26. Política de compartilhamento de dados e informações sobre indícios de fraudes

1. Objetivo

Esta política dispõe sobre as medidas necessárias à execução do compartilhamento de dados e das informações sobre indícios de fraudes.

2. Aplicabilidade

Esta política se aplica a todos os colaboradores da Cogem independentemente do nível hierárquico.

3. Sistema de Compartilhamento de Dados

O sistema de compartilhamento de dados utilizado pela Cogem tem como principal objetivo a disponibilização de componentes específicos de prevenção a fraude que, quando combinados, geram maior confiabilidade para o sistema e decisões para o processo de prevenção a fraude.

4. Avaliação de Riscos de ocorrências de fraudes

A Cogem, face a seu porte e complexidade de operações, possui risco reduzido de ocorrências de fraudes, principalmente pelo fato de não trabalhar com conta corrente (depósitos a vista). Ao mesmo tempo, por ser uma instituição financeira, deverá atender aos normativos emanados pelo Banco Central do Brasil.

Essa política foi aprovada pelo Conselho de Administração com o intuito de reforçar os mecanismos de acompanhamento e de controle na prevenção de fraudes.

São admitidos como associados da Cooperativa somente os funcionários em regime CLT com contrato de trabalho por tempo indeterminado da própria Cooperativa e das empresas conveniadas, não podendo se associar estagiários, terceiros e prestadores de serviço.

Considera-se que as situações e características da Cogem denotam um menor grau de exposição ao risco de situações de suspeita de fraudes, tais como:

- A área de admissão abrange somente os funcionários efetivos das empresas conveniadas à Cooperativa;
- Não há trânsito de numerário em espécie, haja vista não operar com caixa nem oferecer o serviço de conta corrente aos associados;
- Todas as movimentações de recursos são realizadas via conta corrente de titularidade da Cooperativa; e
- Os aportes de capital seguem rigorosamente a política de capital.

Desta forma, a probabilidade de ocorrências é de risco baixo, contudo, em cumprimento a resolução vigente do Banco Central do Central, a Cogem adota controles e mecanismos de prevenção, mitigação e investigação de ocorrências suspeitas de fraudes.

5. Seleção e Critérios de Consultas

- A Cogem fará consulta no sistema de registro de ocorrências de fraudes para solicitações de crédito no valor igual ou superior a R$ 50.000,00 (cinquenta mil reais).
- A área de "*Compliance"* poderá consultar no sistema de registro de ocorrências de fraudes os associados que não se enquadram no critério de solicitação de crédito, mas que possuam situações consideradas como atípicas, desde que tenha subsídios para realizar a consulta.

6. Responsabilidades e Procedimentos de Consultas

6.1 Atendimento

- Responsável por comunicar à Mesa de Crédito as solicitações de crédito no valor igual ou superior a R$ 50.000,00 (cinquenta mil reais);
- Responsável por comunicar o resultado da análise de crédito ao associado, quando reprovado ou aprovado com ressalvas.

A operação de crédito só poderá ser aprovada após o parecer da Mesa de Crédito e quando aplicável, o parecer do "*Compliance",* da Gerência, da Diretoria e do Conselho de Administração.

6.2 Mesa de Crédito

- Responsável por consultar no sistema de registro de ocorrências de fraudes em até 3 (três) dias úteis da data da comunicação do atendimento e quando a solicitação for proveniente dos canais digitais;
- Registrar e fundamentar o parecer no formulário de análise de crédito e enviar a Gerência quando não ocorrer registro de fraude;
- Submeter o formulário de análise de crédito a área de *"Compliance"* quando a consulta de fraude possuir registro de ocorrência;
- Aguardar o parecer do "*Compliance*" e da Gerência para seguir com o processo de análise de crédito.
- Responsável por comunicar o resultado da análise de crédito ao associado, quando reprovado ou aprovado com ressalvas das solicitações provenientes dos canais digitais e compartilhar com o posto de atendimento.

6.3 *"COMPLIANCE"*

6.3.1 Consultas nas solicitações de crédito no valor igual ou superior a R$ 50.000,00 (cinquenta mil reais)

- Responsável por receber comunicação da Mesa de Crédito o formulário de análise de crédito quando ocorrer registro de ocorrência de fraude;
- Registrar e fundamentar o parecer no Formulário anexo nesta política e enviar para Gerência; e
- Armazenar as evidências na pasta de *"COMPLIANCE".*

6.3.2 Consultas Atípicas

- O *"Compliance"* poderá consultar no sistema de ocorrências de fraudes demais situações que não se enquadram na solicitação de operação de crédito, desde que tenha subsídios da situação atípica para tal consulta;
- Registrar e fundamentar o parecer no Formulário de Consulta de registro de ocorrências de fraudes; e
- Para a consulta que não apontar registro de ocorrência de fraude, armazenar as evidências na pasta do *"Compliance"* e quando houver ocorrência, submeter a análise da Gerência e compartilhar a ocorrência com a Mesa de Crédito.

6.4 Gerência

- A Gerência da Cogem é responsável por receber a comunicação da Mesa de Crédito e do Compliance os formulários dos associados com registro de ocorrência de fraude;
- A Gerência deverá emitir parecer sobre a permanência ou não do associado no quadro social, o qual será submetido à análise da Diretoria e ao Conselho de Administração, quando ocorrer registro de fraude;
- O parecer da Gerência deverá ser acompanhado das evidências, dos documentos e do parecer do *"Compliance"*; e
- Receber o parecer da Diretoria e do Conselho de Administração, e tomar as devidas providências, conforme parecer final.

6.5 Diretoria e Conselho de Administração

- Receber o Formulário de Consulta de registro de ocorrências de fraudes, acompanhado das evidências, dos documentos e parecer do *"Compliance"* e Gerência; e
- Emitir o parecer final e comunicar a Gerência da decisão de manter ou não o associado, através do Formulário Anexo nesta política.

6.6 Procedimentos dos Resultados da Análise

- Após consulta realizada, a Mesa de Crédito ou *"Compliance"* deverá informar se houve registro de ocorrência de fraude e emitir o parecer;
- Para os associados que não possuem registro de ocorrência de fraude, e havendo solicitação de crédito, a aprovação será fundamentada e evidenciada pela Mesa de Crédito;
- Para os associados que foram apontados no sistema de registro de ocorrência de fraude, e havendo solicitação de crédito, terá seu crédito recusado e o parecer final deverá ser emitido pela Diretoria e pelo Conselho de Administração; e
- Para situação atípica, e havendo registro de ocorrência de fraude, o parecer final deverá ser emitido pela Diretoria e pelo Conselho de Administração.

7. Declaração de Conformidade

- O "*Compliance*" é responsável por registrar a declaração de conformidade, que deverá ser realizada até o dia 15 (quinze) de cada mês.
- A declaração de conformidade deverá ser registrada e conter:
    - registro dos dados e das informações sobre indícios de ocorrências ou de tentativas de fraudes do mês anterior; ou
    - inexistência de indício de ocorrência ou de tentativa de fraude no mês anterior.
- A declaração de conformidade deverá ser documentada e contemplar as alterações e as exclusões dos dados e das informações registradas sobre indícios de ocorrências ou de tentativas de fraudes.
- A declaração de conformidade deverá ser reportada à Diretoria Executiva e ficar à disposição das auditorias e do Banco Central do Brasil (BCB).

8. Inclusão de ocorrência de fraude

- Todas as áreas da Cogem são responsáveis em comunicar ao "*Compliance*" qualquer situação que possa configurar fraude.
- A comunicação da situação suspeita não pode ser informada ao associado e aos demais colaboradores da Cogem, a informação deverá ser mantida em sigilo entre os envolvidos na comunicação.
- A área de "*Compliance"* é responsável por incluir ocorrências de fraudes, seguindo os procedimentos descritos nesta política.
- Os procedimentos operacionais para o compartilhamento de dados e de informações devem contemplar o registro de dados e de informações sobre indícios de ocorrências ou de tentativas de fraudes em, no máximo, 24 (vinte e quatro) horas contadas do momento da identificação.
- O prazo máximo mencionado aplica-se também à alteração e à exclusão dos dados e das informações registrados sobre indícios de ocorrências ou de tentativas de fraudes, contado do

momento da identificação, pela instituição, da necessidade de alteração ou de exclusão desses dados e dessas informações.

8.1 Procedimentos de registro de ocorrência de fraude

Os dados e as informações a serem registrados devem conter, no mínimo, o seguinte detalhamento:

- identificação de quem, segundo os indícios disponíveis, teria executado ou tentado executar a fraude, quando aplicável;
- nome completo e número no Cadastro de Pessoas Físicas (CPF) ou razão social, número no Cadastro Nacional da Pessoa Jurídica (CNPJ), nome fantasia e, quando disponível, CPF dos representantes legais;
- descrição dos indícios da ocorrência ou da tentativa de fraude;
- data de execução do indício da ocorrência ou da tentativa de fraude;
- horário de execução do indício da ocorrência ou da tentativa de fraude, quando disponível;
- local de execução do indício da ocorrência ou da tentativa de fraude, quando disponível;
- atividade relacionada ao indício da ocorrência ou da tentativa;
- valor da transação de pagamento, caso refira-se à prestação de serviço de pagamento;
- valor contratado, caso a atividade refira-se à contratação de operação de crédito;
- descrição da causa ou procedimento que ensejou o indício da ocorrência ou da tentativa de fraude relacionado à atividade, quando disponível;
- forma de interação ou canal utilizado para a execução do indício da ocorrência ou da tentativa de fraude, quando disponível;
- identificação do dispositivo eletrônico utilizado na execução do indício da ocorrência ou da tentativa de fraude, quando disponível;
- indicação se houve ou não a atuação do associado no indício da ocorrência ou da tentativa de fraude;
- especificação quanto a tratar-se de indício de ocorrência ou de indício de tentativa de fraude;
- identificação da instituição responsável pelo registro dos dados e das informações:
    - nome da instituição;
    - CNPJ da instituição;
- identificação dos dados da conta destinatária e de seu titular, caso a atividade refira-se à prestação de serviço de pagamento contemplando a transferência ou pagamento de recursos:
    - identificador da instituição;
    - código da agência, se houver;
    - número da conta;
    - tipo da conta; e
    - identificação do(s) titular(es) da conta destinatária dos recursos: nome completo e CPF; ou razão social, CNPJ, nome fantasia e, quando disponível, CPF dos representantes legais.

8.2 Classificação dos motivos de fraude

- Fraudador: aquele que é beneficiário em um golpe/fraude.
- Vítima: pessoa que é ludibriada pelo fraudador. Indivíduo que tem seus dados usados de forma ilícita e sem autorização.

8.3 Tabela de motivos de fraude

Abaixo descrevemos os motivos e a descrição de alertas de fraudes disponíveis no sistema de registro de ocorrências de fraudes.

8.4 Motivos de alertas de fraude – Dados do Fraudador

Motivo	Descrição
Auto fraude	O cliente agiu de forma fraudulenta, alegando que uma ação não foi quando foi ou o cliente genuíno agiu fraudulentamente.
Conta de Passagem/Conta Laranja	Uma conta que é suspeita ou foi encerrada por causa de confirmada atividade de crime financeiro, como lavagem de dinheiro ou recebimento de receitas de crime.
Fraude Transacional	Favorecido de créditos espúrios (fraudes transacionais) em quaisquer meios de pagamentos - Crédito Espúrio.
Titular de mais de um CPF	Mesmo nome ou pessoa identificada com mais de um CPF na base.
Favorecido de golpe com cheques	Favorecido utilizado para depósitos a partir de cheques roubados ou clientes enganados.
Telefone utilizado de forma fraudulenta	Telefone (celular ou fixo) utilizado para ações fraudulentas como confirmação de transações ou cargas de celular decorrentes de fraude.
E-mail utilizado de forma fraudulenta	E-mail utilizado em fraudes
Fraude de bônus	O fraudador manipulou os incentivos de bônus dos clientes para receber bônus não autorizados.
Fraude/Golpe de veículos com participação da revenda	Revenda de veículos com a participação comprovada.
Fraude na concessão de crédito (ie: consignado)	O fraudador, em companhia da vítima ou de terceiros, obtêm crédito consignado, antecipação de FGTS, antecipação de Imposto de Renda ou quaisquer outros benefícios por meio de cometimento de fraudes ou golpes.

Motivo	Descrição
Fraude em consórcio	Registros detectados com apontamentos de fraudes em consórcio.
Fraude em sinistro	Fraude de sinistros é qualquer ato cometido para fraudar um processo de seguro.
Fraude em pagamentos	Fraudes com utilização de boletos adulterados ou fraudes com utilização de boleto como meio de pagamento.
Fraude de comprador	O fraudador contata um vendedor e se oferece para pagar por meio de um agente falso ou pagamento indevido para facilitar um reembolso.
Fraude de vendedor	O fraudador publica um anúncio falso na mídia social ou no mercado online para facilitar o pagamento de um item inexistente.
Fraude interna	Um membro interno da equipe ou funcionário cometeu a fraude em um cliente
Fraude de 2ª parte ou fraude amigável	Um conhecido associado do cliente cometeu a fraude como, por exemplo, um pagamento fraude.
Fraude de duas partes	Onde um indivíduo conscientemente empresta sua identidade.
Corretor fantasma	O fraudador vende uma apólice de seguro inválida ou inexistente.
Fraude de benefícios	O cliente agiu de forma fraudulenta ao se inscrever para benefícios do setor público.

Motivo	Descrição
Fraude em reembolso - mercadorias e serviços	O cliente agiu de forma fraudulenta ao não enviar o item original em uma devolução e recebe um reembolso total.
Fraude em reembolso - plano de saúde	O cliente agiu de forma fraudulenta ao solicitar reembolso de despesas médicas ou compartilhou seu acesso com terceiros para solicitação de reembolsos.
Regulatório	A lei proíbe certas atividades como, por exemplo, jogos de azar e outras tipificadas na legislação.

8.5 Motivos de alertas de fraude – Dados da Vítima

Motivo	Descrição
Sequestro ou extorsão	Vítima de sequestro ou extorsão.
SIM SWAP	O fraudador se fez passar pela vítima para redirecionar chamadas e mensagens do cartão SIM da vítima para o cartão SIM do fraudador.
Identidade sintética	O fraudador combinou informações falsas para criar uma nova identidade e usá-las para solicitar uma conta ou crédito de forma fraudulenta.
Manipulação cadastral	O fraudador roubou a identidade genuína da vítima e personificou o cliente para se candidatar de forma fraudulenta a uma conta ou facilidades de crédito.
Falsidade ideológica - Onboarding - sucesso	O fraudador roubou a identidade genuína da vítima e personificou o cliente para se candidatar de forma fraudulenta a uma conta ou facilidades de crédito.
Falsidade ideológica - Onboarding - tentativa	O fraudador roubou a identidade genuína da vítima e personificou o cliente para se candidatar de forma fraudulenta a uma conta ou facilidades de crédito.
Fraude de assinatura	O fraudador roubou a identidade genuína da vítima e se fez passar pelo cliente para contratar de forma fraudulenta serviços de dados, telefonia, imóveis, etc.
Roubo de credencial	O fraudador obteve os dados pessoais do cliente e, com acesso não autorizado, cria e autoriza o fraudulento na forma de pagamento.
Fraude na portabilidade de salário	Situação em que o criminoso, passando-se pelo cliente, com documentos ou informações falsas, abre conta de transação e solicita a portabilidade do salário do cliente.

Motivo	Descrição
Fraude na restituição do imposto de renda	Situação em que o criminoso, passando-se pelo cliente, com documentos ou informações falsas, abre conta de transação e solicita a transferência da restituição do IR que estão liberadas, mas pendentes de pagamento (por erro, encerramento de conta, etc.).
Golpe do falso funcionário / falsa central de atendimento	Caso em que o golpista entra em contato com o cliente se passando por um falso funcionário da instituição com a qual o cliente tem um relacionamento ativo. O criminoso informa que há irregularidades na conta ou que os dados cadastrados estão incorretos. A partir daí, solicita os dados pessoais e financeiros do cliente. Com os dados em mãos, realiza transações fraudulentas em nome do cliente.
Golpe por phishing (pescaria digital) / link falso	Caso de utilização de engenharia social visando obtenção de dados do cliente, principalmente, por meio de mensagens, e-mails falsos ou páginas falsas na internet, que induzem o cliente a clicar em links suspeitos, disponibilizando seus dados pessoais e financeiros.
Golpe do falso motoboy	Caso em que o golpista faz uma ligação para o cliente, passando-se por funcionário da instituição, e informa que o cartão foi clonado e precisa ser bloqueado. Para isso, o golpista pede que a senha seja digitada no telefone e fala que, por segurança, um motoboy irá buscar o cartão, que o próprio cliente é orientado a cortar ao meio. Se o cliente não destruir o chip, o golpista conseguirá realizar transações.

Motivo	Descrição
Golpe do extravio do cartão	Caso em que ocorre a interceptação do novo cartão do cliente no trâmite de entrega. De posse do cartão, o golpista entra em contato com o cliente se passando por um funcionário da instituição financeira, informando que houve problema na entrega do cartão. Para a resolução deste suposto problema, solicita ao cliente seus dados financeiros e, até mesmo a senha do cartão, conseguindo assim realizar transações em nome do cliente.
Golpe do delivery	Caso em que o cliente é enganado pelo entregador de aplicativo, que apresenta uma maquininha com o visor danificado ou que impossibilite a visualização do preço cobrado na tela, cobrando um valor acima do valor da compra efetuada.
Golpe da troca de cartão	Caso em que o golpista troca o cartão após realizar uma transação verdadeira na maquininha. Sem perceber, o cliente vai embora com o cartão trocado. De posse do cartão e da senha (por meio da visualização de digitação), realiza transações fraudulentas.
Engenharia Social e outros (**mídias sociais**)	O cliente foi manipulado pelo fraudador e o cliente, involuntariamente, cria e autoriza a fraude de seu próprio dispositivo. Para golpes de engenharia social não listados nos motivos 36-41.

Motivo	Descrição
Software malicioso / dispositivo não pertencente ao cliente	O fraudador com o uso de software maliciosos obtém acesso não autorizado à conta e cria e autoriza o pagamento fraudulento. Nesse caso, o dispositivo pode ser do fraudador ou de outrem. Nessa situação, não temos a presença do cliente.
Fraude com utilização do dispositivo do cliente (roubo ou furto)	Caso em que o fraudador realiza a transação financeira por meio do dispositivo do cliente (celular, tablet, notebook, por exemplo), mas sem a presença do cliente. Nesse caso, o dispositivo foi furtado ou roubado.
Fraude com utilização do dispositivo do cliente (acesso remoto)	O cliente (vítima) foi manipulado pelo fraudador usando um desktop remoto e o cliente, involuntariamente, cria e autoriza a transação fraudulenta de seu próprio dispositivo.
Autoexclusão	Fraude impetrada pelo cliente em razão de fragilidades sistêmicas da IF.
Outros	Outros tipos de golpes não especificados.

9. Documentos

As seguintes documentações devem ser mantidas a disposição do Banco Central do Brasil (BCB) por 5 (cinco) anos:

- a documentação sobre a declaração de conformidade;
- a documentação dos leiautes padronizados dos arquivos, regras, procedimentos, tecnologias e demais recursos necessários para a troca de informações entre sistemas eletrônicos;
- o contrato de prestação de serviços de compartilhamentos de dados e informações;
- os resultados dos testes de intrusão com execução, no mínimo anual;
- a documentação a respeito dos acordos de níveis de serviço que deve conter:
    - disponibilidade anual do sistema eletrônico em produção de, no mínimo, 99,8% (noventa e nove inteiros e oito décimos por cento);
    - tempo de recuperação objetivado para o sistema eletrônico de, no máximo, 2 (duas) horas;
    - tempo de resposta às consultas realizadas pelas instituições e aos dados e às informações registradas no sistema eletrônico; e
    - tempo de resposta às consultas realizadas por outros sistemas eletrônicos aos dados e às informações registradas no sistema eletrônico para fins de atendimento à interoperabilidade, quando aplicável.
- A documentação a respeito dos parâmetros sobre acordos de níveis de serviço deve conter:
    - os dados e as informações que subsidiem a apuração da disponibilidade do sistema eletrônico e do tempo de recuperação;

- os dados, as informações e os parâmetros que promovam a eficiência na definição dos tempos de resposta às consultas, quando aplicável; e
- os dados, os registros e as informações relativas à aplicação dos mecanismos de acompanhamento e de controle.

Formulário de Consulta de registro de ocorrência de fraude

COGEM Valorizando seu sonho	Formulário de Consulta de registro de ocorrência de fraude		
Dados do Associado			
Nome do Associado		**CPF**	
Valor da Operação		**Produto/Linha de Crédito:**	
Data da Consulta			
Resultado da Consulta			
Parecer *Compliance*			
Resultado da Consulta			
Parecer Gerência			
Parecer Gerência		**Submeter a análise da Diretoria e do Conselho de Administração**	
Parecer Final da Diretoria			
Parecer Final			
Parecer Final do Conselho de Administração			
Parecer Final			

Registro de Alteração			
Data	**Versão**	**Páginas alteradas**	**Informações Relevantes**
fev/2024	1ª	-	Publicação
out/24	2ª	2; 3; e 4	Alteração do responsável de compliance para mesa de crédito para as consultas de ocorrência de fraude.