POLÍTICA PLD E TERRORISMO

Sumário

1. INTRODUÇÃO E OBJETIVOS

Esta Política é uma extensão do Código de Conduta da FACILITAPAY. Seu objetivo é estabelecer a conduta esperada dos funcionários na prevenção e no combate à lavagem de dinheiro e ao financiamento do terrorismo. A FACILITAPAY tem tolerância zero para lavagem de dinheiro e está comprometida em mitigar os riscos de lavagem de dinheiro. A FACILITAPAY tomará as medidas preventivas necessárias e investigará prontamente qualquer suspeita de lavagem de dinheiro.

A Política de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo é periodicamente revisada a fim de alcançar as melhores práticas para o FACILITAPAY. A revisão é realizada através de:

- Revisão periódica de reportagens de mídia relevantes para o setor ou jurisdição em que a FACILITAPAY atua;
- Revisão periódica de alertas e relatórios de aplicação da lei;
- Preste atenção às mudanças nos alertas terroristas e nos regimes de sanções assim que ocorrerem;
- Revisão de publicações temáticas e similares publicadas pelas autoridades competentes;
- Revisão de diretrizes nacionais e internacionais para definição de normas, políticas e procedimentos. Caso não haja orientação, o Comitê de Compliance a procurará por meio de assessoria jurídica (interna ou externa) e seguirá os pareceres formais oferecidos.

1.1 VISÃO GERAL DO FACILITAPAY

A FACILITA PAGAMENTOS S/A (FACILITAPAY) é uma empresa de facilitação de serviços financeiros digitais estabelecida no Brasil. A empresa**,** juntamente com todas as suas subsidiárias, oferece produtos e serviços de facilitação de pagamentos internacionais, como instituição não financeira, no Brasil.

Como o Brasil é membro pleno da ONU, a FACILITAPAY adere às normas de sanções impostas pelas Nações Unidas. Estes regulamentos consistem em sanções aplicadas em Compliance com as Resoluções do Conselho de Segurança das Nações Unidas (CSNU). Além disso, a FACILITAPAY deve seguir as normas impostas pelas leis nacionais de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (Leis nº 9.613/98; nº 12.683/12; nº 13.260/16 e nº 13.810/19). A FACILITAPAY não fará negócios com entidades incluídas nas listas de sanções.

Além disso, no Brasil, a FACILITAPAY é uma pessoa sujeita ao mecanismo de controle previsto no artigo 9º da Lei 9.613/98, que dispõe sobre os crimes de lavagem de dinheiro. Portanto, é obrigação da FACILITAPAY comunicar ao Conselho de Controle de Atividades Financeiras - COAF as operações financeiras a que se refere o Capítulo VII da referida Lei.

2. ESCOPO DE APLICAÇÕES E USUÁRIOS

Este Código aplica-se a todos os funcionários da FACILITAPAY, independentemente do país onde estão a alugar. Os colaboradores são:

- Sócios e acionistas
- Diretores
- Colaboradores
- Temporal
- Interno
- Menores aprendizes
- Clientes e/ou pessoas físicas/jurídicas que estejam comercialmente relacionadas à FACILITAPAY

3. APLICABILIDADE E REGULAMENTAÇÃO

A FACILITAPAY opera em várias jurisdições em todo o mundo. No entanto, a sujeição da atividade empresarial da FACILITAPAY à regulamentação depende das leis e regulamentos de cada jurisdição sobre as instituições que facilitam o pagamento transfronteiriço. Como tal, quando aplicável, a FACILITAPAY operará de acordo com os requisitos regulamentares de uma jurisdição.

4. APLICABILIDADE E REGULAMENTAÇÃO

Lavagem de dinheiro

Lavagem de dinheiro é o termo comum para o processo pelo qual um indivíduo busca ocultar os resultados de um crime trocando a propriedade dos crimes pelo chamado dinheiro "limpo". As seguintes atividades podem estar associadas, mas não se limitando a lavagem de dinheiro:

- Adquirir, utilizar ou possuir bens oriundos de crimes;
- Ocultar, ocultar, transferir ou manipular bens oriundos de crimes como roubo, fraude e sonegação fiscal;
- Estar conscientemente envolvido de qualquer forma com bens derivados de crimes;
- Investir ativos oriundos do crime, seja em produtos financeiros, seja por meio da aquisição de bens ou ativos;
- Transferência de bens criminosos;
- Financiamento de atividades terroristas.

As três fases da lavagem de dinheiro geralmente são:

- Colocação: esta é a primeira fase da lavagem de dinheiro. Implica a inserção, na economia formal, do bem oriundo da atividade ilícita. Exemplo: colocar dinheiro no sistema financeiro convencional.
- Ocultação: Esta segunda fase envolve separar os ativos ilícitos de sua origem, criando camadas complexas de transações financeiras projetadas para disfarçar o rastro de dinheiro auditável e permitir o anonimato.
- Integração: a fase final é dar aparente legitimidade aos bens oriundos de crimes. Se a fase de ocultação foi bem-sucedida, os esquemas de integração inserem dinheiro lavado de volta na economia para que esses ativos voltem a entrar no sistema financeiro que parecem ser fundos regulares.

Com base em várias leis, regulamentos e diretrizes regulatórias do Grupo de Ação Financeira Internacional (GAFI) e outras melhores práticas internacionais aplicáveis, a FACILITAPAY garantirá que as obrigações legais resultantes das regulamentações internacionais de combate à lavagem de dinheiro sejam cumpridas por todos os funcionários e terceiros. Em relação a estes, a FACILITAPAY deve garantir que nosso modelo de negócio seja compreendido e respeitado por qualquer novo comerciante ou cliente, evitando irregularidades como sonegação fiscal e outros crimes.

Quando as regulamentações locais forem mais rigorosas do que as estabelecidas nesta Política, prevalecerão as normas mais rígidas. Caso os padrões mínimos estabelecidos nesta Política não possam ser aplicados em nenhum país, porque sua aplicação seria contrária à legislação local ou porque não poderiam ser impostos por outras razões legais, a FACILITAPAY garantirá que não iniciará, continuará ou realizará relações comerciais nesse país. Se já existir uma relação comercial nesse país, a FACILITAPAY garantirá que ela seja terminada, independentemente de outras obrigações contratuais ou legais.

Financiamento do terrorismo

O financiamento do terrorismo é qualquer envolvimento com fundos ou bens que são certos ou susceptíveis de serem utilizados para fins terroristas, mesmo que liberados na fonte. Para os fins desta Política, a lavagem de dinheiro também inclui qualquer atividade relacionada ao financiamento do terrorismo.

5. DIRETRIZES

5.1 ESTRUTURA ORGANIZACIONAL

A FACILITAPY estabelece e mantém um programa eficaz de Compliance AML. Em geral, os programas de luta contra o branqueamento de capitais devem ser proporcionais aos riscos decorrentes da localização, dimensão, natureza e volume dos serviços financeiros prestados. Um programa eficaz é aquele criado para evitar que a FACILITAPAY seja usada para facilitar a lavagem de dinheiro e o financiamento do terrorismo. Além disso, o Programa de Inteligência Financeira da FACILITAPAY incorpora o Programa de Inteligência Financeira da FACILITAPAY.

O programa de prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo é formulado e gerido pelo Departamento Jurídico e de Compliance:

O Departamento de Compliance/Jurídico reporta-se ao Chief Legal Officer (CLO). Os Oficiais Locais de Denúncia de Lavagem de Dinheiro (MLROs) se reportam à Diretoria Jurídica. A principal responsabilidade da MLRO consiste em assegurar que, se for caso disso, as informações ou outros meios que conduzam ao conhecimento, à suspeita ou às razões de conhecimento ou suspeita de branqueamento de capitais sejam devidamente divulgados e comunicados às autoridades competentes.

5.1.1. Programa de Informação Financeira

A Unidade de Inteligência Financeira (UIF) da FACILITAPAY é um componente do programa global de Prevenção de Risco de Crimes Financeiros e Lavagem de Dinheiro (AML) da FACILITAPAY. O propósito e o trabalho da UIF permitem que a FACILITAPAY execute aspectos de seu Programa de PLD, particularmente em relação a investigações de crimes financeiros, relatórios regulatórios, aplicação da lei e engajamento. O objetivo deste manual é descrever as funções regidas pelo Programa de Inteligência Financeira FACILITAPAY, que se aplica às operações globais e à base de clientes da FACILITAPAY. O programa visa garantir que a FACILITAPAY continue a cumprir os requisitos regulamentares relevantes em torno da comunicação de Compliance com crimes financeiros em todas as jurisdições em que opera.

Além disso, o Programa de Inteligência Financeira gerencia todo o escopo e as respostas da FACILITAPAY às agências de aplicação da lei em relação a investigações criminais, incluindo o cumprimento de intimações e qualquer outro tipo de solicitação legal submetida à FACILITAPAY por agências internacionais e nacionais. A UIF garante que a FACILITAPAY responde às investigações criminais de acordo com as leis locais.

O Programa de Inteligência Financeira FACILITAPAY é responsável por monitorar e identificar todos os tipos de crimes financeiros potencialmente cometidos na plataforma FACILITAPAY, incluindo, mas não se limitando a:

- Branqueamento de capitais, crimes de antecedentes associados

- Financiamento do terrorismo
- fraude
- Suborno e corrupção
- Violações de sanções
- Evasão fiscal
- abuso de mercado
- Práticas anticoncorrenciais

5.1.2. Missão da UIF

A missão da FIU da FACILITAPAY é fornecer uma investigação líder de indústria e capacidade analítica capaz de identificar crimes financeiros emergentes de forma rápida e eficaz. Com uma perspectiva global, coordenando e aprendendo lições entre investigações, países e regiões, a UIF oferece conclusões e recomendações claras que são compartilhadas para impulsionar o gerenciamento de risco proativo e impactante. A UIF facilita o intercâmbio eficaz de informações com as partes interessadas internas e externas, incluindo as agências reguladoras, de aplicação da lei e de segurança. A UIF aproveita as suas conclusões para apoiar a evolução contínua do panorama regulamentar com base em inovações práticas e testadas.

A UIF é responsável pela divulgação dos resultados da sua análise às autoridades competentes e pela tomada das medidas adequadas para mitigar os riscos internos. O programa de inteligência financeira mitiga essas ameaças por meio de várias funções operacionais, como monitorar transações, resposta a inquéritos e investigações policiais, entre outros métodos descritos neste documento.

A UIF se reporta ao Chief Compliance Officer, que tem a responsabilidade final e a autoridade sobre o programa de crimes financeiros.

5.2 RISCOS

A fim de desenvolver um programa abrangente e eficaz de AML, a FACILITAPAY passa por uma avaliação de risco de AML pelo menos uma vez por ano. Essa avaliação de risco serve como um roteiro para orientar a implementação de procedimentos e controles

internos para identificação abrangente de clientes, diligência devida de clientes, sanções, monitoramento de clientes para atividades incomuns, relatórios regulatórios e requisitos de manutenção de registros. A avaliação de risco identifica os direcionadores de risco exclusivos do PLD para a FACILITAPAY que surgem de seu modelo de negócios específico, bem como vários fatores, incluindo: produtos, serviços, métodos de pagamento e gateways, tipos de clientes-alvo, parceiros e outros relacionamentos, localizações geográficas, controles internos e organização. A avaliação de riscos inclui uma revisão dos controles de mitigação em todas as áreas de negócios expostas aos riscos de PLD identificados.

A FACILITAPAY adotará uma abordagem baseada no risco para avaliar a forma mais eficaz e proporcionada de gerir e mitigar os riscos de branqueamento de capitais. Os passos que a FACILITAPAY tomará para atingir este objetivo são:

- Identificar riscos relevantes de lavagem de dinheiro;
- Avaliar os riscos presentes nos clientes, produtos, serviços, transações, canais de entrega e áreas geográficas de atuação da FACILITAPAY,

A avaliação de risco é utilizada para atividades da FACILITAPAY, tais como:

- Desenho e implementação de controles para gerenciar e mitigar os riscos avaliados;
- Monitorizar e melhorar o funcionamento eficaz destes controles.

A avaliação de risco da FACILITAPAY utiliza as seguintes fontes para determinar os riscos de uma jurisdição:

- GAFI
- BASILEIA
- Transparência Internacional
- USDS (Estados Unidos)
- Países/esquemas sancionados pelo HMT*
- Países/regimes sancionados pelo OFAC*

** Todos os regimes/áreas onde foram impostas sanções complexas estão bloqueados devido ao risco que representam.*

A FACILITAPAY avaliará o risco de cada cliente, levando em consideração a finalidade da conta ou relacionamento, o nível de ativos ou o tamanho das transações a serem executadas e a regularidade ou duração da relação comercial. A avaliação de risco também considerará fatores de risco do cliente, produtos, serviços, transações, canais de entrega e áreas geográficas.

É importante fornecer o nível de risco atual do cliente:

- Fatores de risco significativos;
- Pesquisa de notícias negativas sobre gerentes de conta, beneficiários efetivos e pessoas de controle associadas à conta;
- Processos/apresentações anteriores; se houver, forneça uma visão geral dos resultados.

Fatores de risco de baixo risco para o cliente:

- Empresas públicas cotadas em bolsa e sujeitas a regras de divulgação (quer por regras de mercado, quer por obrigação legal) que impõem requisitos para assegurar uma transparência adequada dos beneficiários finais;
- Clientes residentes em áreas geográficas de baixo risco.

Fatores de risco de clientes de alto risco:

- Relacionamento comercial realizado em circunstâncias incomuns;
- Clientes residentes em áreas geográficas de alto risco;
- Pessoas coletivas constituídas por pessoas físicas com a finalidade específica de gerir ativos para investimentos (veículos de detenção de ativos pessoais);
- Empresas que tenham acionistas registrados ou ao portador;
- Pessoas politicamente expostas e empresas que tenham tais pessoas físicas como acionistas e/ou representantes legais;
- Empresas cuja parcela significativa da receita é em dinheiro;

- Empresas cuja estrutura societária se afigura incomum ou muito complexa, dada a natureza dos negócios da empresa.

A pontuação de risco do cliente é a base dos requisitos de KYC. A FACILITAPAY implementa uma abordagem baseada no risco ao realizar a classificação de risco. Esse processo consiste em avaliar os fatores de risco do cliente com um valor numérico durante o processo de integração.

O risco do produto é equivalente a 25%. O risco do produto inclui os serviços que a FACILITAPAY oferece a um cliente e os serviços/produtos que um cliente corporativo pode realizar ou oferecer aos seus usuários. Com uma ponderação de 25%, o fator de risco do produto leva em conta o risco de transação do cliente, observando o volume de transações previsto e o tipo de atividade, bem como as expectativas de negociação. Vários produtos e serviços de alto risco são medidos na metodologia de pontuação de risco do produto. Existem serviços adicionais que os clientes podem oferecer que apresentam um risco maior. Uma lista completa pode ser encontrada na matriz de escore de risco.

Fatores de risco para produtos, serviços, transações ou canais de entrega de baixo risco:

- Produtos ou serviços financeiros que ofereçam serviços definidos e limitados a determinados tipos de clientes, a fim de aumentar o acesso para fins de inclusão financeira;
- Produtos em que o risco de lavagem de dinheiro e financiamento do terrorismo é gerenciado por outros fatores, como transparência na estrutura societária.

Fatores de risco de produtos, serviços, transações ou canais de entrega de alto risco:

- Private banking;
- Produtos ou transações que possam promover o anonimato;
- Relações comerciais ou transações virtuais sem salvaguardas, como assinaturas digitais;
- Pagamentos recebidos por terceiros desconhecidos ou não associados;

- Novos produtos e novas práticas de negócios, incluindo novos mecanismos de entrega, e o uso de novas tecnologias para produtos novos e pré-existentes.

Fatores de risco geográfico de baixo risco:

- Países com sistemas eficazes de combate à lavagem de dinheiro;
- Países que têm uma baixa taxa de corrupção e outras atividades criminosas, de acordo com fontes confiáveis;
- Países que, segundo fontes fiáveis, têm requisitos para combater a lavagem de dinheiro e o financiamento do terrorismo e que os implementam eficazmente.

Fatores de risco geográfico de alto risco:

- Países que não possuem sistemas eficazes de combate à lavagem de dinheiro;
- Países que têm uma taxa significativa de corrupção e outras atividades criminosas, de acordo com fontes confiáveis;
- Países sujeitos a sanções, embargos ou medidas similares aplicadas, por exemplo, pela Organização das Nações Unidas (ONU);
- Países que financiam ou apoiam atividades terroristas ou que têm organizações consideradas terroristas em seu território.

Os clientes serão classificados em categorias de risco: alto, médio ou baixo. Aqueles classificados como de "alto risco" terão que passar por um processo de Due Diligence Aprimorada (EDD).

5.2.1. Seção Nível de Risco (Avaliação e Categorização):

No processo de avaliação e verificação do cliente e seu nível e risco, a FACILITAPAY avaliará os documentos e informações fornecidos a fim de avaliar a categoria de riscos, podendo ser realizadas as seguintes ações:

a) Após a análise das informações, uma decisão de "Alerta" ou "Não Correspondência" deve ser tomada utilizando critérios definidos pelo Comitê de Compliance.

b) O seguinte código de motivo só deve ser usado se aprovado pela administração e devidamente documentado:

- Emparelhado, mas irrelevante

c) Se qualquer um dos seguintes códigos de motivo for usado, você deve adicionar escalonamento:

- Informações insuficientes (requer dimensionamento)
- Sem correspondência de local (requer uma nota detalhando pelo menos um outro ponto de dados usado para negação)
- Não está mais associado (requer uma nota detalhando as medidas tomadas para garantir que o relacionamento não exista mais)
- Não é uma correspondência (requer uma nota detalhando dois motivos para a recusa)
- Sem relação com PLD (requer uma nota detalhando o motivo da negativa)
- Pré-corrigido (requer uma nota detalhando o alerta anterior e qualquer nova informação)

Quando uma correspondência positiva é identificada, ela é marcada como um alerta e requer escalonamento. O processo de escalonamento varia de acordo com o tipo de alerta.

d) Alerta de sanções

As correspondências de sanções apresentam um risco regulatório significativo e exigem ação imediata. Portanto, uma vez confirmada uma correspondência positiva, ela deve ser imediatamente enviada a um Gerente de Compliance ou a uma pessoa designada para as próximas etapas. As partidas devem ser rastreadas no registro de rastreamento de sanções.

5.2.2. Bandeiras vermelhas (RED FLAGS)

O principal foco do FACILITAPAY é relatar atividades suspeitas para determinar se as transações estão de fato ligadas à lavagem de dinheiro, abuso de mercado, financiamento do terrorismo ou um crime específico. Os exemplos a seguir são sinais de alerta de RED FLAGS que, quando encontrados, podem merecer uma análise mais aprofundada. Esta não é uma lista exaustiva e a mera presença de uma bandeira vermelha não é, por si só, evidência de atividade criminosa. Um exame mais atento deve ajudar a determinar se a atividade é suspeita ou se não parece haver um objetivo comercial ou legal razoável.

Exemplos de bandeiras vermelhas:

- Os documentos de identificação fornecidos à FACILITAPAY parecem ser fraudulentos ou modificados.
- Os intervalos de endereços IP não correspondem aos intervalos de IP associados correlacionados com a localização da conta.
- O nome do usuário aparece em uma lista de observação de sanções.
- O usuário é alvo de notícias que indicam possíveis violações criminais, civis ou regulatórias.
- Fundos provenientes de atividades ilegais ou da intenção de ocultar fundos derivados de atividades ilegais.
- Fundos feitos de uma forma que indique uma atividade semelhante à estruturação, numa tentativa considerada por esse transator para evitar requisitos de manutenção de registos ou relatórios.
- Transação sem propósito legítimo aparente.
- Atividade que não é compatível com as atividades normais do consumidor.
- O volume de transações de usuários tem um grande aumento que não pode ser explicado.
- O usuário deposita e retira fundos sem negociação.
- Picos súbitos de atividade após longos períodos de inatividade.
- Citações policiais indicando que um usuário pode estar envolvido em um crime financeiro.
- Um usuário demonstra mudanças em recursos, por exemplo, estilos de vida luxuosos.
- Negociação significativa inconsistente com os fundamentos do mercado.
- Uma negociação específica causou um lucro ou perda excepcionalmente grande para o usuário.

5.3 AUDITORIA LEGAL

Um cliente é qualquer indivíduo ou empresa (usuário ou comerciante) a quem a FACILITAPAY oferece, pretende oferecer ou já ofereceu no passado um serviço e/ou um

produto. Por isso, os potenciais clientes também estão incluídos nesse conceito. Clientes anônimos ou transações de indivíduos ou empresas anônimas não serão aceitos.

Um parceiro é qualquer indivíduo ou empresa (fornecedor, instituição financeira, agente, referência, profissional independente) que fornece produtos e/ou oferece serviços à FACILITAPAY.

Antes de incorporar qualquer novo Comerciante, usuário ou parceiro, a FACILITAPAY deve realizar o processo de Due Diligence. Alguns terceiros oferecerão um risco maior do que outros. Para determinar o nível de risco oferecido por um terceiro, todos eles passarão por um processo implícito de Due Diligence e terão seu risco definido por meio do plano de Avaliação de Risco.

A Matriz de Riscos baseia-se em critérios relacionados a fatores de risco geográficos, financeiros e de negócios do terceiro, entre outros. Esses critérios serão classificados em baixo, médio e alto, e uma pontuação diferente será atribuída a cada nível de risco. O conjunto de critérios permitirá definir o risco que cada terceiro representa para a FACILITAPAY. Terceiros avaliados como de "médio risco" passarão por um processo de due diligence padrão. Aqueles avaliados como de "alto risco", da Enhanced Customer Due Diligence.

5.3.1. Due Diligence Simplificada

A due diligence simplificada envolve a coleta de informações e documentos que permitem:

- Identificar o terceiro e verificar sua identidade;
- Estabelecer a natureza da relação comercial;
- Realizar uma verificação para identificar se o terceiro é uma Pessoa Politicamente Exposta (PEP) e/ou está sujeito a sanções;
- Garantir que qualquer pessoa agindo em nome do terceiro esteja autorizada a fazê-lo, bem como identificar e verificar essa pessoa;

- Uma vez concluído esse processo, a Avaliação de Risco será conduzida para determinar o nível de due diligence necessário.

5.3.2. Due Diligence Padrão

Para cada cliente e usuário, a FACILITAPAY fará uma visão geral, que inclui o relacionamento com o cliente, o documento contendo a data de início do relacionamento, o nível de risco, a finalidade da conta, os administradores de conta autorizados e as contas associadas.

Além das verificações realizadas no processo de Due Diligence Simplificada, terceiros cujo nível de risco é médio devem passar pelo processo de Due Diligence Padrão, que envolve:

- Identificação e verificação completa de qualquer beneficiário que detenha 25% ou mais da empresa (caso o beneficiário efetivo seja outra empresa, a verificação deve ser feita apenas em relação à empresa acionista, e não aos seus administradores);
- Verificação de mídia negativa de todos os envolvidos.

A panorâmica deve igualmente incluir as seguintes informações:

- Número
- Tipo de cliente
- Estrutura jurídica, se aplicável (Sociedade Limitada, Sociedade Limitada, etc.)
- Identificador único (CNPJ, etc.)
- Incorporação de informações (país, estado, data, etc.)
- Localização física (pesquisa no Google Map) países de operação
- Descrição da participação acionária
- Breve descrição da natureza do negócio, produtos e serviços
- Website (se disponível)

Em resumo, ao abrir a conta, a FACILITAPAY obtém determinadas informações de identificação sobre todos os clientes e usuários através de uma abordagem baseada em risco, indicando: A classificação do cliente como pessoa física ou jurídica, a determinação do proprietário ou beneficiários finais para pessoas jurídicas, a identificação de pessoas politicamente expostas e o tipo de produto ou serviço a ser utilizado. Isso permite que a FACILITAPAY entenda se o cliente ou as transações representam um risco de crime financeiro e se determinados clientes, como aqueles identificados como de alto risco, exigem mais diligência em relação à clientela.

Um processo de revisão também é conduzido para concluir a devida diligência sobre essas solicitações. Assim que a revisão for concluída, ela será dimensionada para aprovação.

5.3.2.1 Seleção das sanções e das listas de vigilância

A seleção de sanções e as listas de observação são realizadas por um provedor terceirizado. Isso inclui a detecção de sanções, pessoas politicamente expostas (PEP) e notícias negativas. A seleção será feita em todos os clientes e usuários (inclui nome da conta, acessos autorizados e beneficiários efetivos). A triagem ocorrerá durante a integração e, a partir daí, diariamente, usando uma abordagem baseada em risco.

Todas as avaliações correspondem às jurisdições em que a FACILITAPAY opera.

Durante o curso da seleção, se uma possível combinação não puder ser decidida, documentação adicional pode ser solicitada.

5.3.2.2. Controlo das sanções

A FACILITAPAY analisa os clientes em relação a todas as listas de sanções exigidas para as jurisdições em que opera. Comentários adicionais de governos são considerados sob várias sanções globais e direcionadas.

Qualquer entidade que tenha obtido licenças, isenções, autorizações ou certificados da autoridade relevante para realizar negócios com jurisdições ou atividades sancionadas será escalada e revisada pela Compliance. Eles podem ser encaminhados para um

administrador de Compliance para análise caso a caso. Além disso, a aprovação da alta administração é necessária antes de permitir qualquer atividade.

5.3.2.3 Pessoas politicamente expostas

Os clientes existentes terão uma decisão de retenção tomada durante a revisão. O alerta WBS de origem é rastreado no log de rastreamento.

5.3.2.4. Alerta de notícias negativas

Novos clientes determinados como associados a notícias negativas terão o registro negado no momento do embarque. O cliente existente associado a notícias negativas será encaminhado para uma revisão do EDD, que quando concluída determinará o risco que apresenta e se a FACILITAPAY prosseguirá com o encerramento da conta. Alertas de notícias negativas são rastreados na trilha.

A FACILITAPAY verifica os clientes (incluindo gerentes de conta e beneficiários efetivos) em busca de notícias negativas. Os clientes associados a notícias negativas serão analisados pela equipe de Compliance para determinar o risco apresentado à FACILITAPAY. A detecção de notícias negativas incluirá o seguinte:

- Atos ou declarações falsas com a intenção de obter ou privar dinheiro, bens ou serviços em erro; inclui fraudes, golpes, esquemas Ponzi, esquemas de pirâmide, fraude eletrônica, golpes de caridade, iscas e esquemas de troca;
- Infracções relacionadas com a ocultação ou ocultação da origem do produto do crime; inclui branqueamento de capitais, esquemas de financiamento ilícito, estratificação de fundos, branqueamento de produtos do crime, contrabando de dinheiro, transações cambiais estruturadas;
- Crimes relacionados a grupos/gangues do crime organizado; inclui crime organizado, associação criminosa, extorsão;
- Crimes relacionados a grupos ou indivíduos terroristas;
- Entidades listadas sob vigilância governamental.

5.3.2.5. Escritório de Controle de Ativos Estrangeiros (OFAC):

A FACILITAPAY avaliará os clientes (incluindo usuários, administradores de contas e beneficiários efetivos) para garantir que eles não apareçam na lista de Cidadãos Especialmente Designados (SDN). A FACILITAPAY também garantirá que não se envolva em transações ou atividades proibidas por sanções econômicas e embargos administrados e aplicados pelo OFAC. Todas as sanções do OFAC serão aplicadas globalmente dentro da estrutura corporativa da FACILITAPAY.

Como a lista SDN e as listas de sanções econômicas e embargos são atualizadas com frequência, verificaremos com eles regularmente para garantir que as atualizações automáticas da lista sejam precisas e oportunas em nosso provedor terceirizado.

5.3.3. Diligência reforçada

Este manual será usado para complementar os requisitos do programa PLD, aplicando EDD às funções de alto risco identificadas. Este documento detalha os procedimentos pelos quais a equipe de Compliance será responsável pelo cumprimento de cada função. Esses processos e procedimentos aprimorados serão usados para avaliar e mitigar riscos, garantindo a implementação de uma abordagem eficaz baseada no risco.

O papel da subequipe de Due Diligence Aprimorada (EDD) é implementar processos e procedimentos aprimorados para clientes e atividades que apresentam um risco maior do que o normal de lavagem de dinheiro e financiamento do terrorismo, ou outro risco inerente de Compliance. As áreas identificadas como de maior nível de risco serão definidas neste documento, juntamente com os controles em vigor para mitigar esses riscos. A equipe de Compliance EDD tem o papel e a responsabilidade de conduzir revisões EDD iniciais e periódicas de clientes de maior risco.

Há categorias para cada tipo de conta de usuário. O nível de conta Pro é para pessoas físicas de alto volume e todas as contas corporativas. As contas profissionais passam por due diligence, incluindo todos os requisitos do nível anterior, juntamente com documentação adicional, demonstrações financeiras, atividade prevista, pesquisa de código aberto e muito mais.

Além das verificações realizadas nos processos de Due Diligence Simplificada e Padrão, terceiros classificados como de alto risco devem passar pelas seguintes verificações:

- Fonte de renda dos sócios da empresa – no caso do PEP, a comprovação é exigida por meio de documentos;
- Identificação e verificação completa de todos os beneficiários, incluindo verificação dos diretores da empresa;
- Identificação do beneficiário final, quando aplicável, verificando sua identidade e buscando entender a estrutura de controle da empresa, quando aplicável.

As medidas reforçadas de diligência devida também incluem:

- Aumento da frequência de revisão para verificar se a FACILITAPAY ainda é capaz de gerenciar o risco associado ao relacionamento comercial e ajudar a identificar quaisquer transações que exijam revisão adicional;
- Aumento da frequência de revisão da relação comercial para verificar se o perfil de risco do terceiro mudou e se o risco permanece gerenciável;
- Obter a aprovação da MLRO local para iniciar ou continuar a relação comercial, a fim de garantir que a alta administração esteja ciente dos riscos aos quais a FACILITAPAY está exposta e para permitir que eles tomem decisões informadas sobre o quanto podemos gerenciar esses riscos;
- Rastreie as transações com mais frequência ou com maior profundidade, a fim de identificar quaisquer transações incomunsou inesperadas que possam levantar suspeitas de lavagem de dinheiro ou financiamento do terrorismo. Isso pode incluir definir o destino dos fundos de terceiros ou definir o motivo de determinadas transações.

O processo de due diligence também deve ser executado a qualquer momento quando a FACILITAPAY suspeitar ou tiver motivos para suspeitar de lavagem de dinheiro ou quando se acreditar que documentos ou informações vencidas ou inexatas foram fornecidas. Qualquer relação comercial com um comerciante ou usuário estará sujeita a monitoramento constante, o que pode resultar em funcionários sendo solicitados a

qualquer momento a realizar diligências ou buscar informações adicionais sobre tais indivíduos e empresas. As relações e transações comerciais devem ser consistentes com o conhecimento que a FACILITAPAY tem sobre o Comerciante, o usuário ou o parceiro, bem como sobre seus negócios, perfis de risco e fontes de renda.

Quando o risco excede o apetite do negócio, o terceiro não será integrado à FACILITAPAY. Se a área requerente considerar que a oportunidade é suficientemente importante e que controlos alternativos podem reduzir o risco identificado, podem aplicar-se excepções formais.

5.3.3.1 Procedimentos Operacionais do EDD: Avaliações de Casos

Conforme detalhado nas seções anteriores, quando um cliente é identificado pela primeira vez como de alto risco, uma revisão inicial do EDD é necessária. Isso acontecerá no momento da detecção durante a seleção da lista de observação ou uma vez encaminhado para o Comitê deOmpliance durante a integração do cliente. Após uma revisão inicial, os clientes automatizados de alto risco manterão uma revisão periódica semestral, enquanto todos os outros manterão uma revisão anual.

Quando a revisão for concluída, ela será encaminhada para um Gerente de Compliance ou designado para aprovação.

A pessoa que conclui a revisão do EDD é responsável por completar a seleção do caso do EDD. No log de rastreamento, todos os números de casos são predeterminados e esse número exclusivo será usado durante todo o ciclo de vida de alto risco do cliente. Se forem necessárias revisões periódicas, a mesma entrada de rastreamento será atualizada com as informações atuais. Dentro do log de rastreamento, várias colunas foram fornecidas com valores definidos para garantir a consistência.

A próxima data de revisão no rastreamento é definida usando a data de término da revisão atual, que é a data em que a revisão do EDD é concluída e dimensionada para aprovação. O registro de acompanhamento de casos do EDD também manterá uma data de aprovação, que é a data em que um gerente de supervisão C ou designado aprova a revisão.

5.3.3.2. Metodologia de pontuação de risco

A) Tipos de clientes de alto risco

Esse fator inclui tipos de clientes de maior risco, bem como produtos e serviços oferecidos por clientes que foram identificados como de alto risco para lavagem de dinheiro e/ou financiamento do terrorismo. Esses tipos de clientes são determinados por meio de requisitos regulatórios ou orientação internacional e podem mudar ao longo do ciclo de vida dessa metodologia de classificação de risco. A metodologia de pontuação de risco é revisada anualmente para garantir que a pontuação esteja alinhada com as tendências e práticas atuais.

B) Lista de Observação de Risco - Alto Risco Automático

A FACILITAPAY utiliza um provedor externo para a seleção automatizada de pessoas politicamente expostas, indivíduos e entidades sancionados e notícias negativas. Qualquer cliente que retorne como uma correspondência positiva para esses itens é automaticamente considerado de alto risco.

Os clientes automatizados de alto risco serão identificados durante o processo de integração com base nos tipos de produtos e serviços oferecidos. Esses tipos específicos de clientes passarão pelo processo normal de pontuação de risco para identificar uma pontuação de risco para cada fator de risco específico. No entanto, sua pontuação de risco final será definida automaticamente para a pontuação máxima de risco para se alinhar com o escalonamento automático de alto risco do cliente. Esses clientes precisarão de documentação adicional e informações de diligência durante a integração. Além disso, serão sujeitos a revisões semestrais periódicas do EDD, garantindo a devida diligência e monitoramento contínuo. Os tipos de clientes que serão considerados automáticos de alto risco são os seguintes:

Tipo de Cliente	Risco	Cronograma de revisão	Documentação/Informações

Instituições financeiras /correspondentes bancários (excluindo instituições de pagamento, instituições financeiras não bancárias e atividades e profissões não financeiras designado (APNFD). Definição: Instituições Finanças e crédito tradicionais	Alto Risco Automático	Semestral	Requisitos de Due Diligence: • Documentos de identificação padrão da trading company; • Questionário de Due Diligence; • Cópia das políticas de Compliance (PLD e sanções, se separadas); Guia de revisão do EDD: • Avaliar questionário, políticas e procedimentos • Revisão da licença regulatória, se aplicável • Meios adversos para a companhia, acionistas, acionistas, cotas, controladoras, controladas e diretores • Avaliação de: o Jurisdições em que a empresa opera o Base de clientes o Produtos & Serviços o Atividade de correspondente bancário
Pessoas Politicamente Expostas (PEP) Definição: são consideradas pessoas politicamente expostas: os titulares de mandatos eletivos dos Poderes Executivo e Legislativo da União, os ocupantes do cargo, no Poder Executivo da União, de: Ministro de Estado ou equivalente; Natureza especial ou equivalente; Presidente e, Vice-Presidente e Diretor, ou equivalente, de entidades da administração pública indireta; e Grupo Superior de Administração e Assessoramento - DAS, nível 6, ou equivalente; os membros do Supremo Tribunal Federal, dos Tribunais Superiores e dos Tribunais Regionais Federal, do Trabalho e Eleitoral; o Procurador-Geral da República, o Procurador-Geral do Trabalho, a Procuradoria-Geral da Justiça Militar e a Procuradoria-Geral dos Estados e do Distrito Federal; os membros do Tribunal de Contas da União e do Ministério Público Procuradoria-Geral do Tribunal de Contas da União;	Alto Risco Automático	Semestral	Requisitos de Due Diligence: • A avaliação do PEP é feita por meio de um provedor externo e é revisada pela Compliance antes da integração. • Fonte de renda • Fonte de riqueza Guia de revisão do EDD: • Cargo ocupado • Responsabilidades oficiais • Papel específico em relação à sua autoridade no governo • Acesso a fundos governamentais • Fonte de riqueza - Riscos do país/governo - Riscos globais para os

presidentes e tesoureiros nacionais, ou equivalentes, de partidos políticos; os governadores e secretários de Estado e do Distrito Federal, os Deputados de Estado e Distritos, os presidentes, ou equivalentes, de entidades da administração pública indireta estadual e distrital e dos presidentes de Tribunais de Justiça, Militares, de Contas ou equivalentes do Estado e do Distrito Federal; os Prefeitos, Vereadores, Presidentes de Tribunais de Contas ou equivalentes dos Municípios; Chefes de Estado ou de Governo; políticos de alto escalão; ocupantes de cargos públicos em níveis superiores; funcionários gerais e membros dos altos escalões do Poder Judiciário; altos executivos de empresas públicas; ou dirigentes de partidos políticos; Dirigentes de instâncias superiores de entidades regidas pelo direito internacional público ou privado.			países - Abordar especificamente o risco de corrupção e suborno estabelecido na jurisdição - Abordar especificamente se os crimes financeiros e a corrupção política/governamental foram criminalizados • Relacionamentos associados (por exemplo, eles mantêm uma relação corporativa, são um UBO de qualquer conta da empresa mantida pela FACILITAPAY, mantêm qualquer fatura, etc.) Eliminação do Monitoramento Automático de Alto Risco: Os indivíduos identificados como PEP podem ser removidos do alto risco automático se não atenderem mais aos requisitos do PEP e/ou mantiverem suas posições por um período de 5 anos ou mais.
Outros serviços financeiros Definição: • Trader ou cambista • Emissor de Cheque de Viagem, Ordens de Pagamento • Vendedor ou caixa de cheques de viagem, ordens de pagamento • Facilitadores e pagadores ou trocadores Gerente de Moeda Virtual e Comerciante • Plataformas de intercâmbio virtual e • Fornecedores de carteira Fiat	Automático de alto risco	Semestrais	Requisitos de Due Diligence: • Documentos de identificação padrão da trading company; • Questionário de Due Diligence; • Cópia das políticas de Compliance (PLD e sanções, se separadas); • Guia de Revisão de Licença Regulatória do EDD: • Avaliar questionário, políticas e procedimentos • Revisão da licença regulatória, se aplicável •Avaliação de risco dos produtos/serviços oferecidos •Avaliação de risco de clientes e jurisdições atendidas

Detecção de lista de observação (excluindo PEPs): Definição: As sanções e os meios adversos serão imediatamente encaminhados para revisão pelo Compliance. Abolição da vigilância automática de alto risco das sanções e Os meios adversos serão determinados por uma avaliação do risco apresentado	Correspondência positiva automática/alto risco	Semestrais	Requisitos de Due Diligence: • Requisitos de integração padrão • Documentação adicional pode ser solicitada para determinar se o risco do cliente pode ser mitigado.

C) Outros tipos de clientes de alto risco:

Os clientes que não atendem aos critérios automáticos de alto risco ainda podem classificar o alto risco com base nos fatores de risco combinados. Uma vez que esses clientes são identificados como de alto risco por meio do processo de integração, eles passam para a supervisão EDD de contas de alto risco.

A seguir estão todos os outros tipos de clientes:

Tipo de Cliente	Risco	Cronograma de revisão	Documentação/Informações

Instituições financeiras não bancárias, excluindo instituições de pagamento e bolsas de valores. Definição: Uma entidade que executa serviços financeiros diferentes de um banco tradicional. • Entidades que prestam serviços no mercado de capitais, incluindo empresas de valores mobiliários e de mercadorias, corretoras, consultores de investimento, fundos mútuos, fundos de cobertura, comerciantes de mercadorias, etc. • Seguradoras • Empresas de crédito e financiamento • Empresas Fiduciárias • Revendedores de metais preciosos, pedras ou joias; Credores • Consultores financeiros • Empresas de serviços financeiros • Revendedores de metais preciosos, pedras preciosas ou joalharia • Jóias • Cambistas • Vendedor de artigos de luxo Cassinos ou estabelecimentos de jogo equivalentes.	Alto Médio Baixo	Anual Nenhum Nenhum	RequisitosdeDue Diligence: •Requisitos de integração padrão •Programa AML e KYC •Licença regulatória, se aplicável Guia de revisão do EDD: •Pesquisas de proprietários, controladores e diretores •Jurisdições em que a entidade opera •Base de clientes •Risco de produtos e serviços •Riscos associados a notícias regulatórias, se aplicável.
Operadores de ATM privados Definição: Entidades que possuem ou operam caixas eletrônicos, podendo ou não incluir criptomoedas.	Alto Médio Baixo	Anual Nenhum Nenhum	Requisitos de Due Diligence: • Requisitos de integração padrão; • questionário ATM; • Programa PLD/KYC, quando aplicável; • Licença regulatória, se aplicável; • Contrato ATM; • Questionário de Due Diligence ATM necessário: • Quantos caixas eletrônicos você possui e opera? • Em muitos lugares, os caixas eletrônicos funcionam eletronicamente? Forneça endereços para todos os locais. • Os caixas eletrônicos oferecem

			serviços de compra e venda? • Se você oferece serviços de venda automática, quem é responsável por reabastecer o caixa eletrônico com moeda? Você é uma pessoa confiável? • Para a compra de serviços, um serviço de mensagens instantâneas é usado para entregar moeda a uma instituição financeira? • Quais moedas são aceitas no caixa eletrônico? • Quais são os limites de transação em dólar para compra e/ou venda? • Quais procedimentos de verificação de identidade o caixa eletrônico oferece? • Qual é o volume esperado de transações ATM diárias/mensais na sua conta? Guia de revisão do EDD: • Avaliar questionário ATM; • Avaliar políticas e procedimentos de Compliance; • Atender às exigências regulatórias do país; • Analise o risco de localização com os serviços prestados.
Processadores de pagamento de terceiros Entidades que prestam serviços de processamento de pagamentos aos seus clientes, tais como entidades baseadas na Internet, empresas de jogos na Internet, pagamentos com cartão de crédito, etc.	Alto Médio Baixo	Anual Nenhum Nenhum	Requisitos de due diligence: -Requisitos de integração padrão: • Programa AML/KYC, se aplicável; • Detalhes sobre a base de Clientes Comerciais; • Detalhes sobre as atividades comerciais do cliente; • Lista dos 10 melhores clientes; • Uma cópia dos materiais de marketing; Guia de revisão do EDD:

			• Avaliação de controles; • Políticas e procedimentos; • Busca de reclamações; • Uso de pesquisas de código aberto, incluindo pesquisas em sites de proteção ao consumidor.
Prestadores de Serviços Profissionais (PSPs) e Atividades e Profissões Não Financeiras Designadas (DNFBPs). Definição: PSPs e DNFBPs recebem um valor de risco adicional com base no tipo de atividade. Essas empresas e profissões incluem o seguinte: • Prestadores de serviços corporativos; • Empresas; • Fiduciário; • Agentes imobiliários; • Advogados/profissionais do direito; • Contadores; Consultores fiscais, auditores	Alto Médio Baixo	Anual Nenhum Nenhum	Requisitos de Due Diligence: - Requisitos de integração padrão: • Carteira Profissional Ativa junto ao órgão regulador; • Log de monitoramento; • Política PLD; • Estrutura da organização. Guia de revisão do EDD: • Serviços e produtos; • Jurisdições; • Registro ativo de licença.
Outro Definição: Todos os outros tipos de clientes que se qualificam como de alto risco com base nos fatores de risco combinados na matriz. Exemplo: um cliente recebe uma pontuação de alto risco com base em sua atividade, nenhuma atividade é relatada na conta do cliente. Se os fatores de risco não corresponderem ao risco real apresentado, o cliente pode ser eliminado.	Alto Médio Baixo	Anual Nenhum Nenhum	Requisitos de Due Diligence: - Requisitos de integração padrão: Documentação adicional pode ser solicitada para mitigar o risco do cliente. Eliminação: Os clientes que obtiverem uma pontuação de alto risco com base em seus fatores de risco combinados podem ser removidos do monitoramento de alto risco se for determinado que sua pontuação de risco não corresponde ao risco real apresentado.

5.3.3.3 Processo de aprovação de clientes de alto risco

Como os clientes de alto risco apresentam riscos significativos, eles devem ser aprovados por vários níveis de senioridade dentro da organização. O processo geral de aprovação do cliente começa durante a integração e verificação. Durante esse processo, os clientes identificados de alto risco devem cumprir os requisitos de diligência de clientes aqui estabelecidos. Depois que todos os requisitos de CDD forem atendidos, eles serão escalados para Compliance.

Os clientes de alto risco terão uma revisão inicial do EDD concluída pelo Departamento de Compliance, que avaliará ainda mais a pontuação de risco do cliente e quaisquer outros riscos relevantes que possam estar presentes. A revisão do EDD também conterá uma revisão de todos os fatores atenuantes, conduzirá pesquisas de código aberto e análise transacional. A Compliance fará uma recomendação com base em suas descobertas e no risco geral do cliente.

Uma vez por trimestre fiscal, uma lista de todos os clientes de alto risco será enviada ao Diretor de Compliance para aprovação da Gerência Sênior/Executiva. Essa lista refletirá com precisão nosso perfil de cliente de alto risco para garantir que nosso perfil de risco e níveis de tolerância estejam alinhados em toda a organização.

5.3.3.4. Pontuação contínua de risco e remoção da categoria de alto risco

A FACILITAPAY analisa continuamente os clientes usando uma abordagem baseada em risco. Se for identificado que foram feitas alterações no modelo de negócios, na estrutura ou no negócio geral de um cliente, isso pode justificar a solicitação de documentação adicional e uma reavaliação de sua pontuação de risco. O Comitê de Compliance pode identificar tais mudanças durante o curso regulatório dos negócios, conduzindo análises de EDD de clientes de alto risco. Se identificado, o cliente será enviado à equipe do Customer Engagement (EC) para realizar uma nova avaliação da pontuação de risco do cliente. O EC também pode executar uma pontuação de risco contínua do cliente com base em vários eventos de disparo que resultam em uma mudança potencial no risco geral do cliente. Esses gatilhos incluem o seguinte:

• Uma alteração na estrutura de propriedade que resulte em alterações significativas (por exemplo, uma empresa que já foi propriedade de um único indivíduo é agora identificada como propriedade de uma holding, sendo a UBO detida pela holding).

Pode-se identificar que um cliente não atende aos fatores de risco apresentados ao estabelecer a conta ou não mantém atividade significativa para justificar o risco inerente. Exemplos destas situações podem ser encontrados no quadro dos clientes de alto risco (ponto 5.3.3.2). Caso tal situação ocorra e o cliente não divulgue o risco, vários resultados podem ser obtidos. Por exemplo:

• Se a conta do cliente estiver inativa sem atividade por um período de um ano. A conta do cliente pode ser bloqueada até que o cliente inicie o contato. O cliente pode ser removido da supervisão de alto risco se a conta for bloqueada. Caso o cliente deseje desbloquear a conta, o relacionamento do cliente será avaliado posteriormente para determinar se ainda há justificativa para o monitoramento de alto risco;
• Se o risco não estiver presente, como um erro de integração ou remoção de PEP, a pontuação de risco do cliente é atualizada e o cliente pode ser removido da supervisão de alto risco.

5.3.4. A Facilitapay não fará negócios com:

• Pessoas ou empresas suspeitas de lavagem de dinheiro e/ou financiamento do terrorismo;
• Bancos de fachada;
• Pessoas físicas ou jurídicas para as quais o nível exigido de Due Diligence NÃO tenha sido realizado;
• Usuários listados como não aceitáveis pelas Políticas da FACILITAPAY;
• Empresas sediadas em países sancionados.

Em relação à incorporação específica de Comerciantes, alguns tipos de negócios não são aceitos pela FACILITAPAY. Consulte nossas listas de produtos e serviços restritos e proibidos no apêndice deste manual.

5.3.5. Eventuais ações de recomendação

Os resultados da análise global devem ser documentados por uma recomendação geral. Isso deve incluir razões para apoiar uma das seguintes recomendações:

• Reter o cliente no nível de risco existente com revisão periódica;
• Reter o cliente e encaminhá-lo para investigação da FIU;
• Encaminhar o cliente para a UIF com recomendação de encerramento da conta;
• Remover o cliente da categoria automática de alto risco após a revisão do caso;
• Recomendar o encerramento da conta com base no risco apresentado pelo cliente.

5.3.6. Sanções

A FACILITAPAY bloqueará Comerciantes, usuários e/ou entidades oriundas de países que não respeitem os programas de sanções, a fim de garantir que a empresa não faça negócios com pessoas e organizações sancionadas, combatendo, financiando e proliferando armas de destruição em massa.

Algumas jurisdições representam um risco excepcional em relação ao branqueamento de capitais e à criminalidade financeira. Essas jurisdições são identificadas pelo GAFI como tendo controles fracos ou exigindo ação ou são regimes sancionados pelos Estados Unidos da América ou pelo Reino Unido. O risco geográfico deve ser revisto e atualizado anualmente. Comerciantes, usuários e parceiros são verificados quanto a sanções por meio de um banco de dados global com acesso a mais de centenas de milhares de fontes de lista de sanções.

Analiticamente, a FACILITAPAY analisa todos os indivíduos, empresas, entidades e beneficiários efetivos, incluindo clientes já registrados, contra várias listas de transações proibidas para confirmar que a FACILITAPAY não autoriza uma transação com qualquer pessoa ou entidade proibida. Essas pessoas físicas e jurídicas são identificadas em listas disponíveis publicamente que exigem o cumprimento de sanções financeiras direcionadas com base em resoluções do Conselho de Segurança das Nações Unidas ou na lista do Escritório de Controle de Ativos Estrangeiros (OFAC) do Escritório de Cidadãos Especialmente Designados dos EUA.

Quando apropriado, a FACILITAPAY bloqueará e/ou congelará ativos financeiros e reportará o incidente à autoridade competente.

O processo de bloqueio de fundos varia de acordo com os fundos envolvidos. Se a FACILITAPAY mantiver a custódia de títulos, bloqueará os fundos e os colocará em uma conta remunerada estabelecida em uma instituição correspondente. A conta será rotulada como "Fundos Bloqueados" até que o OFAC ou outra autoridade competente emita orientações sobre a ação necessária.

O FACILITAPAY registrará todas as transações rejeitadas e bloqueadas por meio de rastreamento de Compliance e logs de auditoria para garantir uma trilha de auditoria clara do processo.

5.3.7. Análise da Compliance

A) Visão geral

Será realizada uma visão geral do relacionamento do cliente com a FACILITAPAY contendo: data de início do relacionamento, nível e finalidade da conta, administradores de conta autorizados e contas associadas. A visão geral também deve incluir as seguintes informações:

• Número
• Tipo de cliente
• Estrutura jurídica, se aplicável (Unipessoal, Limitada, S/A, etc.)
• Identificador único (CNPJ)
• Incorporação de informações (país, estado, data, etc.)
• Localização física (pesquisa no Google Map) países de operação
• Descrição da estrutura societária
• Breve descrição da natureza do negócio, produtos e serviços
• Website (se disponível).

B) Análise de transações

Além da visão geral, é imprescindível que a FACILITAPAY realize uma análise da transação que forneça: tipo de cliente (pessoal/empresarial), nível categórico (Básico, Intermediário, Avançado), uma revisão da atividade nos últimos 90 dias ou desde o início do relacionamento. Além disso, a análise deve incluir:

• Saldo total na conta
• Análise de depósitos e levantamentos
• Detalhamento do uso do fundo, incluindo negociação de margem, se aplicável.

C)Notificação de alterações

Quando os alertas são gerados por meio de classificação inicial ou contínua, a equipe de supervisão C será responsável por revisar e decidir sobre os alertas. Se uma indicação não puder ser decidida com base nas informações detidas pela FACILITAPAY, poderá ser solicitada documentação adicional a um cliente. Se um cliente não responder, o aplicativo ou a conta, esse fato pode justificar a rejeição ou a rescisão.

Qualquer alteração na entidade legal de um Comerciante deve desencadear uma revisão da OC nesse Comerciante.

É da responsabilidade do Comerciante notificar a FACILITAPAY sempre que houver alterações em relação a:

• Estrutura societária e controle da empresa (diretores e beneficiários finais);
• Controladoria da empresa;
• outras pessoas autorizadas a assinar pela empresa;
• Mídia negativa, quando são divulgadas ou conhecidas pelo Comerciante, e outras informações relevantes.

D)Avaliação do risco de sanções

A FACILITAPAY deve proceder a uma avaliação anual do risco de sanções. Este analisará os riscos inerentes associados ao modelo de negócio da FACILITAPAY, incluindo produtos e serviços, jurisdições econtrolos internos. Esses fatores serão

analisados juntamente com a mitigação implementada para reduzir o risco global apresentado. O resultado será o risco residual, que é o risco final apresentado à FACILITAPAY. Uma vez que todos os riscos residuais tenham sido obtidos, a média será o risco global de sanções da FACILITAPAY.

E) Revisão dos casos de EDD

O modelo de revisão de caso EDD descreve as seções que precisam ser concluídas e serão usadas para monitorar contas EDD de alto risco.

Determinação da revisão de casos de EDD: as revisões de casos de EDD manterão recomendações predefinidas para seleção para garantir uma abordagem padronizada para essas recomendações e seus procedimentos subsequentes. As recomendações constam do quadro seguinte:

1. Reter e monitorar	Reter o cliente para acompanhamento periódico.
2. Reter e consultar	Manter o acompanhamento do jornal do cliente e encaminhá-lo à UIF para investigação da AML.
3. Ver e fechar conta	Encaminhe o cliente para o encerramento da conta e uma investigação de AML na UIF.
4. Eliminação do monitoramento de alto risco	Remova o cliente dos testes de alto risco e do monitoramento contínuo da EDD.
5. Recomendar o encerramento da conta	Recomende o encerramento da conta.
6. Aguarde informações adicionais	Aguarde informações/documentação adicionais para concluir a revisão do EDD.

Um caso de EDD é encaminhado para a UIF quando uma atividade possivelmente suspeita ou incomum é identificada. Isso pode ser determinado quando o revisor tem motivos para suspeitar que a atividade pode estar relacionada à lavagem de dinheiro,

financiamento do terrorismo ou outro crime financeiro. A UIF investiga a remessa com base nos seus procedimentos internos.

As PEPs confirmadas passarão por uma revisão EDD para determinar o risco que apresentam. Essa revisão deve ser concluída antes que a integração de novos clientes seja concluída. O leitor é responsável por adicionar a EAP à folha de acompanhamento de revisão de casos EDD.

5.3.8. Redução dos riscos

O Comitê deve fornecer quais medidas de mitigação estão em vigor para que o cliente se enquadre na tolerância ao risco da FACILITAPAY. A indicação deve incluir:

• Questões adicionais de due diligence abordando fatores como fonte de recursos/patrimônio, modelo de negócios, atividades comerciais, atividade prevista, objetivo da conta;
• Política de PLD apropriada e/ou outra documentação;
• Ambiente regulatório;
• Licença/registro/licença federal e estadual;
• Extratos bancários;
• Declaração de imposto de renda;
• Cópia de contratos de locação;
• Organograma.

5.3.9. Due diligence para instituições terceirizadas e potenciais investidores

A FACILITAPAY realizará due diligence em clientes para o uso de opções de financiamento de terceiros, bem como em potenciais investidores. Eles não são designados como de alto risco para monitoramento contínuo. Esse processo é uma avaliação exclusiva do risco apresentado para determinar se a ação está dentro da nossa tolerância ao risco ou se controles adicionais de mitigação são necessários.

5.4 ARMAZENAMENTO DE DADOS

A FACILITAPAY armazenará os dados de todos os dados obtidos a fim de identificar os Comerciantes, usuários e parceiros, bem como seus documentos, de acordo com os regulamentos.

Em geral, os registros relacionados ao Programa FACILITAPAY PLD devem ser mantidos por um período de cinco anos a partir da data da transação. Se uma jurisdição específica exigir a retenção de registros por mais de cinco anos, a UIF manterá os registros de acordo com as leis locais. Esse período de retenção inclui toda adocumentação relacionada à UIF, incluindo revisões de alertas, investigações, consultas de aplicação da lei e muito mais. As cópias de todos os relatórios arquivados e o original ou cópias de qualquer documentação comprovativa são conservadas durante cinco anos a contar da data de apresentação desse relatório. A FACILITAPAY retém todos os documentos necessários sob todas as leis e regulamentos e é regida por seu programa de PLD em todas as jurisdições em que opera.

A FACILITAPAY armazenará:

5.4.1. Informações do Cliente

•Todas as etapas para identificar os interessados em estabelecer relações comerciais com a FACILITAPAY ou as razões pelas quais essas medidas foram tomadas;

• Nome completo e data de nascimento das pessoas com quem a FACILITAPAY faz negócios;

•a forma e a origem dos fundos e/ou títulos;

•a forma e o destino dos fundos pagos ou entregues ao cliente ou a outra pessoa em seu nome;

5.4.2. Informações sobre transações

•As transações financeiras executadas pela FACILITAPAY com ou para cada cliente;

•Relatórios de atividades internas e externas suspeitas, motivos para não reportar. Esses documentos deverão ser retidos por 5 (cinco) anos após a elaboração do relatório.

5.4.3. Treinamento

• Materiais e testes;
• Resultados de testes;
• Datas de treinamento;
• Natureza da formação;
• Quem foi treinado;

5.4.4. Tomada de Decisão

Relatórios e reportes ao Nível Executivo de ações e omissões, acompanhados das razões para tal;

Os dados e informações podem ser armazenados das seguintes maneiras:

• Documentos originais;
• Cópias de documentos originais;
• Cópias digitalizadas;
• Formatos eletrônicos;

No final do período de cinco anos, a FACILITAPAY eliminará quaisquer dados pessoais, a menos que a empresa seja obrigada a manter dados que contenham dados pessoais por razões legais ou devido a um processo judicial ou ao indivíduo. A quem os dados pertencem deu o seu consentimento expresso para que sejam conservados.

5.5 MONITORAMENTO

A FACILITAPAY realizará um acompanhamento regular dos clientes e das transações de acordo com a sua Avaliação de Risco. O monitoramento também deve ser feito para garantir que as políticas e os procedimentos sejam implementados corretamente.

Comportamentos do cliente ou problemas com o negócio do cliente podem ser alertas de que uma investigação mais aprofundada pela FACILITAPAY será considerada "Red Flags". Exemplos de bandeiras vermelhas são:

• O cliente é relutante ou evasivo em fornecer informações;

• O estilo de vida do cliente é incompatível com sua fonte de renda;
• A estrutura de negócios do cliente é desnecessariamente complicada;
• Há participação de terceiros sem qualquer motivo válido;
• O cliente passa instruções incomuns;
• Há alterações repetidas ou inexplicadas nas instruções;
• Utilização da conta bancária sem motivo válido;
• O cliente parece desinteressado em preços, comissões, custos, etc.;
• Existem transações diferentes das esperadas do cliente;
• Transferências de fundos inexplicadas.

Se forem identificadas bandeiras vermelhas nos processos de Due Diligence ou monitoramento de clientes, os responsáveis devem notificar o MLRO imediatamente.

A FACILITAPAY utiliza uma solução interna ou monitoramento profundo para identificar qualquer transação incomum ou inesperada que possa levar a suspeitas de lavagem de dinheiro ou financiamento do terrorismo.
Com base no conhecimento da FACILITAPAY sobre o cliente, o acompanhamento buscará:
• Comportamento incomum: mudanças abruptas ou significativas nas atividades de transação, em valor, volume ou natureza, como mudança de beneficiário ou destino de dinheiro;
• Relacionamentos conectados: beneficiários e remetentes comuns em contas e/ou clientes nos quais aparentemente não há relacionamento;
• Países, regiões e instituições de alto risco geográfico: aumentos significativos da atividade ou níveis elevados consistentes de atividade com países, regiões ou instituições de alto risco geográfico;
• Outros comportamentos típicos de lavagem de dinheiro: indícios de possível lavagem de dinheiro, como transações abaixo dos limites relatados, em números redondos ou extremamente complexos;
• Relacionamentos atuais: A FACILITAPAY realizará revisões retroativas e de clientes para garantir que o negócio em andamento seja consistente com o que foi acordado quando o cliente entrou.

A FACILITAPAY realizará o acompanhamento das transações, verificando seus valores, volumes e velocidade. Os alertas mais intensos estarão ligados àqueles que representam maior risco.

Alertas serão disparados para garantir que monitoramos transações e relatamos transações suspeitas.

Todos os novos produtos propostos pela FACILITAPAY devem passar por uma análise de Compliance. A análise visa identificar riscos financeiros específicos e áreas que precisam ser analisadas, para que esses riscos sejam mitigados.

5.5.1. Detecção e comunicação de atividades suspeitas: monitoramento de alertas

A FACILITAPAY utiliza um método de vigilância manual e automatizado para monitorar atividades não maliciosas ou suspeitas; esses métodos de vigilância são aplicados a todos os tipos de transações e clientes em todo o mundo. A UIF é responsável pela análise de alertas emitidos por várias fontes, incluindo a fiscalização do mercado e o acompanhamento de transações. A UIF analisa alertas sobre todos os tipos de transações que ocorrem na plataforma de pagamento, determina os riscos de crimes financeiros representados pelas transações e toma medidas para mitigar os riscos (por exemplo, registrar um relatório de atividades suspeitas).

Clientes de alto risco geralmente exigem documentação e/ou informações adicionais para mitigar parte do risco associado ao seu relacionamento. Ao fazer isso, a devida diligência que foi obtida durante as revisões do EDD garantirá que essas informações e documentação permaneçam atualizadas. Ao coletar essa documentação, uma revisão de EDD pode exceder a data de expiração de uma revisão subsequente em 30 dias, se aprovada por um gerente. Essas extensões devem ser raras e apenas se forem necessárias informações ou documentação adicionais.

5.6 ENCERRAMENTO

É possível que a FACILITAPAY tenha que encerrar uma relação comercial após identificar atividades suspeitas. Mesmo que não haja nenhuma atividade suspeita, o

MLRO local ainda pode recomendar que o relacionamento com comerciantes, parceiros ou outros terceiros seja encerrado com base no risco que eles apresentam.

As recomendações de encerramento de conta serão analisadas e aprovadas. Informações adicionais sobre as etapas de encerramento de conta podem ser encontradas no Processo de Indicação de Encerramento de Conta descrito abaixo.

5.6.1. Processo de Encerramento de Conta

As recomendações de encerramento de conta exigirão aprovação do Gerenciamento de Compliance. Os quadros superiores e os antigosquadros devem ser notificados do encerramento durante os processos normais de comunicação de informações ou diretamente em casos excecionais em que possam surgir riscos adicionais, como o risco reputacional. A aprovação será na forma de comunicação eletrônica ou documentada em atas de reuniões.

Os fechamentos podem ser recomendados com base no risco inerente e residual apresentado por um cliente. Tais riscos incluem o modelo de negócio, atividade profissional, recusa em fornecer documentação ou informação, notícias negativas associadas ao cliente ou outro motivo que coloque o cliente fora da tolerância ao risco da FACILITAPAY.

Você documentará uma recomendação de fechamento na revisão do caso, que detalhará os motivos específicos por trás do fechamento.

5.6.2. Encerramento da conta

A FACILITAPAY tomará medidas para mitigar os riscos associados às contas de clientes envolvidas em atividades suspeitas que não podem ser mitigadas e/ou estão acima da nossa tolerância ao risco. A UIF tem autoridade para fechar contas suspeitas e proibir os clientes de usar qualquer conta FACILITAPAY no futuro. As contas dos clientes envolvidos nas seguintes atividades (lista ilustrativa) serão encerradas e o uso futuro de qualquer conta no FACILITAPAY será proibido:

•Clientes que assediam, ameaçam, intimidam ou tentam coagir, persuadir ou subornar um funcionário para não preencher qualquer formulário de notificação de AML exigido.
•Clientes que intencionalmente enganam os funcionários da FACILITAPAY em relação à identidade ou finalidade da conta ou transações.
•Clientes que são identificados como sujeitos nos relatórios e o Compliance Officer ou AMU faz uma determinação para fechar a conta.
•Clientes designados como clientes proibidos sob programas de detecção de OFAC ou sanções.

5.7 FORMAÇÃO

A FACILITAPAY garantirá que todos os funcionários sejam treinados para garantir que entendam suas obrigações com relação a esta Política e os requisitos para identificar terceiros. Também serão oferecidos treinamentos específicos para diversas áreas, dependendo de suasresponsabilidades específicas e de sua exposição ao risco.

Os funcionários devem estar cientes de que o não cumprimento de suas responsabilidades pode resultar em ações disciplinares e/ou sanções criminais.

5.8 AUDITORIA INTERNA E EXTERNA

Os controlos de criminalidade financeira da FACILITAPAY serão auditados.

A auditoria interna informará a alta administração sobre o status dos controles e das áreas de remediação. Esse relatório deve ser transmitido à entidade reguladora e a terceiros.

O Departamento de Compliance/Jurídico receberá todos os relatórios de auditoria para garantir que os controles necessários sejam implementados de forma eficaz.

5.9 MEDIDAS DISCIPLINARES

Qualquer funcionário que viole esta Política pode estar sujeito a medidas disciplinares de acordo com a Política de Medidas Disciplinares. As violações serão devidamente apuradas, de acordo com os procedimentos do Comitê de Ética, garantindo o anonimato

dos envolvidos. Todos os funcionários são obrigados a cooperar com as investigações em andamento.

5.10 COMUNICAR ATIVIDADE SUSPEITA

Todas as transações de clientes estão sujeitas a monitoramento e revisão constantes. Quando o MLRO local decide que um determinado cliente ou transação deve passar por uma investigação adicional, incluindo assistência adicional, os funcionários devem executá-la, fornecendo informações e solicitações.

Qualquer diretor ou funcionário que suspeite de lavagem de dinheiro deve comunicar imediatamente suas suspeitas à MLRO local por escrito, incluindo detalhes completos. Todos os indícios de suspeita de lavagem de dinheiro são reportáveis, mesmo que cheguem ao conhecimento do funcionário após a transação ter ocorrido, a conta ter sido fechada ou a transação ter sido feita por outra pessoa. Ao fazer o relatório, o diretor ou funcionário terá cumprido com suas obrigações legais. Revelar a uma pessoa suspeita ou a terceiros que uma denúncia é feita ao MLRO ou às autoridades locais, ou que uma investigação está em andamento, é uma violação de conduta, pois pode prejudicar as investigações. Questionar um cliente sobre uma transação específica para saber sua identidade ou definir sua fonte de renda não constitui uma violação. Caso tenha sido feita umadenúncia de atividade suspeita, deve-se tomar muita cautela para que o cliente não tenha conhecimento disso. Se forem identificados sinais suspeitos de lavagem de dinheiro, a transação deve ser bloqueada e não deve prosseguir sem autorização do MLRO local. O MLRO local receberá relatórios relacionados a qualquer suspeita de lavagem de dinheiro ou lavagem de dinheiro real e registrará, investigará e relatará a suspeita às autoridades competentes, se necessário.

A notificação de suspeitas de branqueamento de capitais às autoridades não constitui uma violação da obrigação de confidencialidade com o cliente e fornece salvaguardas importantes à FACILITAPAY. Caso os relatórios não sejam transmitidos às autoridades, todos os detalhes da tomada dessa decisão devem ser registrados. Todas as notificações feitas serão processadas com extrema confidencialidade. No entanto, pode haver circunstâncias em que a FACILITAPAY deve revelar a identidade dos envolvidos na suspeita, como, por exemplo, quando exigido por lei. Neste caso específico, o anonimato

não pode ser garantido. Qualquer funcionário que não relatar uma transação conhecida por ser suspeita de lavagem de dinheiro ou lavagem de dinheiro estará sujeito a medidas disciplinares e legais, a menos que demonstre motivos razoáveis para não relatar ao MLRO local.

Dessa forma, os funcionários são informados de que devem relatar essas transações ao MLRO, por mais superficiais que possam parecer. O funcionário pode discutir a situação com antecedência com seu gerente direto, que pode aceitar a responsabilidade de se reportar ao MLRO. Listamos abaixo exemplos de transações que podem levantar suspeitas de lavagem de dinheiro, mas por si só não necessariamente geram suspeita suficiente para fazer uma denúncia:

•Liquidação de grandes ou incomuns quantias de dinheiro;
•Transações de compra e venda sem um propósito claro ou em circunstâncias incomuns;
•Instruções para direcionar valores para uma conta corrente diferente da previamente acordada ou em nome de terceiros;
•Qualquer transação em que uma das partes não seja conhecida ou que tenha um volume ou frequência atípicos;
• Transações em que o investidor é estrangeiro e ambos estão sediados em países com altas taxas de produção ou tráfico de drogas.

Não é responsabilidade dos funcionários saber ou estabelecer a natureza exata de qualquer crime ou que fundos ou bens específicos são definitivamente o resultado de um crime ou financiamento do terrorismo.

A FACILITAPAY é classificada como instituição obrigada a cumprir as obrigações da Lei 9.613/1998, bem como as demais regulamentações do Banco Central do Brasil, da CVM e do COAF. Todos os requisitos de comunicação serão preenchidos quando a FACILITA PAY obtiver informações durante o curso normal dos negócios em que saiba ou suspeite que uma pessoa ou entidade está sujeita a um congelamento de bens, quando uma pessoa suspeita ou é conhecida por ter cometido uma violação de sanções financeiras, ou se os ativos de uma pessoa ou entidade designada foram congelados.

As informações a serem relatadas incluirão o seguinte:

•as informações ou outros assuntos em que se baseiam conhecimentos ou suspeitas
•qualquer informação que se tenha sobre a pessoa designada ou a pessoa pela qual possa ser identificada
•a natureza e o montante dos fundos/ativos detidos pela FACILITAPAY.

A UIF monitora ativamente funcionários e clientes em busca de atividades suspeitas. Quando a FACILITAPAY sabe, suspeita ou tem motivos para suspeitar que uma transação ou padrão de transações é suspeito, um caso é aberto e atribuído à UIF para uma investigação mais aprofundada.

5.10.1Arquivos/divulgações regulatórias

Se a FACILITAPAY tiver conhecimento ou suspeita de atividades criminosas por parte de clientes ou funcionários, isso deve ser comunicado imediatamente à UIF. A UIF coordenará a investigação, analisará as circunstâncias, reunirá documentação de apoio e determinará se deve ser apresentado um relatório de atividade suspeita (SAR). Se a investigação for considerada suspeita, o caso é encaminhado para uma RAS, que é submetida às autoridades governamentais competentes (dependendo da jurisdição). Os relatórios de atividades suspeitas formam a base do sistema de notificação de crimes financeiros. O RAS fornece informações financeiras que são críticas para a capacidade do regulador e da aplicação da lei de combater o financiamento do terrorismo, lavagem de dinheiro e outros crimes financeiros.

5.10.1.1 Responsabilidade de arquivamento do RAS

Um gerente de UIF ou diretor de Compliance é responsável por tomar a decisão final de se um RAS será ou não arquivado. Se, após a investigação, a UIF determinar que nenhuma SAR foi conduzida, o motivo para não completar o RAS deve ser documentado, e toda a documentação relacionada à investigação é retida por cinco (5) anos após a investigação.

5.10.1.2. Calendário de Relatórios RAS

A FACILITAPAY apresentará um RAS 30 dias a partir da determinação de que a transação em análise é suspeita de acordo com os regulamentos do RAS (na jurisdição relevante). Se nenhum suspeito foi identificado na data de detecção do incidente que requer apresentação, em alguns casos a FACILITAPAY pode atrasar a apresentação de um RAS por mais tempo.

30 dias corridos para identificar um suspeito. Em caso algum os relatórios serão atrasados mais de 60 dias de calendário após a data de deteção inicial de uma transação relatável, salvo especificação em contrário e exigido pela jurisdição aplicável. Em situações que envolvam violações que exijam atenção imediata, como quando uma violação reportável está em andamento, a UIF deve notificar imediatamente uma autoridade policial competente por telefone e apresentar um RAS em tempo hábil.

5.10.1.3. Atividade continuamente incomum ou suspeita

Quando uma atividade suspeita de um cliente FACILITAPAY está em andamento, a FACILITAPAY pode registrar um RAS a cada 120 dias, o que inclui uma revisão de 90 dias da atividade a partir da data da última solicitação de RAS, para atualizar a atividade e os valores. FACILITAPAY adiciona o valor em dólar da atividade relatada anteriormente e o valor em dólar da atividade recente nas RAs mais recentes.

5.10.1.4. Correção/modificação de relatórios

Nas situações em que a FACILITAPAY tenha apresentado um RAS anterior com erros ou tenha descoberto novas informações, a Empresa apresentará um RAS corrigido/modificado se exigido pelos requisitos regulamentares da jurisdição correspondente. Se necessário, um relatório corrigido será arquivado em um RAS previamente arquivado sempre que forem descobertos erros nos dados relatados nesse primeiro RAS. Um relatório corrigido deve ser apresentado em uma RAE previamente arquivada ou em suas versões anteriores sempre que novos dados sobre uma atividade suspeita relatada forem descobertos e as circunstâncias não justificarem a conclusão de um relatório contínuo.

5.10.1.5. Confidencialidade dos relatórios

Todos os RAS registrados pela FACILITAPAY em todas as jurisdições são confidenciais. Nenhum funcionário da FACILITAPAY pode discutir um registro RAS ou a possibilidade de um registro com um cliente ou outro funcionário , a menos que o funcionário esteja envolvido em pesquisas RAS ou tenha outro privilégio legal e não desconfie da transação. Esta obrigação aplica-se não só ao relatório em si, mas também às informações que revelariam a sua existência.

5.10.2. Consultas sobre os serviços responsáveis pela aplicação da lei

A FACILITAPAY pode receber solicitações de investigações legais formais de agências governamentais em todo o mundo em conexão com investigações criminais.
Essas investigações geralmente podem exigir que a FACILITAPAY forneça informações internas relacionadas às contas de clientes, funcionários ou outras áreas operacionais a agências governamentais, como órgãos reguladores e políticos. Nos casos que requerem contato direto com as autoridades policiais, a UIF é responsável por lidar e cumprir as solicitações, incluindo toda a comunicação, coleta e divulgação das informações solicitadas às autoridades policiais.

O tipo mais comum de solicitação é uma intimação ou ordem judicial, que obriga a FACILITAPAY a produzir e divulgar documentos e registros específicos a um órgão governamental autorizado dentro de um determinado período de tempo.

Além das intimações, a FIU também é responsável pelo processamento de todas as outras ordens que a FACILITAPAY possa receber em conexão com investigações governamentais criminais e regulatórias (em todas as jurisdições), incluindo: ordens de confisco de ativos, ordens e pedidos de congelamento, manutenção em aberto, entre outros. Qualquer pessoa associada à FACILITAPAY que receba ou seja notificada com uma intimação ou ordem judicial relacionada ao Programa FACILITAPAY PLD deve entrar em contato imediatamente com a UIF.

5.11 PEDIDOS DE INSTITUIÇÕES DE PAGAMENTO DE TERCEIROS

As solicitações de instituições de pagamento de terceiros ocorrem quando um cliente opta por usar um terceiro para depósitos/retiradas em sua conta FACILITAPAY. Isso se deve a razões legítimas, como obter acesso a uma moeda fiduciária que seu banco atual não oferece. Também pode ocorrer com base na falta de aceitação institucional financeira com base na redução de riscos dentro de jurisdições específicas. Nessas situações, o cliente pode solicitar o uso de um processador de pagamentos terceirizado, banco privado ou corretora. Permitir tais métodos de financiamento pode aumentar o risco do FACILITAPAY.

5.11.1 Seção de Aplicações

Esta seção refere-se aos casos em que uma descrição do pedido do cliente deve ser fornecida.

Exemplo: O cliente deseja depositar na conta de uma subsidiária integral OU o cliente solicita o uso de uma instituição de pagamento terceirizada.

A descrição deve incluir:

• Descrição geral da aplicação;

• Detalhar a instituição de pagamento de terceiros e o motivo da utilização de um terceiro;

•Detalhar qualquer informação que exija mais detalhes da avaliação de risco, como notícias negativas, licenças regulatórias, etc.

Mitigação de riscos
O cliente e a instituição terceirizada são entidades reguladas com licença confirmada? Sim = 0; Não = 10
O cliente ou instituição terceirizada está localizada em um país de alto risco? Sim = 10; Não = 0
O cliente forneceu todos os documentos AML, se houver? Sim = 0; Não = 10; Não aplicável = NA
A FACILITAPAY entende o modelo de negócio e a razão de ser de uma instituição terceirizada? Sim = 0; Não = 10
A FACILITAPAY mantém informações atualizadas sobre o beneficiário final para cumprir os requisitos da UBO? Sim = 0; Não = 10

O cliente forneceu um parecer jurídico fundamentado detalhando a relação e/ou as obrigações de PLD? Sim = 0; Não = 10
A empresa terceirizada é de propriedade do cliente ou vice-versa? Sim = 0; Não = 10
Notícias negativas fueron Identificado durante qualquer .part envolvidas? Sim = 10; Não = 0
O cliente forneceu um comprovante de conta (por exemplo, extrato, notificação bancária, etc.)? Sim = 0; Não = 10
As transações serão exibidas com o nome e o número da conta do cliente? Sim = 0; Não = 10
O cliente ou instituição terceirizada está constituída ou operando em um centro financeiro offshore? Sim = 10; Não = 0
Sob a estrutura da entidade ou jurisdição em que o cliente está registrado, o cliente ocultou seus acionistas beneficiários finais de seus acionistas beneficiários finais? Sim = 10; Não = 0
A jurisdição do banco ou regulador financeiro tem uma reputação ou Histórico de permitir a operação de empresas de fachada/bancos ou envolvimento em outras atividades financeiras ilícitas? Sim = 100; Não = 0
A natureza do negócio declarado no pedido corresponde ao que consta da análise da FACILITAPAY? Sim = 100; Não = 0
Pontuação: **0-30 = Baixo: Geralmente aceitável para aprovação** **40-60 = Médio: documentação adicional pode ser necessária** **70-100 = Alto: documentação/análise adicional necessária** *** Respostas específicas para as perguntas acima podem exigir um análise adicional para garantir que os requisitos de KYC sejam satisfatórios.**

5.12 PEDIDOS DE POTENCIAIS INVESTIDORES

As relações comerciais com potenciais investidores e a FACILITAPAY requerem a devida diligência para garantir que conhecemos a sua identidade, origem dos fundos de investimento e identificamos quaisquer sinais de alerta que possam ser prejudiciais para

a FACILITAPAY. Ao analisar esses pedidos, as seguintes informações devem ser levadas em consideração:

• Identidade do investidor
• Fonte de riqueza
• Outra sociedade comercial conhecida, se aplicável
• Riscos, se aplicável
• Notícias negativas

6. REFERÊNCIAS NORMATIVAS

Código de Conduta FACILITAPAY.

7.PUBLICAÇÃO E DISTRIBUIÇÃO

Qualquer nova política ou modificação de um documento existente deve ser disponibilizada a todas as partes interessadas.

Os documentos públicos podem ser encontrados nos sites da FACILITAPAY.

Maio de 2023.

DocuSigned by:
Stephano Maciel
AA05FE84FFAE436...

Stephano Maciel, CEO

DocuSigned by:
Ricardo Reis
F148429D819247C...

Ricardo Reis, CLO

DocuSigned by:
Daniel Alves
7106FCC1366547B...

Daniel Alves, COO