

**COMISSÃO PARLAMENTAR DE INQUÉRITO  
GOLPES COM PIX E CLONAGEM DE CARTÕES**

**26.09.2023**

\* \* \*

- Abre a reunião o Sr. Itamar Borges.

\* \* \*

**O SR. PRESIDENTE - ITAMAR BORGES - MDB** - Havendo número regimental, declaro aberta a reunião da Comissão Parlamentar de Inquérito que apura Golpes com Pix e Clonagem de Cartões. Solicito à equipe da TV Alesp que inicie a transmissão da reunião. Registro, com muito prazer, a presença dos nobres deputados Maria Lúcia Amary, deputado Marcos Damasio, deputado Rômulo Fernandes, deputado Luiz Claudio Marcolino, deputado Altair Moraes e o deputado Capitão Telhada.

Esta Presidência solicita à secretaria a leitura da Ata da reunião anterior.

**O SR. ALTAIR MORAES - REPUBLICANOS** - Sr. Presidente, pela ordem.

**O SR. PRESIDENTE - ITAMAR BORGES - MDB** - Pela ordem, deputado Altair Moraes.

**O SR. ALTAIR MORAES - REPUBLICANOS** - Para ser dispensada a leitura da Ata anterior.

**O SR. PRESIDENTE - ITAMAR BORGES - MDB** - É regimental o pedido de Vossa Excelência. Havendo acordo, dou por lida e aprovada a Ata da reunião anterior.

Nós temos hoje três convidados para ouvirmos aqui na nossa Comissão Parlamentar de Inquérito. Lembrando que, depois dessa reunião, nós teremos um intervalo de, pelo menos, uma semana, para que as nossas equipes possam se reunir e propor a continuidade das oitivas. Antes, porém, nós temos aqui o item um, que foi apresentado pela deputada Maria Lúcia Amary, requer a prorrogação dos trabalhos da CPI por mais 60 dias. Em discussão.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Pela ordem, Sr. Presidente.

**O SR. PRESIDENTE - ITAMAR BORGES - MDB** - Pela ordem, deputado Luiz Claudio Marcolino.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Pedir vista ao item um.

**O SR. PRESIDENTE - ITAMAR BORGES - MDB** - É regimental, vista para o deputado Luiz Claudio Marcolino. Vamos agora convidar os nossos convidados. Registro a presença da deputada Valeria Bolsonaro e já convido para que possa sentar aqui ao meu lado o Sr. João Henrique Martins, coordenador geral do Centro Integrado de Comando e Controle da Secretaria da Segurança Pública do Estado de São Paulo, a fim de prestar esclarecimentos. Já está aqui ao meu lado.

Já convido também o Sr. Walter Tadeu Pinto de Faria, diretor adjunto de serviços da Federação Brasileira de Bancos, a Febraban. Já vem se dirigindo. E convido o Sr. Ricardo de Barros Vieira, vice-presidente executivo da Associação Brasileira das Empresas de Cartão de Crédito e Serviços, Abecs.

E já convido para nos acompanhar também o nosso orientador e apoio deliberado nesta Casa, nesta comissão, o advogado Dr. Pedro Iokoi, para que possa sentar aqui à minha esquerda e nos dar o apoio para a condução desta reunião.

Eu gostaria de passar aos nossos convidados e aos nossos colegas: a Casa vai entrando no ritmo de final de ano, e nós temos alguns projetos e congressos de comissões, entre outras coisas, acontecendo.

Eu preciso, com muito respeito, pedir gentilmente que nós pudéssemos ter as apresentações de forma resumida porque às 15 horas nós vamos começar a perder colegas aqui na comissão porque terão que ir para o congresso de comissões, além de termos outras comissões.

Então se a gente conseguisse aí, dentro de dez minutos, cada um puder fazer a sua apresentação e na sequência a gente registra as perguntas para que possamos aqui então dar andamento e aproveitar ao máximo a presença dos colegas aqui nesta CPI. Agradeço mais uma vez a todos os colaboradores da Casa, da comissão e dos gabinetes dos nossos parlamentares.

Já passo a palavra, então, ao Dr. João Henrique Martins, coordenador do Centro Integrado de Comando e Controle da Secretaria da Segurança Pública para se pronunciar e fazer a sua apresentação. Com a palavra, doutor.

**O SR. JOÃO HENRIQUE MARTINS** - Boa tarde a todos. Primeiramente quero agradecer o convite, em nome do secretário de Segurança, Guilherme Derrite, e estender o agradecimento e o cumprimento a todos os deputados da Casa, na pessoa do presidente da comissão.

Dado o tempo exíguo, eu vou tentar ser bem célere. Vou pedir já para que suba aqui a apresentação e enquanto isso eu vou, rapidamente, explicando o que é o Centro Integrado de Comando e Controle.

O CICC é o órgão de formulação de políticas públicas integradas da Secretaria de Segurança. Ele existe formalmente desde 2014, mas ele pouco exerceu esse tipo de função e, na atual gestão, a gente tem colocado em prática uma metodologia de trabalho que envolve todas as 18 instituições que participam do CICC, que são... Além dos quatro órgãos de Segurança Pública, temos órgãos municipais ligados a trânsito, ligados a concessionárias de serviços públicos, como energia e, cada vez mais, inclusive, entidades privadas que têm conexão com a Segurança Pública

Dentro desse bojo - pode avançar, por favor -, esse fluxo na montagem de agenda, nós temos um órgão na Secretaria de Segurança, que é a Coordenadoria de Análise e Planejamento, que define os temas centrais, ou os temas prioritários de Segurança para a população e a demanda.

Uma vez que a CAP define um tema, ela envia para nós, e nós iniciamos um processo, chamado Comitê de Formulação de Política Pública, com o objetivo, ao final dele, de construir uma política que pode inclusive resultar em uma estrutura normativa, uma resolução, a construção de uma política que envolva a compra de uma tecnologia, mas que o fator principal é envolver todos os atores que são necessários para a construção dessa política, em especial aqueles que de alguma maneira estão conectados com as vítimas.

Então, assim que nós recebemos essa demanda, diretamente por conta do secretário, em meados de janeiro, nós iniciamos um Comitê de Formulação. Esse comitê envolveu os órgãos especializados da Polícia Militar, que é principalmente a unidade da Polícia Militar que mais conseguiu resgatar vítimas de cativo na região norte.

Então, nós trouxemos o próprio burocrata em nível de rua, o capitão comandante de Companhia de onde isso mais ocorria, trouxemos, pelo lado da Polícia Civil, o principal especialista da Divisão Antissequestro, que lidava com essas circunstâncias e, por parte da Polícia Técnico-Científica, a Superintendência Técnico-Científica, a equipe que fazia, ou que tentava trabalhar na perícia digital desses casos.

Porque existe toda uma dificuldade entre... Depois que a Polícia consegue livrar as vítimas do cativo, ainda que seja o cativo provisório, e o criminoso fez vários saques, você tem todo um trabalho de conseguir conectar as ações digitais que foram feitas em nome da vítima, para provar que isso foi um crime, e depois conectar isso com os contadores, que é quem recebe o dinheiro nesse desenho.

Então, o papel da Polícia Técnico-Científica, em um primeiro momento colocamos todos na mesa e trouxemos pela primeira vez a parte operacional de 16 instituições financeiras, em especial os bancos digitais, que eram os bancos mais fáceis de ter as contas, inclusive as empresas também de meio de pagamento, que têm sido utilizadas cada vez mais para isso, e colocamos todos à mesa para iniciar esse trabalho de formulação da política.

Porque isso é necessário? Porque ele não é um crime fácil, primeiro, de ser registrado. Você encontra isso dentro da própria Secretaria de Segurança como roubo, como extorsão ou como extorsão mediante sequestro. Ele também pode ser detectado diretamente pelas agências, pelas instituições bancárias, pelos seus sistemas de inteligência, quando ele percebe algum tipo de movimentação anômala, seja na quantidade, seja no horário, e essas instituições podem gerar alertas.

O fato é que, para ser bastante rápido e objetivo, a primeira contribuição desse processo foi criar um fórum, que é o comitê. Esse fórum resultou em uma resolução do secretário - pode avançar na apresentação - que foi a Resolução nº 18, que cria o SPFAD, que é o Sistema de Informação e Prevenção a Crimes Financeiros em Ambiente Digital.

Esse fórum, quem tem assento são as instituições financeiras mais as polícias, e a gente entende as instituições financeiras nesse pedaço como aquela que está mais próxima de trazer informações diretamente da vítima, e também como vítima nesse processo.

Esse sistema, nós temos reuniões a partir aí do mês de junho, mais ou menos. Passamos a ter reuniões mensais, de forma que a gente consiga reunir todo mundo que de alguma maneira tem uma parte da informação do problema, e aí a gente consegue definir prioridades. Percebe? As prioridades são transferidas ao CICC, onde é feito um comitê para tratar aquele tema específico.

Porque toda vez que a gente tenta resolver o problema de maneira geral, por exemplo, crimes no ambiente financeiro, é o melhor caminho para não conseguir resolver nenhum. Então, qual foi o nosso foco? Foi onde a vítima tem o maior nível de risco de morte, que é o momento da vítima arrebatada para o criminoso, em cativo físico, estável ou móvel, e a sequência dos gastos.

Uma vez que a gente consegue criar um protocolo de operações e ações integradas para resolver esse problema, uma vez que a gente consegue fechar esse nicho, caminharemos para os vários outros temas. Aí pode avançar um pouquinho.

Para isso, e parece pouco... É óbvio, para a vítima que está arrebatada é o principal momento da vida dela, porque está em risco, mas há vários outros eventos que nós, em um primeiro momento não priorizamos, para poder priorizar esse, que tem a vítima.

Só para tratar desse tema nós fizemos dez reuniões técnicas. Por que essas reuniões são determinantes? Porque cada banco tem um sistema de alerta. Cada banco tem um protocolo de como interpretar as situações de risco.

Eu poderia dizer também que, como o evento é novo, não é claro para as polícias como elas tratam isso. É um sequestro relâmpago? É um sequestro clássico, normal? É um roubo com retenção de vítima provisório? Então nós precisamos, durante essas reuniões, primeiro, colher informações do mundo real: o capitão da companhia, o delegado que atende as famílias. Descobrimos várias formas de início dessa ocorrência.

Às vezes, é o familiar que percebe que o parente não chegou em casa naquele horário; às vezes, tem uma conta conjunta, tem uma movimentação, ele vai até a delegacia ou ele liga 190 - já são duas fontes diferentes - ou ele vai até a rua, vê uma viatura. Nós temos casos relatados dessas três formas de iniciar, por exemplo.

Essas três formas sempre precisam da informação que vem da instituição financeira, que é confirmar se, de fato, há um comportamento financeiro, um saque anômalo e se existe alguma informação sobre localização: onde foi feito esse saque, se foi feito pelo celular, se tem a geolocalização. Algumas instituições têm esse controle, outras instituições não têm, porque tudo depende também da vítima e cliente autorizar isso.

Bem, feito essa análise dos dados empíricos, reais, do que nós temos de casuística, nós avançamos para como dar a melhor resposta para esse caso. A própria ação das polícias, junto aos bancos, já deu um caminho de como isso é possível ser resolvido.

Então, todos os bancos tinham contato com alguma unidade policial, que o acionava quando tinha um caso desse em tela, mas era um acionamento officioso, e não acionamentos oficiais.

Então havia uma margem de insegurança. Como era um caso de sequestro, de periclitção à vida, então, muitas vezes, tanto as instituições quanto as forças policiais assumiam o risco do acesso ali ao dado, porque não dá tempo de você fazer todo um processo burocratizado para ter essa informação. A vítima está tomada em sequestro, é um crime em andamento.

Bem, então o que nós procuramos fazer é criar um protocolo de ação, em que a gente institucionaliza essa relação entre forças de segurança e instituições, e a parte de inteligência das instituições bancárias, inteligência pró-cliente ali, naquele desenho de toda vez que ela cria um alerta interno, de maneira que esse alerta também chegue para a polícia.

E o contrário também, quando a polícia tem uma vítima em mãos, que ela consiga essa informação. Por exemplo, informação de qual instituição bancária ela tem conta, se houve movimentação naquele momento, se tem alguma informação sobre localização e a própria informação da família. Quer dizer, é combinar essas informações e dar escala a elas. Porque veja, às vezes, o banco ou a unidade tem contato, que são pessoas que se conhecem, que confiam e, para resolver um caso, salvar uma vida, elas entram em contato.

Mas a gente não consegue dar escala para esses casos e conter um crime já tem uma certa característica de epidemia em algumas áreas, então a gente precisa também digitalizar esses processos, para conseguir a escala, e não dá para fazer isso sem segurança jurídica.

Por isso, em várias reuniões nós fizemos uma discussão em cima do que é possível dentro da legislação da LGPD, que aí ela tem o Art. 4º, em que ela descreve a possibilidade de troca de informações pessoais em casos como esse. Só que ela precisa de uma regulamentação, no mínimo, normativa em termos de procedimentos operacionais e foi para isso que nós iniciamos.

Nós chegamos, inclusive, a convidar o Dr. Renato Opice Blum, que é uma das autoridades no País sobre o tema dados pessoais; ajudou tanto e participou tanto das audiências públicas que formularam a lei no Congresso Nacional, quanto nas primeiras composições do Colegiado Autoridade Nacional. E aí discutimos em quais mandatos legais isso era possível - pode avançar, por favor - que é essa lista das dez reuniões. Construimos esse fluxo operacional.

Então, hoje o banco tem um protocolo de operações. Quer dizer, cada banco tem o seu protocolo de operações e, às vezes, cada banco, mais de um protocolo de operações. As polícias, cada uma tem o seu protocolo. Nós criamos um único protocolo, tanto para

as polícias quanto para as instituições que aderirem, de maneira: quem informa quem, o quê, em quanto tempo.

Esse protocolo precisa ser operacionalizado por um sistema digital, uma espécie de um e-mail criptografado que permita a comunicação entre as partes e que permita a salvaguarda dessa informação, com aquela proteção de cadeia de custódia. Chegamos a essa conclusão.

Então, basicamente, para concluir o processo, de um lado nós temos as polícias, às vezes, com as vítimas; do outro, nós temos as instituições bancárias, também com as vítimas. E havia um “gap” aqui, informacional, uma fragilidade tanto técnica quanto jurídica de como fazer essa informação se comunicar, uma vez que a vítima está arrebatada. É aí que nós, no Centro Integrado de Comando e Controle, entramos e nós iniciamos.

Hoje nós estamos em um processo de licitação, tanto da compra de uma tecnologia que prevê que essa cadeia de custódia, a proteção da cadeia de custódia, quanto um time físico, um tipo humano, que está ali para receber as requisições de cada um dos lados.

Quando o banco percebe algo e quer comunicar à polícia, ele vai comunicar via CICC; quando as polícias têm algo com as vítimas e querem comunicar os bancos, vão comunicar via CICC. O CICC passa a ser a autoridade responsável por anonimizar as informações, proteger as informações, por isso a aquisição desse sistema.

O sistema será gerido pela Polícia Técnico-Científica para proteger a cadeia de custódia em todo o desenho e, ao final, pode avançar que nós temos, que é o “status quo”.

A integração desses processos, hoje, já ocorre via CICC. Então as instituições que hoje já estão conectadas a nós por meio do termo de adesão, ao CICC, quando precisam, fazem essa comunicação, ainda oficiosamente. A partir do CICC, a gente registra - não é oficiosamente, é analogicamente, ainda - e a gente comunica isso às polícias. O contrário é a mesma coisa.

Nós estamos no processo de licitação dessa aquisição técnica, para transformar isso em uma comunicação digital contínua, a alocação de equipe, para manter aquilo que eu falei no início: enfrentar a questão da vítima arrebatada em sequestro é só o primeiro deles.

Porque a gente sabe que tem vários outros crimes digitais que essa própria estrutura, que está sendo criada, vai poder fornecer meios para que outras políticas sejam construídas a partir disso.

Iniciamos o monitoramento, para ter uma ideia: a polícia tinha um número, a Polícia Civil tinha um número, a Polícia Militar tinha outro número, os bancos tinham outros números, nenhum batia. A gente está criando um sistema único de quantificação desses dados, porque eles têm tipos penais distintos.

E, por último, também como nós conseguimos reunir especialista em nível operacional, ao mesmo tempo, com especialistas do mundo jurídico, tanto do lado das polícias, como os delegados de polícia, quanto membros da sociedade civil, como o Dr. Renato Opice Blum.

Nós, também ao final desse processo que vai encerrar ao final da compra e da operacionalização de fato, nós vamos apresentar sugestões de inovação legislativa, tanto para esta Casa, quanto para o Congresso Nacional, para reformar a legislação para se adequar e criar instrumentos para enfrentar esse problema.

Vou dar um exemplo rápido aqui da questão do Congresso Nacional. Há uma dificuldade, por parte das autoridades policiais, dos delegados de polícia, de conseguir... Uma vez na investigação, teve a prisão em flagrante de quem estava com a vítima em cativo ou tinha uma conexão imediata. Mas na hora de conectar o conteiro, que é quem abre a conta para receber o dinheiro, há uma extrema dificuldade do Poder Judiciário de entender que isso faz parte da organização criminosa. E muitas vezes vira um elemento fundamental desse tipo de crime.

Ele vai abrindo, ele abre uma, duas, quarenta contas correntes, e não é possível ele ser indiciado. Então, nós estamos preparando uma sugestão de texto, de maneira que o conteiro passe, também, a ser enquadrado no mesmo crime, e a possibilidade de a autoridade policial colocar como organização criminosa, solicitar mandado de busca, que existe uma certa resistência.

Esse é um trabalho técnico muito difícil de ser construído, porque são partes com condições diferentes, que nós estamos na fase final já, que ele fecha com a aquisição de uma tecnologia que permite esse fluxo de informação.

Esse é o Comitê de Formulação de Política Pública Integrada. Foi o primeiro comitê implementado e ele já tem resultados, mesmo antes da concepção da tecnologia, que é essa integração que já ocorre em termos de procedimentos. Presidente, é isso.

**O SR. PRESIDENTE - ITAMAR BORGES - MDB** - Obrigado, Dr. João Henrique Martins, depois nós teremos aí as perguntas. Na sequência já convido o Sr.



Walter Tadeu Pinto, da Febraban - Federação Brasileira dos Bancos - para que possa fazer a sua apresentação.

Agradeço aí, hoje, quase que quórum completo, faltou apenas o deputado Paulo Correa, que justificou que está acompanhando o secretário de Turismo lá no litoral. Agradeço a todos os colegas entendendo as demandas das comissões. Com a palavra, o nosso convidado Walter Tadeu Pinto de Faria.

**O SR. WALTER TADEU PINTO DE FARIA** - Obrigado, presidente. Cumprimento a todos aqui, agradeço pela oportunidade.

A Febraban tem trabalhado muito na questão de prevenção a fraudes e golpes. E é uma preocupação constante do sistema financeiro.

Pelo o que nós observamos no ano de 2022, de cada dez transações realizadas pelos nossos clientes, oito são realizadas por meios eletrônicos. A partir da pandemia, nós tivemos uma digitalização fenomenal, com todos os nossos clientes partindo para utilizar os meios digitais.

Pelo o que podemos ver ali na apresentação, a grande maioria utiliza o “mobile banking”, ou seja, utiliza o aplicativo do celular, e aqui eu gostaria de fazer uma ressalva com relação a isso: os aplicativos dos bancos, mais o Pix, o sistema do Pix, são extremamente seguros. Desde a sua concepção até a instalação nos celulares dos nossos clientes, eles são extremamente seguros. O que nós temos aqui é a utilização dessas ferramentas mediante a engenharia social, que eu vou falar um pouquinho mais à frente aqui.

Então, com a digitalização, os golpistas, os fraudadores mudaram também. Até antes da pandemia, eles faziam ataques físicos às agências, estouravam caixas eletrônicos e, a partir da digitalização, eles migraram também para o crime digital. Com isso, eles deixam ter o risco de vida deles, porque eles estão ali atrás de um computador, para poder fazer toda uma transação utilizando os dados que eles obtêm. O próximo “slide”, por gentileza.

Aqui, então, o que a gente gostaria de dizer? Temos dois tipos de ações: as fraudes, que são feitas mediante o golpista e o fraudador obtendo as informações do cliente e indo, se passando por cliente; e tem o golpe, onde a vítima é envolvida pela engenharia social que o golpista faz. É quando recebemos um telefonema dizendo que é da central de atendimento do banco. Isso é o que nos traz mais preocupação. Próximo, por favor.

Então, o que temos aqui? A engenharia social; é a manipulação psicológica. Essas pessoas conseguem se passar e convencer as vítimas com uma tranquilidade enorme. Eles têm uma - usando um termo normal - lábia enorme, porque eles convencem as pessoas de que, sim, eles são de banco ou de que são de alguma outra entidade que está querendo protegê-lo. Próximo slide.

Aqui, só para vocês terem uma ideia, a gente teve, no ano de 2022, um crescimento de 165% nos golpes financeiros, e aí, de novo, utilizando engenharia social. Volto a dizer: os aplicativos dos bancos e o sistema Pix são extremamente seguros desde sua concepção. Próximo, por favor.

O que temos aqui? Quais são as metodologias, o modus operandi dos golpistas? Como eles acessam as pessoas? Eles se passam por um falso funcionário, uma falsa central de atendimento. Eu, pessoalmente, antes de ontem, recebi uma ligação dizendo que era do meu banco, querendo obter meus dados.

Também a gente tem a questão da mão fantasma, em que a pessoa entra e te manda uma mensagem se passando por um conhecido, pedindo para você instalar um sistema para melhorar a performance do seu celular. Eles acabam entrando em todos os seus dados ali dentro do celular.

O golpe do falso motoboy. Isso a gente vê, é normal ligarem pedindo para você picotar o seu cartão magnético, mas sem cortar o chip, para ele poder usar. Antes disso, ele já fez toda a engenharia social para obter os dados de conta, senha.

Temos a questão do “phishing”, quando eles mandam para você um email solicitando informações e, se a pessoa não estiver atenta, acaba passando as informações bancárias, a que eles passam a ter acesso.

E tem a questão do WhatsApp, que é um golpe mais recente, em que, via de regra, eles mandam uma mensagem para você dizendo para você fazer algum ajuste. Tem que digitar um código que vem dentro da mensagem deles. No momento em que você digita aquele código, ele passa a ter acesso à sua relação de contatos do WhatsApp, onde ele começa a emitir mensagens pedindo dinheiro, dizendo que está com alguma dificuldade financeira. Próximo slide, por favor.

Bom, de que forma o sistema financeiro está atuando? Em 2022, nós investimos, o sistema financeiro investiu cerca de 3,4 bilhões de reais em sistemas de segurança e em sistemas de prevenção a fraudes. Além disso, o que nós fazemos? Nós compartilhamos informações.

Como o colega da Secretaria de Segurança colocou, nós temos todo um relacionamento com as Polícias Civis, com a Polícia Federal, para que a gente possa ter esse trabalho de troca de informações, para a gente poder chegar rapidamente aos golpistas e tentar prendê-los, apesar que, muitas vezes, o trabalho é feito, muito bem feito pelas polícias.

Mas, na audiência de custódia, o juiz acaba por liberar o golpista, porque o juiz entende que não houve um atentado físico à pessoa, e sim só um golpe; acabam liberando a pessoa. No final de 2021, tivemos um hacker que foi preso.

Dali a dois dias, ele estava solto. Ele foi preso não porque estava com oito milhões de reais em dinheiro no apartamento dele; foi preso porque estava com anfetamina. Dali a dois dias, ele foi solto na audiência de custódia. Hoje, está em Miami operando via criptomoeda. Então, a gente tem uma defasagem também na questão legislativa, para poder prender essas pessoas efetivamente.

Fazemos um trabalho constante de conscientização. A Febraban e os bancos -vou mostrar mais para frente para vocês - têm feito campanhas de conscientização para que nossos clientes estejam cientes do que acontece quando se tem uma tentativa de golpe, como proceder e como se resguardar dessas ocorrências.

E o combate e a repressão. Como falei há momentos, a gente tem acordos com as polícias. Temos acordo com a Polícia Federal, que chamamos de “Projeto Tentáculos”. Temos também um acordo com relação à criação de um laboratório de combate ao crime cibernético, principalmente atacando o crime de “ransomware”, que é quando eles capturam as informações da empresa e solicitam um resgate daquelas informações, ou para liberar sistemas. Por gentileza, o próximo.

Temos mecanismos de prevenção a fraudes. Apesar de termos diversas ocorrências em que são registrados questionamentos ou reclamações da forma que é aberta a conta corrente pelos bancos, a gente tem todo um ecossistema de controle disso. Fazemos consultas às bases governamentais de informações, fazemos todo um processo de biometria facial, e aí também utilizando bases, base de CPF. Então, a gente tem todo um processo que nos traz segurança na abertura de conta corrente, no processo de “onboarding”.

Com relação ao Pix, especificamente: nós temos, dentro do Banco Central - que é o gestor do Pix - um sistema que se chama MED, que é Mecanismo Especial de Devolução, em que, no momento que um banco detecta um golpe, ele comunica via esse

sistema o banco para onde foi destinado o valor, tentando bloquear e recuperar aquele valor.

Nós temos, dentro de uma empresa que é do sistema financeiro - que se chama Núcleo, antiga CIP -, um sistema parecido com MED, só que para TED e cobrança. Uma diferença é que lá no MED só vai ter a primeira camada, e nesse nosso sistema da Núcleo vai até a quinta camada.

Temos também uma base negativa de fraudes, uma base onde nós temos informações de golpes efetivos, ou seja, nós temos mais de três milhões de CPFs dentro dessa base de efetivos fraudadores, de efetivos golpistas, que passaram por todo um processo de apuração criminal e, realmente, eram culpados disso. Por gentileza, o próximo.

Bom, como eu falei no início da minha fala, a prevenção a fraudes para a Febraban é um projeto, é um processo de extrema preocupação, de extrema importância. Então nós criamos aqui um plano executivo de prevenção a fraudes, que é tentar mitigar todo esse risco que a sociedade passa, e para isso nós definimos três pilares dentro desse processo, desse plano executivo. Por gentileza, o próximo.

Um dos pilares é melhorar a jornada do cliente. Hoje, quando um cliente sofre um golpe, ele é correntista de três, quatro bancos, tem que ir a cada um desses bancos solicitar para que bloqueiem sua conta, para evitar ter a recorrência de um golpe. Nós estamos em processo de criação de um sistema em que eu entro em um dos meus bancos, comunico o golpe, o atendente desse banco vai perguntar se eu sou correntista em alguma outra instituição.

Se sim, se eu autorizo que este banco comunique as demais instituições de que houve um golpe na minha conta e, então, que as instituições também tomem todas as precauções de prevenção a fraudes para evitar que se tenha aqui ocorrência de golpe em outras instituições. Aqui a gente já está bem adiantado nesse processo, estamos definindo qual o canal de comunicação entre cada instituição. Acreditamos que para o início de 2024 ele esteja operando já.

O segundo ponto é a gente ter uma base centralizada de informações de prevenção a fraudes. Como eu mostrei no slide anterior, nós temos o MED para o Pix, temos lá na Núcleo o Detecta Flow, para cobrança DOC e TED. A gente pretende conversar com o Banco Central para que a gente consiga centralizar tudo isso no próprio Banco Central, visto que ele já tem uma base lá, toda a base do Pix.

Então a gente agregaria mais as informações de TED e DOC lá. E, por fim, o terceiro pilar dessa nossa frente é com relação ao estabelecimento de um selo de prevenção a fraude das instituições financeiras. Esse processo também já está em andamento pela Febraban.

O que significa isso? Significa que nós vamos elaborar um regulamento ou uma convenção em que teremos as exigências mínimas para abertura de conta corrente, para todo um processo de movimentação de conta corrente. E uma consultoria contratada por nós irá às instituições verificar se aquela instituição está fazendo tudo aquilo que foi recomendado. Se estiver, ela passará a ter esse selo. Isso vai ser feito anualmente.

Eventualmente, se a instituição deixou de observar qualquer uma daquelas condições que estão no regulamento, ela pode perder o selo. Então aqui também é uma forma de dizer para a sociedade que os bancos, sim, têm preocupação com os seus clientes, estão trabalhando na prevenção a fraudes. Próximo, por favor.

Bom, então as principais frentes são ações que a gente faz de prevenção a fraude utilizando os canais de imprensa, as campanhas de conscientização, que são mensais. A cada data específica - Dia das Mães, Dia dos Pais, Dia dos Namorados, Black Friday, Natal - o sistema financeiro sai com informações aos seus clientes, e uma campanha nacional que nós fizemos em 2021 de forma massiva em mídia televisiva.

Em 2022, fizemos nos canais digitais e este ano voltaremos a fazer amplamente utilizando novamente mídia televisiva, que é a campanha “Pare e pense, pode ser golpe”, para que a gente... De forma bem-humorada, a gente vai usar uma música que deve colar na cabeça da gente, para que as pessoas tomem consciência disso com relação à prevenção a fraudes. “Pare e pense, pode ser golpe.” Próximo, por gentileza.

Ali é uma relação das campanhas de conscientização que fizemos no decorrer de 2022 e 2023. Aqui é importante ressaltar que, tanto em 2022 quanto em 2023, em parceria com a Polícia Federal, tivemos duas operações, denominadas “Não seja um laranja”. Essas operações da Polícia Federal foram especificamente para ir naquelas pessoas que emprestam suas contas para receber dinheiro oriundo de golpe e fraude. Infelizmente, essa é uma prática comum e isso traz grande prejuízo.

Estamos tentando melhorar - mais a frente eu vou falar aqui também -, junto ao Banco Central, que essas pessoas que emprestam suas contas para receber dinheiro oriundo de fraude fiquem proibidas de operar no sistema financeiro durante um período, como é no caso de cheque sem fundo, que a gente fica cinco anos sem receber um talão

de cheques. A gente está conversando com o Banco Central nesse sentido. (Vozes fora do microfone.) Tem que ser punido, né?

E, normalmente, quando a pessoa que emprestou a conta é presa e vai à audiência de custódia, ela alega que o sobrinho pediu a conta emprestada, que ela não sabia qual era a finalidade e a vida segue, não acontece nada. Próximo, por favor.

Campanha de “Pare e Pense, Pode Ser Golpe”. Em dois anos, como eu falei para vocês, 2021 e 2022, a gente teve aí um bilhão de impressões, 250 mil engajamentos. Então a gente vê que essa campanha atingiu um público bem amplo na questão de prevenção a fraudes e prevenção a golpes. O próximo, por favor.

Então, aqui, só com relação ao combate à repressão, nós temos o Projeto Tentáculos, que a gente tem um acordo com a Polícia Federal. São 29 bancos que participam, diversas ações já feitas pela Polícia Federal com as informações entregues pelo sistema financeiro. Nós temos o Projeto Acar, que é aquele que eu falei no início, de combate a “ransomware”, que a Febraban e a Polícia Federal têm agido aí bastante, e a criação de um laboratório.

Com relação ao Projeto Tentáculos, a Polícia Federal está indo aos estados para que o Projeto Tentáculos seja repassado para as polícias civis também, para que a gente tenha uma amplitude maior de ação e de investigação. E, por fim, com as operadoras de telefonia, nós estamos aí junto com a Anatel e com o Ministério da Justiça em vias de lançar um app que se chama Celular Seguro, no qual eu vou poder pedir para que a minha operadora trave o meu celular para caso de eventual roubo desse celular.

E, a partir desse app, essa informação vai chegar aos bancos também, para que os bancos possam fazer todo um processo de prevenção a fraudes. Próximo slide, por gentileza.

Bom, aqui, nas considerações finais, é muito do que eu falei, a questão que a pandemia levou à questão do uso dos meios digitais. A engenharia social é o principal meio, a principal forma de acesso dos golpistas às informações bancárias das pessoas. E aqui, como eu falei agora há pouco, os sistemas são tão seguros que eles vão no elo mais fraco do processo, que é a pessoa, que muitas vezes não está preparada para saber que aquilo ali que está acontecendo com ela é um golpe. A questão do relacionamento com os órgãos de segurança e todos os investimentos que fizemos.

E aqui, no próximo slide, um ponto importante. Nós estamos com um PL, o 2254/22, tramitando lá no Congresso, no Senado, melhor dizendo, que é justamente o combate às contas laranjas e sequestro Pix. E aqui nós estamos pedindo, se possível, que

os senhores, junto às suas bancadas federais, nos auxiliem na aprovação, porque a gente amplia a penalização para as pessoas que emprestam conta, amplia a penalização para aquelas pessoas que praticam a extorsão mediante sequestro.

E, por fim, um outro pedido aos senhores, se possível. A partir do momento que nós divulgarmos a campanha do “Pare e Pense, Pode Ser Golpe”, muito provavelmente no final de outubro, se poderíamos encaminhar aos senhores para que pudesse ser publicado na Alesp, na TV da Alesp, em outras televisões estatais, para que a gente tenha uma amplitude maior nesse processo.

Bom, acho que é isso que eu tinha a falar. De novo, a Febraban tem na questão da prevenção a fraudes e golpes um mote muito importante para 2023 e para 2024 e estamos inteiramente à disposição dos senhores.

**O SR. PRESIDENTE - ITAMAR BORGES - MDB** - Obrigado ao Sr. Walter da Febraban. Consulto o deputado Luiz Claudio Marcolino. Ok, você já está inscrito como primeiro a dirigir pergunta aos nossos convidados.

Então eu convido agora para a última participação antes de entrarmos para a fase de perguntas, o Sr. Ricardo de Barros Vieira, representando aqui a Associação Brasileira das Empresas de Cartões de Crédito e Serviços.

**O SR. RICARDO DE BARROS VIEIRA** - Obrigado, Sr. Presidente. Eu cumprimento todos os parlamentares. A Abecs agradece a oportunidade de estar aqui e apresentar as informações e os esclarecimentos solicitados pela CPI.

Em função do tempo, eu não vou passar a apresentação. Ela está disponível para todos, impressa e eletronicamente, com todos os dados. Ele vai tentar perseguir o meu discurso. Eu não vou ficar...

Ela tem uma parte que fala dos números e do crescimento da indústria nos últimos 15 anos, mas só a última fotografia talvez valha. No final de 2022, o volume transacionado foi de 3 trilhões e 300 bilhões de reais com cartões, representando quase 40% do PIB brasileiro e quase 60% do consumo das famílias.

É um crescimento a dois dígitos há 15 anos consecutivos. O número de fraudes... Nós estamos falando de mais de 100 milhões de brasileiros portadores de cartões, de quase 22 milhões de máquinas disponíveis em todos os estabelecimentos comerciais neste País, fora transações por e-commerce.

O nosso número de fraude, é a informação, nós temos a série histórica, está em 0.049% e uma curva descendente...

Nós temos talvez um dos melhores... Os melhores índices de fraudes da indústria de cartões no mundo, porque eu acho que é motivo de orgulho, se nós não formos a mais, nós estamos entre as três mais modernas indústrias de meios de pagamento do mundo.

Por exemplo, no Brasil, o que todo mundo chama de clonagem, isso foi erradicado em 2005, quando começou-se a adotar chip e senha. Quer dizer os cartões no Brasil não são clonados mais. No início eles eram clonados e utilizados no exterior, que ainda tinha leitura de trilha magnética, por isso que os bancos bloquearam.

Quando você vai para o exterior, você tem que desbloquear seu cartão para ir para o exterior, porque no Brasil não é mais possível. Todas as máquinas estão preparadas para leitura de chip e todos os cartões são com chip.

Então os nossos números são muito bons, a gente tem uma preocupação histórica com isso, mesmo aquela transação NFC, que tem muito vídeo na internet falando que é fácil de fraudar, os nossos índices de fraude são de 0,007%, o menor índice de fraude que tem em todos. E não podemos esquecer que alguma coisa tem também a questão de, infelizmente, auto fraude que a gente não pode deixar de considerar.

Preocupações com isso a gente tem “n”, como o colega da Febraban colocou, a gente tem fóruns permanentes de discussão e um acompanhamento constante. Só quero tentar fechar o pensamento. Basicamente é o seguinte, a indústria, ao longo das cinco, seis, sete décadas, se preocupou em desenvolver buscando tecnologias seguras e a facilidade, a usabilidade - fácil de ser usado.

E como ela não é imposta, ele tem que convencer tanto pessoas físicas a terem o cartão quanto estabelecimentos comerciais a aceitarem o cartão, ela tem que oferecer vantagens e seguranças. Então ela cresce, porque ela é, teoricamente, boa para todas as partes. Ela é boa para o estabelecimento comercial, boa para o consumidor e boa para o País, porque ela evita descaminhos ou sonegação. Toda operação com o cartão é rastreável e informada aos fiscos.

Então ela desenvolveu dois mecanismos, o modelo do cartão, por si só, empodera o consumidor, porque ele não tem a liquidação on-line “real-time”, que tem, por exemplo, no Pix. Então ele sempre um tempo para discutir e questionar qualquer transação.

Existe um mecanismo consagrado na indústria de cartões no mundo inteiro que chama “chargeback”, em que o consumidor tem o direito: “Essa transação não é minha, eu não me lembro dessa transação”. E pode ser um equívoco, um engano, o nome que



vem lá na transação é diferente, é um nome de fantasia, do nome que vem impresso na fatura.

E nesse processo ele questiona junto ao banco, e tem todo um processo, documentado, rastreável em que o banco conversa com a credenciadora, que conversa com o estabelecimento a fim de se comprovar, quem tiver agindo de boa-fé tem o seu direito preservado, seja o estabelecimento comercial, seja o consumidor.

Esse é o modelo do nosso negócio, diferente do Pix, é que a liquidação on-line “real-time”, nesse tempo o dinheiro já foi transferido. E um outro detalhe é que todos os três trilhões e trezentos bilhões em volume transacionado, ano passado, no cartão são feitos exclusivamente para compra de produtos e serviços.

Os cartões são a maior linha de financiamento ao consumo do País, mas muito longe do segundo colocado, são três trilhões e trezentos bilhões que ele financia, a maioria sem custo de financiamento ao consumo.

Então a gente tem muita preocupação... Não é que a gente está confortável; a gente é muito vigilante quanto a isso. Além de ter processos e tecnologias, a gente acompanha todos os envolvimento da indústria.

Então a gente está atento com regras e mudanças de regras, por exemplo, na internet, no “e-commerce”, o consumidor não tem risco, zero de risco, ou o risco é do estabelecimento comercial, ou o risco é do banco, porque não tem a leitura do chip na transação.

Então tem regras aprovadas pelo Banco Central, que tentam preservar o consumidor de todo o tipo de fraude possível. Obviamente, a gente tem que estar sempre atento, porque as pessoas são muito inventivas nessa área. Com essa preocupação, a gente investe. Só para terminar rapidamente para ter tempo das perguntas. A gente investe muito forte em educação financeira também.

A gente tem contratados... Gera videoaulas, a gente tem mais de 380 milhões de “views”. A gente tem um professor que explica como usar cartão, como evitar fraudes, como planejar para não se endividar. Nós temos canais com mais de 600 mil seguidores no Facebook. Então a gente tem toda uma preocupação com educação financeira.

E notem, a preocupação da Abecs é marginal, os principais propagadores de boas práticas e de educação financeira são os bancos e as credenciadoras, a gente ajuda marginalmente nesse processo e a gente tem essa quantidade de “views” e essa quantidade de videoaulas.

Olhe, só para os senhores terem ideia... Dois números, clonagem de cartão, que foi erradicada, mas ainda é usada a terminologia no sistema de defesa do consumidor, nós fomos pegar os números do Consumidor.gov: em 2021, foram 2.224 ocorrências; e em 2022, 1.962. E eu posso garantir aos senhores que nenhuma delas é clonagem efetivamente, é algum outro problema na fatura que a pessoa encaixa na árvore como clonagem.

O investimento da indústria de meios de pagamento no mundo inteiro são bilhões e bilhões de dólares. E a tecnologia que investe no Brasil, que existe no Brasil é a mesma que existe em Nova Iorque, no Japão, em Tóquio, é mundial. Então ela é testada e é segura muito antes de ser colocada à disposição no Brasil.

Então, Sr. Presidente, correndo atropelando todos, eu acho que a principal mensagem é investimento em soluções de concepção de produtos com tecnologias seguras e modos de procedimento - como eu disse, “criação de regras de chargeback” - que permitam ao consumidor discutir e recuperar efetivamente os bens, atribuindo a quem quer que seja que participou ou que foi, de alguma forma, negligente nesse processo, a responsabilidade pelo dano financeiro. É assim que o cartão funciona, no Brasil e no restante do mundo.

Agradeço. Desculpem o atropelo da fala. Eu estou tentando preservar os dez minutos. Eu acho que eu fiquei em oito. E abrir espaço para alguma pergunta. Mas, independentemente disso, a Abecs, eu e a assessoria estamos 100% à disposição. Se quiser uma conversa com assessores, a gente está à disposição para apresentar, explicar todos os números e o funcionamento da indústria de meios de pagamento.

A preocupação com combater a fraude é uma preocupação de todos, e a Abecs com certeza é muito preocupada com isso. Obrigado. E, novamente, desculpe o atropelo da fala.

**O SR. PRESIDENTE - ITAMAR BORGES - MDB** - Nós é que agradecemos. E também ao Sr. Ricardo de Barros Vieira e a todos os nossos convidados. E já passo a palavra para o deputado Luiz Claudio Marcolino.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Primeiro, presidente, agradecer tanto ao João Henrique, ao Walter e ao Ricardo por trazerem aqui as informações para a nossa CPI. Eu queria, inicialmente, dialogar com o João Henrique. Nós tivemos aqui, João,

o pessoal da Polícia Civil de São Paulo, da Divisão de Crimes Cibernéticos. E eu não vi, na sua apresentação, nenhuma relação em relação a essa estrutura da polícia também.

Eles vieram, apresentaram para a gente aqui todo o organograma de Divisão de Crimes Cibernéticos, e eu não ouvi na sua apresentação se existe uma relação, se vocês estão trabalhando em conjunto ou não. Porque, pela sua exposição, eu não vi nenhuma menção em relação aos crimes cibernéticos. Está tendo uma atuação conjunta ou não?

**O SR. JOÃO HENRIQUE MARTINS** - Temos sim, deputado. Como eu disse ali no início, a gente tem duas estruturas na secretaria: uma é o Sistema Sobre Crimes em Ambiente Digital, onde vários atores têm assento, um deles é essa delegacia.

Quando a gente instaurou o comitê lá no Centro Integrado de Controle, é para tratar de um problema específico, que é a vítima de sequestro, a vítima arrebatada, e com as transferências de Pix. Neste caso específico, a própria Polícia Civil indicou, como participante, por parte dela, a Divisão Antissequestro. Porque, no momento em que a vítima está arrebatada, ela passa a ser o elemento principal.

Então, esse protocolo que a gente construiu foi com a DAS. Nos próximos protocolos, provavelmente a Divisão de Crimes Digitais deve ser o ator principal por parte da Polícia Civil. Então, a relação é sempre a própria polícia que indica. Nós somos um órgão de construção da formulação. A gente garante a metodologia e o resultado. Mas quem indica os componentes são as próprias instituições. E nós temos contato com todas.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - O outro ponto que eu queria que fosse apresentado para a CPI é: quando eles apresentaram aqui, eles colocaram que eles têm 83 policiais à disposição, dez delegados, 19 escrivães, 38 investigadores, 12 agentes policiais, dois agentes da Telecom e dois papiloscopistas. Qual é a estrutura que vocês têm hoje, pela Segurança Pública do estado de São Paulo, para dar conta dessa demanda do Centro Integrado?

**O SR. JOÃO HENRIQUE MARTINS** - No Centro Integrado? Nós temos algo em torno de... É porque dentro do Centro Integrado eu tenho várias estruturas. Eu tenho a equipe que organiza toda a estrutura para atender: o Disque Denúncia, a Sala Cioc, o Centro Integrado de Inteligência e o Sistema Pró-Carga. Eu não tenho aqui de cabeça cada um, mas eu vou te dar um número estimativo.

Dentro da estrutura do CICC, a gente tem algo em torno de 40 agentes, que se dividem entre a Polícia Militar, Polícia Civil, Polícia Técnico-Científica e servidores civis. Estrutura. No Disque Denúncia, que recebe a maior parte das estruturas, há algo em torno de 35 policiais, mais uma parte do Instituto São Paulo Contra a Violência.

Dentro da Sala Cioc, que é a sala onde operacionaliza as ações, em torno de 84 pessoas. E no Centro Integrado de Inteligência, a gente tem dedicada, hoje, uma equipe de sete policiais, mais outros policiais que compõem outras ações. Então, ela é modular.

Em determinadas ações, a gente requisita de outros times para montar. Por exemplo, durante os ataques contra as escolas, a gente forma forças-tarefas e operacionaliza a partir delas.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - A última pergunta: em relação a essa estrutura do grupo de trabalho, o senhor comentou que tem bancos digitais e empresas de meios de pagamento, mais instituições financeiras. Qual foi o critério que vocês adotaram para escolher essas instituições?

**O SR. JOÃO HENRIQUE MARTINS** - Nós fizemos comunicação a todas as instituições...

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - E quais são as instituições, hoje, que fazem parte?

**O SR. JOÃO HENRIQUE MARTINS** - Eu posso enviar para a comissão quais são as que participaram? Eu não vou saber de cor aqui.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Pode. Mas eu queria saber se a maioria que acabou aceitando o convite é de instituições financeiras comerciais ou bancos digitais.

**O SR. JOÃO HENRIQUE MARTINS** - Nós fizemos comunicação com todas as instituições que em algum momento fizeram contato com as polícias em razão dessas... Ou elas foram provocadas pela polícia ou elas provocaram a polícia. Então, nós buscamos, dentro dos nossos registros com as unidades especializadas, quais instituições já possuíam uma estrutura de enfrentamento ao problema. E aí fizemos convite a todas

elas, e eu não vou cravar aqui, mas eu acho que 100% de quem recebeu o convite respondeu a ele e passou a integrar a comissão. Mas eu também posso passar essa informação de maneira mais fidedigna depois aqui para...

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Eu acho importante saber... A gente tem percebido que boa parte dos crimes digitais acabam vindo das fintechs, por meio de pagamento... Também tem instituições financeiras, mas é um número menor.

**O SR. JOÃO HENRIQUE MARTINS** - As principais fintechs, todas estão.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Todas estão?

**O SR. JOÃO HENRIQUE MARTINS** - Todas. Porque a nossa preocupação na hora de construir o comitê, deputado, é sempre de sair do problema para a solução. Então a gente procura quem está lidando com ele agora. Então, por exemplo, em vez de trazer o comandante do batalhão, que é um coronel, a gente traz o comandante da companhia, que é quem está literalmente com a mão na massa, o delegado que faz a investigação na delegacia específica.

A gente quando solicita a apresentação, seja de um policial ou seja com as entidades privadas com quem a gente se comunica, a gente sempre pede que a informação seja levada sem filtro. Então, quem é que dá, que apronta a resposta, porque ele vai dizer: “Isso funciona, isso não funciona”.

Então para chegar nisso, a pergunta não foi acionar todos os bancos, mas quais são aqueles que já se apresentaram porque têm... Estão preocupados com isso, têm estrutura instalada. E depois não há nenhum problema em ampliar. Mas é necessário começar com quem realmente está lidando com o problema. Por isso essa... Esse foi o critério.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Obrigado, João. Para o Walter... Esteve aqui também, há alguns dias, o Banco Central. Eu fiz essa pergunta para o Banco Central e queria fazer também para a Febraban.

Quando foi feita a Resolução Conjunta nº 6, de 23 de maio de 2023, em relação à questão do Pix, eles caracterizam aqui que consideram para a adequação dessa resolução, a resolução... A Lei Complementar nº 105, de 10 de janeiro de 2021, as instituições financeiras... Hoje a Febraban, ela representa todas as instituições financeiras. Ela está

representando os bancos (Inaudível.). Qual a relação que tem a Febraban com as empresas de meios de pagamento? E se essa resolução do Banco Central atinge só vocês ou atinge também os bancos digitais?

**O SR. WALTER TADEU PINTO DE FARIA** - Bom, a Febraban atualmente tem cerca de 113 filiados, certo? A grande maioria bancos tradicionais. Temos alguns bancos digitais que estão conosco lá. Mas a maioria dos bancos digitais pertencem a outras associações.

Com relação à Resolução nº 6, do Banco Central, aquela base que falei para os senhores, que a gente já tem cerca de três milhões de CPFs ali, base negativa de fraudes, ela já é visando a atender a essa resolução. Então no que nós estamos trabalhando? Nós estamos trabalhando agora na adequação dessa nossa base à Resolução nº 6.

Estamos trabalhando na conversa entre a nossa prestadora de serviço, que é a Acode, junto com as outras empresas que pretendem prestar o serviço de base negativa também, para que tenha interoperabilidade para atender à Resolução nº 6, e possa ter essa troca de informações sobre os golpistas e fraudadores.

**O SR. RICARDO DE BARROS VIEIRA** - O senhor me permite, deputado? A Abecs representa mais de quase 100 empresas. A gente participa das discussões com o Banco Central sobre a Resolução nº 6 e tem até um pleito nosso para que os cartões entrem junto com o Pix, para que todo o processo caminhe para um melhor nível de segurança em conjunto.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Até aproveitando, essa Resolução nº 6, que por essa lei de 2021 pega as instituições financeiras. E hoje os bancos digitais, alguns estão na Febraban, são filiados, outros não estão. Esses bancos que não são filiados hoje à Febraban, eles seguem também a Resolução nº 6?

**O SR. WALTER TADEU PINTO DE FARIA** - Sim, porque o Banco Central regula todos eles. Para um banco digital poder funcionar, ele tem que ter autorização do Banco Central. E com essa norma, com essa resolução do Banco Central, atinge todo o ecossistema do sistema financeiro para poder atender o que demanda a resolução.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Mais uma pergunta ainda. Em relação também com o Banco Central. O senhor colocou, Sr. Walter, em relação ao Pix, que é a formação segura desde a sua criação. E nós vimos, conversando com o Banco Central, que várias dessas resoluções foram feitas só a partir da sua... Do seu funcionamento.

Inclusive o projeto, pelo menos a resolução, que trata da questão do Pix MED, que é o Mecanismo Especial de Devolução, só vai ser implementado no ano que vem. Quer dizer, nós já estamos percebendo que tem problemas agora. Só que essa execução só vai ser em 2024. Nós já estamos percebendo já que tem muitos problemas em relação ao Pix agora e durante o processo da sua execução.

O meu questionamento, que nós fizemos... Se o Banco Central incluiu o Pix dentro da estruturação do sistema financeiro, dentro do tempo adequado ou ele antecipou um processo que deveria ser debatido um pouco mais com a sociedade? Vocês que representam as instituições financeiras, que hoje executam a questão do Pix. Foi muito rápido ou foi no tempo adequado, a questão da administração do Pix?

**O SR. WALTER TADEU PINTO DE FARIA** - Olhe, o sistema financeiro apoiou integralmente a implantação e a operacionalização do Pix. O Pix foi um instrumento de pagamento importante, que trouxe inclusão financeira. E ele passa, sim, por constantes melhorias. A gente tem... Teve o Pix original, que era a transferência minha para o senhor e agora a gente está trabalhando junto com o Banco Central em processos de melhoria para que a gente atenda toda a população. Fora só a transferência, débito, Pix agendado, Pix débito automático.

No nosso entendimento, não houve uma antecipação. Ele foi amplamente discutido. Lá dentro da Febraban nós temos um grupo específico que trata de Pix. Temos um outro grupo que trata da segurança do Pix, eu participo inclusive. Então nós estamos buscando sempre esse aperfeiçoamento.

Com relação ao MED, nós, Febraban, denominamos de MED 2.0, que é esse que o Banco Central falou que vai ser implementado no ano que vem. Dentro das nossas propostas, que nós pretendemos conversar com o Banco Central, é antecipar esse MED 2.0 para que a gente possa ter mais agilidade e ampliar a abrangência dele.

Como eu falei agora há pouco, hoje vai até a primeira camada, ou seja, de um banco para o outro. Nós pretendemos que ele vá até a quinta camada para a gente poder rastrear o mais longe possível as transferências de valores, que nós chamamos de triangulação.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Essa seria a minha próxima pergunta. Se para executar foi rápido, agora para fazer a devolução para o cliente nós estamos jogando só para 2024. Então tem a possibilidade de a Febraban antecipar esse processo para adequar a necessidade do cliente?

**O SR. WALTER TADEU PINTO DE FARIA** - Exatamente. A gente pretende antecipar e incluir aí TED e cobrança dentro desse mesmo processo.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - A última pergunta. O senhor colocou aqui que em relação ao Projeto Tentáculos, hoje tem 29 bancos dentro dessa estrutura. Houve algum diálogo também com os bancos virtuais que não fazem representação hoje da Febraban? Eles estão abertos para esse debate também?

Em relação as empresas de meio de pagamento. Como que tem sido essa relação da Febraban com essas empresas de meio de pagamento, visto que elas têm ampliado bastante aqui no estado de São Paulo e no Brasil?

Como que tem sido essa relação com esses segmentos, visto que são segmentos, até do ponto de visto concorrencial, que acabam ocupando um espaço considerado do sistema financeiro nacional com estruturação de um custo bem menor. Eles estão investimento também, como vocês estão fazendo, em tecnologia para tentar barrar as fraudes do Pix de outras fraudes?

**O SR. WALTER TADEU PINTO DE FARIA** - Com relação ao Projeto Tentáculos, existe um acordo entre a Febraban e a Polícia Federal, mas sabemos que essas entidades que representam que o IPs e Fintechs também já estão celebrando esses acordos. Então vai abranger também esse outro seguimento.

No meio de prevenção a fraudes nós não temos concorrência. Pelo contrário, a gente tem um trabalho muito colaborativo. As entidades que representam IPs e Fintechs, nós temos um fórum que nós conversamos rotineiramente para trabalhar na prevenção a golpes e fraudes. Porque da mesma forma que nós, Febraban, que temos os bancos de maior rede e bancos mais tradicionais, eles também têm problemas graves de tentativas de golpes lá.



A gente sempre faz um trabalho conjunto. Dentro desse GE-SEG, que eu falei para vocês que é do Pix, eles estão conosco lá também. Então toda solução que a gente leva para o Pix é de comum acordo entre as associações.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Muito obrigado. A última pergunta, que agora eu queria direcionar também para o Ricardo. Tanto as empresas que a Febraban representa, como a Abecs, quantas dessas instituições estão no estado de São Paulo?

**O SR. RICARDO DE BARROS VIEIRA** - É bem difícil dizer, deputado. Eu creio que a grande maioria está, mas a Abecs tem afiliados e empresas no Rio Grande do Sul, no Ceará, porque a nossa atuação é nacional. Mas a gente tem 24 credenciadoras, que devem ser quase todas que têm autorizadas no Brasil. Eu acho que a grande maioria, todas não, está sediada no estado de São Paulo.

Mesma coisa dos emissores, sejam bancos virtuais ou bancos tradicionais, a maioria também é sediada aqui ou no Rio de Janeiro, mas tem em todos os estados. O Banrisul tem credenciadora, tem emissão de cartão, é filiado à Abecs, assim como outros bancos estaduais ou bancos sediados fora de São Paulo.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Se puder depois passar para a CPI.

**O SR. RICARDO DE BARROS VIEIRA** - No material tem a lista de todos os associados. No material que nós preparamos, que eu não apresentei, tem a lista de todos os associados da Abecs.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Está ótimo, mas se puder definir quais são no estado de São Paulo. Mesmo sabendo que tem de outros estados, mas fazer uma separação dos que estão sediados no estado de São Paulo.

**O SR. RICARDO DE BARROS VIEIRA** - A gente manda para o senhor.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Muito obrigado. E a última pergunta também é em relação aos cartões de crédito. Quando você pega as mesmas fintechs e tem uma parte de instituições de pagamento, em relação a questão dos cartões,

de fato a gente percebeu que diminui muito a clonagem de cartões. Mas está muito vinculado ainda à questão dos crimes em relação aos cartões, às maquininhas.

Como é que tem sido feito essa relação da Abecs com essas empresas de maquininhas? Muitas vezes você vai lá... Você pagou ali o produto a partir do motoboy, ou você vai numa loja, você tem ali o seu cartão clonado. Existe por parte da Abecs o levantamento desses CNPJs que acabam se utilizando de má-fé para poder depois fazer a clonagem do cartão? Há um procedimento de descredenciamento automático?

Quando vocês têm essa informação, essa informação quando vai para a estrutura da Segurança Pública, tem algum mecanismo de bloqueio automático desses CNPJs e abre-se um processo contra essas instituições, esses CNPJs que detectaram que houve uma fraude a partir da utilização das maquininhas?

O cartão é uma consequência da maquininha que é utilizada; você tem uma quantidade de maquininha sendo autorizada hoje como meio de pagamento. Então como é que tem feito essa integração? Vale para o senhor, mas vale também para o João Henrique, como que está essa relação, a questão das maquininhas?

**O SR. RICARDO DE BARROS VIEIRA** - Deputado, existem as fraudes da maquininha, mas normalmente elas consistem em mostrar um valor e digitar outro. A pessoa acaba autorizando, colocando o seu cartão e digitando a sua senha em cima de um valor que ele não viu. Muitas vezes alegam que a tela está estragada.

São golpes disso, porque não tem como copiar os dados do cartão. O cartão é leitura de chip e a segurança do chip não foi quebrada em nenhum lugar ainda do mundo. Então ele não clona, ele falsifica uma transação, o cliente coloca a senha em uma transação, cartão e senha em uma transação de valor alterado pela pessoa que leva lá.

Você tem mecanismo, o primeiro passo é ele que tem que identificar, porque em 90% dos casos ele recebe um SMS do banco falando: “Olhe, você fez uma transação de 500 reais”. Se não é dele, ele tem como bloquear imediatamente e é bloqueado online, “real time”, toda transação do cartão.

Se ele responder isso de imediato, só tem um golpe, uma única fraude naquele cartão, e ele pode entrar com mecanismo de “chargeback”, ele vai conversar com seu banco emissor. É difícil aí ser ressarcido porque houve a importação da senha e do chip, senha que só ele sabe.

Mas o estabelecimento comercial, a credenciadora, que é dona da maquininha, ela é informada, abre-se o processo, porque tem todo o registro do “chargeback”, e tem uma

apuração, porque as credenciadoras também são reguladas pelo Banco Central, elas são obrigadas a ter o mesmo cuidado que o banco tem ao abrir uma conta. Ela tem que ter o mesmo cuidado de conhecer o cliente, combater a lavagem de dinheiro, que tem um banco na hora de abrir uma conta.

Quando ela abre uma conta e dá uma máquina para o estabelecimento comercial, é a mesma coisa de o Walter estar dando um cheque, um talão de cheque, para quem abre uma conta: ela tem responsabilidade, a gente controla e cobra esse tipo, e o Banco Central monitora esse tipo de fraude. Estão todas contidas naquele percentual.

**O SR. JOÃO HENRIQUE MARTINS** - A questão das maquininhas não é o objeto. A formulação de política pública integrada tem que ter objeto bem delimitado, então o foco principal foi aquele onde há mais gravidade, que é a vítima tomada em cativeiro. Então, nesses casos, quase nunca envolve, por exemplo... Ele envolve muito mais a questão dos aplicativos de relacionamento, onde a gente já está iniciando uma negociação.

Ele pode vir a se tornar um objeto específico quando as próprias polícias, ou outros atores, entendem que é necessária uma integração entre diferentes órgãos. Quando a própria polícia consegue conduzir isso, a gente só entra como linha de apoio se ela acionar.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Ainda a última para a Abecs, hoje você vê que tem muitas transações também por compras online, você coloca o número do cartão, você coloca depois lá o seu código de segurança no final, que a maioria das empresas acaba pedindo que você tenha que colocar esse código de segurança.

Sei que hoje a maioria dos bancos tem orientado a fazer os cartões virtuais, para usar uma única vez, mas ainda tem muita gente que não usa esses cartões virtuais, continua usando o cartão principal. Existe algum mecanismo que possa ser feito para essas compras, para que elas não tenham necessariamente que colocar a senha de segurança? Por que eu estou perguntando isso?

Porque hoje uma coisa é você ir lá, e você está trabalhando e que você está fazendo uma compra segura, que de repente você está até fazendo uma compra de fato seguro; só que hoje nós sabemos que ainda a questão do crime cibernético, que hoje o pessoal consegue entrar e hackear a página das instituições, a página das empresas, e acaba tendo acesso a todas as informações do cliente. Como é que vocês estão vendo para de repente

tentar diminuir essa fraude também, que acaba acontecendo com essa relação com os sites hoje?

**O SR. RICARDO DE BARROS VIEIRA** - Duas informações. Existe tecnologia, tem o “click to play”, tokenização, em que você manda um token, e não o número do cartão; existe tudo isso à disposição, mas é uma questão cultural, como o senhor disse, as pessoas são acostumadas.

Mas aí a própria regra do cartão protege o consumidor, porque quando não há a leitura do chip, você não coloca o chip em uma máquina, o risco nunca é do consumidor: ou é do banco, ou é do estabelecimento comercial. Uma fraude vai ser por conta do estabelecimento comercial ou do banco, nunca é responsabilidade do consumidor. Então a regra de negócio protege o consumidor nesse caso.

Ele pode colocar lá o número, obviamente ele tem que entrar com um pedido de “chargeback”, vai ser examinado. Obviamente tem que olhar se todo mundo está agindo de boa-fé. Aquilo é examinado, mas agindo de boa-fé, não sendo ele, ele não corre risco, não é imputada a ele nenhuma responsabilidade, nenhum custo.

Ou o custo da fraude fica com o estabelecimento comercial, ou com o banco. No estabelecimento comercial, quando ele é credenciado pela credenciadora, ele faz o acordo, lá prevê que no caso de transações com cartão não presente que a gente chama o risco é dele, ou, dependendo do grau de tokenização que ele use, é do banco, mas nunca é do consumidor. Mas existem mecanismos, a gente tem que ajudar a, culturalmente, as pessoas usarem tokenização.

**O SR. LUIZ CLAUDIO MARCOLINO - PT** - Presidente, estou satisfeito com as respostas. Só solicitar depois que ficassem disponíveis as apresentações que vocês apresentaram, até para a gente poder, caso seja necessária alguma outra informação complementar, a gente solicita a vocês.

**O SR. PRESIDENTE - ITAMAR BORGES - MDB** - Vamos encaminhar para todos os gabinetes e assessorias as apresentações, bem como vamos aguardar encaminhamento do João Henrique Martins com relação à solicitação do deputado, e disponibilização sua também. Com a palavra o deputado Capitão Telhada.

**O SR. CAPITÃO TELHADA - PP** - Muito obrigado, Sr. Presidente. Sem maiores delongas, em decorrência do avançar do horário, eu gostaria de agradecer aos presentes hoje com os esclarecimentos, professor João Henrique Martins, Dr. Walter, Dr. Ricardo.

Primeiramente ao Prof. João, a gente tem visto o futuro muito promissor que a Secretaria de Segurança Pública tem adotado nessa nova gestão do governo Tarcísio de Freitas, colocando profissionais que conhecem de fato de Segurança Pública à frente da pasta e nas suas coordenadorias.

Então gostaria de em seu nome parabenizar o secretário de Segurança Pública, Guilherme Derrite, pela atuação à frente da pasta, e a todo o seu staff, a sua equipe, que tem realizado um trabalho frente ao CICC, ao Centro Integrado de Comando e Controle, também inédito e, de fato, colocada essa unidade, digamos assim, esse órgão à altura que ele merece, coordenando os trabalhos, integrando e trazendo tecnologia.

Como o senhor mesmo citou, muitos dados e informações que às vezes não batiam, não tinham ligação uma com a outra, dentro até da própria secretaria, hoje têm uma integração, têm uma liderança única, integrada à sociedade civil, aos bancos, a todas as polícias, aos órgãos municipais. Então, eu tenho certeza que, dessa união de esforços, surgirão muitas novidades boas.

Inclusive eu gostaria de deixar registrado para que nos integrem também, como Poder Legislativo, certo, presidente? Colocar-nos também a par de todos esses feitos da Secretaria de Segurança Pública, na criação de legislação, na criação de dispositivos que possam auxiliar e dar ferramentas para as polícias exercerem o seu trabalho, que não é só de enxugar gelo, não pode ser visto dessa maneira.

Mas nossas polícias têm que trabalhar, têm que levar os indivíduos à prisão. Nós temos que criar dispositivos legais, aqui no estado e em Brasília, que mantenham esses indivíduos presos, encarcerados, que não mais atentem e agridam a nossa sociedade, os nossos cidadãos de bem.

Eu não vou realizar perguntas, eu me dou por satisfeito com a apresentação de todos os senhores. Agradeço a participação e cogito para que estejam conosco também nos trabalhos Legislativos aqui o Sr. Walter, o Dr. Ricardo, bem como com a Segurança Pública, abrilhantando os serviços e trazendo informações que, sem dúvida, são primordiais para o bom andamento dos trabalhos, está bom?

Contem com o nosso mandato aqui, com a Comissão, com a CPI, que busca a elucidação de fatos e também a proposta de novas políticas públicas positivas, está bom? Muito obrigado, Sr. Presidente. Uma excelente semana a todos.

**O SR. PRESIDENTE - ITAMAR BORGES - MDB** - Muito obrigado, deputado Capitão Telhada, deputado Luiz Claudio Marcolino. Reforçar essa colocação do deputado Capitão Telhada da importância, porque daqui sairão propostas de políticas públicas, propostas de procedimentos que serão encaminhados àquilo que é de competência do Estado, das secretarias.

Mas também poderão sair contribuições de pleitos na esfera federal, que eventualmente não sejam da nossa competência. Então é importante que nós possamos receber como contribuição, além da apresentação, das respostas, eventualmente sugestões que possam ser encaminhadas a essas sugestões para aperfeiçoar essa questão. Para concluir aqui as abordagens de pergunta, o nosso consultor e convidado para dar o suporte jurídico, Dr. Pedro Ivo Iokoi vai dirigir as últimas perguntas.

**O SR. PEDRO IVO GRICOLI IOKOI** - Obrigado, presidente. Professor João Henrique Martins, vou seguir direto para as perguntas por conta do adiantado da hora. Senhor, o divisionário da DCCIBER veio aqui à CPI e nos explicou que acaba tendo que concentrar, nas quatro delegacias, casos de maior repercussão financeira ou mais graves, da mesma forma como o Centro Integrado vem fazendo aí, tratando de casos mais ligados à Delegacia de Sequestro.

O senhor enxerga, para um futuro próximo, que o Centro Integrado possa funcionar como um órgão de inteligência para consolidar informações do estado todo? Porque uma das propostas que vem aparecendo aqui na CPI é de que eventualmente o governo destaque um escrivão de cada delegacia do estado para cuidar das fraudes relacionadas ao Pix e a cartões de crédito, porque elas são muitas.

Para que se tenha um trabalho de inteligência, é preciso consolidar essas informações e tentar identificar semelhanças entre os golpes. Porque, uma vez que esses golpes são praticados à distância, eu posso ter um golpe registrado aqui no 11º DP da João Dias, e outro no 23º DP de Perdizes, cometidos pela mesma quadrilha e no mesmo momento. Então, é possível fazer essa integração lá no Centro ou é necessário que outro órgão de inteligência trabalhe com isso?

**O SR. JOÃO HENRIQUE MARTINS** - Bem, primeiro, sempre é possível. A função do CICC... Ele tem duas condicionantes: primeiro, sempre que as polícias demandarem, porque o CICC é o órgão operacional do secretário de Segurança Pública e

de certa forma do Estado. Nós somos ligados a outras cinco secretarias de Estado que também têm seus membros conectados lá.

O “core” quanto à coleta, à curadoria e à sedimentação de dados é o “core” principal do CICC, porque uma das funções dele é reunir dados para transformar a informação e devolver para as polícias, devolver para os outros órgãos conectados, para atuarem dentro das suas áreas de competência.

O fato é que o CICC nunca fez isso até aqui, nos seus quase dez anos de existência. Nós estamos, neste momento, equipando-nos, tanto com a equipe quanto com tecnologia para prover isso. Eu vou dar um exemplo: nós temos o Sistema de Registro de Boletins de Ocorrência e nós temos o Sistema de Registros de Emergências Policiais da Polícia Militar e o primeiro da Polícia Civil.

Os dois, hoje, possuem um nível de integração que o software (Inaudível.) detecta, em que o investigador, quando vai lá e faz uma consulta, encontra os dois. Só que não existe nenhuma inteligência de curadoria dessa informação para identificar que determinado registro feito no boletim de ocorrência está conectado a outros dez chamados de emergência.

Então, imagina uma vítima que registra um roubo de celular, um roubo de residência, um roubo no Pix, um roubo que gerou um sequestro Pix, e que outras cinco pessoas perceberam a ação e fizeram um chamado no 190. Essas informações estão conectadas, nós estamos iniciando um trabalho para fazer esse processo de conexão.

Esse trabalho de produção de inteligência não só pode como será feito e ocorrerá no nível que as polícias demandarem ou necessitarem, porque dentro do CICC também funciona o Centro Integrado de Inteligência e de Segurança Pública, do qual eu também sou coordenador, acumulando, neste momento.

Então também é uma função que o CIISP, tem dez anos, e não desenvolveu essa atividade até hoje. Nós estamos iniciando esse processo exatamente para dar suporte às polícias, como o divisionário da delegacia de crimes digitais destacou.

**O SR. PEDRO IVO GRICOLI IOKOI** - Perfeito.

**O SR. JOÃO HENRIQUE MARTINS** - Essa é uma maratona que a gente está começando, não é?

**O SR. PEDRO IVO GRICOLI IOKOI** - Conte conosco para fazer força nessa maratona. Segundo ponto, o divisionário do DCCIBER trouxe uma preocupação, que é necessário que a Polícia Civil tenha acesso aos dados e às movimentações de contas utilizadas por fraude, que hoje ainda existe muita dificuldade, apesar de haver um permissivo na Complementar nº 105, que autoriza as instituições financeiras a fornecerem tais informações. Será que o CICC não pode servir como um catalisador para um Bacen Jud da polícia?

**O SR. WALTER TADEU PINTO DE FARIA** - Bom, como eu falei há instantes aqui, nós já temos um trabalho de cooperação entre a polícia e os bancos muito ativo. Nós temos aqui a questão de simplesmente combinar de que forma vai chegar isso. No ano passado, nós temos um órgão que são...

**O SR. PEDRO IVO GRICOLI IOKOI** - Não era para você essa, viu, Walter? Era para o CICC, mas eu já entendi.

**O SR. WALTER TADEU PINTO DE FARIA** - É que também está bem afeto a nós ali. Mas ano passado nós tivemos uma demanda, que existe um organismo, um órgão que congrega todos os chefes de polícia civis, e eles nos procuraram para que a gente pudesse fazer esse processo de troca de informações ágeis.

Nós estamos em negociação com eles para ver, sistemicamente, de que forma a gente pode fazer essa troca de informações. Também tem a questão da Lei Complementar nº 105, que a gente tem que observar, e agora também a LGPD. Então, apesar de ser golpista, a gente tem que observar a LGPD também, mas a gente já está em tratativas.

**O SR. PEDRO IVO GRICOLI IOKOI** - Perfeito. E a última pergunta para você, professor João Henrique, aí fugindo um pouquinho do tema Pix: é possível facilitar à população um “onboarding”, um Sistema Detecta mais rápido? Digo em outras palavras, eu e os meus vizinhos temos uma preocupação com Segurança Pública.

Podemos fornecer para o CICC, para o Sistema Detecta, uma câmera na minha rua ligada à internet de alta velocidade, mas não sabemos qual é a porta para que essa câmera seja ligada ao Detecta, porque se ela for exclusiva minha e dos meus vizinhos ela não serve para absolutamente nada. Vai haver uma campanha para permitir que os particulares e as instituições financeiras ampliem a rede do Detecta?



**O SR. JOÃO HENRIQUE MARTINS** - Na verdade, isso é o programa “Muralha Paulista”, que vai muito além do que o software Detecta. Ele é um software de situações, um sistema crítico, mas a gente está, neste momento, em processo de definição de termos de referência, porque a gente está construindo uma rede.

Na verdade, a gente precisa construir uma rede, ampliar os sistemas de câmeras em posições estratégicas, possuir uma plataforma que consiga, de fato, integrar. O Detecta não se mostrou capaz de fazer isso ao longo do tempo, apesar de ser um sistema crítico de geração de alertas.

Então, o conjunto dessas ações é exatamente o programa “Muralha Paulista”. Então, indo direto para a resposta, sim, o cidadão e as empresas em São Paulo vão poder fazer isso, mas antes a gente está reorganizando os sistemas e nos capacitando.

É importante destacar que o CICC será o foco do “Muralha Paulista” como foco de soluções de políticas públicas integradas, no sentido que o senhor está destacando, quer dizer, o relacionamento que existe, vou pegar os bancos, porque é o foco e é o exemplo, mas isso pode acontecer em outros exemplos. Eu vou dar um segundo exemplo aqui, mas o primeiro vou dizer dos bancos.

Toda vez que o banco estabelece uma relação com uma unidade policial, só os casos que passam por essa unidade policial receberão um tratamento qualificado, com a informação do banco.

Quando a gente estabelece um protocolo de cooperação e a gente tem mandato legal para isso, tanto no nível de inteligência de Segurança Pública quanto no nível de integração de ações no CICC, qualquer informação que o banco envie eu consigo acessar, qualquer polícia, em qualquer nível, garantida a cadeia de custódia e vencido todos os entraves legais. É isso que nós construímos ao longo do tempo.

Então foram consideradas a LGPD, a Lei Complementar nº 105. Nós trouxemos isso para que eu institucionalize em nível de secretaria e possa atender as polícias para que elas fiquem com a entidade operacional. Eu vou dar um exemplo.

Nós acabamos de fazer um acordo de cooperação com a empresa Eletromídia, que tem aqueles totens nos pontos de ônibus. Ela já tinha uma iniciativa de tratar lá com as pessoas. Eu pedi para que a equipe entrasse em contato perguntando o seguinte: “O que você faz com a informação se a mulher contata no totem e diz que está com medo, tem um crime em andamento?”. Ela falou: “A gente liga para a polícia, 190”.

Eu falei: “Não”. Eu incorporei eles dentro do processo que o secretário iniciou, de ampliação da integração, nós incorporamos dentro do CICC e hoje, se a mulher, no ponto de ônibus, à noite, sozinha, diz: “Olhe, acabou a luz, eu estou com medo”, bem, acabou a luz, a Enel está dentro do CICC e está do lado, como nós estamos aqui.

Ele passa essa informação para a gente, da Enel, “priorize essa rua”, passa a informação para a Guarda Municipal, para Polícia Militar, para colocar uma viatura naquele momento até que chegue, existem mulheres que estão sozinhas ali.

Então, esse processo de integração e fluxo de dados está sendo ampliado, tanto do ponto de vista digital, que é isso que a gente está discutindo, quanto do ponto de vista operacional. Então, o CICC é a casa paulista, é a casa da Muralha Paulista e a casa da integração em São Paulo para essas medidas.

Aliás, eu convido os deputados a conhecerem o CICC. A gente está ali na Jorge Miranda, ali na Tiradentes. O CICC está aberto a todos os deputados que tiverem interesse de conhecer essa estrutura que a gente está ampliando.

**O SR. PEDRO IVO GRICOLI IOKOI** - Obrigado, professor. Dr. Walter, o representante do Banco Central esteve aqui nesta CPI e informou que um dos motivos que impedem a implementação imediata do MED 2.0 são as dificuldades técnicas dos bancos. Esta informação está correta?

**O SR. WALTER TADEU PINTO DE FARIA** - Pelo contrário. A criação do MED 2.0 foi sugestão dos bancos. Nós, dentro daquele grupo que eu falei, o GSEG, junto com as demais associações, propusemos para eles a criação do MED 2.0. Como eu falei, a dificuldade técnica está do lado do Banco Central, porque ele tem um cronograma de melhorias no Pix. Então, ele colocou isso mais para frente lá.

Dentro daquela proposta que nós trouxemos de melhoria no processo da base centralizada, nós vamos levar ao Banco Central uma proposta de nós, sistemas financeiros, assumirmos o desenvolvimento do MED 2.0 para agilizar a implementação.

**O SR. PEDRO IVO GRICOLI IOKOI** - Então, hoje a dificuldade técnica é do Banco Central?

**O SR. WALTER TADEU PINTO DE FARIA** - É do Banco Central.

**O SR. PEDRO IVO GRICOLI IOKOI** - Perfeito. Dr. Walter, o senhor considera que o MED 2.0 vai ser eficiente para a redução de golpes relacionados ao Pix?

**O SR. WALTER TADEU PINTO DE FARIA** - Olhe, nós entendemos que é uma ação conjugada. A base Dict, que é a base de chaves de Pix, na qual são registradas ocorrências de golpes com Pix, trazendo as cobranças, o DOC e a TED ali para dentro, a gente tem uma base de participação obrigatória de todo o sistema financeiro em que vai poder ser consultada as informações do golpista.

O MED é complementar, porque é o sistema que vai bloquear e tentar recuperar o valor. Então, o Dict é para reduzir a ocorrência de golpes e o MED é para a gente pode recuperar o valor e devolver para a vítima.

**O SR. PEDRO IVO GRICOLI IOKOI** - Do ponto de vista de Segurança Pública, muito se conclui de que uma das formas de combate à migração do crime armado nas instituições financeiras, saidinhas de banco, etc. para os crimes digitais, decorre da facilidade que as quadrilhas têm de tirar o dinheiro do sistema financeiro. Existe algum outro mecanismo que está sendo utilizado até a implementação do MED 2.0 para evitar que eles consigam colocar a mão no dinheiro?

**O SR. WALTER TADEU PINTO DE FARIA** - Os bancos têm mecanismos vários de prevenção à fraude. Como o colega da Secretaria de Segurança falou, os bancos fazem análise de perfil, análise de transação. Se aquela transação, eventualmente, estiver fora do perfil, o banco entra em contato com o cliente por qualquer meio de comunicação para que o cliente confirme ou não aquela operação.

A gente tem feito um trabalho rotineiramente aqui para trazer mais segurança para o cliente e conscientização. A questão é que, independente do MED 2.0... A questão é a engenharia social, a questão é a gente fazer um trabalho constante de conscientização dos nossos clientes, para que eles não caiam em golpe. É o que a gente tem procurado fazer com as nossas campanhas.

O MED vai facilitar, vai ajudar? Vai ajudar na recuperação do valor, não no combate efetivo à fraude. O combate efetivo à fraude, ao golpe, é o que a gente tem feito aqui nas nossas campanhas e nas parcerias com as polícias, inclusive, a Polícia Federal.

**O SR. PEDRO IVO GRICOLI IOKOI** - Dr. Walter, muito obrigado. Dr. Ricardo Barros, existe um... O deputado Luiz Claudio Marcolino não está mais aqui, mas já se falou outras vezes aqui na CPI, que existe uma percepção - que não sei se é verdadeira, gostaria de o questionar - de que as instituições de pagamentos ou os bancos digitais, são os grandes responsáveis pela facilitação de abertura de contas, com um processo menos rigoroso de “Know Your Client”. Existe algum estudo nesse sentido? É verdade? Existe um processo de aprimoramento da indústria? Como estamos?

**O SR. RICARDO DE BARROS VIEIRA** - Veja - o Walter pode me corrigir -, o Banco Central criou uma conta eletrônica mais simplificada para abertura, mas tanto as instituições financeiras que optarem, não precisa ser Fintech, não, um banco tradicional pode ter esse tipo de conta, conta eletrônica.

As instituições de pagamento têm que seguir essa regulação. Em nenhum momento o Banco Central flexibilizou nenhuma norma relativa ao “Conheça Seu Cliente”, ao combate à lavagem de dinheiro, a nada disso.

Vou falar do lado de cartões. A gente tem algumas fraudes com essa questão da maquininha, que a pessoa falsifica o número lá, mas a indústria está discutindo agora, transferir essa responsabilidade, o ônus financeiro desse tipo de fraude, para credenciadora, porque ela cometeu...

Teoricamente, ela não foi perfeita e perfeição não existe com 150 milhões de contas, ela não foi perfeita no “Conheça Seu Cliente”, permitiu que um... Então, já tem consulta pública de uma grande bandeira.

Nós estamos levando, provavelmente esse mês, ao Banco Central, uma proposta de que toda regra seja alterada. Quando houver algum tipo de fraude em D0, antecipação, on-line, desses recursos, em que houver comprovada uma negligência da credenciadora que forneceu uma máquina, eventualmente, para uma pessoa inidônea, é que ela fique com o ônus financeiro daquela fraude. Aí é uma forma que a gente entende que, colocando o ônus no lugar correto, todos vão trabalhar para evitar esse tipo de problema.

**O SR. PEDRO IVO GRICOLI IOKOI** - Essa proposta é parecida com a que vai ser implementada no Reino Unido, de colocar o custo da fraude eletrônica, tanto de onde saiu para onde chegou o dinheiro, e dividir esse custo?

**O SR. RICARDO DE BARROS VIEIRA** - Não. Hoje as regras estão estabelecidas no mundo inteiro. Transações eletrônicas, por exemplo, o consumidor não tem risco algum, ou é comércio ou é banco. Nós estamos admitindo o seguinte. O nosso sistema foi criado em D+2 para frente. Mas tem jeito de você antecipar para D0 aquele valor. Então corre o mesmo risco do Pix.

Quer dizer, o dinheiro foi e você tem que correr atrás. Aí fica o mesmo problema que os bancos têm, de como é que você recupera. Você tem que correr atrás, o dinheiro já some, ele faz um Pix para outro lugar, você está sempre correndo sempre para atrás. O que nós estamos trabalhando é colocar mais força no “onboarding” desses clientes, no caso, estabelecimentos comerciais.

Ou seja, a proposta das bandeiras, que nós vamos levar ao Banco Central, é responsabilizar pecuniariamente, pela fraude, quem fizer essa antecipação em D0 que dê causa a uma fraude nesse movimento.

**O SR. PEDRO IVO GRICOLI IOKOI** - Só fazer uma pergunta para ver se eu entendi. Então vamos imaginar assim. Credenciadora “a” credenciou esse estabelecimento comercial. Mas essa antecipação pode ser feita por uma instituição financeira “b”. Quem paga? A credenciadora ou a instituição financeira?

**O SR. RICARDO DE BARROS VIEIRA** - A informação em D0 não existe em instituição financeira. Ela é D+1. Porque o arquivo é (Inaudível.) em D0.

É a própria credenciadora quem faz. Ela não está disponível. Depois ele registra todos os recebíveis na Central de Recebíveis, essa coisa toda. Mas, em D0, online só pode ser feita pela própria credenciadora. Ou seja, eu credencio a sua loja, e eu antecipo para a sua loja. Ninguém mais tem acesso a essa agenda naquele exato momento. Aí é mudança de regra, adaptação à regra, a um desenvolvimento ruim da sociedade com esse tipo de fraude.

**O SR. PEDRO IVO GRICOLI IOKOI** - Ricardo, última pergunta, mas voltada para a Abecs. Em relação aos cartões, nós escutamos, num passado recente, casos de vazamento de bases de cartões, e o uso permanente ou a comercialização, em Deep Web, de prestadoras de cartões. A Abecs faz esse monitoramento de Deep Web e repressão a esse tipo de conduta?

**O SR. RICARDO DE BARROS VIEIRA** - Não, nós não fazemos esse tipo de monitoramento. Mas, as regras de cartão, isso gera um transtorno imenso. O resultado financeiro é neutro para o consumidor. Gera transtorno você ter o seu cartão, você ter uma fraude, você ter que pedir um “chargeback”, falar que foi fraudado. Eu já fui, sei dos transtornos.

Mas a gente não faz esse tipo de acompanhamento. Porque, não obstante a gente lamentar o transtorno, a gente tem mecanismos para evitar isso. A tokenização é disponível mundialmente para todos os emissores. E nós garantimos que não há risco financeiro nenhum para o consumidor. Então ele não é responsável. Se ele comprovar, de boa-fé, que não foi ele, esquece. Vai ser responsabilidade de quem vendeu, ou do banco.

Tem mecanismos de tokenização para evitar isso. Mas, se ele não usa, o uso do número, aquela coisa toda, para a gente é indiferente. O risco financeiro não está com o consumidor, por regra mundial.

**O SR. WALTER TADEU PINTO DE FARIA** - Eu só queria complementar que a abertura de conta corrente é totalmente regulada pelo Banco Central. Existe uma norma. Essa norma foi revista há questão de dois ou três anos atrás, em que houve uma facilidade para que houvesse inclusão financeira. Todas as instituições, aí incluindo as instituições de pagamento e as fintechs, são reguladas pelo Banco Central e devem observar essas normas.

E o Banco Central fiscaliza. Final de 2022, todo o sistema financeiro passou por uma fiscalização muito grande, por parte do Banco Central, justamente na questão de prevenção a fraudes.

Então todo mundo é regulado, todo mundo tem que prestar contas. Tem questão de LGPD, tem questão de conhecer o cliente. O que infelizmente acontece é que uma boa parcela de pessoas empresta a sua conta. São contas legítimas, abertas de forma correta, com todo o processo de “onboarding” feito pelo banco.

Mas a pessoas acaba emprestando a conta, e é para onde é direcionado o dinheiro que é oriundo de golpe. E nós somos extremamente regulados e muito bem fiscalizados. Então todo mundo tem que cumprir aquelas regras ali.

**O SR. PRESIDENTE - ITAMAR BORGES - MDB** - Agradeço ao deputado Capitão Telhada e todos que por aqui passaram. Ao Dr. Pedro Iokoi, Dr. João Henrique

*Divisão de Registro de Pronunciamentos*

do CICC, ao Dr. Walter Tadeu da Febraban, e ao Ricardo de Barros, da Abecs, e a todos os amigos colaboradores desta Casa.

Nada mais havendo a tratar, declaro encerrada a reunião. Muito obrigado, e uma boa tarde a todos.

\* \* \*

- Encerra-se a reunião.

\* \* \*