois não se consulta diariamente as movimentações da conta corrente ou os lançamentos contra o cartão de crédito. Daí, acaba-se à mercê da decisão da IF em estornar, ou não, lançamentos contestados.

Aqui há espaço para o legislador federal: a lei pode atribuir ao banco ou credenciado dos sistemas de pagamentos a responsabilidade pela identificação do usuário do cartão[31]. A mudança tende a induzir a licitude das transações, associada à conferência de dados do titular do cartão, hoje inexistente, reforçando as legislações já existentes em alguns estados e municípios que preveem apresentação de documento público de identificação mediante uso de cartão.

(iv) **A prática tornou obsoleta a assinatura no verso do cartão**. Como regra, nenhum estabelecimento comercial credenciado solicita documento de identificação para comprovar a legitimidade da pessoa comandando a operação com cartão magnético. Dispensa-se a identificação do usuário mediante a interposição de senha, afastando importante mecanismo complementar de segurança que torna o sistema menos suscetível ao crime. Com isso, apenas a identificação correta de senha e cartão gera a autorização de operações pelas IFs e o pagamento aos estabelecimentos credenciados, independente da ocorrência de crime financeiro derivado de roubo de cartão ou extorsão de senha. Esse risco é ainda maior para os cartões sem *chip,* baseados apenas em tarja magnética, que são mais vulneráveis por serem usados sem interposição de senha. Nesse caso, a assinatura do usuário no papel de autorização da operação precisa ser conferida para constituir mecanismo de segurança efetivo. Mas depende de incentivo regulatório o estabelecimento comercial atentar para a legitimidade do cliente para garantir seu faturamento[32].

(v) **As IFs não se responsabilizam pelo que acontece dentro de estabelecimentos credenciados**. As IFs focam na ampliação de suas redes por meio de credenciamento de qualquer estabelecimento que pague o aluguel mensal do terminal POS, o que vai permitir ampliar o faturamento das taxas cobradas sobre cada transferência financeira efetuada a partir do terminal. Não se observa uma política "conheça seu credenciado", o que abre espaço para o credenciamento de estabelecimentos inidôneos, hipótese ignorada pelas IFs, que não se responsabilizam por falhas e fraudes impetradas eventualmente com a anuência dos estabelecimentos.

---

[31] É o teor do PLC nº 137, de 2011, e do PLS nº 243, de 2014, que tramitam no Congresso Nacional. Podem ajudar a ilidir as práticas criminosas, ao repassar ao lojista a assunção do ônus da prova em caso de não reconhecimento de uma transação, diante da falta de conferência de documento de identificação.

[32] De fato, um princípio econômico básico é de que agentes respondem a incentivos, pois as políticas públicas mudam os custos ou benefícios com que as pessoas se deparam e, portanto, alteram comportamentos (MANKIW, 2001).

O crime que ronda o setor pode contar com a cumplicidade de operadores credenciados que efetuam lançamentos indevidos, sem fundamentação econômica, contra os cartões[33].

Ocorre pouca atenção com a fundamentação econômica das operações introduzidas nos sistemas de pagamentos, a despeito da legislação de lavagem de dinheiro no País (baseada na Lei nº 9.613, de 1998). A pouca preocupação com a qualidade do credenciado, e sua movimentação financeira, permite até que traficantes operem no sistema, utilizando terminais POS para faturar o crime com cartão de crédito[34]. Entretanto, cabe às IFs a segurança e licitude das operações conduzidas nos sistemas de pagamentos. Ao regulador cabe prever requisitos mínimos para qualificar o credenciamento de estabelecimentos, bem como supervisionar o monitoramento das operações financeiras.

(vi) **Há uma clara assimetria de segurança entre os meios de acesso remoto aos sistemas de pagamentos com cartões**, sendo o terminal POS o ponto mais frágil. Na prática, a senha numérica está sendo usada justamente nos ambientes onde os usuários ficam mais expostos, em ambientes comerciais que não possuem o mesmo nível de segurança de uma agência bancária, constituindo estímulo latente ao crime. Há falta de privacidade do consumidor ao usar o terminal POS, especialmente porque permite o acesso visual ostensivo da senha inserida nesse terminal. Trata-se de situação de risco. Soma-se a isso a fragilidade do acesso de uso consolidado baseado apenas na senha de seis dígitos ou menos em terminais POS, que constitui mecanismo extremamente vulnerável. O uso de cartão com *chip* em terminais ATM é menos suscetível a fraudes e roubos do que o acesso remoto via terminais POS, diante dos instrumentos de segurança complementares já implementados.

(vii) **A desregulamentação não incentiva o aumento do nível de segurança dos terminais POS**. As IFs estão ganhando as tarifas pelo uso de cartão, independente da ocorrência de crime ou não. Daí a inércia em implementar mudanças, perpetuando o cenário atual de fragilidades: bancos e administradoras de cartões postergam investimentos em segurança de TI o máximo que podem, pois não assumem ônus de

[33] Muitas vezes, fraudadores "associam-se" com estabelecimentos credenciados aos sistemas de pagamentos, para uso do cartão roubado. Assim, ocorrem casos de o cartão ser utilizado na maquininha do taxista para subtrair valores elevados mediante comissão de 15% do valor, sem questionamento da licitude da operação.

[34] Veja em http://blogs.ne10.uol.com.br/jamildo/2015/02/20/no-recife-traficante-vende-drogas-ate-no-cartao-de-credito/. Acesso em: 14 dez. 2016.

perdas. Essa prática não incentiva a introdução tempestiva de novas tecnologias, ou o aprimoramento de sistemas de controles internos.

Lojistas não precisam averiguar a devida identificação do cliente, pois recebem sua receita com o uso do cartão, independente de ser utilizado pelo titular; de outro lado, bancos com controles internos restritos de inteligência e monitoramento insuficiente de transações, permitindo restaurantes e bares populares captem senhas e debitem cartões de clientes em movimentações de valores expressivos não condizentes com o perfil operacional do estabelecimento. A redistribuição da responsabilidade pelas perdas, a partir de produção normativa, poderá alterar esse quadro e incentivar a redução de fragilidades em ritmo maior do que o atual.

(viii) **As orientações do Sistema Procon também não são observadas pelo SFN**, que se mostra pouco permeável à regulação, sendo o setor recordista em reclamações nos Procons (COSTA, 2013). Na ótica do Sistema Nacional de Defesa do Consumidor (SNDC), do Ministério da Justiça, formado por Procons, Defensorias Públicas, Ministérios Públicos, entidades civis de defesa do consumidor e delegacias do consumidor, o uso indevido de cartões, resultante de clonagem, fraude, furto e roubo, é enquadrado como vício de qualidade de serviços financeiros[35]. Entretanto, os contratos sujeitam o cliente às condições impostas pelo contratante, contingenciados à adesão aos produtos e serviços bancários com o nível de segurança apresentado. São, portanto, dependentes das soluções de segurança oferecidas pela indústria de cartões. Nesse caso, a regulação deve impor limites e ditar as características dos produtos financeiros, pois regulação e política pública têm um impacto direto no tipo e nos termos contratuais oferecidos (BIS, 2014a).

(ix) **Há indícios que mostram falhas nos sistemas de monitoramento das IFs,** o que contribui para o aumento do crime (CRUZ, 2006). A aprovação de operações financeiras desproporcionais e incompatíveis com o perfil econômico-financeiro do correntista ou do estabelecimento comercial credenciado demonstra falhas de controles internos e de monitoramento das transações. Transações financeiras baseadas em sistemas de processamento com acesso remoto requerem controles correlatos, para certificação da liberação de recursos ao cliente verdadeiro. Procedimentos de controle devem ser suficientemente sofisticados para permitir não somente a identificação de

[35] Veja em www.consumidor.gov.br.

todas as operações financeiras realizadas pelos clientes, de forma tempestiva, dentro dos limites disponibilizados pelas IFs, como também a identificação de operações que, por sua habitualidade, valor ou forma, configurem movimentação atípica tanto para o perfil do cliente como para o perfil de operação dos estabelecimentos comerciais autorizados a operar nos sistemas de pagamentos. Isso envolve também o monitoramento de operações consecutivas que, mesmo dentro de limites unitários para uma transação, configurem impossibilidade real de se associar a uma transação econômica real legítima[36].

Essa necessidade se torna mais premente à medida que o volume de pagamentos é crescente, pois aumenta a probabilidade de que incidentes causem perdas mais severas e, provavelmente, maiores do que no passado. Por isso, não se pode afastar das IFs a prerrogativa de melhorar continuamente seus mecanismos de segurança e controles internos. Mesmo pequenos aumentos marginais na eficiência e na segurança dos sistemas de pagamentos podem gerar benefícios consideráveis para a sociedade como um todo (HEINRICH, 2006).

(x) **Nesse cenário, a complexidade de operacionalização de um arranjo de pagamento não pode servir de barreira para o aprimoramento de controles e do nível de segurança**. Um sistema de pagamento com cartões possui uma estrutura basicamente derivada da associação de um banco a uma administradora de cartões. O serviço financeiro envolve a administradora de cartões credenciando os estabelecimentos comerciais e processando os dados dos cartões para liberação das transações, e o banco gerenciando a adesão e contato com os usuários e efetuando as transferências financeiras a partir de contas correntes, no caso de operação de débito a partir de um terminal POS.

No caso do cartão de crédito, uma série de atividades é conduzida nas agências bancárias. Os bancos centralizam o contato com os clientes, fornecendo o cartão, geralmente com as duas funções de crédito e de débito. É o banco que mantém a relação com o titular do cartão, envolvendo-se em etapas importantes como a identificação, autorização e habilitação de acesso ao sistema; definição de programa de benefícios e também a análise de limite de crédito e monitoramento do risco. São atividades

[36] Por exemplo, é fora de padrão de consumo normal gastos somando mil reais em uma lanchonete em 5 minutos e mais dois mil reais numa farmácia também em poucos minutos, assim como torrar 23 mil reais em duas horas. Veja casos III e V anexo.

realizadas, precipuamente, pelos estabelecimentos bancários, por meio do gerente de contas, constituindo etapa integrante do serviço prestado de cartão magnético como meio de pagamento. Diante dessas características, a responsabilidade pelo nível de segurança dos sistemas de pagamentos deve ser compartilhada entre as IFs (banco e administradora de cartões), pois o cartão magnético faz parte da promoção do negócio bancário.

(xi) **O formato atual de mensagens de confirmação de operações nao presenciais com dados de cartões, enviadas *ex post* pelos bancos por SMS, poderia ser aprimorado e direcionado** para a mitigação efetiva de fraudes e crimes financeiros. Para tanto, precisa ser adaptado para constituir mecanismo complementar de autenticação *ex ante* à operação, com o envio, por exemplo, de uma senha aleatória para confirmar uma operação de valor elevado ou identificada como fora de padrão. O formato atual do envio de SMS apenas cria uma sensação ilusória de segurança dos sistemas, que é falsa. A desconsideração da possibilidade de roubo do celular junto do cartão magnético, que impossibilita a ligação imediata para contestação de uma operação, já compromete sua real eficácia.

Também não prevê que, de noite, o titular está dormindo e só verá no dia seguinte as mensagens no celular pedindo para ligar "imediatamente" no caso de não reconhecimento de uma transação efetuada na madrugada por terceiro. Mesmo que o uso indevido ocorra durante o dia, o mecanismo pressupõe que o celular do titular esteja ligado e com bateria suficiente para contestar tempestivamente a compra não autorizada – e que o serviço de atendimento ao cliente bancário seja suficientemente adequado para atender o cliente. O mesmo problema se apresenta para titulares de cartões em viagem. São muitos pressupostos falhos que impedem uma maior utilidade derivada do mecanismo corrente. Há também o custo de ligação impedindo a eficácia do instrumento, pois o telefone disponibilizado pelas IFs para os grandes centros urbanos, em geral, não é gratuito. Caso esteja na rua, o cliente pode não ter crédito para fazer uma ligação por celular[37]. Daí não se pode descartar que o titular nem sempre consegue comunicar à entidade bancária a subtração do cartão em tempo hábil.

[37] Com o advento dos celulares e a redução de pessoas usando linhas fixas, os custos de ligações também aumentaram, já que a ligação em redes móveis é ainda mais cara do que em linhas fixas. Por isso, muitas empresas pararam de disponibilizar o 0800 pelo menos para celulares, passando a usar os números 3003, 4003 e 400, que são pagos. Aqui, a regulação poderia direcionar as IFs a disponibilizar um canal gratuito de comunicação por telefone, assim como ocorre para outros setores econômicos regulados.

Há, portanto, diversas situações que apontam a fragilidade da configuração atual de mensagem via torpedo em celulares, não servindo ao propósito de tornar mais segura uma transação remota. Além disso, uma mensagem de contestação *ex post,* ainda que tempestiva, não impede o crime, que já ocorreu.

(xii) **Os dados de crimes parecem estar sendo mantidos em âmbito privado**. A verdadeira magnitude do problema é conhecida apenas pelas IFs, por meio de reclamações de golpes contra seus clientes, não chegando a conhecimento nem da autoridade reguladora nem das autoridades de investigação. Esse comportamento, ainda que racional no sentido econômico, não permite alcançar uma situação socialmente eficiente, pois informação é essencial para iniciar o processo de combate ao crime. Isso potencializa o cenário de insegurança que assola o SFN.

Há evidências de que suspeitas de ocorrências de crime financeiro não estão sendo investigadas nem pela IF, nem pelo BC nem pela autoridade policial. Reclamações relativas a fraude e roubo de cartões estão sendo ignoradas, sem comunicação dos crimes ao regulador ou ao poder de polícia constituído. Com efeito, não se observa uma tradição de ação conjunta SFN-Polícia, como existe na Europa desde 2003, quando começou a convergência de esforços para tratar a segurança do sistema financeiro e reduzir fraudes contra cartões de pagamento bancários, que foi considerada associada ao crime organizado (ROBINSON *et al,* 2011). Porém, a apuração investigativa criminal depende do compartilhamento dos registros de movimentações financeiras atípicas mantidos pelas IFs, inclusive dados de tentativas negadas de uso de cartão e arquivos de filmagem de circuitos internos de TV. É preciso, portanto, reforçar a parceria público-privada e superar a inércia institucional no combate a crimes na esfera do SFN, assegurando a coordenação da distribuição da informação entre os agentes na esfera privada e na pública.

Em relação ao regulador, sem a imposição de ônus às IFs que incentive o aprimoramento dos níveis de segurança dos serviços de intermediação financeira, afasta-se, também, o interesse do BC, que está precipuamente focado na robustez do SFN. Se as perdas não são assumidas pelas IFs, não há risco a ser monitorado nem pela IF nem pela Autarquia.

(xiii) **O BC deve também comunicar a prática de crime da esfera penal ao Ministério Público (MP), em decorrência de sua ação de supervisão**. Há indícios de crime contra o SFN que não estão sendo comunicados ao MP, mesmo tendo os clientes

lesados recorrido ao atendimento ao cidadão do BC. A Autarquia não investiga crimes impetrados no âmbito do SFN que, porventura, são identificados em seu processo normal de supervisão financeira. Isso vai de encontro à vontade do legislador, expressa tanto na Lei Complementar nº 105, de 2001, quanto na Lei nº 7.492, de 1986, que indica a comunicação ao MP da ocorrência de fatos passíveis de apuração criminal[38] [39].

Há uma dificuldade operacional intrínseca a processos investigativos de ilícitos financeiros que, não raro, acaba agravada pela falta de comunicação entre os órgãos públicos, muitas vezes detentores de indícios de crimes. Os registros dos cidadãos no BC, relatando ações fraudulentas contra o SFN, deveriam levar à apuração penal posterior, se a Autarquia conduzisse uma investigação própria, confirmando os indícios de ilícitos relatados.

(xiv) **Por fim, a classificação de crime de clonagem deve ser repensada**. A Lei nº 12.737, de 2012 (lei "Carolina Dieckmann"), recentemente tipificou a falsificação de cartões no Código Penal, equiparando cartão de crédito ou débito a documento particular – a nosso ver, de forma equivocada. A natureza do cartão bancário é muito mais complexa e se assemelha à da moeda e à do cheque bancário, como meio de pagamento com poder liberatório para quitar transações econômicas. Deriva, daí, que a clonagem constitui crime contra o SFN, equiparado à falsificação de moeda, que é assunto de interesse coletivo e difuso, e de bancos centrais. Já a falsificação de documento particular é assunto apenas da esfera da ação cível.

O objeto jurídico a ser protegido pelo Estado é a higidez do SFN, pois o crime está afetando a segurança do tráfego da informação bancária. Na verdade, trata-se de crime complexo, que envolve a captura de dados bancários e o posterior acesso não autorizado ao SFN para subtração de recursos. Nesse caso, a vítima é a IF e não o titular do cartão. Ainda que o possuidor do cartão seja seu titular, seu proprietário é o banco emissor (CRUZ, 2006). Além disso, o cartão falsificado só pode ser detectado pelos mecanismos de identificação dos sistemas de segurança do SFN. O dispositivo legal

---

[38] "Art. 9º. Quando, no exercício de suas atribuições, o Banco Central do Brasil e a Comissão de Valores Mobiliários verificarem a ocorrência de crime definido em lei como de ação pública, ou indícios da prática de tais crimes, informarão ao Ministério Público, juntando à comunicação os documentos necessários à apuração ou comprovação dos fatos" (Lei Complementar nº 105, de 2001, "Lei do Sigilo Bancário").

[39] "Art. 28. Quando, no exercício de suas atribuições legais, o Banco Central do Brasil ou a Comissão de Valores Mobiliários verificar a ocorrência de crime previsto nesta lei, disso deverá informar ao Ministério Público Federal, enviando-lhe os documentos necessários à comprovação do fato" (Lei nº 7.492, de 1986, lei do "Colarinho Branco").

corrente acaba confundindo a real natureza do crime e a própria definição da vítima do crime. Corre-se, inclusive, o risco de se atribuir toda a responsabilidade pela insegurança inerente do serviço prestado pela IF ao titular do cartão. O que não estimula a assimilação de novos mecanismos de segurança no mesmo ritmo exigido diante da agilidade do crime financeiro.

3.3. O PROCESSO DE CONTESTAÇÃO INDIVIDUAL

Além das características anteriores, infere-se que a estrutura institucional de proteção do cliente bancário não constitui um instrumento indutor de redução de riscos de fraudes e promoção da higidez do SFN.

O repasse de perdas é imediato ao cliente, contrapondo-se a um processo de contestação longo e custoso, existindo uma série de barreiras que impõem custo não desprezível ao titular de cartão na busca de reparação de perdas. Após identificada a subtração de recursos e informada a IF, esta conduzirá uma investigação preliminar que demora no mínimo dez dias, mas há relatos de perdas relacionadas a cartões pré-pagos com prazo de investigação de até 120 dias[40]. Assim, enquanto a transação fraudulenta leva poucos instantes para ser executada, seus efeitos deletérios podem ser sofríveis por meses, algumas vezes por anos na forma de litígios morosos e custosos[41].

Em nível administrativo, o contato com a IF envolve duas etapas de SAC compulsórias, com prazos dilatados, antecedendo a recorrência à Ouvidoria, que

---

[40] Veja matéria "Fraudes com cartões de crédito estão entre as maiores reclamações". Disponível em: http://g1.globo.com/jornal-hoje/noticia/2013/05/fraudes-com-cartoes-de-credito-estao-entre-maiores-reclamacoes.html. Acesso em: 14 dez. 2016.

[41] Existem inúmeros casos de clientes que se surpreendem com dívidas a que não deram causa – pelo uso não autorizado de seus dados – e que resultam na inclusão indevida de seu nome nos cadastros negativos de crédito. O dano começa quando o cliente recebe a fatura do cartão de crédito e se depara com compras não autorizadas, acionando a IF diretamente para estorno. No mês seguinte, vê cobrança de juros caso não tenha pago compras a ele atribuídas – aumentando o prejuízo. No segundo mês, aparecem mais juros, e a IF manda uma carta informando que o não pagamento de compras realizadas em seu nome gerará negativação de seu nome nos cadastros de proteção ao crédito – impondo outro custo adicional decorrente de uma posterior limpeza de nome. No caso de clonagem, o usuário do cartão de crédito desconhece inteiramente sua utilização fraudulenta até o recebimento da fatura mensal, quando constata lançamentos de compras que não realizou – o que ocorrerá em até 40 dias após os eventos criminosos. No caso do cartão de débito, o dano começa com a indisponibilidade de recursos subtraídos de conta bancária, que possuem caráter alimentar para a ampla maioria dos clientes, pois constitui montante significativo para as finanças pessoais das famílias. Os clientes acabam tendo de lidar com falta de recursos para fazer frente às despesas correntes rotineiras, e até tendo de sustar cheques que acabam não sendo compensados por falta de saldo bancário. Assim, o potencial de dano de um evento de fraude envolve o risco de acabar devendo também para credores habituais, diante da indisponibilidade de saldo para pagamento das contas mensais, seja para pagamento do financiamento do carro, da casa própria ou o aluguel, e até mesmo a conta mensal do cartão de crédito.

consome mais tempo. Trata-se de instância que não beneficia a ampla gama dos clientes bancários, com os bancos alegando que não lhes cabe responsabilidade ou que não possuem ingerência em assunto que seria uma questão de segurança pública, à parte do SFN.

A instância recursal do BC parece ter ingerência limitada sobre questões de fraudes e roubos impostas aos clientes bancários. Não há regulamentação própria da Autarquia equacionando o assunto e definindo responsabilidades. Assim, o registro de menos de 380 ocorrências no segundo semestre de 2014, relativos a ações praticadas por eventuais golpistas foram classificadas como "reclamações não reguladas", não relacionadas à regulamentação do BC. Em sua visão, reclamações registradas no SAC da IF relativas a cláusulas contratuais abusivas estariam no âmbito da competência do Sistema Nacional de Defesa do Consumidor. Não fariam parte, portanto, dos assuntos de fiscalização da Autarquia (veja Sinal, 2014). Lá já se recomendará o registro da reclamação junto ao Procon, que também não possui ingerência sobre o SFN[42].

Na esfera criminal, o registro de ocorrência na delegacia policial acaba tendo utilidade muitas vezes apenas formal, pois não tem capacidade de iniciar um processo de investigação repressivo próprio do Estado. Na verdade, o próprio tratamento individual das fraudes contra cartões impede a ação do poder público de polícia, que geralmente trabalha apenas sob acionamento das IFs, o que pode estar relacionado à dependência do fornecimento de provas necessárias para a investigação que são mantidas pelas instituições financeiras, cujo compartilhamento não costuma ocorrer nesses casos individuais. Pode-se, ainda, efetuar a reclamação em portais como reclameaqui.com.br ou consumidor.gov.br, todavia de eficácia restrita e facultativa do mercado[43].

---

[42] O sistema Procon não tem mandato legal para acionar judicialmente os estabelecimentos supervisionados. Além disso, não possui poder coercitivo extrajudicial sobre as empresas objeto de reclamação, o que torna restrito esse fórum para solução de conflitos sobre as IFs. A aprovação do PL nº 5.196, de 2013, tramitando na Câmara dos Deputados, pode mudar esse quadro, ao atribuir aos Procons poderes semelhantes aos dos Juizados Especiais, conferindo status de título executivo judicial às suas decisões. Pelo texto, as medidas dos procons tornam-se mandatórias. Isso é importante porque, hoje a empresa pode não aceitar a decisão administrativa, o que leva o consumidor a ir a um juizado especial e começar a ação desde o início. Além disso, demandas que não compensam entrar na Justiça poderão ser solucionadas diretamente pelo sistema.

[43] A iniciativa, incipiente, está baseada na ideia de que a publicidade negativa das reclamações constituiria incentivo microeconômico suficiente para solução de conflitos consumeristas. Após o registro, há um prazo de resposta de dez dias para manifestação da empresa citada, com mais vinte dias para réplica do consumidor, registrando o resultado obtido. E ponto final: a iniciativa acaba aí.

Resta o acesso ao Judiciário, onde as perdas por fraudes acabam resolvidas. Mas a falta de regulamentação adequada e eficaz acaba onerando a Justiça, que vai decidir caso a caso conforme for demandada. Aqui, observa-se a prerrogativa da inversão do ônus da prova à IF, em caso de contestação do cliente. Porém, muitos acabam desistindo antes dessa etapa, pois o caminho até lá é custoso. Assim, ainda que possa parecer que o cliente bancário conte com uma ampla estrutura institucional para sua proteção, a realidade mostra que essa estrutura não cumpre essa função. O processo de contestação é longo e tortuoso e, muitas vezes, acaba sendo menos custosa a assunção direta da perda financeira atribuída ao titular do cartão[44].

Resulta que a real reparação individual de danos acaba sendo para poucos, apenas para aqueles que suportam todos seus custos. A ampla parcela de vítimas de fraudes acaba nem reportando os crimes além da primeira etapa da esfera administrativa bancária. A baixa probabilidade de retorno diante das reiteradas negativas de reparação pelos bancos gera expectativa de um resultado econômico desfavorável à reparação de danos, aprofundando as perdas. Além disso, com o passar do tempo, a IF vai impondo cobrança de juros contra o cliente, que corre o risco de ter, ainda, o nome negativado em cadastros como SPC e Serasa.

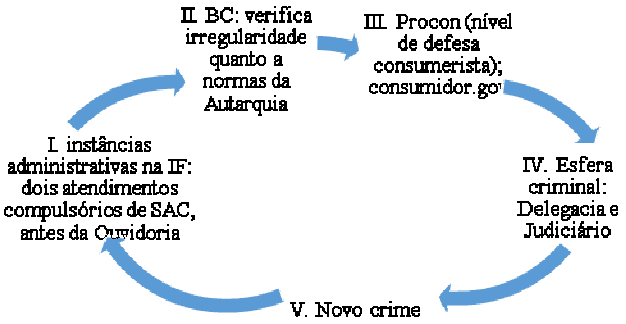
Figura 2. Pirâmide de reparação de danos

Fonte: elaboração própria.

[44] Assim, por exemplo, um débito não autorizado de mil reais de uma conta bancária não chegará a ser questionada no Judiciário, pelos custos maiores envolvidos. O que também reduz dados conhecidos e a verdadeira dimensão das fraudes nos sistemas de pagamentos.

Só para aqueles clientes que efetivamente entram na Justiça ocorre ressarcimento, mas, por serem poucos, não têm capacidade de alterar o estado atual de riscos. Daí que o processo, na prática, acaba por favorecer as IFs, pois é esperado que o custo que assumem após todas essas etapas é menor do que o custo direto de perdas diretas de fraudes repassadas aos clientes e do investimento que seria necessário para evitá-las. Gera-se, assim, um ciclo que é vicioso, envolvendo a ocorrência de crime, a atribuição de prejuízo ao cliente bancário e a posterior busca de ressarcimento do dano – via de regra, inefetiva. O ciclo se retroalimenta, diante de novos crimes. Com isso, perpetua-se o cenário de crimes, pois o repasse de perdas não tem a funcionalidade de alterar ou minimizar os riscos dos sistemas de pagamentos[45]. Isso sugere que é preciso uma ação institucional baseada em outras premissas.

Figura 3. Ciclo de contestação individual de fraudes bancárias



Fonte: elaboração própria.

4 A AÇÃO PREVENTIVA DA INDÚSTRIA E DO REGULADOR

A tecnologia *per se* é insuficiente para coibir o crime no âmbito do SFN, sendo a prevenção uma combinação do nível de segurança tecnológica e de medidas complementares (FPEG, 2007; LEACH, 2014). Nesse caso, é a ação preventiva tanto da indústria quanto do regulador que, somadas, poderão equacionar uma solução para a prevenção e mitigação mais eficiente de riscos dos sistemas de cartões.

A Lei nº 12.865, de 2013, já é clara ao estabelecer a segurança como item básico das diretrizes a serem observadas pelos sistemas de pagamentos. Como se observou na seção 2, entretanto, no Brasil a regulação infralegal acaba afastando o BC desse tema,

[45] Essa ideia não é nova. Cruz (2006) já havia concluído que a falta de regulação tratando de aspectos mais contestados e problemáticos nos contratos de cartões bancários – como é o caso da relação de responsabilidade das partes contratantes – impossibilita a assunção adequada dos riscos inerentes ao sistema, perpetuando o quadro de insegurança.

sendo contraditório em relação à abrangência do papel dos bancos centrais (DURAN *et al,* 2015). Isso explica, em parte, a prática de repasse de perdas aos clientes no País, e o cenário de fragilidades. Há, portanto, um caminho a ser perseguido especialmente na implementação efetiva da regulação e da supervisão quanto ao nível de segurança dos sistemas de cartões no País.

A atuação do setor público no combate ao crime financeiro está, hoje, a cargo apenas do sistema policial. Ainda que a ação policial possa ser bem-sucedida a partir da investigação individual de crimes, não se pode esperar que a ação repressiva seja eficaz na prevenção de novos delitos, pois isso depende, *a priori,* dos sistemas de segurança da informação das redes privadas das IFs. Considerações similares podem ser feitas sobre o processo judicial, que foca sobre a reparação de danos repassados aos clientes bancários. Além de serem custosos para a sociedade, também não são eficazes para coibir novos crimes, por definição.

É, portanto, ineficaz o uso da estrutura judiciária brasileira para tratar lesões de forma individual, sendo que são de interesse coletivo, afetando a todos. Acaba atestando a ineficiência da máquina pública, indo de encontro ao princípio constitucional. Em ambas as instâncias, o tratamento de crimes de forma individualizada onera e perpetua estruturas que não têm capacidade de acompanhar a evolução e a dinâmica social. O tempo requerido para a análise e a série de considerações envolvidas em cada caso torna-os incompatíveis com o ritmo das demandas sociais.

As características dos crimes também dificultam o combate *ex post,* pois, muitas vezes, ocorre a violação da informação privada por meio da simples memorização de dados digitados em um terminal bancário. Esse caráter imaterial torna possível a subtração de dados sem que saiam da esfera de domínio de seu titular. Isso dificulta a identificação de autoria de um crime, que acaba levando, muitas vezes, ao simples arquivamento de casos, sem ações investigativas que esgotem todas possibilidades viáveis (COLLI, 2010).

A solução para esses problemas precisa ser distinta, com o necessário reforço da ação preventiva. Enquanto a criminalização é uma abordagem para combater o problema, há um argumento que prevenção é mais custo-eficiente. Ao atacar o desafio de fraude e clonagem de dados, a prevenção torna-se mais adequada do que a ação posterior, como já foi salientado por Robinson *et al* (2011). A prevenção tem a

capacidade de evitar ou desincentivar a ocorrência do crime, por meio da imposição de maiores custos ao criminoso.

O referencial teórico provido pela Economia do Crime ajuda a entender essa racionalidade. A Teoria Econômica do Crime, que possui como precursor o trabalho de Becker (1968), pressupõe que o criminoso econômico efetua uma análise custo-benefício para impetrar sua conduta. Nesse caso, os criminosos respondem por incentivos, ou seja, tomam decisões comparando custos e benefícios. Isso implica que seu comportamento pode mudar quando essa relação se altera.

O nível elevado da atividade econômica criminosa relaciona-se com probabilidade alta de retorno do crime. Quanto maior for o potencial de benefício líquido auferível, maior a incidência das atividades criminosas. Mas, assim como em qualquer atividade econômica, os ganhos na atividade empresarial do crime são incertos, e dependem essencialmente da probabilidade de sucesso de suas operações. E essa probabilidade está diretamente relacionada ao desempenho do criminoso, por um lado, e por outro à eficácia de medidas contrárias ao crime. Tanto a prevenção da firma quanto do regulador devem ser tais que reduzam o retorno esperado da atividade criminosa, ou seja, que reduzam os incentivos inviabilizando-a economicamente.

A simples equação formaliza a função-utilidade esperada que pode ser associada à racionalidade criminosa:

$$E[Payoff] = p * U[Y] - (1-p) * U[Y-f], \text{ onde}$$

p é a probabilidade de o criminoso auferir o resultado almejado, sem ser pego;

$1-p$, a probabilidade de ser pego e punido;

U[ ], a função utilidade do indivíduo;

Y, o retorno esperado do crime, e

f, custos judiciais e punições, caso pego e condenado.

A primeira parte da equação mostra que a redução da probabilidade de sucesso do resultado do crime (p) e do retorno esperado do crime (função U) constituem os principais fatores que determinam os ganhos esperados do crime. Isso implica que ações de fiscalização preventiva – seja do próprio instituidor do arranjo de pagamento, seja

das normas do regulador bancário ou das ações de órgãos policiais, ambos de forma *ex ante* – podem atuar para coibir, de forma efetiva, a criminalidade.

A segunda parte da equação pode ser lida como a repressão ao crime, que atua sobre a probabilidade de o criminoso ser pego e punido, e o custo penal e judicial imposto à conduta delitiva. A baixa probabilidade de ser pego (*1-p*) aumenta o *payoff* esperado, e constitui incentivo econômico para o crime. É o caso brasileiro, derivado do sistema policial repressivo corrente. Também o custo de punição baixo, ou menor do que o retorno monetário esperado do crime, também atua no sentido de não coibir o crime.

Sem a modificação dos termos da equação, a incidência de crimes e fraudes financeiras deve continuar sendo assunto persistente, particularmente devido à sua lucratividade e à aparentemente baixa taxa de prevenção e repressão. Em outras palavras, é preciso alterar as variáveis determinantes da equação, para reduzir o resultado auferível da ação criminosa. Considerando-se que já existe fiscalização e aparato repressivo instalados e organizados institucionalmente na esfera pública, o cenário esperado que gera o maior benefício social é quando ocorre a junção das forças de fiscalização e de punição. Ambas atuam na redução do retorno esperado do crime. Sob essa visão, a ação preventiva tem um papel maior a cumprir nesta equação.

A prevenção deve contar com medidas que aumentem a resiliência dos sistemas ao crime. Isso requer um conjunto de dispositivos que permitam vigilância e controle mais eficiente, até mesmo com a implementação de medidas simples como autenticação de acesso multifatorial, ou aposição de foto do titular no cartão magnético. A incorporação de tecnologias de comunicação e informação nos processos de trabalho também pode permitir formas ostensivas e tempestivas de vigilância, integradas aos sistemas de autorização de transações financeiras. Atualmente, sistemas de detecção de fraudes baseiam-se no acompanhamento de perfis de uso de determinado produto ou serviço, verificando aqueles que se afastam da normalidade, com o sistema de redes neurais percebendo quando há movimentação financeira em padrão diferente ou excessivo.

Medidas preventivas, adotadas pelas IFs, associam-se ao devido *enforcement* regulamentar, pois lacunas de supervisão acentuam a fragilidade dos sistemas de pagamentos monitorados. Isso pressupõe a intensificação da coordenação público-privada entre autoridades e indústria de cartões, formando o que o BIS (2014b) chama

de abordagem integrada para garantir a resiliência dos sistemas de pagamentos. A ação público-privada deve ser primordialmente *ex ante*, ao ritmo da ação conjunta das IFs, BC e Procon, que são instituições com capacidade de resposta tempestiva às demandas sociais, com foco em soluções de forma coletiva. Isso reduzirá o desenvolvimento de crimes de forma reiterada, diante da fragilidade e riscos não desprezíveis intrínsecos aos produtos e serviços financeiros. Por isso, supervisão e *enforcement* robustos têm o papel de garantir um sistema financeiro mais hígido.

A abordagem também pressupõe criação de grupo de trabalho, a exemplo da experiência europeia, para avaliar a política pública de combate ao crime financeiro. A articulação institucional permite troca de visões e experiências complementar entre setor público – inclusive MP e polícia – e entidades da indústria de cartões, comércio e consumidores. Essa iniciativa permitirá uma avaliação mais holística dos riscos, levando à adoção de ações mais tempestivas para o aperfeiçoamento regulatório.

A regulação deve garantir não apenas o funcionamento eficiente do SFN, bem capitalizado, provisionado e competitivo, mas também seguro e provedor de serviços de qualidade, atendendo às necessidades do País e dos cidadãos. Como Cruz (2006, p.200) já ressaltou, quando se roubam dados de um cartão, afeta-se a confiança no próprio sistema de pagamentos bancários. Isso significa que é preciso ir além do marco regulatório atual, especificando parâmetros e limites mínimos para a atuação da indústria. Isso significa também que não se pode tratar condutas criminosas apenas no âmbito contratual da esfera do direito privado. A magnitude da repercussão e abrangência dos danos potenciais aponta que a problemática constitui questão de segurança pública, de interesse coletivo e difuso. A segurança, a integridade e o fortalecimento institucional dos sistemas de pagamentos com cartões merecem atenção especial, pois permeiam toda a economia e a sociedade.

Isso implica a convergência da regulação doméstica aos padrões globais avançados, o que também desonerará o sistema de proteção do consumidor. Também implica padronização do nível de segurança no acesso aos sistemas de pagamentos com cartões por terminais ATM e POS, mitigando riscos de forma global e uniforme, e acesso a canais de contestação efetivos e economicamente racionais. O ciclo de contestação atual é pouco efetivo para a solução de controvérsias simples, impondo custo que inviabiliza a proteção de direitos individuais.

Essas diretrizes ajudarão a construir o novo paradigma requerido para reduzir fragilidades dos sistemas de pagamentos com cartões, viabilizando o novo cenário que se quer alcançar. Isso inclui, por exemplo, alteração dos aspectos relacionados a seguir.

Tabela 5. Novo paradigma para o uso de cartão bancário em terminais POS

Item	Modelo atual	Novo paradigma
Critério de Segurança no uso do Cartão.	Busca a agilidade.	Garantia da autenticidade do cliente e da autorização da operação.
Nível de Segurança em relação a operações em terminais ATM.	Menor.	Igual.
Foco da Ação da Indústria no Tratamento das Perdas.	Individual, *ex post,* sobre o efeito do crime, baseado no repasse de perdas.	Coletivo *ex ante,* baseado em prevenção e mitigação de riscos.
Ciclo de contestação individual.	Longo e custoso.	Adequado e rápido.
Responsabilidade atribuída ao Titular do Cartão.	Sem limite imponível ao cliente.	Seguindo padrões internacionais.
Cooperação Público-Privada.	Não há.	Grupo de trabalho permanente.
Regulação e Supervisão.	Não há.	Monitoramento contínuo.

Fonte: elaboração própria.

5 CONSIDERAÇÕES FINAIS

A tipologia de crimes que rondam o SFN sugere um quadro de insegurança permeando os sistemas de pagamentos com cartões no Brasil, com amplo espaço para aprimoramento. Ainda que a introdução de *chips* tenha mitigado, parcial ou temporariamente, a ocorrência de fraudes e roubos em relação ao padrão tecnológico precedente baseado em tarja magnética, o padrão corrente tem demonstrado ser incapaz de fazer frente à agilidade crescente dos fraudadores especializados em estelionatos financeiros.

Associamos esse quadro a fragilidades dos próprios terminais POS, que contribuem significativamente para tornar vulnerável ao crime os sistemas de pagamentos com cartões. Isso também não se dissocia da própria carência de regulamentação, que permite o repasse a terceiros de responsabilidade por perdas

decorrentes de fraudes e roubos no âmbito dos sistemas de pagamentos e não direciona a incorporação de novas medidas de segurança aos produtos e serviços bancários. Sem regulação estrita, a tendência é a continuidade do nível restrito de segurança dos sistemas, especialmente a partir do acesso em terminais POS. As regras precisam incentivar a adoção de novas soluções de segurança.

A agilidade do crime, em constante transformação e adaptado a brechas de tecnologia do mercado de cartões, supera a capacidade corrente de resposta das instituições envolvidas, cujo desempenho deve ser promovido. Permanece, portanto, o desafio para as instituições locais lidarem com essa problemática, pela incorporação de soluções e instrumentos mitigadores de riscos para reduzir as ameaças que comprometem a adesão da população ao cartão magnético. Isso pode resgatar com plenitude a proposta original de que usar o cartão magnético é menos arriscado do que carregar dinheiro no bolso.

REFERÊNCIAS BIBLIOGRÁFICAS

ACI WORLDWIDE (2014). *2014 Global Consumer Fraud Survey*. Disponível em**:** http://www.aciworldwide.com/2014fraudsurvey.aspx. Acesso em: 21 jul. 2015.

BANCO CENTRAL DO BRASIL (2015). *Relatório de Vigilância do Sistema de Pagamentos Brasileiro 2014*. Brasília: BC/Deban, 24p.

BANK FOR INTERNATIONAL SETTLEMENTS – BIS (2014a). *Non-banks in retail payments*. Basel: Committee on Payments and Market Infrastructures, Sept. 2014.

BANK FOR INTERNATIONAL SETTLEMENTS – BIS (2014b). *Cyber resilience in financial market infrastructures*. Basel: Committee on Payments and Market Infrastructures, Nov. 2014.

BECKER, G.S. (1968). Crime and punishment: an economic approach. *Journal of Political Economy*. V.76, n.01, p.175-209.

CANADIAN BANKERS ASSOCIATION – CBA (2004). *Consumer and Debt Cards*: Canadian Code of Practice for Consumer Debt Card Services. Prepared by the Electronic Funds Transfer Working Group. 2004 Revision.

CANADIAN BANKERS ASSOCIATION – CBA (2013). *Credit Card Fraud*. Disponível em: http://www.cba.ca/en/consumer-information/42-safeguarding-your-money/58-credit-card-fraud. Acesso em: 13 fev. 2015.

CIELO (2015). *Saiba como se prevenir das fraudes e evitar prejuízos nas vendas pela internet.* Disponível em: https://www.cielo.com.br/. Acesso em: 23 jan. 2015.

COLLI, M. (2010). *Cibercrimes*: limites e perspectivas para a investigação preliminar policial brasileira de crimes cibernéticos. Curitiba: Editora Juruá, 204p.

COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES – CPMI (2014). *Non-banks in retail payments*. Basel: Sept, 2014. Disponível em: http://www.bis.org/cpmi/publ/d118.pdf. Acesso em: 10 fev. 2015.

COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS – CPSS (2005). *Central bank oversight of payment and settlement systems*. Basel: May 2005. Disponível em: http://www.bis.org/cpmi/publ/d68.pdf. Acesso em: 10 fev. 2015.

COSTA, F.N. (2013). *Prejuízo com Fraudes Bancárias*. Disponível em: https://fernandonogueiracosta.wordpress.com/2013/03/28/prejuizo-com-fraudes-bancarias/. Acesso em: 14 dez. 2016.

CRUZ, D.R. (2006). *Criminalidade Informática*: Tipificação Penal das Condutas Ilícitas Realizadas com Cartões de Crédito. Rio de Janeiro: Ed. Forense.

DURAN, C.; BORGES, C.; FERREIRA, V. (2015). Uma agenda política para a reforma do Banco Central. São Paulo: *Valor Econômico*, 13 fev, 2015.

EUROPEAN CENTRAL BANK – ECB (2014). *Third Report on Card Fraud*. Feb, 2014.

FEBRABAN (2014). *Pesquisa Febraban de Tecnologia Bancária 2013*. Disponível em: http://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/RPSP-6021-14%20FEBRABAN_Pesquisa%20Tecnologia%20Banc%E1ria_2013%207.5.2014_vf.pdf. Acesso em: 14 dez. 2016.

FEDERAL TRADE COMISSION – FTC (2015). *Lost or Stolen Credit, ATM, and Debit Cards.* Disponível em: http://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards. Acesso em: 14 dez. 2016.

FRAUD PREVENTION EXPORT GROUP – FPEG (2007). *Report on Identity Theft/Fraud*. Brussels, 22 Oct, 2007. Disponível em: http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf. Acesso em: 14 dez. 2016.

HEINRICH, G. (2006). *Operational risk, payments, payment systems, and implementation of Basel II in Latin America*: recent developments. XI Encuentro Latinoamericano de Usuarios SWIFT, ELUS 2006, "Creciendo en Competitividad", Santiago de Chile, 3-5 July 2006. Disponível em: https://www.sadcbankers.org/subcom

mittees/PaySystem/media/Documents/Developments%20in%20Other%20Regions.pdf. Acesso em: 14 dez. 2016.

HILLEBRAND, G. (2008). Before the grand rethinking: five things to do today with payments products and new payments law. Published in the *Chicago-Kent Law Review Symposium*: Rethinking Payments Law, 83 Chi.-Kent L. Rev. nº 2, 769 (2008). Disponível em: http://consumersunion.org/wp-content/uploads/2013/04/WhereisMyMoney08.pdf. Acesso em: 14 dez. 2016.

LEACH, T. (2014). *Statement of Troy Leach, Chief Technology Officer of the Payment Card Industry Security Standards Council,* before the Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit. Washington, DC. Disponível em: http://financialservices.house.gov/uploadedfiles/hhrg-113-ba15-wstate-tleach-20140305.pdf. Acesso em: 14 dez. 2016.

MANKIW, N. G.(2001). *Introdução à Economia*: Princípios de Micro e Macroeconomia. Rio de Janeiro, Editora Campus Ltda, 2ª Ed.

MIERZWINSKI, E. (2014). *Testimony of Edmund Mierzwinski*, U.S. PIRG Consumer Program Director at a hearing on "Data Security: Examining Efforts To Protect Americans' Financial Information," Before the House Financial Services Subcommittee on Financial Institutions and Consumer Credit, 5 March 2014. Disponível em: http://financialservices.house.gov/uploadedfiles/hhrg-113-ba15-wstate-emierzwinski-20140305.pdf. Acesso em 14 dez. 2016.

MIRANDA, M.B. (2010). Aspectos Jurídicos do Contrato de Cartão de Crédito. *Revista Virtual Direito Brasil*. Vol.4, nº 1, 2010.

NATIONAL FRAUD AUTHORITY – NFA (2015). *Support for the victims of fraud.* Disponível em: http://eprints.port.ac.uk/3990/1/support-for-victims-of-fraud.pdf. Acesso em: 26 jan. 2015.

OFFICE OF THE COMPTROLLER OF THE CURRENCY – OCC (2001). *Advisory Letter*. Sept 7, 2001. Disponível em: http://www.occ.gov/static/news-issuances/memos-advisory-letters/2001/advisory-letter-2001-9.pdf. Acesso em: 14 dez. 2016.

PRADO, W. (2005). *Responsabilidade Civil das Administradoras de Cartões de Crédito*. São Paulo: Ed. Pilates.

ROBINSON, N.; GRAUX, H.; PARRILLI, D.M.; KLAUTZER, L.; VALERI, L. (2011). *Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime*: Final Report, June 2011. Disponível em: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-

human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf. Acesso em: 14 dez. 2016.

SANGER, D.; PERLROTH, N. (2015). *Bank Hackers Steal Millions via Malware.* New York: The New York Times. Fev, 14, 2015. Disponível em: http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r=0. Acesso em: 16 fev. 2015.

SCHWARTZ, M. (2014). *Why Global Card Fraud Doesn't Decline.* June 27, 2014. Disponível em: http://www.bankinfosecurity.com/global-card-fraud-doesnt-decline-a-7000/op-1. Acesso em: 28 jan. 2015.

SERASA (2014). *Serasa Experian traz ao Brasil ex-fraudador Frank Abagnale Jr. e apresenta nova solução para combater a indústria da fraude online*. Disponível em: http://noticias.serasaexperian.com.br/serasa-experian-traz-ao-brasil-ex-fraudador-frank-abagnale-jr-e-apresenta-nova-solucao-para-combater-a-industria-da-fraude-online/ Acesso em: 6 fev. 2015.

SERVIÇO DE PROTEÇÃO AO CRÉDITO – SPC (2013). *Fraudes com Cartões de Crédito*: Quem é o Responsável? Disponível em: http://www.boavistaservicos.com.br/pme/seguranca-e-fraude/fraudes-com-cartoes-de-credito-quem-e-o-responsavel/. Acesso em: 23 jan. 2015.

SINAL (2014). Os Limites da Fiscalização Remota. *Revista Por Sinal*. Brasília: Sindicato dos Funcionários do Banco Central. Pg.42-44.

UNITED STATES (1974). *Fair Credit Billing Act.* Disponível em: http://www.ftc.gov/sites/default/files/fcb.pdf. Acesso em: 14 dez. 2016.

UNITED STATES (1978). *Electronic Fund Transfer Act.* Disponível em: https://www.fdic.gov/regulations/laws/rules/6500-1350.html. Acesso em: 15 jan. 2015.

UNITED STATES HOUSE OF REPRESENTATIVES – USHR (2014). *Hearing entitled "Data Security: Examining Efforts to Protect Americans' Financial Information". March 5, 2014.* Disponível em: http://financialservices.house.gov/calendar/eventsingle.aspx?EventID=371096. Acesso em: 14 dez. 2016.

WHITE HOUSE (2015). *Fact Sheet*: White House Summit on Cybersecurity and Consumer Protection. Washington, DC: The White House, Office of the Press Secretary, February 13, 2015. Disponível em: http://www.whitehouse.gov/the-press-office/2015/02/13/fact-sheet-white-house-summit-cybersecurity-and-consumer-protection. Acesso em: 14 dez. 2016.

ANEXO

Casos Ilustrativos de Falhas de Controles Internos e de Segurança em Sistemas de Pagamentos com Cartões

Caso I
(falha de segurança junto a terminais POS)

Ladrão clona cartão sem sair do carro (09/05/2013)

A polícia flagrou, na noite de anteontem, um novo e sofisticado golpe de clonagem de cartões de crédito e débito: um bacharel em direito foi detido sob a suspeita de capturar dados de clientes sem sair do carro. Estima-se que, com os dados obtidos por um sistema wi-fi, o hacker possa ter causado um prejuízo de R$ 2 milhões. De acordo com o delegado do Deic (Departamento Estadual de Investigações Criminais), o homem de 36 anos, instalou um mecanismo *bluetooth*, capaz de transmitir dados a distância, em um chupa-cabra (a máquina clonadora). "No golpe tradicional, o criminoso coloca na máquina só um chip que armazena os dados", diz o delegado. "Depois, arruma um meio de trocar a máquina original de um comércio pela clonadora, que é idêntica. Em geral, se passam por técnicos." O modo tradicional de aplicar o golpe, porém, traz uma dificuldade para o bandido: ele tem de voltar ao comércio, recuperar a máquina e copiar os dados. "Com a inovação, o criminoso conseguiu capturar os dados a distância." Na casa do homem, foram apreendidos *pen-drives* com mais de 3 mil dados de clientes e uma parafernália usada para fabricar a máquina clonadora. Outros 14 clonadores foram detidos, ontem, pela Polícia Federal na Operação Príncipe Imperial.

Fonte: http://blog.brsafe.com.br/tag/cartao-de-debito-clonado/. Acesso em: 14 dez. 2016

Caso II
(sistema suscetível a operadores criminosos)

Novo Golpe no Cartão de Débito (23 Set, 2014)

Abasteci o carro e na hora de pagar, o frentista fez a 'gentileza' de me alcançar a maquininha, só que nesse momento os dedos dele taparam o visor. Digitei a senha e ele colocou de volta na bancada, aí veio a minha sorte. Por engano, digitei um número a menos e o cara sem querer falou: 'tá faltando um número'. Como eu estava ao lado, *olhei rapidamente para o visor e minha senha estava ali digitada, ao invés dos tradicionais asteriscos*:**** !!! Como já conheço o gerente do posto (Ipiranga) chamei-o na hora e perdi mais umas duas horas na delegacia.

Lá veio o esclarecimento do novo golpe: O atendente faz uma 'gentileza' e segura a máquina pra digitarmos a senha, neste momento, tapando o visor com a ponta dos dedos, na verdade ele não colocou o valor da compra, e os dígitos da senha aparecem no visor ficando expostos como se fossem o valor da compra. Ele anota a senha e diz que não funcionou por qualquer motivo. Faz novamente o procedimento só que correto e a gente paga a despesa.

PRONTO: O cara tem a senha anotada e o número do cartão que fica registrado na bobina. Segundo a delegada, em dois dias um cartão clonado com qualquer nome está na mão da quadrilha e os débitos caem direto na sua conta!!! O frentista confessou que 'nem conhece quem são as pessoas por trás disso' um motoqueiro passou no posto, ofereceu R$ 600,00 por semana e passava lá pra pegar a lista de cartões e senhas e para deixar o dinheiro pro cara. Segundo a delegada está acontecendo muito em barzinhos, botecos, danceterias, lojas de conveniência, posto de gasolina, etc.

Fonte: http://www.conquistanews.com.br/novo-golpe-no-cartao-de-debito/. Acesso em: 14 dez. 2016

Caso III

(movimentação financeira atípica não autorizada com envolvimento de estabelecimento comercial credenciado)

Reclamação

Em 20/07/2014, ao verificar extrato bancário no celular, me surpreendi com 8 cobranças no cartão de crédito somando R$ 4.939,89, mais 6 no débito somando R$ 2.253,20, totalizando R$ 7.183,09. As operações foram efetuadas em um grupo de 8 estabelecimentos de pequeno porte, durante menos de 4h seguidas naquele mesmo dia. Vale destacar a inviabilidade prática de consumo desses gastos: R$ 953 numa lancheria; R$ 920 num bar; R$ 4.030 numa Drogaria – entre outros. Foram efetuadas *14 operações com menos de 15 minutos de intervalo médio entre cada uma, incluindo tempo de deslocamento* (vide anexo). À mesma ocasião, houve *mais 06 tentativas de uso do cartão de crédito nesse mesmo grupo de estabelecimentos,* que somaria outros R$ 4.600,00 – porém as tentativas foram negadas devido ao limite do cartão excedido. Concluí que não havia perdido o cartão, mas que fora objeto de furto sem eu perceber, e que a senha também fora interceptada por algum dispositivo imperceptível, ao usar o cartão horas antes das fraudes. Mantive diversos contatos com o Banco do Brasil (BB) mas o banco não esclareceu meus questionamentos e ignorou absolutamente todas as evidências de fraude e crime, não fazendo qualquer menção a respeito disso. Inclusive, o BB não atendeu ao disposto no boletim de ocorrência policial, que orientava para o banco retornar à polícia em caso de fraude. Os contatos realizados com o banco foram 4: direto na agência Paraíso/SP, nas datas de 22/jul./2014 e 11/ago./2014; no SAC sob reclamação nº 32608159; e na ouvidoria do BB. Considerando o cenário de riscos no entorno de cartões bancários, vale destacar legislação cabível: o art. 6º, incisos I e VI, e o art. 14, § 1º incisos I e II do CDC, que indicam a obrigação de reparar danos aos clientes em situações de falha de segurança. Entretanto, o banco entendeu unilateralmente que o cliente deveria pagar a conta, mesmo dispensando a apuração criminal. Na prática, o BB transferiu para o cliente todos os riscos de fraude que fazem parte da cadeia operacional do sistema de cartão bancário, arbitrariamente, e ignorou qualquer hipótese de crime contra o sistema bancário, desprezando todas as evidências gritantes. Ainda, o regramento estabelece que bancos têm obrigação de fornecer meios para garantir a segurança das transações, de modo que toda instituição séria deve dispor de mecanismo eficaz de monitoramento, capaz de identificar as transações feitas com o cartão do cliente fora do seu padrão de uso, podendo bloquear imediatamente o cartão ou alertar o cliente. Os valores contestados estão absolutamente fora do meu padrão de uso durante 12 anos como cliente no Banco do Brasil, onde jamais gastei em nenhum mês inteiro – nem em crédito, nem em débito – valores que chegassem próximo desses (R$ 4.939,89 e R$ 2.253,20, respectivamente). Os gastos no dia 20.07 foram efetuados rapidamente, num período inferior a 4h. Assim, informo ao Banco do Brasil que não tenho elementos para concordar e acolher esses débitos.

Pedido à empresa

Solicito que o Banco do Brasil: 1) Estorne os valores não reconhecidos que somam R$ 7.183,09, mais os respectivos encargos desde 20.07.2014; 2) Na hipótese de negação (1), considerando meu histórico de gastos através de cartão bancário no período de 12 anos, solicito que o Banco do Brasil informe: qual a probabilidade que um cliente com o meu perfil de uso do cartão tem de gastar R$ 7.183,09 num intervalo de 4h

Resposta do Banco do Brasil

Davi, não foi possível atender seu pedido de devolução dos valores. O setor responsável, por meio de equipe especializada, procedeu com as apurações e identificou que as transações foram realizadas com uso de cartão, validação de chip e impostação de senha, todos de uso pessoal e intransferível, cuja a guarda e sigilo é de responsabilidade única do cliente. Prestadas essas

informações, reafirmamos nosso compromisso com o melhor atendimento e permanecemos à disposição para quaisquer outros esclarecimentos.

Avaliação
Nota 1. Me considero muito insatisfeito com a resposta do Banco do Brasil (BB), pelas razões que segue: 1) Mais uma vez, após recorrer ao BB num *caminho tortuoso em torno de 8 instâncias*, o BB não respondeu nem atingiu o foco dos meus questionamentos; 2) O BB não atendeu nem se manifestou sobre a legislação em defesa do consumidor extraída do CDC; 3) O BB não fez qualquer menção sobre o seu suposto sistema de monitoramento (obrigatório por regulamento), o qual autorizou gastos absolutamente fora do meu perfil; 4) O BB desconsiderou os relatos de fraude e crime, não fazendo qualquer menção ao disposto no BO policial, o qual orientava para o banco retornar à polícia em caso de fraude; 5) O BB decidiu, unilateralmente, que o cliente deveria pagar a conta, dispensando apurações policiais. Assim, só me resta recorrer às instituições cabíveis, inclusive em defesa da coletividade. Reitero ao Banco do Brasil que não tenho condições nem argumentos para pagar tais valores.

Fonte: Reclamação aberta em 05/03/2015 no portal do Procon São Paulo. Disponível em: www.consumidor.gov.br. Acesso em: 14 abril, 2015.

Caso IV

(movimentação financeira incompatível; pagamento não autorizado a terceiros)

Apelação Cível nº 1.0106.12.002116-2/001 – Comarca de Cambuí
Apelante: Banco Santander (Brasil) S.A.

Trata-se de apelação interposta à sentença que, nos autos da ação ordinária movida por Ademilson Evaristo Teodoro em face de Banco Santander Brasil S.A., julgou procedentes os pedidos iniciais, condenando o réu ao pagamento de indenização por danos materiais, no valor de R$8.457,94, bem como por danos morais, no importe de R$15.000,00. Inconformado, o requerido interpôs apelação às f. 52/59, defendendo a ocorrência de culpa exclusiva de terceiro, visto que o autor foi vítima de sequestradores que realizaram saques e compras em seu nome. Alega que não houve defeito na prestação de seus serviços e que a segurança pública é responsabilidade do Estado. Sustenta que não é devida qualquer restituição, uma vez que as operações financeiras empreendidas pelos criminosos ocorreram mediante o fornecimento da senha pessoal do cliente. (...) No caso em tela, conforme se infere do boletim de ocorrência de f. 16/18, o apelado foi vítima de um sequestro relâmpago, ocasião em que os criminosos, após coagi-lo a fornecer a sua senha bancária, efetuaram saques em caixas eletrônicos e compras em estabelecimentos comerciais. É certo que as operações financeiras empreendidas pelos sequestradores não são compatíveis com o perfil econômico-financeiro do autor, visto que alcançaram o montante de *R$8.457,94 em um só dia***.** De sorte que era perfeitamente possível ao banco réu constatar a irregularidade de tais movimentações bancárias, antes de aprová-las, não sendo difícil, por exemplo, identificar a anormalidade de um *gasto de R$4.000,00 em uma pizzaria*. Ora, não há dúvida de que as instituições financeiras devem zelar pelos valores que lhe são confiados, implementando uma política de segurança hábil a promover o acompanhamento das movimentações financeiras, a fim de detectar alguma circunstância anômala que possa implicar prejuízo aos seus clientes.

Fonte: Acórdão reproduzido em *Jurisprudência Mineira*, Belo Horizonte, ano 63 (203): 57-246, out/dez 2012

Caso V

(controle interno frágil quanto ao uso de limite de crédito contratado)

Falta de respeito em sequestro relâmpago e descaso para reembolso mesmo com o próprio setor de fraudes ligando para confirmar os gastos e ter sido informado de sequestro relâmpago
Banco Itaú S/A

No dia 26/06 realizei uma reclamação do *Reclame aqui* sobre a forma desrespeitosa que o banco Itaú conduziu os gastos feitos em um sequestro relâmpago que sofri. Primeiramente me causa uma grande estranheza eu ter um limite de R$ 13.500 para gastos a crédito no Visa e R$ 1.000,00 para saque no mesmo credito e a [editado pelo Reclame Aqui] conseguir sacar R$ 1.000,00 reais em dinheiro e gastar R$ 23.000,00 reais sem ter bloqueio do cartão. O mesmo ocorreu no meu cartão múltiplo de débito e crédito bandeira MASTER onde tenho um limite de R$ 4.300,00 para crédito e R$ 1.000,00 para saque em caixa eletrônico.
Bem, os [editado pelo Reclame Aqui] conseguiram sacar mil reais via cartão Visa o caixa eletrônico que possui uma câmera e pode evidenciar que NÃO fui eu, bem como *TORRAR R$ 23.000,00 em gastos dentro as 20 horas e 22 horas* do dia 24 de junho. Já no cartão Master, sacaram mais R$ mil reais e *gastaram R$ 2.500 reais em débito em uma papelaria* cujo descritivo na fatura e PAPELARIA MERCADÃO. O Setor de fraudes achou estranho um lançamento em débito nesse valor em uma papelaria e ligou para o telefone de minha mãe para confirmar a compra antes de aprová-la (o banco tem a ligação gravada – Jane Maria Castiglia fones 51-33432692 no dia 24 de junho de 2013, entre 20 horas e 22 horas) e a minha mãe que estava comigo no telefone na hora do [editado pelo Reclame Aqui] sabia do sequestro, indicou que eu estava sendo sequestrada. Mesmo assim, o banco autorizou o débito, bem como o saque. (...)
A porcaria do setor de [editado pelo Reclame Aqui] *desconfiou do ocorrido, ligou e soube do sequestro e ainda por cima autorizou.* (...) Não recebo ligações alguma de status, tenho que ficar indo a agência sem retorno. Hoje tenho a OS 116858 interna pleiteando o ressarcimento dos R$ 3.400 da minha conta corrente, bem como multas e juros por ter ficado no vermelho.
Como uma porcaria de um banco, toma conhecimento do sequestro relâmpago (ligação gravada pelo banco) e ainda assim alega se eximir dessas despesas? Como essa porcaria de *banco permite gastos acima dos limites e 2 saques de R$ MIL reais cada, quando o limite do banco e de R$ mil*? O que mais me revolta e que o banco foi comunicado do sequestro e, ainda sim, permitiu os débitos em minha conta corrente e agora, quer se eximir alegando que eu não aderi a um seguro que sequer há evidência de que eu realmente NÃO aderi, não há documento sequer mencionando a oferta desse seguro pela minha gerente e a minha não adesão.

Fonte: http://www.reclameaqui.com.br/5865324/banco-itau-s-a/falta-de-respeito-em-sequestro-relampago-e-descaso-para-reem/ Acesso em: 29 jan, 2015

Missão da Consultoria Legislativa

Prestar consultoria e assessoramento especializados ao Senado Federal e ao Congresso Nacional, com o objetivo de contribuir com o aprimoramento da atividade legislativa e parlamentar, em benefício da sociedade brasileira.

Núcleo de Estudos e Pesquisas

Consultoria Legislativa

SENADO FEDERAL

ISSN 1983-0645