ENCCLA 2025

Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro

AÇÃO 01/2025

PRODUTO II

MEDIDAS OPERACIONAIS E NORMATIVAS MITIGADORAS PARA FRAUDES BANCÁRIAS POR FALSAS CENTRAIS DE ATENDIMENTO.

PRODUTO II

MEDIDAS OPERACIONAIS E NORMATIVAS MITIGADORAS PARA FRAUDES BANCÁRIAS POR FALSAS CENTRAIS DE ATENDIMENTO.

EIXO I - SISTEMA FINANCEIRO E FRAUDES ELETRÔNICAS

Ação 01/2025: Mapear e definir mecanismos de prevenção e combate a fraudes bancárias eletrônicas por meio de falsas centrais de atendimento.

Coordenador: FEBRABAN, PF

Colaboradores: AGU, AJUFE, BB, BCB, CAIXA, CGU, CNMP, CVM, DRCI, MPGO, MPPB, MPPE, MPPR, MPRJ, MPS, MPSE, PCDF, PCMA, PCRJ, PCRS, PCSP, PREVIC, REDE-LAB, RFB, SAL/MJSP, SENASP/MJSP.

Convidado: ANATEL.

SUMÁRIO EXECUTIVO

Este documento consolida um conjunto abrangente de propostas de medidas operacionais e normativas destinadas ao combate efetivo dos golpes bancários perpetrados por falsas centrais de atendimento. As proposições estão organizadas em quatro eixos estratégicos que abordam aspectos tecnológicos, institucionais, regulatórios e penais. O desenvolvimento destas recomendações considerou as melhores práticas disponíveis e a necessidade urgente de uma resposta coordenada que acompanhe a constante evolução das técnicas criminosas.

As medidas aqui **sugeridas** representam o consenso alcançado entre as instituições participantes da Ação, refletindo tanto a experiência prática no enfrentamento desses crimes, quanto a análise técnica das vulnerabilidades identificadas no sistema atual.

Resumo das Propostas por Eixo:

a) **Tecnológico**: medidas focadas em autenticação, controle de dispositivos e detecção.

b) **Institucional**: iniciativas para fortalecimento de plataformas e alianças existentes.

c) **Regulatório**: alterações normativas para setores bancários , telecomunicações e plataformas digitais.

d) **Penal**: propostas de tipificação específica e alterações processuais.

1. EIXO TECNOLÓGICO

1.1 PROPOSTAS PARA AUTENTICAÇÃO DE CHAMADAS

1.1.1 Resumo das Medidas Propostas

AÇÃO 01: Medidas para expansão da origem verificada (Stir/Shaken) para telefonia móvel

AÇÃO 02: Obrigatoriedade do uso da "Notificação Falsa Central" pelas operadoras.

1.1.2 Detalhamento das Medidas Propostas

AÇÃO 01: MEDIDAS PARA EXPANSÃO DA ORIGEM VERIFICADA (STIR/SHAKEN) PARA TELEFONIA MÓVEL.

Fundamentação: Embora o foco atual da expansão da solução "Origem Verificada" esteja voltado principalmente para a rede fixa, é importante destacar que a Resolução nº 777/2025 da Anatel, em seu artigo 60, não restringe a aplicação da autenticação de chamadas apenas a esse tipo de rede.

O texto da resolução estabelece que a autenticação deve ser realizada pelas prestadoras de serviços de telecomunicações, sem especificar limitações quanto à tecnologia de acesso. Dessa forma, entende-se que a obrigatoriedade pode ser estendida também às redes móveis, reforçando o compromisso com a segurança e a confiabilidade das comunicações de voz em todo o ecossistema de telefonia.

Essa interpretação abre espaço para futuras implementações da solução em ambientes móveis, alinhando o Brasil às melhores práticas internacionais de combate a fraudes como o *spoofing*.

Responsabilidade: Anatel

AÇÃO 02: OBRIGATORIEDADE DO USO DA "NOTIFICAÇÃO FALSA CENTRAL" PELAS OPERADORAS.

Fundamentação: Como medida complementar essencial, propõe-se a implementação obrigatória, por todas as operadoras, da ferramenta "Notificação Falsa Central", desenvolvida pela ABR Telecom em parceria com a Anatel. O sistema permite que agentes notificadores registrem ocorrências suspeitas em uma plataforma centralizada, que será monitorada pela ABR Telecom e pela Anatel. A ideia é que, ao identificar um número utilizado indevidamente, seja possível suspender ou bloquear esse número, evitando que continue sendo usado para fraudes

Esta solução visa combater golpes envolvendo falsas centrais telefônicas, especialmente no contexto do Serviço Telefônico Fixo Comutado (STFC).

Responsabilidade: Anatel

1.2 CONTROLE DE DISPOSITIVOS

1.2.1 Resumo das Medidas Propostas:

AÇÃO 01: Autenticação biométrica obrigatória para habilitação de chips (aplicação de medidas concretas de Conheça seu Cliente (KYC) pelas Telecoms).

AÇÃO 02: Limitação de linhas telefônicas por CPF.

AÇÃO 03: Aplicação de medidas concretas de conheça seu cliente (KYC) pelas Telecoms.

AÇÃO 04: Sistema de score de risco comportamental.

1.2.2 Detalhamento das Medidas Propostas:

AÇÃO 01: AUTENTICAÇÃO BIOMÉTRICA OBRIGATÓRIA PARA HABILITAÇÃO DE CHIPS.

Fundamentação: O fortalecimento dos controles na habilitação de dispositivos móveis constitui elemento fundamental no combate à criação de estruturas fraudulentas. Propõe-se a implementação de autenticação biométrica obrigatória, com validação em tempo real junto às bases de dados oficiais.

Responsabilidade: Anatel

AÇÃO 02: LIMITAÇÃO DE LINHAS TELEFÔNICAS POR CPF.

Fundamentação: Proposta para limitação do número de linhas telefônicas por CPF, estabelecendo o máximo de três linhas pré-pagas e cinco linhas pós-pagas por pessoa física. Para linhas adicionais, seria exigida justificativa detalhada, acompanhada de monitoramento sistemático de padrões de uso anômalos. Exceções poderiam ser contempladas para pessoas jurídicas com atividade empresarial comprovada, mediante apresentação de documentação específica.

Responsabilidade: Anatel

AÇÃO 03: APLICAÇÃO DE MEDIDAS CONCRETAS DE CONHEÇA SEU CLIENTE (KYC) PELAS TELECOMS.

Fundamentação: O KYC, tradicionalmente associado ao setor financeiro, consiste em um conjunto de práticas voltadas à verificação da identidade e da legitimidade dos clientes. Quando aplicado pelas Telecoms, o KYC pode impedir que golpistas obtenham linhas telefônicas ou serviços de comunicação.

Responsabilidade: Anatel

AÇÃO 04: SISTEMA DE SCORE DE RISCO COMPORTAMENTAL.

Fundamentação: Sugere-se a implementação de sistema de score de risco baseado em padrões comportamentais, permitindo a identificação proativa de tentativas suspeitas e o bloqueio automático quando detectadas inconsistências de linhas telefônicas e envios de SMS.

Responsabilidade: Anatel

1.3 DETECÇÃO E BLOQUEIO

1.3.1 Resumo das Medidas Propostas:

AÇÃO 01: Correlação com bases de dados da Resolução Conjunta nº 6 e Tentáculos.

AÇÃO 02: Adesão das Telecoms à Plataforma Tentáculos, a fim de compartilhar dados de ocorrências de fraudes e golpes digitais.

AÇÃO 03: Controles específicos para serviços de SMS.

1.3.2 Detalhamento das Medidas Propostas:

AÇÃO 01: CORRELAÇÃO COM BASES DE DADOS DA RESOLUÇÃO CONJUNTA Nº 6 E TENTÁCULOS.

Fundamentação: A correlação com bases de dados de fraudes conhecidas, incluindo a Resolução Conjunta nº 6 do Banco Central e a Plataforma Tentáculos, representaria marco na prevenção proativa desses crimes.

Responsabilidade: Bacen e Polícia Federal

AÇÃO 02: ADESÃO DAS TELECOMS À PLATAFORMA TENTÁCULOS, A FIM DE COMPARTILHAR DADOS DE OCORRÊNCIAS DE FRAUDES E GOLPES DIGITAIS.

Fundamentação: Propõe-se a adesão das Telecoms à Plataforma Tentáculos, a fim de compartilhar dados de ocorrências de fraudes e golpes digitais, auxiliando nas investigações e repressões.

Responsabilidade: Anatel e Polícia Federal

AÇÃO 03: CONTROLES ESPECÍFICOS PARA SERVIÇOS DE SMS.

Fundamentação: O *Smishing*, combinação de SMS com *Phishing*, representa modalidade crescente nos golpes digitais. Propõe-se a implementação de medidas técnicas, regulatórias e jurídicas específicas:

Autenticação reforçada de remetentes:

- Exigência de cadastro prévio de remetentes comerciais;
- Aplicação de medidas de Conheça seu Cliente (KYC);
- Consulta às bases negativas de mercado;
- Bases mantidas pelas operadoras e reguladores;
- Integração com sistema Origem Verificada (Stir/Shaken).

Limitação de disparos automatizados:

- Imposição de tetos diários de envios para pessoas físicas;
- Controle de sistemas não cadastrados;
- Prevenção do uso de gateways ilegais de SMS.

Responsabilidade: Anatel

2. EIXO INSTITUCIONAL

2.1 FORTALECIMENTO DA PLATAFORMA TENTÁCULOS

2.1.1 Resumo das Medidas Propostas:

A Plataforma Tentáculos da Polícia Federal representa um dos principais instrumentos de combate às fraudes bancárias eletrônicas no país, tendo registrado mais de 570 operações

policiais realizadas. No entanto, sua efetividade poderia ser significativamente ampliada através da expansão operacional planejada.

AÇÃO 1: Expansão para 100% das polícias civis estaduais.

AÇÃO 2: Dashboard para análise conjunta com funcionalidade de vínculos.

AÇÃO 3: Módulo de análise de redes criminosas com *business intelligence*.

2.1.2 Detalhamento das Medidas Propostas:

AÇÃO 1: EXPANSÃO PARA 100% DAS POLÍCIAS CIVIS ESTADUAIS.

Fundamentação: Atualmente, apenas quatro Polícias Civis estaduais estão integradas à plataforma, situação que se recomenda rápida modificação. A meta sugerida prevê a integração de 100% das polícias civis estaduais (apenas 6 integradas até setembro de 2025). Esta ampliação permitirá cobertura nacional completa e acesso a um espectro mais amplo de informações relevantes para as investigações.

Responsabilidade: Polícia Federal

AÇÕES 2 E 3: DASHBOARD PARA ANÁLISE CONJUNTA COM FUNCIONALIDADE DE VÍNCULOS; MÓDULO DE ANÁLISE DE REDES CRIMINOSAS COM *BUSINESS INTELLIGENCE*.

Fundamentação: Os aprimoramentos tecnológicos propostos incluem o desenvolvimento de dashboard especializado para análise conjunta de fraudes com funcionalidade de análise de vínculos entre suspeitos, módulo avançado de análise de redes criminosas e integração completa com sistemas de *business intelligence.* O prazo sugerido para esses desenvolvimentos seria de 36 meses, considerando a complexidade técnica e a necessidade de coordenação entre múltiplas instituições.

Responsabilidade: Polícia Federal

2.2 CONSOLIDAÇÃO DA ALIANÇA NACIONAL DE COMBATE A FRAUDES

2.2.1 Resumo das Medidas Propostas:

A Aliança Nacional estabelecida entre o Ministério da Justiça e Segurança Pública e a FEBRABAN constitui iniciativa pioneira na articulação público-privada contra fraudes bancárias. Sua consolidação através do fortalecimento de três eixos fundamentais representaria prioridade estratégica.

AÇÃO 01: Padronização de protocolos antifraude com emprego unificado de tipologias.

AÇÃO 02: Ampliação de bases: telecomunicações, fintechs, corretoras de cambio e criptoativos.

AÇÃO 03: Protocolo de atendimento padronizado às vítimas.

2.2.2 Detalhamento das Medidas Propostas:

AÇÃO 01: PADRONIZAÇÃO DE PROTOCOLOS ANTIFRAUDE COM EMPREGO UNIFICADO DE TIPOLOGIAS.

Fundamentação: O eixo de boas práticas pode promover a padronização de protocolos antifraude em todas as instituições do sistema financeiro nacional, com ênfase no emprego unificado das tipologias identificadas nesta Ação. Esta padronização facilitaria o compartilhamento de informações e a coordenação de respostas entre diferentes instituições.

Responsabilidade: MJSP e Febraban

AÇÃO 02: AMPLIAÇÃO DE BASES: TELECOMUNICAÇÕES, *FINTECHS*, CORRETORAS DE CAMBIO E CRIPTOATIVOS.

Fundamentação: O eixo de compartilhamento de dados prevê significativa ampliação das bases atualmente disponíveis. A integração com dados de telecomunicações permitiria correlações mais precisas entre chamadas suspeitas e transações fraudulentas. O compartilhamento com fintechs, meios de pagamento e corretoras de criptoativos garantiria cobertura completa do ecossistema financeiro digital.

Responsabilidade: MJSP e Febraban

AÇÃO 03: PROTOCOLO DE ATENDIMENTO PADRONIZADO ÀS VÍTIMAS.

Fundamentação: O eixo de atendimento às vítimas pode ser fortalecido através da implementação de protocolo de atendimento padronizado que garanta tratamento uniforme e eficaz em todo o território nacional, complementado por campanhas educativas direcionadas aos grupos mais vulneráveis.

Responsabilidade: MJSP e Febraban

2.3 COOPERAÇÃO DE PLATAFORMAS DIGITAIS

2.3.1 Resumo das medidas propostas:

A crescente utilização de plataformas digitais para divulgação de anúncios fraudulentos e recrutamento de contas laranjas exige resposta regulatória específica. Propõe-se marco legal que estabeleça obrigação de verificação rigorosa de anunciantes através de procedimentos de conhecimento do cliente e prevenção à lavagem de dinheiro, remoção de conteúdo denunciado de forma ágil e eficiente.

AÇÃO 01: Remoção ágil de anúncios fraudulentos.

AÇÃO 02: Verificação rigorosa de anunciantes (Conheça seu Cliente obrigatório).

AÇÃO 03: Remoção imediata de conteúdos denunciados por autoridades.

AÇÃO 04: Remoção imediata de domínios denunciados por instituições financeiras.

AÇÃO 05: Detecção automática, bloqueio e remoção de grupos e perfis que promovem conteúdos de atividades criminosas, comercializam ferramentas ou dados para aplicação de golpes.

AÇÃO 06: Compartilhamento de dados sobre contas suspeitas com autoridades.

AÇÃO 07: Cooperação ativa com campanhas educativas oficiais.

2.3.2 Detalhamento das Medidas Propostas:

AÇÃO 01: REMOÇÃO ÁGIL DE ANÚNCIOS FRAUDULENTOS.

Fundamentação: A velocidade na remoção de anúncios fraudulentos é essencial para mitigar os impactos de golpes financeiros. *Big techs*, ao operarem plataformas com alto volume de publicidade, têm a responsabilidade de implementar sistemas automatizados e equipes dedicadas para identificar e retirar rapidamente conteúdos que promovam fraudes e golpes bancários. Essa ação reduz significativamente o tempo de exposição das vítimas a armadilhas digitais, protegendo consumidores e instituições financeiras.

Responsabilidade: Google e META

AÇÃO 02: VERIFICAÇÃO RIGOROSA DE ANUNCIANTES (CONHEÇA SEU CLIENTE OBRIGATÓRIO).

Fundamentação: A exigência de processos robustos de verificação de identidade para anunciantes, "Conheça Seu Cliente" (KYC), é uma medida preventiva fundamental. *Big techs* devem garantir que apenas empresas ou pessoas legítimas e verificadas possam anunciar em suas plataformas. Isso inclui validação documental, análise de histórico e monitoramento contínuo. Tal rigor impede que golpistas utilizem canais oficiais para disseminar fraudes e golpes bancários, aumentando a confiança no ecossistema digital.

Responsabilidade: Google e META

AÇÃO 03: REMOÇÃO IMEDIATA DE CONTEÚDOS DENUNCIADOS POR AUTORIDADES.

Fundamentação: A colaboração direta com autoridades policiais e regulatórias exige que as *big techs* tenham fluxos ágeis e eficazes para remoção de conteúdos denunciados. Ao atender prontamente às solicitações oficiais, essas empresas demonstram compromisso com a segurança pública e ajudam a interromper esquemas criminosos em tempo hábil, evitando que mais pessoas sejam prejudicadas.

Responsabilidade: Google e META

AÇÃO 04: REMOÇÃO IMEDIATA DE DOMÍNIOS DENUNCIADOS POR INSTITUIÇÕES FINANCEIRAS.

Fundamentação: Domínios utilizados para simular páginas de bancos ou realizar *phishing* devem ser removidos imediatamente quando denunciados por instituições financeiras. *Big techs*, especialmente aquelas que operam mecanismos de busca e redes sociais, devem agir com prioridade máxima nesses casos, bloqueando o acesso e a divulgação desses links maliciosos. Muitas das vezes as vítimas relatam em suas contestações o endereço eletrônico malicioso acessado. Essa ação é vital para proteger clientes bancários e preservar a integridade do sistema financeiro.

Responsabilidade: Google e META

AÇÃO 05: DETECÇÃO AUTOMÁTICA, BLOQUEIO E REMOÇÃO DE GRUPOS E PERFIS QUE PROMOVEM CONTEÚDOS DE ATIVIDADES CRIMINOSAS, COMERCIALIZAM FERRAMENTAS OU DADOS PARA APLICAÇÃO DE GOLPES.

Fundamentação: A tecnologia de inteligência artificial deve ser empregada pelas *big techs* para identificar, de forma proativa, grupos e perfis que promovem atividades criminosas, como venda de dados pessoais, ferramentas de invasão ou tutoriais de golpes. A remoção imediata e o bloqueio desses perfis são medidas que interrompem redes de fraude antes que causem danos maiores, além de dificultar a reincidência dos criminosos nas plataformas.

A propósito, essas empresas já possuem mecanismos sofisticados para identificar e remover conteúdos que violam direitos autorais (músicas) ou de temas sensíveis, como violência, suicídio e discurso de ódio.

Responsabilidade: Google e META

AÇÃO 06: COMPARTILHAMENTO DE DADOS SOBRE CONTAS SUSPEITAS COM AUTORIDADES.

Fundamentação: O compartilhamento responsável de dados com autoridades é uma peça-chave na investigação e repressão de crimes digitais. *Big techs* devem manter canais seguros e ágeis para fornecer informações sobre contas suspeitas, respeitando a legislação de proteção de dados. Essa cooperação fortalece a capacidade de resposta das forças de segurança e contribui para a responsabilização dos envolvidos em fraudes.

Responsabilidade: Google e META

AÇÃO 07: COOPERAÇÃO ATIVA COM CAMPANHAS EDUCATIVAS OFICIAIS.

Fundamentação: Além das ações repressivas, a prevenção é um pilar essencial no combate às fraudes. *Big techs* devem apoiar e amplificar campanhas educativas promovidas por órgãos oficiais, utilizando seu alcance para conscientizar usuários sobre práticas seguras, sinais de golpe e formas de proteção. Essa atuação conjunta contribui para a formação de uma sociedade digital mais informada e resiliente.

Responsabilidade: Google e META

3. EIXO REGULATÓRIO

3.1 REGULAÇÃO OFENSORES DE TELECOMUNICAÇÕES

3.1.1 Resumo das medidas propostas:

AÇÃO 01: Obrigatoriedade da tecnologia Origem Verificada (Stir/Shaken), com cronograma para conclusão.

AÇÃO 02: Plano de aceleração da adesão à Origem Verificada (Stir/Shaken).

AÇÃO 03: Sistema de compartilhamento de linhas suspeitas, similar à Resolução Conjunta nº 6 do Banco Central do Brasil.

AÇÃO 04: Responsabilização ampliada das operadoras por monitoramento ativo.

AÇÃO 05: Controles Rigorosos para Números 0800.

AÇÃO 06: Regulação de envio massivo de SMS.

AÇÃO 07: Expansão do uso do Bloqueio Cautelar.

AÇÃO 08: Recomendação às juntas comerciais para reforço nos mecanismos para aberturas de empresas.

3.1.2 Detalhamento das Medidas Propostas:

AÇÃO 01: OBRIGATORIEDADE DA TECNOLOGIA ORIGEM VERIFICADA (STIR/SHAKEN), COM CRONOGRAMA PARA CONCLUSÃO.

Fundamentação: A obrigatoriedade da tecnologia Origem Verificada (Stir/Shaken) deve ser estabelecida através de regulamento específico da Anatel com prazos definidos e consequências claras para o descumprimento. Atualmente, apenas empresas que originam mais de 500 mil chamadas por mês estão obrigadas a implementar a tecnologia.

Responsabilidade: Anatel

AÇÃO 02: PLANO DE ACELERAÇÃO DA ADESÃO À ORIGEM VERIFICADA (STIR/SHAKEN).

Fundamentação: Propor medidas para aceleração do cronograma de implantação e expansão da Origem Verificada (Stir/Shaken), que atualmente está estipulado em 3 anos.

Responsabilidade: Anatel

AÇÃO 03: SISTEMA NACIONAL DE COMPARTILHAMENTO DE LINHAS SUSPEITAS.

Fundamentação: Propõe-se a criação de sistema regulatório similar à Resolução Conjunta nº 6 do Banco Central, específico para o setor de telecomunicações. Este sistema obrigaria as operadoras a reportar e compartilhar informações sobre linhas telefônicas e respectivos titulares em casos de suspeita de utilização para cometimento de fraudes.

Por meio desse sistema, as operadoras reportariam imediatamente:

(i) Linhas utilizadas para disparos massivos suspeitos;
(ii) Números objeto de denúncias fundamentadas por vítimas;
(iii) Padrões de uso compatíveis com atividades fraudulentas;
(iv) Titulares com histórico de linhas bloqueadas por fraude.

A base de dados unificada permitiria:

(i) Consulta obrigatória antes da habilitação de novas linhas;
(ii) Bloqueio preventivo de números com histórico suspeito;
(iii) Correlação entre linhas e padrões criminosos conhecidos;
(iv) Compartilhamento com autoridades competentes e sistema financeiro.

As possíveis penalidades por descumprimento incluiriam:

(i) Multas proporcionais ao faturamento das operadoras;
(ii) Suspensão temporária de licenças para casos graves;
(iii) Auditoria compulsória de procedimentos internos;
(iv) Publicização de não conformidades.

Responsabilidade: Anatel

AÇÃO 04: RESPONSABILIZAÇÃO AMPLIADA DAS OPERADORAS POR MONITORAMENTO ATIVO.

Fundamentação: A responsabilização ampliada das operadoras abrangeria o monitoramento ativo de chamadas suspeitas através de sistemas automatizados, bloqueio imediato de números objeto de denúncia fundamentada e compartilhamento sistemático de dados com as autoridades competentes, respeitadas as garantias legais aplicáveis.

Responsabilidade: Anatel

AÇÃO 05: CONTROLES RIGOROSOS PARA NÚMEROS 0800.

Fundamentação: Uma das estratégias utilizadas pelos golpistas é a contratação de números 0800, tradicionalmente associados a serviços oficiais. Esses números são informados nos ataques de *Smishing*, sob alegação de ser a central telefônica para contestações de supostos débitos.

Apesar do Despacho Decisório nº 68/2023, que determinou suspensão de vendas de números 0800 até que ocorresse organização cadastral estruturada e segura, nota-se que os números continuam em uso pelos golpistas.

Propõe-se:

a) **Controles na Comercialização:**
   (i) Verificação de Idoneidade da Empresa:
   (ii) Cruzamento com dados da Receita Federal;
   (iii) Consulta às bases negativas de mercado (Resolução Conjunta nº 6);
   (iv) Verificação do tempo de constituição da empresa;
b) **Verificação dos Sócios/Representantes:**
   (i) Autenticidade e idoneidade dos representantes;
   (ii) Cruzamento com bases negativas;
   (iii) Histórico de envolvimento com fraudes;
c) **Critérios Restritivos:**
   (i) Tempo mínimo de constituição da empresa (12 meses);
   (ii) Capital social mínimo comprovado;
   (iii) Atividade empresarial compatível com solicitação;

Responsabilidade: Anatel

AÇÃO 06: REGULAÇÃO DE ENVIO MASSIVO DE SMS

Fundamentação: Recomendação para estudo e proposta de regulamentação para implementação de sistema de bloqueio de envio em massa de mensagens com indícios de uso para fraudes e golpes.

Responsabilidade: Anatel

AÇÃO 07: EXPANSÃO DO USO DO BLOQUEIO CAUTELAR.

Fundamentação: O aprimoramento do Bloqueio Cautelar PIX constitui medida de implementação imediata com impacto direto na redução de prejuízos. Ampliações propostas incluem extensão de prazo em casos de valores elevados, expansão para demais serviços transacionais e favorecidos pessoa jurídica.

Responsabilidade: Bacen

AÇÃO 08: RECOMENDAÇÃO ÀS JUNTAS COMERCIAIS PARA REFORÇO NOS MECANISMOS PARA ABERTURAS DE EMPRESAS

Fundamentação: Recomendação para Juntas Comerciais, a teor do art. 9º, parágrafo único, inciso XIII, da Lei nº 9.613 de 1998, para que adotem medidas efetivas para o cumprimento dos deveres estabelecidos nos subsequentes artigos 10 e 11, quando do arquivamento de atos societários, a fim de mitigar o risco de constituição de sociedades empresariais de fachada, utilizadas para práticas criminais diversas e para lavagem de dinheiro.

Responsabilidade: DREI

4. EIXO PENAL

4.1 APRIMORAMENTOS NO CÓDIGO PENAL

4.1.1 Resumo das medidas propostas:

AÇÃO 01: Tipificação do *Phishing* e respectivas variantes.

AÇÃO 02: Tipificação da comercialização e da posse de dados bancários de terceiros.

AÇÃO 03: Sanções administrativas para o uso, empréstimo, venda de contas.

AÇÃO 04: Alterações na Competência Territorial.

AÇÃO 05: Medidas Processuais.

4.1.2 Detalhamento das Medidas Propostas:

AÇÃO 01: TIPIFICAÇÃO DO *PHISHING* E RESPECTIVAS VARIANTES.

Fundamentação: Diariamente a população brasileira recebe inúmeras mensagens SMS, emails, ligações telefônicas, seja por meio de aplicativos de mensagerias ou outros sistemas análogos, que têm como objetivo a captura de informações bancárias ou outras fornecidas pela vítima a fim de se obter vantagem financeira ilícita. A ideia é tipificar a conduta do *phishing, vishing e smishing*. O atual arcabouço legal não prevê a tipificação do envio, distribuição e transmissão de mensagens eletrônicas com o intuito de induzir o cidadão a erro.

Dessa forma, sugere-se a seguinte inclusão no arcabouço legal:

Art. 171, § 2º – Nas mesmas penas incorre quem:

VII - Enviar, distribuir, transmitir mensagem eletrônica ou realizar ligação telefônica com o fim de capturar informações de terceiros ou de obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento.[1]

A tipificação específica para golpes bancários representa necessidade urgente diante da inadequação dos tipos penais existentes para o enfrentamento dessas condutas. A proposta de novo Artigo 171-C com o texto abaixo:

Proposta Artigo 171-C. *Induzir ou manter alguém em erro, mediante uso de sistema de telecomunicações ou informático, fazendo-se passar por funcionário de instituição, financeira ou não, para obter vantagem ilícita em prejuízo alheio:*

Pena - reclusão de 4 a 8 anos e multa.

§1º Se o crime é cometido:

I - contra pessoa maior de 60 anos: pena aumentada de 1/3

[1] Combate Digital, Prevenção e Repressão de Fraudes Bancárias eletrônicas, Siqueira, Erik 2024.

II - com uso de dados obtidos ilicitamente: pena aumentada de 1/2

III - por organização criminosa: pena aumentada de 2/3

§2º Se o valor da vantagem ilícita for superior a 20 salários mínimos, a pena é aumentada de 1/3 a 2/3."

O dispositivo proposto inclui causas de aumento de pena que refletem a maior gravidade de determinadas modalidades criminosas. Quando o crime é cometido contra pessoa maior de 60 anos, a pena será aumentada de um terço, reconhecendo a particular vulnerabilidade deste grupo. O uso de dados obtidos ilicitamente resultará em aumento de pena de metade, desestimulando a utilização de informações provenientes de vazamentos. A prática por organização criminosa acarretará aumento de dois terços, proporcionando resposta adequada ao caráter estruturado dessas atividades. Quando o valor da vantagem ilícita for superior a 20 salários mínimos, a pena será aumentada de um terço a dois terços, estabelecendo proporcionalidade com o prejuízo causado.

Responsabilidade: MJSP

AÇÃO 02: TIPIFICAÇÃO DA COMERCIALIZAÇÃO E DA POSSE DE DADOS BANCÁRIOS DE TERCEIROS.

Fundamentação: As inúmeras investigações realizadas na repressão às fraudes bancárias eletrônicas se deparam com situações de cumprimento de mandados de busca e apreensão nos quais os policiais federais/policiais civis encontram grande quantidade de cartões de débito/crédito de terceiros, dados de cartões armazenados em dispositivos computacionais (computadores, telefones etc.) e dados de contas bancárias e contas de pagamento de terceiros para o cometimento dos mais diversos tipos de fraudes.

Além disso, diversos grupos ou perfis em redes sociais, marketplaces criminosos, dentre outros, oferecem para a venda dados de cartões de crédito/débito de terceiros para a utilização em fraudes bancárias eletrônicas, bem como para realização de compras sem a autorização e o conhecimento do titular.

Nesse sentido, sugerimos a inclusão das seguintes condutas nos tipos penais relacionados ao furto e à receptação:

TÍTULO II – DOS CRIMES CONTRA O PATRIMÔNIO, CAPÍTULO I, DO FURTO

Art. 155, §3º-A – Na mesma pena incorre quem oferece, troca, disponibiliza, transmite, distribui, vende ou expõe à venda, publica ou divulga por qualquer meio, inclusive por meio de sistema de informática ou telemático, cartões de crédito ou débito de terceiros ou seus dados, bem como dados de contas bancárias e contas de pagamento de terceiros com respectivas credenciais de acesso, sem o consentimento do titular.[2]

[2] Fonte: livro Combate Digital, Prevenção e Repressão de Fraudes Bancárias eletrônicas, Siqueira, Erik 2024.

CAPÍTULO VII, DA RECEPTAÇÃO

Receptação de dados bancários

Art. 180-B. Adquirir, receber, possuir, ocultar ou armazenar, sem o consentimento do titular, por qualquer meio, cartões de crédito ou débito de terceiros ou os seus dados, bem como dados de contas bancárias e contas de pagamento de terceiros com respectivas credenciais de acesso, que, por sua natureza, deve presumir-se obtida por meio criminoso.

Responsabilidade: MJSP

AÇÃO 03: SANÇÕES ADMINISTRATIVAS PARA O USO, EMPRÉSTIMO, VENDA DE CONTAS.

Fundamentação: Identificar ou propor regulamentações ou projetos de lei a fim de aplicar penalidade ao uso indevido de contas de depósitos à vista, contas de depósitos de poupança e contas de pagamento pré-pagas em atividades ilícitas.

Responsabilidade: MJSP

AÇÃO 04: ALTERAÇÕES NA COMPETÊNCIA TERRITORIAL.

Fundamentação: Uma das principais dificuldades enfrentadas na investigação e persecução penal das fraudes digitais reside na definição da competência territorial. Atualmente, a aplicação das regras tradicionais de competência frequentemente resulta em distribuição dos casos para comarcas onde não se encontram nem os criminosos nem os principais elementos de prova, prejudicando significativamente a efetividade da resposta estatal.

A alteração legislativa proposta estabelece como foro competente para o processo e julgamento das fraudes digitais o local onde o criminoso ou grupo criminoso está efetivamente atuando, considerando-se como tal o local onde se encontra a infraestrutura tecnológica utilizada para a prática dos crimes, onde residem ou atuam os principais investigados, ou onde se concentram os elementos de prova relevantes para a elucidação dos fatos.

Esta modificação fundamenta-se na constatação prática de que a concentração das atividades investigativas no local de atuação dos criminosos facilita significativamente a obtenção de provas, permite melhor coordenação entre os órgãos envolvidos e possibilita respostas mais rápidas e efetivas. A medida também contribui para evitar a dispersão de inquéritos e processos relacionados a uma mesma organização criminosa em múltiplas jurisdições.

Responsabilidade: MJSP

AÇÃO 05: MEDIDAS PROCESSUAIS.

Fundamentação: O sequestro facilitado de bens representa instrumento fundamental para garantir o ressarcimento das vítimas. As alterações propostas permitem o sequestro imediato de valores equivalentes ao prejuízo identificado, independentemente da conclusão do processo criminal, e estabelecem bloqueio automático de bens dos investigados quando demonstrada a probabilidade de dissipação do patrimônio.

A aplicação da inversão do ônus da prova para bens sem origem comprovada, casos de enriquecimento ilícito e contas com movimentação atípica representará instrumento adicional para a recuperação de ativos, especialmente relevante diante da sofisticação das técnicas de ocultação de patrimônio utilizadas pelos grupos criminosos.

Responsabilidade: MJSP

5. CRONOGRAMA DE IMPLEMENTAÇÃO

O cronograma de implementação será apresentado pelas entidades que forem destinadas as medidas, conforme suas capacidades.

6. CONCLUSÕES

6.1 Síntese das Medidas

Este conjunto de medidas operacionais e normativas representa resposta abrangente e coordenada ao desafio das fraudes bancárias por falsas centrais de atendimento. A implementação escalonada e monitoramento contínuo garantirão adaptação às evoluções do cenário criminoso.

6.2 Fatores Críticos de Sucesso

Coordenação Interinstitucional: Alinhamento permanente entre todos os atores.

Investimento Adequado: Recursos suficientes para implementação completa.

Adaptabilidade: Capacidade de evolução conforme novas ameaças.

Monitoramento Rigoroso: Avaliação constante de efetividade.

6.3 Impacto Esperado

A implementação integral destas medidas deve resultar em:

- Redução significativa nas fraudes via central em 24 meses.
- Fortalecimento da confiança no sistema financeiro.
- Posicionamento do Brasil como referência internacional no combate a fraudes digitais.

ENCCLA 2025

Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro

AÇÃO 01/2025

PRODUTO II

MEDIDAS OPERACIONAIS E NORMATIVAS MITIGADORAS PARA FRAUDES BANCÁRIAS POR FALSAS CENTRAIS DE ATENDIMENTO.