BlackRock

Política de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo

Data: 2 de Setembro de 2022

1. Objetivo e Escopo

1.1 Objetivo

Esta política foi elaborada para estabelecer princípios e normas robustos que devem ser utilizados pelas unidades de negócios e pessoas jurídicas da BlackRock sujeitas às leis e regulamentações de AML e CFT, a fim de ajudar a se proteger contra tentativas de lavagem de dinheiro e financiamento do terrorismo, seja diretamente por meio da BlackRock ou com relação a quaisquer de seus produtos ou serviços.

Para efeitos desta Política, um cliente da BlackRock pode ser uma pessoa física ou jurídica conforme definição abaixo:

Uma pessoa física ou jurídica que esteja contratando a BlackRock ou um de seus veículos de fundo de investimento para serviços, incluindo, entre outros, consultoria de investimento, gestão de investimento, serviços de avaliação, serviços de consultoria, gestão de riscos, serviços de gestão de transição ou oferta de produtos para distribuição; ou quando a BlackRock estiver vinculada a um terceiro por meio de uma operação de investimento que crie um potencial risco reputacional à BlackRock; ou seus clientes ou fundos.

Esta Política deve ser lida juntamente com as Políticas e os Procedimentos a seguir:

- Política Global de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo
- Política Global de Combate ao Suborno e à Corrupção
- Política Global de Classificação de Risco-País
- Política Global contra Fraude
- Política Global de Pessoas Politicamente Expostas (PEPs)
- Política Global de Sanções
- Política Global de Gestão de Registros
- Política Global de Litígios
- Procedimentos de Exceções da Política de Crimes Financeiros
- Procedimentos de Triagem de Nomes e do Manual de Usuário Bridger
- Diretrizes de Escalonamento e Disposição de Sinais de Alerta

1.2 Escopo

Esta política rege a responsabilidade da BlackRock Brasil Gestora de Investimentos Ltda. (“BlackRock") e seus funcionários (incluindo trabalhadores contingentes) para o cumprimento das leis e regulamentações de AML e CFT. Se a Política Global de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo tiver uma exigência que ultrapasse uma exigência semelhante nesta política, prevalecerá a exigência superior.

A BlackRock deve garantir o cumprimento dos princípios desta política e assegurar que todos os seus funcionários (incluindo trabalhadores contingentes) e unidades de negócios sejam bem informados e

devidamente treinados com relação a seus clientes, suas operações e/ou atividades de negócio no que diz respeito aos riscos de lavagem de dinheiro e financiamento do terrorismo, e a esta política.

2. Sumário Executivo

A BlackRock é a subsidiária brasileira de uma empresa de investimento global conceituada que realiza negócios com integridade e os mais elevados padrões éticos e profissionais. Sem prejuízo e em adição às leis e regulamentações a que está sujeita, na qualidade de subsidiária local de uma instituição financeira regulada do sistema financeiro global, a BlackRock tem a obrigação de manter um programa de prevenção à lavagem de dinheiro ("AML") e financiamento do terrorismo ("CFT"). Esta política sumariza de que forma o programa Global de AML e CFT da BlackRock ("Programa de AML Global" ou o "programa") é constituído e complementa as normas e as exigências desse programa.

Política / Documentos Exigidos e Declarações

3. Adesão à política da BlackRock

A BlackRock tem tolerância zero para qualquer forma de atividade criminal e está comprometida a estabelecer políticas, procedimentos e controles para administrar e mitigar de maneira eficaz os riscos de lavagem de dinheiro e financiamento do terrorismo. Esta política aplica, especificamente, os seguintes princípios essenciais para reger e controlar o risco de AML e CFT:

- Cumprimento das leis e dos regulamentações associadas de AML e CFT;
- Atender a seus clientes e fornecer produtos e prestar serviços consistentes com o apetite de risco de AML da BlackRock;
- Cooperação com, e apoio a, órgãos regulatórios e autoridades policiais, a fim de prevenir, detectar e controlar crimes financeiros de maneira proativa e denunciar quaisquer suspeitas de atividade de lavagem de dinheiro e financiamento do terrorismo;
- Conscientização e entendimento das exigências legais e infrações de AML, bem como do processo e das expectativas estabelecidos nesta Política pelos funcionários da BlackRock (incluindo trabalhadores contingentes); há apoio e treinamento adequados para garantir o cumprimento desta política;
- Adesão às exigências do Programa de AML Global e Estrutura de Gestão de Compliance de AML da BlackRock, conforme definidas nas cláusulas 6 e 7 abaixo; e
- Manutenção de registros abrangente e manutenção de registros de verificações e preocupações relativas à lavagem de dinheiro.

O não cumprimento das exigências das leis e das regulamentações de AML e CFT pode resultar em multas significativas e processo civil ou criminal contra a BlackRock por:
- Não possuir controles internos adequados em vigor;
- Falha por parte de funcionários individuais (incluindo trabalhadores contingentes) em notificar e/ou denunciar quaisquer suspeitas ou ter conhecimento real de uma irregularidade; e
- Dano reputacional e redução da confiança na BlackRock e nos serviços que a empresa presta.

É proibido por lei e esta política que qualquer funcionário (incluindo trabalhadores contingentes) "ajude ou incite" lavagem de dinheiro, financiamento do terrorismo, evasão fiscal, fraude ou quaisquer outras infrações à lei, tais como, entre outros:
- Quando um funcionário (incluindo trabalhador contingente) fornece assistência substancial para um transgressor, informando a um Cliente como estruturar operações para evitar relatório de operação;
- Exigências de manutenção de registros;
- Como burlar controles de AML; ou
- Os funcionários que violarem esta política ou suas políticas e procedimentos relacionados poderão estar sujeitos à ação disciplinar, incluindo possível rescisão do contrato de trabalho.

3.1 Apetite de Risco

A BlackRock pretende fazer negócios somente com investidores respeitáveis, utilizando seus produtos e serviços para fins legítimos e cujas identidades possam ser determinadas e verificadas. Abaixo estão exemplos de relacionamentos de negócio nos quais a BlackRock não tem nenhum apetite para entrar ou manter:

- Pessoas e contas anônimas em que a identidade e/ou a titularidade da entidade não pode ser determinada;
- Pessoas cuja fonte de riqueza e/ou fonte de recursos esteja vinculada a atividades de lavagem de dinheiro de alto risco tais como empresas de prestação de serviços monetários, metais ou pedras preciosas, negócios com necessidades intensas de caixa e atividades de criptomoeda ou dinheiro virtual, em que a fonte de riqueza, recursos ou os beneficiários finais são difíceis de verificar ou validar por meio de fontes independentes.
- Pessoas, cuja fonte de riqueza é conhecida ou suspeita de ser o produto de atividade criminosa ou é conhecida ou suspeita de ser uma organização terrorista ou criminosa, que foram processadas ou condenadas por crimes de lavagem de dinheiro ou infrações de terrorismo, conforme definidos pelas leis às quais a BlackRock esteja sujeita, mas não está limitada a;
- Estabelecer ou manter relacionamentos comerciais com uma pessoa identificada em uma Lista de Sanções ou esteja localizada em um país sancionado ou entidades nas quais o beneficiário final esteja identificado uma Lista de Sanções ou esteja localizado em países sancionados, conforme a Política Global de Sanções; ou
- Bancos de fachada (definido pela FATF como um banco que não possui presença física no país no qual foi constituído e licenciado e que não seja afiliado a um grupo financeiro regulado que esteja sujeito à supervisão efetiva consolidada) e a outras entidades que prestem serviços a bancos de fachada;
- Instituições financeiras não licenciadas, tais como instituição financeira não bancária, casas de câmbio e instituições de transferência monetária;
- Lançar ou alterar produtos e serviços e canais de entrega, sem garantir que haja controles de mitigação adequados.

A BlackRock não efetua nem recebe pagamentos de terceiros em nome de clientes. Além disso, a lista abaixo é uma lista não exaustiva de métodos de pagamento proibidas que estão frequentemente envolvidas em esquemas de lavagem de dinheiro. Esses métodos de pagamento podem incluir pagamentos que não identifiquem o pagador, por exemplo:

- Cheque administrativo e outros cheques bancários;
- Pagamentos por terceiros; e
- Pagamentos de instituições financeiras não bancárias, tais como instituições de transferência monetária e casas de câmbio.

Todos os pagamentos devem ser recebidos pelo cliente na forma de transferência eletrônica de uma conta mantida no nome do cliente em um banco em um local que esteja compatível com o perfil do cliente. As formas aceitáveis e proibidas de pagamento devem ser comunicadas de maneira eficaz aos clientes. Os sinais de alerta sobre clientes e pagamentos que sejam indicativos de lavagem de dinheiro podem ser encontrados no Anexo A abaixo.

Embora fundos mútuos, programas de investimento coletivo e outros “pools de fundos” sejam considerados de menor risco de AML do que produtos bancários tradicionais, esses produtos de gestão de recursos (asset management) podem ser atraentes para lavadores de dinheiro na etapa de ocultação (layering) ou integração da lavagem de dinheiro. O lavador de dinheiro pode ser atraído por alto risco/alta remuneração de veículos de fundo porque o custo do investimento é baixo e a potencial alta remuneração pode acelerar o processo de integração. Da mesma forma, a capacidade de direcionar um investimento (por exemplo, por empréstimo em relação a uma carteira ou via empréstimos lastreados em dinheiro) também podem ser atraentes para um lavador de dinheiro, pois alinha um negócio financeiro legítimo a uma demanda genuína daqueles que possam querer restringir ou confiscar os ativos do lavador de dinheiro

4. Definições

4.1 Lavagem de Dinheiro

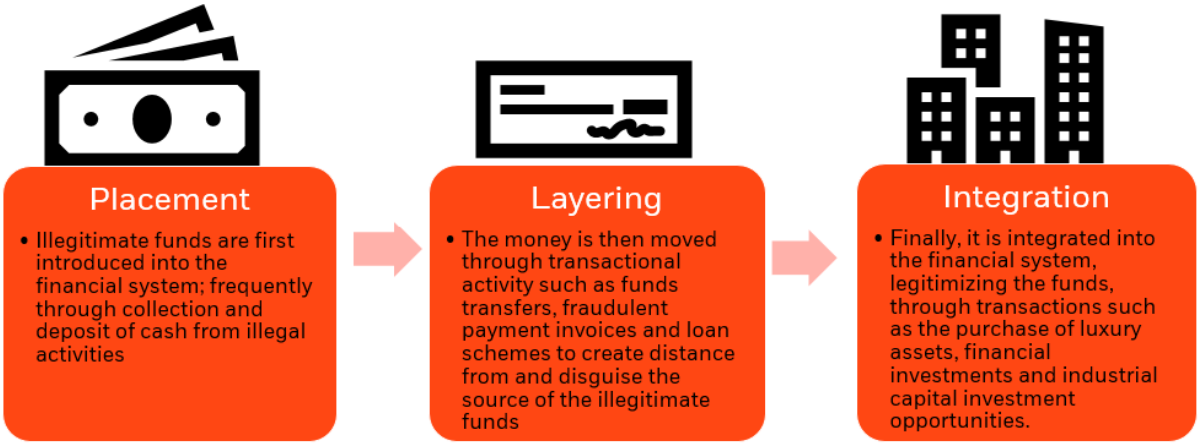
A Lavagem de Dinheiro é um processo pelo qual pessoas físicas ou jurídicas procuram disfarçar ativos financeiros para que tais ativos possam ser utilizados sem detecção de atividade ilícita que os gerou. A Lavagem de Dinheiro, tradicionalmente, envolve três etapas:

a. Colocação (Placement): A primeira etapa da lavagem de dinheiro. Recursos ilícitos são introduzidos no sistema financeiro (por exemplo, casa de câmbio);

b. Ocultação (Layering): A segunda etapa da lavagem de dinheiro e frequentemente denominada como estruturação. Aqui, os recursos ilícitos são movimentados para gerar confusão a fim de separar os recursos ilícitos de sua fonte, (às vezes por transferência eletrônica ou transferência de recursos por meio de diversas contas); e

c. Integração: A terceira etapa da lavagem de dinheiro e envolve a integração de recursos ilícitos no sistema financeiro por meio de operações financeiras complexas até que tais recursos pareçam ser lícitos (por exemplo, por meio de aquisições de imóveis, obras de arte, joias e outros artigos e investimentos de valor elevado).

As três etapas da Lavagem de Dinheiro.



Recursos ilícitos são primeiramente introduzidos no sistema financeiro; frequentemente por meio de arrecadação e depósito de dinheiro originário de atividades ilícitas.	O dinheiro é, posteriormente, movimentado por meio de atividades transacionais, tais como transferências de recursos, faturas de pagamento fraudulentas e esquemas de empréstimo para gerar distanciamento e ocultar a fonte dos recursos ilícitos.	Por último, o recurso é integrado ao sistema financeiro, tornando-o lícito por meio de transações, tais como compra de bens de luxo, investimentos financeiros e oportunidades de investimento de capital industrial.

4.2 Combate ao Financiamento do Terrorismo

Combate ao Financiamento do Terrorismo ("CFT") é um termo dado aos organismos jurídicos internacionais, e programas correspondentes da BlackRock, cuja finalidade é prevenir, detectar e denunciar atividade que constitua ou possa constituir financiamento do terrorismo. Financiamento do terrorismo inclui o financiamento de atos terroristas e de terroristas e organizações terroristas. O esquema de financiamento do terrorismo pode envolver recursos provenientes de atividades ilícitas que são fracionadas para ocultar seu destino final e,

posteriormente, colocadas nas mãos de grupos ou indivíduos terroristas. A motivação por trás do financiamento do terrorismo é, em geral, ideológica, em oposição à busca por lucros, que é geralmente a motivação para a maioria dos crimes associados à lavagem de dinheiro. As leis de combate à lavagem de dinheiro tornaram uma infração penal manusear os recursos de quaisquer crimes graves (frequentemente qualificados) incluindo fraude fiscal, insider dealing, suborno e extorsão, traficantes de armas, drogas e outros tráficos de narcóticos, tráfico humano e financiamento do terrorismo.

4.3 Cliente

- Uma pessoa física ou jurídica que esteja contratando a BlackRock ou um de seus veículos de fundo de investimento para serviços, incluindo, entre outros, consultoria de investimento, gestão de investimento, serviços de avaliação, serviços de consultoria, gestão de riscos, serviços de gestão de transição ou oferta de produtos para distribuição; ou

- Uma pessoa física ou jurídica vinculada à BlackRock por meio de uma operação de investimento na qual exista um potencial risco reputacional à BlackRock ou a seus clientes ou fundos.

5. Exceções à Política

As solicitações de exceções a esta política devem ser submetidas ao Regional Head of Financial Crime. As exceções requerem aprovação do AML officer do grupo ("GAMLO"), do Regional Head of Financial Crime e do Diretor de PLD da BlackRock Brasil ("MLRO"), conforme aplicável. Consulte o Procedimento de Exceção à Política de Crimes Financeiros ("Procedimento de Exceção") para obter detalhes adicionais.

Em algumas jurisdições, a lei ou a regulamentação prevê isenções a determinadas exigências de Due Diligence de Cliente ("CDD"). Quando houver um conflito entre esta política e a Política Global de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo, deverá ser aplicada a norma mais rigorosa, quando permitido por lei, a menos que uma exceção tenha que ser aprovada.

Caso a BlackRock Brasil não seja capaz de cumprir esta política, a BlackRock Brasil deve notificar o respectivo Regional Head of Financial Crime, que irá consultar o MLRO da BlackRock Brasil e o Global Head of Financial Crime (quando aplicável) para solucionar o conflito e identificar uma conciliação razoável.

6. Programa e Normas de Compliance de AML Global

6.1 Visão Geral do Programa de AML CFT Global ("Programa de AML Global"):

A fim de cumprir as leis e as regulamentações de AML aplicáveis, a BlackRock, Inc., bem como suas subsidiárias, afiliadas e entidades controladas relevantes estabeleceu e mantém um Programa de AML Global (o "Programa") para ajudar a proteger tanto seus clientes quanto a empresa contra riscos associados à lavagem de dinheiro e outros crimes financeiros. O Programa de AML Global fornece um sistema consistente de controles para identificar e mitigar riscos de lavagem de dinheiro, de acordo com as leis e as regulamentações aplicáveis.

6.2 Elementos do Programa de AML Global

Alguns dos principais elementos que consistem no Programa de AML Global são compostos, entre outros, por:

- Diretores e/ou MLROs de Compliance de AML Globais, Regionais e Locais;
- Estrutura de governança, incluindo políticas e procedimentos por escrito, e um sistema de controles internos desenvolvido para avaliar e fornecer uma supervisão baseada em risco dos riscos de lavagem de dinheiro e financiamento do terrorismo, e promover uma cultura de compliance;
- A aplicação, internamente ou via de terceiros prestadores de serviços, de procedimentos de CDD razoavelmente desenvolvidos para identificar e verificar todos os clientes e, quando aplicável, beneficiários finais,

fonte dos recursos e a natureza e a finalidade pretendida do relacionamento comercial, na medida do justificável pelo risco de lavagem de dinheiro ou financiamento do terrorismo ou conforme exigido pela regulamentação;
- Estrutura de avaliação de risco desenvolvido para avaliar periodicamente o nível de exposição ao risco de lavagem de dinheiro enfrentado pela BLACKROCK.
- Sistemas e controles internos desenvolvidos para deter, prevenir e denunciar possíveis infrações a esta Política, à Política Global de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo e às leis e regulamentações de AML;
- Treinamento anual em toda a empresa;
- Estrutura de monitoramento e investigação que avalia controles críticos de AML e prevê a detecção e denúncia oportuna de atividade suspeita; e
- Manutenção de registros.

6.3 Governaça e Supervisão do Programa de AML Global

A administração sênior da BLACKROCK, conforme representada pelo Comitê de Gestão de Risco Empresarial ("ERMC") é responsável pela supervisão do Programa de AML Global e risco empresarial de toda a empresa. O ERMC escalona os casos para Comitê de risco do Conselho de Administração e Comitê de Auditoria da BLACKROCK para análise e aprovação, conforme apropriado.

A governança do Programa de AML Global é fornecida pelo Comitê Global de Risco-País e Crimes Financeiros ("GFCCRC") que reporta no ERMC. O GFCCRC é responsável por estabelecer e promover um Programa Global de Compliance de Crimes Financeiros robusto e sustentável, incluindo o Programa de AML Global. O GFCCRC conta com o apoio do subcomitê do Comitê de Supervisão de Combate à Lavagem de Dinheiro ("AMLOC"), que supervisiona as políticas e as normas de AML Global. O AMLOC fornece uma estrutura de governança em âmbito empresarial para garantir que seja criada uma estrutura de gestão de risco de AML baseada em risco e que recursos necessários sejam aplicados para apoiar o Programa de AML Global.

6.4 Execução do Programa de AML Global

A estrutura de gestão de risco de compliance de AML Global da BLACKROCK é baseada em um modelo de três linhas de defesa, conforme abaixo descrita:

- Primeira Linha de Defesa (Negócios): A primeira linha de defesa também é responsável e presta contas pelos controles internos e implementação de ações corretivas para abordar as deficiências nos controles.
- Segunda Linha de Defesa (Compliance): A segunda linha de defesa é uma função de supervisão independente e é responsável por elaborar, implementar e manter um programa de compliance de gestão de risco empresarial, e ferramentas para avaliar e administrar riscos em nível empresarial. A segunda linha de defesa também trabalha junto com a primeira linha de defesa para avaliar riscos e estabelecer políticas e diretrizes, conforme necessário. Além disso, como parte das funções de controle independentes, a segunda linha de defesa fornece consultoria, monitora os controles operacionais da primeira linha de defesa para administrar riscos e, quando aplicável, fornece treinamento, conforme a necessidade.
- Terceira Linha de Defesa (Auditoria): A Auditoria Interna analisa, de maneira independente, as atividades das primeiras duas linhas de defesa com base em um plano e metodologia de auditoria baseada em risco. As avaliações ou análises independentes também podem ser realizadas por terceiros externos, a fim de garantir consistência com o apetite de risco da empresa.

Todas as três linhas de defesa são responsáveis por promover uma cultura de compliance robusta e ética.

6.5 Funções e Responsabilidades

O Programa de AML Global abrange um conjunto distinto de funções e responsabilidades, a fim de garantir a implementação e a manutenção do programa.

6.5.1 Diretor de AML do Grupo ("GAMLO")

O Head Global de Compliance de AML atua como o Diretor de AML Global ("GAMLO") da BLACKROCK, que supervisiona o Programa de AML Global da BLACKROCK e é responsável por administrar os riscos de compliance de lavagem de dinheiro de AML da empresa por meio de implementação e manutenção de monitoramento e controles adequados.

As responsabilidades do GAMLO incluem, entre outros:

- Supervisionar a operação do programa (incluindo Supervisão da avaliação de risco de AML em toda a empresa);
- Coordenar e comunicar as exigências de compliance de AML e CFT Global;
- Fornecer atualizações e orientação por meio da estrutura de Governança da BLACKROCK com relação aos esforços de compliance de AML, incluindo quaisquer resultados da auditoria do programa global e o status de quaisquer ações corretivas;
- Apoiar a adesão às políticas e aos procedimentos de AML, em coordenação com os heads regionais de Crimes Financeiros e Diretores de compliance de AML locais ("AMLCOs") ou MLROs;
- Coordenar com stakeholders auditorias relevantes e inspeções regulatórias;
- Comunicar-se com agências regulatórias e emitir relatórios de atividades suspeitas (SARs) ou seu equivalente; e
- Fornecer treinamento anual de AML e CFT para todos os funcionários (incluindo trabalhadores contingentes).

6.5.2 Head Regional de Crimes Financeiros

O Head Regional de Crimes Financeiros é responsável por supervisionar a implementação regional do programa de Crimes Financeiros em sua região. Suas funções e responsabilidades incluem, entre outros:

- Implementação regional das exigências do Programa de AML e CFT Global, incluindo por meio de políticas, procedimentos e documentação relacionada, por escrito e específicos à região, incluindo a conclusão das Avaliações de Risco, conforme necessário;
- Fornecer orientação e apoio aos AMLCOs com relação a seus respectivos programas nessa região;
- Apoiar a análise e a implementação de alterações regulatórias locais em programas de AML local; e
- Escalonar compliance de AML e outros assuntos de crimes financeiros, incluindo a adequação de recursos para manter programas robustos de AML local por meio de estrutura de governança, quando necessário e apropriado.

6.5.3 Diretor de Compliance de AML Local/Diretor de Denúncia de Lavagem de Dinheiro

Cada Programa de AML local deve designar um Diretor de Compliance de AML Local ("AMLCO") exclusivo, também denominado em determinados países como Diretor de Denúncia de Lavagem de Dinheiro ("MLRO"), conjuntamente referidos nesta política como AMLCO.

As responsabilidades do AMLCO incluem, entre outros:

- Estabelecer e implementar um Programa de AML Local que seja compatível com as exigências desta política, bem como quaisquer exigências regulatórias e legais locais aplicáveis.
- Elaborar e implementar um Programa de AML Local que reduza os riscos de AML consistente com o apetite de risco de AML da BLACKROCK e que atenda as exigências regulatórias locais e esteja consistente com as normas locais do programa referidos nesta política.
- Receber divulgações sobre atividade de lavagem de dinheiro ou financiamento do terrorismo e garantir que a emissão oportuna de relatórios de atividades suspeitas, e fornecer notificações internas de atividade suspeita, conforme apropriado. O AMLO determinará se um relatório deve ser feito para as

autoridades regulatórias em consulta com o Head Regional de Crimes Financeiros pertinente, juntamente com o GAMLO e o Head Global de Crimes Financeiros, se apropriado.

- Fornecer apresentação de relatórios regulatórios ou retornos de maneira pontual e precisa, quando exigido;
- Coordenar comunicações de programa de AML local, interna e externamente, e ser o ponto de contato central para os respectivos reguladores e funcionários com relação a dúvidas sobre AML e CFT, inspeções regulatórias e apresentação de relatórios periódicos; e
- Quando exigido pela legislação local, a administração sênior de cada pessoa jurídica deve aprovar a Política de AML local e fornecer supervisão do Programa de AML local.

6.5.4 Gerentes de Negócio

Os Gerentes de Negócio são responsáveis por supervisionar e fiscalizar as atividades dos funcionários sob seu gerenciamento para garantir que tais atividades estejam alinhadas com os objetivos da empresa.

- Algumas de suas responsabilidades incluem, entre outros:
- Trabalhar estreitamente com os respectivos AMLCO, Head Regional de Crimes Financeiros e GAMLO relevantes, a fim de garantir que as leis e regulamentações estejam sendo cumpridas;
- Atuar como ponto de escalonamento de assuntos relacionados temas, questões e desafios recorrentes de risco e/ou controle de compliance de AML em suas áreas de negócio ou áreas de responsabilidade operacional; e
- Promover uma cultura de compliance junto a todos os funcionários sob seu gerenciamento e fornecer apoio aos funcionários, conforme necessário.

6.6 Normas do Programa de AML Global

A conformidade com o Programa de AML Global da BLACKROCK requer conscientização, entendimento e participação ativa de todos os funcionários da BLACKROCK. A gestão de negócios é responsável por estabelecer uma cultura adequada de compliance que enfatize e promova um entendimento dos riscos gerais de lavagem de dinheiro apresentados por cada relacionamento com clientes e atividade de investimento.

Um conjunto de Normas de AML ("Normas") foi desenvolvido e implementado para cobrir os 5 (cinco) principais pilares do Programa que inclui:

- **Due Diligence: Due Diligence de Cliente (CDD) e Due Diligence Reforçada (EDD)**
  - Descreve os elementos dos procedimentos de KYC da BLACKROCK e fornece diretrizes para obter e corroborar a identificação de clientes e outras informações. Um componente crítico desta estrutura baseada em risco é a realização de uma avaliação de risco do cliente no estabelecimento inicial de uma relacionamento para determinar o nível adequado de Due Diligence de Cliente ("CDD") a ser aplicada. Em algumas jurisdições, as leis e regulamentações locais podem precisar de isenções às exigências de CDD; contudo, a política da BlackRock é realizar CDD em todos os clientes.
  - Deve-se dar consideração adicional para classificar clientes como de alto risco, cujas atividades sejam particularmente vulneráveis à lavagem de dinheiro e financiamento do terrorismo. Futuros clientes que celebrem um contrato diretamente com a BLACKROCK que sejam classificadas como de alto risco requerem medidas de Due Diligence Reforçada ("EDD") juntamente com aprovação adicional antes da conclusão do processo de integração (onboarding).

- **Governança e Supervisão, incluindo Inspeções Regulatórias**

  - Descreve as exigências para uma boa estrutura de governança para um programa de AML/CFT eficaz. Essencial para uma boa governança é um conselho de administração comprometido e uma administração sênior que estabeleça o tom adequado nas altas instâncias, contratando um diretor de

AML qualificado e equipando adequadamente as três linhas de defesa que são essenciais para a estrutura geral de gestão de riscos da empresa.

- **Estrutura de Controle Interno, incluindo Exigências de Políticas e Procedimentos**

  - Fornece normas e orientação sobre a implementação de políticas, procedimentos e controles internos de AML/CFT elaborados para mitigar os riscos inerentes identificados pela avaliação de riscos. As políticas e os procedimentos de AML devem estar por escrito e atender à finalidade de prevenir, detectar e denunciar atividade potencialmente suspeita, cumprindo as leis locais e estabelecendo um ambiente sólido de controle interno e gestão de riscos.

- **Avaliação de Risco**

  - Descreve os elementos de identificação e avaliação do nível de riscos de lavagem de dinheiro enfrentados pela empresa. O processo inclui uma avaliação dos riscos de lavagem de dinheiro e financiamento do terrorismo nessas categorias de risco específicas, fatores de riscos inerentes que impactam o perfil de risco de AML da empresa (por exemplo, produtos, serviços, clientes e localizações geográficas da BLACKROCK atendidas por suas áreas de negócios), riscos residuais e outros risos que são únicos à empresa, ao negócios ou à pessoa jurídica da BLACKROCK.
  - Os resultados da avaliação de risco devem ser utilizados pela administração para tomar decisões fundamentadas sobre o apetite de risco e implementação de esforços de controle e garantir que os recursos e as prioridades estejam alinhados com os riscos da empresa.

- **Supervisão, Monitoramento e Relatório de Operações**

  - Descreve as expectativas quanto ao monitoramento de cliente e atividade de investimento para verificação de atividade potencialmente suspeita, juntamente com medidas a serem tomadas para denunciar essa atividade quando houver uma obrigação legal de fazê-lo. Todos os funcionários têm uma obrigação segundo esta política de submeter qualquer atividade potencialmente suspeita para a equipe de Crimes Financeiros.

Essas Normas estabelecem as exigências mínimas necessárias para atender a cada Programa de AML Local e as funções e responsabilidades do AMLCO.

Cada Norma, incluindo esta política, deve ser lida juntamente com a Política Global de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo.

6.6.1 Aprovações de Cliente de Alto Risco

Qualquer futuro cliente classificado como de alto risco deve ser encaminhado ao(s) Comitê(s) pertinente(s) ou grupo delegado para que seja analisado e aprovado antes da conclusão da integração (onboarding). A integração (onboarding) de futuros clientes de alto risco somente estará concluída depois que todas as aprovações do negócio e de conformidade forem obtidas, conforme descrito nos Termos de Referência do GFCCRC.

Novos clientes domiciliados ou com afiliadas em países “Consultar” conforme a Matriz Global de Risco do País da BLACKROCK devem ser aprovados pelo GFCCRC antes da conclusão do processo de integração. Um link para a Matriz Global de Risco do País da BLACKROCK está disponível na intranet.

Toda identificação de cliente e documentação de verificação relevantes devem ser obtidas para clientes antes de a BLACKROCK aceitar quaisquer recursos de clientes.

7. Monitoramento e denúncia de atividade suspeita

A BlackRock monitora seus clientes e suas atividades de investimento para verificar atividade potencialmente suspeita e denunciará essa atividade, quando exigido. Todos os funcionários têm uma obrigação segundo esta política de submeter qualquer atividade potencialmente suspeita para a equipe de Crimes Financeiros ou para o MLRO local. Os Anexos A e B são listas não exaustiva de potenciais sinais de alerta.

7.1 Encaminhamento de suspeitas na BlackRock

Caso um funcionário (incluindo trabalhador contingente) tenha conhecimento ou suspeite de um crime financeiro ou outra atividade potencialmente suspeita, ele tem obrigação de informar a equipe de Crimes Financeiros ou o MLRO local. Os procedimentos locais de denúncia devem ser seguidos e, quando permitido, uma notificação deverá ser enviada ao GAMLO e ao Head Regional de Crimes Financeiros. Uma notificação pode incluir o preenchimento de um Formulário de Encaminhamento de Atividade de Crimes Financeiros Potencialmente Suspeita (disponível no site de Recursos de Compliance e no Anexo C, ou entrando em contato com um membro da equipe de Crimes Financeiros, conforme apropriado.

As denúncias e as notificações devem ser mantidas confidenciais e os funcionários (incluindo trabalhadores contingentes) devem ter cuidado ao se comunicar com clientes e não divulgar a existência de uma notificação ou a preocupação de atividade suspeita.

Uma divulgação não autorizada pode configurar crime. Muitos países veem a "delação" de um cliente ou quaisquer esforços de impedir uma investigação oficial como uma infração penal. Quando aplicável, essas restrições devem ser descritas de maneira clara nas políticas do país ou pessoa jurídica pertinentes. Depois de reportar uma preocupação, os funcionários que prestam atendimento a clientes devem coordenar com a equipe de Crimes Financeiros antes de continuarem a manter contato com o cliente.

7.2 Denúncia de atividade suspeita às autoridades apropriadas

O Diretor de Compliance tem a responsabilidade final de avaliar quaisquer denúncias internas de atividade suspeitas feitas, determinar qual investigação adicional é necessária e denunciar quaisquer questões de preocupação de maneira pontual aos órgãos externos, incluindo aos órgãos governamentais, reguladores e autoridades policiais, em linha com as leis e regulamentações locais. O Diretor de Compliance poderá delegar atividades de investigação; contudo, a decisão final de denúncia e a apresentação das atividades permanecem com o Diretor de Compliance.

O GAMLO deve ser notificado pelo Diretor de Compliance pertinente sobre quaisquer Relatórios de Atividade Suspeita (SARs) ou relatório equivalente apresentado por eles. Na medida em for permitido pelas leis e regulamentações, essas informações devem ser compartilhadas. O GAMLO determinará se o assunto acarretará uma necessidade de denunciar em outra jurisdição ou para outro regulador ou autoridade policial.

7.3 Solicitações Externas de Informações

Quando a BlackRock receber solicitações para fornecimento de informações relacionadas à AML por parte dos reguladores ou autoridades policiais, a pessoa deve notificar o Diretor de Compliance imediatamente. O Diretor de Compliance, então, notificará prontamente o Head Regional de Crimes Financeiros e o GAMLO e/ou o departamento de Engajamento e Auditoria Regulatória, que avaliará e responderá às solicitações em consulta e coordenação com o departamento Jurídico, quando apropriado.

8. Supervisão de terceiros que realizam funções de AML

A BlackRock terceiriza determinadas exigências ou funções de AML para agentes de transferência ou outros terceiros, tais como integração e manutenção de clientes, que investem nos fundos combinados administrados e

mandatos segregados da BlackRock. Nessa estrutura, a BlackRock detém a responsabilidade final pelas obrigações delegadas e assumidas em seu nome e deve garantir que o prestador dos serviços terceirizados tenha implementado sistemas, controles e políticas adequadas de AML e CFT e que eles atendam às exigências desta política e de quaisquer exigências do Programa Local.

A equipe de Crimes Financeiros deve monitorar se os terceiros estão cumprindo suas responsabilidades, conforme estabelecido na política e nas normas de gestão de fornecedores da BlackRock e conforme descrito nesta política. Além disso, a equipe de Crimes Financeiros faz parceria com a RQA na prestação de certas atividades de avaliação de risco para terceiros potenciais e existentes, incluindo vendedores, ao longo do ciclo de vida da relação com terceiros, tal como descrito na Política de Gestão de Risco de Terceiros da BLACKROCK.

9. Treinamento

A fim de atender às exigências regulatórias, legais e da política e para ajudar a garantir que os funcionários da BlackRock, incluindo trabalhadores contingentes, leiam e entendam essa política, especialmente no que diz respeito às suas funções, responsabilidades e equipe. Será fornecido um treinamento anual obrigatório de Crimes Financeiros, por computador, em toda a empresa para todos os funcionários e trabalhadores contingentes. Este treinamento cobre as principais áreas de risco de Crimes Financeiros de Compliance como parte do currículo mais vasto de Crimes Financeiros e o material é regularmente revisto e atualizado. Além dos treinamentos anuais por computador, o Regional Heads of Financial Crime e o MLRO local é responsável por determinar se treinamentos complementares opcionais são ou não necessários para endereçar as necessidades de treinamento local, específico ao negócio ou baseado na função.

Todos os novos funcionários devem concluir o treinamento de AML [e CFT] pertinente dentro um período razoável após ingressar na empresa, geralmente de 30 dias, mas nunca superior a 60 dias.

10. Teste Independente

Quando for necessário um teste independente, o Programa de AML Local será revisado periodicamente ou conforme determinado pelas leis e regulamentações locais pertinentes. Essa revisão ou auditoria será realizada por uma parte independente, normalmente, ou pelo departamento de Auditoria Interna da BlackRock ou por uma empresa externa que seja independente dos responsáveis pelo Programa de AML Global. O teste, quando aplicável, deve ser realizado por meio de uma abordagem baseada em risco e quaisquer constatações resultantes de uma revisão independente devem ser documentadas por escrito e reportadas à administração sênior da respectiva unidade de negócio e/ou da BlackRock no prazo de 60 dias da conclusão da avaliação.

11. Manutenção de registro

A manutenção de registro é uma parte essencial da trilha de auditoria que as regulamentações procuram estabelecer para auxiliar a investigação e garantir que fundos criminosos sejam mantidos fora do sistema financeiro. As empresas devem manter registros referentes a verificações e operações de clientes como prova do trabalho que elas realizaram para cumprir com as exigências. Consulte a Política Global de Gestão de Registros da BLACKROCK para obter orientação adicional.

- Informações e Operações de Clientes: A BlackRock deve manter comprovação de verificação de clientes e documentos comprobatórios por um período mínimo de cinco anos ou conforme obrigado pelas exigências locais após o encerramento do relacionamentos. Detalhes completos de operações devem ser mantidos por um período mínimo de cinco anos a partir da criação; processos pendentes e/ou exigências de país local.
- Registros de Treinamento: Detalhes completos de treinamento fornecido a funcionários devem ser mantidos indefinidamente, incluindo as datas do treinamento, a natureza do treinamento, os nomes dos funcionários que receberam o treinamento e os resultados de quaisquer testes realizados pelos funcionários;
- SARs ou equivalente e Documentação Comprobatória: Cópias de quaisquer SARs ou documento equivalente apresentadas pela BlackRock ou em seu nome devem ser mantidos pelo Diretor de Compliance, juntamente com

as versões originais de toda a documentação comprobatória. Esses registros devem ser mantidos por um período de cinco anos, a partir da data da apresentação de um SAR ou documento equivalente e deverão ser disponibilizados ao órgão regulatório mediante solicitação;

- Avaliações de Risco Periódicas: Inclui uma avaliação dos controles implementados que individualmente ou em combinação ajudam a mitigar os riscos de lavagem de dinheiro e financiamento do terrorismo e devem ser mantidas por um período de, no mínimo, cinco anos ou conforme obrigados pelas exigências locais; e
- Documentação Legal/Regulatória: Inclui documentação relacionada a investigações, violações, renúncias e dispensas, que deve ser mantida por um período de, no mínimo, cinco anos ou conforme obrigado pelas exigências locais.

Os órgãos regulatórios e as autoridades policiais podem, de tempos em tempos, solicitar cópias de nossos registros de CDD e de outros materiais relevantes. Quaisquer dessas solicitações feitas diretamente a um funcionário devem ser enviadas ao MLRO local imediatamente. O MLRO, então, notificará prontamente o Regional Head of Financial Crime, o GAMLO e/ou o departamento de Regulatory Engagement and Audit, que avaliará e responderá às solicitações em consulta com o departamento Jurídico, quando apropriado.

O GAMLO, Head Regional de Crimes Financeiros e o Diretor de Compliance devem, de maneira oportuna, ter acesso a todos os registros e outras informações relevantes necessárias para cumprir suas responsabilidades.

Anexo A: Sinais de Alerta de Lavagem de Dinheiro

Os exemplos a seguir têm um propósito ilustrativo e não são uma lista exaustiva de sinais de alerta. Esses exemplos têm o propósito de descrever os potenciais riscos associados ao relacionamento comercial, à(s) operação(ões) envolvida(s) ou a uma combinação de ambos. A mera presença de um sinal de alerta não é por si só evidência de atividade criminosa. Antes da integração (onboarding) e durante a revisão da(s) conta(s) do(s) cliente(s), deverá ser realizada análise adicional para determinar se a atividade é ou não suspeita ou que não parece ser um negócio ou finalidade legal razoável. Deve-se levar em conta, entre outros:

- Qual é o relacionamento exato com o cliente/entidade (por exemplo, cliente direto, entidade afiliada ao cliente)?
- Quais são os riscos que o cliente representa para a BlackRock (por exemplo, riscos de lavagem de dinheiro)?
- Qual seria a consequência para a BlackRock se recursos ilícitos, uma potencial atividade ou operação ilícita for processada para o cliente ou a entidade?

Clientes que Fornecem Informações Insuficientes ou Suspeitas incluem, entre outros:

- Um cliente utiliza documentos de identificação incomuns ou suspeitas que não podem ser prontamente verificados;
- Um cliente fornece um número de CPF após ter utilizado anteriormente um número de Previdência Social;
- Um cliente utiliza números de CPF diferentes com variações de nome;
- Uma empresa se mostra relutante, ao abrir uma nova conta, em fornecer informações completas sobre a natureza e a finalidade de seus negócios, previsão de atividade da conta, relacionamentos bancários anteriores, os nomes de seus diretores e conselheiros ou informações sobre a localização da empresa;
- O telefone residencial ou comercial do cliente está desligado;
- Os antecedentes do cliente diferem do que se previa com base em suas atividades comerciais;
- Um cliente faz operações grandes ou frequentes e não possui registros de experiência profissional passada ou presente; e
- Um cliente é um trust, empresa de fachada ou Empresa de Investimento Privado que se mostra relutante em fornecer informações sobre partes controladoras e beneficiários subjacentes. Os beneficiários finais podem contratar serviços de constituição nomeados para estabelecer empresas de fachada e abrir contas bancárias para essas empresas de fachada e, ao mesmo tempo, blindar a identidade do proprietário.

Esforços para Evitar a Exigência de Apresentação de Relatórios ou Manutenção de Registros incluem, entre outros:

- Um cliente ou grupo tenta persuadir um funcionário do banco a não apresentar o relatório exigido ou a manter os registros exigidos;
- Um cliente se mostra relutante em fornecer informações necessárias para apresentar um relatório obrigatório, para que um relatório não seja apresentado, ou para prosseguir com uma operação após ser informado que o relatório deve ser apresentado;
- Um cliente se mostra relutante em fornecer identificação ao adquirir instrumentos negociáveis em valores passíveis de registro;
- Uma empresa ou um cliente pede isenção das obrigações de apresentação de relatórios ou manutenção de registros;
- Uma pessoa utiliza de maneira costumeira o caixa eletrônico para fazer diversos depósitos bancários abaixo de um limite especificado;
- Um cliente deposita fundos em diversas contas, geralmente em valores inferiores a US$3.000, que são subsequentemente consolidados em uma conta máster e transferidos para fora do país, particularmente para ou por meio de um local de preocupação específica (por exemplo, países designados pelas autoridades nacionais e Força Tarefa de Ação Financeira Contra Lavagem de Dinheiro (FATF) como países e territórios não colaboradores); e

- Um cliente acessa um cofre após concluir uma operação envolvendo uma grande quantidade de dinheiro ou acessa o cofre antes fazer depósitos de dinheiro estruturados no valor de ou pouco inferior a US$10.000, a fim de burlar as exigências de apresentação de CTR.

Transferências de recursos incluem, entre outros:

- Diversas transferências de recursos são enviadas em grandes valores, round dollar e centenas de dólares ou milhares de dólares;
- A atividade de transferência de recursos ocorre de ou para um paraíso fiscal financeiro, ou de ou para um local geográfico de risco mais elevado sem um motivo comercial aparente ou quando a atividade é incompatível com o negócio ou histórico do cliente;
- A atividade de transferência de recursos ocorre de ou para uma instituição financeira localizada em uma jurisdição de risco mais elevado distante das operações do cliente;
- Recebimento de diversas pequenas transferências de recursos, ou depósitos são feitos utilizando cheques ou ordens de pagamento. Quase que imediatamente, todos ou a maioria das transferências ou depósitos são enviados para outra cidade ou país de maneira incompatível com o negócio ou histórico do cliente.
- Recebimento de grandes transferências de recursos em nome de um cliente estrangeiro com pouca ou nenhuma razão explícita;
- A atividade de transferência de recursos é inexplicável, recorrente ou demonstra padrões incomuns;
- Pagamentos ou recebimentos sem qualquer vínculo aparente com contratos, produtos ou serviços legítimos são recebidos;
- As transferências de recursos são recebidas da mesma pessoa de ou para diferentes contas; e
- As transferências de recursos contêm conteúdo limitado e faltam informações da parte relacionada.

Atividade Incompatível com o Negócio do Cliente inclui, entre outros:

- Os padrões de operação de câmbio de um negócio demonstram uma alteração repentina incompatível com as atividades normais;
- Um grande volume de cheques administrativos, ordens de pagamento ou transferências de recursos é depositado em uma conta, ou adquiridos por meio de uma conta, quando a natureza do negócio do correntista parece não justificar tal atividade;
- Um negócio de varejo tem padrões drasticamente diferentes de depósitos de dinheiro provenientes de negócios similares no mesmo local geral;
- Transferência de recursos incomuns ocorrem entre contas relacionadas ou entre contas que envolvam os mesmos titulares ou titulares relacionados;
- O proprietário tanto de um negócio de varejo quanto de um serviço de desconto de cheques não pede dinheiro ao depositar cheques, indicando possivelmente a disponibilidade de outra fonte de dinheiro;
- Os produtos ou serviços adquiridos pela empresa não correspondem com a linha de negócio declarada pelo cliente; e
- Os pagamentos de produtos ou serviços são feitos por cheques, ordens de pagamento ou saques bancários não sacados da conta da entidade que fez a compra.

Atividade de Empréstimo inclui, entre outros:

- Empréstimos garantidos por ativos cedidos em garantia detidos por terceiros não relacionados ao tomador;
- Empréstimos garantidos por depósitos ou outros ativos prontamente negociáveis tais como valores mobiliários, particularmente quando de propriedade de terceiros aparentemente não relacionados;
- Inadimplência do tomador em um empréstimo garantido por dinheiro ou qualquer empréstimo que seja garantido por ativos que sejam prontamente conversíveis em dinheiro;
- Empréstimos que são realizados para um terceiro ou que são pagos em nome de um terceiro sem uma explicação razoável;
- Para garantir um empréstimo, o cliente adquire um certificado de depósito utilizando uma fonte de recursos desconhecida, particularmente quando os recursos são fornecidos por meio de dinheiro ou diversos instrumentos monetários; e

- Empréstimos sem uma finalidade de negócio legítima, fornecem ao banco taxas significativas por assumir pouco ou nenhum risco, ou tendem a encobrir a movimentação de recursos (por exemplo, empréstimos realizados a um tomador e imediatamente vendidos para uma entidade relacionada ao tomador).

Financiamento de Operações Comerciais incluem, entre outros:

- Produtos embarcados que sejam incompatíveis com a natureza do negócio do cliente (por exemplo, uma empresa de aço que começa a lidar com produtos de papel, ou uma empresa de tecnologia da informação que começa a lidar com grandes volumes de produtos farmacêuticos);
- Clientes que estejam conduzindo negócios em jurisdições de risco mais elevado;
- Clientes que embarquem produtos por meio de jurisdições de risco mais elevado, incluindo trânsito por meio de países não colaboradores;
- Clientes envolvidos em atividades potencialmente de risco mais elevado, incluindo atividades que possam estar sujeitas a restrições de exportação/importação (por exemplo, equipamentos para organizações militares ou policiais de governos estrangeiros, armamentos, munições, misturas de produtos químicos, artigos de defesa classificados, dados técnicos sensíveis, materiais nucleares, gemas preciosas ou determinados recursos naturais tais como metais, minério e petróleo bruto);
- Evidente superfaturamento ou subfaturamento de produtos e serviços;
- Evidente declaração falsa de quantidade ou tipo de mercadorias importadas ou exportadas;
- A estrutura da operação parece ser desnecessariamente complexa e destinada a encobrir a verdadeira natureza da operação;
- O cliente solicita pagamento de recursos para um terceiro não relacionado;
- Locais de embarque ou a descrição das mercadorias inconsistentes com a carta de crédito; e
- Cartas de crédito com alterações significativas sem justificativa razoável ou alteração do beneficiário ou local de pagamento. Quaisquer alterações nos nomes de partes devem desencadear uma análise adicional de OFAC.

Atividade de Empresa de Fachada inclui, entre outros:

- Um banco é incapaz de obter informações suficientes ou as informações estão indisponíveis para identificar positivamente originadores ou beneficiários de contas ou outra atividade bancária (utilizando a Internet, pesquisas em bancos de dados comerciais, ou consultas diretas a um banco correspondente);
- Os pagamentos de ou para a empresa não têm nenhuma finalidade declarada, não mencionam produtos ou serviços, ou identificam somente um número de contrato ou fatura;
- Os produtos ou serviços, se identificados, não correspondem com o perfil da empresa fornecido pelo banco correspondente ou o caráter da atividade financeira; a empresa referencia produtos e serviços notadamente diferentes nas transferências de recursos relacionadas; a explicação fornecida pelo banco correspondente estrangeiro é incompatível com a atividade de transferência de recursos observada;
- As empresas na transação compartilham o mesmo endereço, fornecem somente um endereço do agente de registro ou têm outras inconsistências de endereço;
- Um número e variedade excepcionalmente grande de beneficiários estão recebendo transferências de recursos de uma empresa;
- Envolvimento frequente de diversas jurisdições ou beneficiários localizados em centros financeiros no exterior de risco mais elevado;
- Um banco correspondente estrangeiro excede o volume previsto em seu perfil de cliente para transferência de recursos, ou uma empresa individual apresenta um alto volume e padrão de transferências de recursos que é incompatível com sua atividade de negócio normal;
- Diversos pagamentos ou transferências de alto valor entre empresas de fachada sem qualquer finalidade legítima aparente; e
- A finalidade da empresa de fachada é desconhecida ou imprecisa.

Funcionários (incluindo trabalhadores contingentes) incluem, entre outros:

- O funcionário apresenta um estilo de vida luxuoso que não pode ser sustentado pelo seu salário;
- O funcionário não cumpre com as políticas, procedimentos e processos reconhecidos, particularmente no que diz respeito a private banking.

- O funcionário se mostra relutante em sair de férias; e
- O funcionário desrespeita uma retenção imposta em uma conta identificada como suspeita para que operações possam ocorrer na conta.

Anexo B: Sinais de Alerta de Financiamento do Terrorismo

Os exemplos a seguir de atividade potencialmente suspeita que possam indicar financiamento do terrorismo são baseados principalmente na "Orientação para Instituições Financeiras para Detectar Financiamento do Terrorismo" fornecida pela FATF. A FATF é um órgão intergovernamental, cuja finalidade é o desenvolvimento e a promoção de políticas, em nível nacional e internacional, para combater a lavagem de dinheiro e financiamento do terrorismo.

Atividade Incompatível com o Negócio do Cliente inclui, entre outros:

- Os recursos são gerados por um negócio de propriedade de pessoas da mesma origem ou por um negócio que envolve pessoas da mesma origem de países de risco mais elevado (por exemplo, países designados pelas autoridades nacionais e FATF como países e territórios não colaboradores);
- A ocupação declarada do cliente não é compatível com o tipo ou o nível de atividade;
- As pessoas envolvidas nas operações em dinheiro compartilham um endereço ou número de telefone, particularmente quando o endereço também é o local de negócio ou parece não corresponder com a ocupação declarada (por exemplo, estudante, desempregado, ou autônomo);
- Com relação a organizações sem fins lucrativos ou beneficentes, ocorrem operações financeiras para os quais parece não haver nenhuma finalidade econômica ou nas quais parece não haver qualquer vínculo entre a atividade declarada da organização e as outras partes na operação; e
- Um cofre aberto em nome de uma entidade comercial quando a atividade comercial do cliente é desconhecida ou essa atividade parece não justificar a utilização de um cofre.

Transferências de recursos incluem, entre outros:

- Ocorre um grande número de recebimento ou saída de transferências de recursos por meio de uma conta comercial e parece não haver nenhuma finalidade comercial lógica ou outra finalidade econômica para as transferências, particularmente quando essa atividade envolve locais de risco mais elevado;
- As transferências de recursos são solicitadas em pequenos valores em um esforço aparente de evitar o desencadeamento de exigências de identificação e apresentação de relatórios;
- As transferências de recursos não incluem informações sobre o originador, ou a pessoa em nome da qual a operação é realizada, quando a inclusão dessas informações seria esperada;
- Diversas contas pessoais e comerciais ou as contas de organizações sem fins lucrativos ou beneficentes são utilizadas para coletar e canalizar os recursos para um pequeno número de beneficiários estrangeiros; e
- Operações de câmbio são realizadas em nome de um cliente por um terceiro, seguido de transferências de recursos para locais que não tenham nenhuma conexão comercial aparente com o cliente ou para países de risco mais elevado.

Outras Operação que Pareçam Incomuns ou Suspeitas incluem, entre outros:

- Operações envolvendo câmbios são seguidas dentro de um curto prazo por transferências de recursos para locais de risco mais elevado;
- Diversas contas são utilizadas para coletar e canalizar os recursos para um pequeno número de beneficiários estrangeiros, tanto pessoas físicas e jurídicas, particularmente em locais de risco mais elevado;
- Um cliente obtém um instrumento de crédito ou se envolve em operações financeiras comerciais que envolvam a movimentação de recursos de ou para locais de risco mais elevado quando parece não haver quaisquer motivos comerciais lógicos para tratar nesses locais;
- Banco de locais de risco mais elevado abrem contas;
- Os recursos são enviados ou recebidos por meio de transferências internacionais de ou para locais de risco mais elevado; e

- Empréstimos de apólice de seguro ou valor de resgate de apólice que estão sujeitos a um encargo de resgate substancial.

Exemplos relacionados a clientes

- As solicitações pelos clientes para serviços de gestão de investimento (com relação a valores mobiliários, contratos de futuros ou contratos de câmbio alavancados) quando a fonte dos recursos não for precisa ou incompatível com a situação aparente dos clientes.
- Um cliente abriu diversas contas com os mesmos beneficiários finais ou partes controladoras sem qualquer motivo comercial aparente;
- As informações fornecidas são inconsistentes ou de natureza suspeita;
- O cliente se recusa a fornecer as informações solicitadas sem uma explicação razoável ou, por outro lado, se recusa a cooperar com o processo de CDD e/ou monitoramento contínuo;
- A pesquisa de antecedentes de clientes revela uma reputação, ou rumores persistentes, de comportamento antiético;
- Negociações complexas ou estruturas organizacionais desnecessárias que refletem ausência de finalidade comercial (especialmente envolvendo holdings no exterior em paraísos fiscais ou países com leis severas de sigilo bancário) ou condições de pagamento favoráveis incomuns;
- O cliente forneceu informações falsas, enganosas ou substancialmente incorretas relacionadas à fonte dos recursos, fonte de riqueza ou se recusa a identificar ou não indica uma fonte legítima dos recursos ou sugere à BlackRock uma modificação nos procedimentos de aceitação de cliente para evitar as exigências de verificação de identidade; e
- O cliente deseja adquirir um produto que parece ser incompatível com as necessidades, objetivos financeiros ou comerciais declarados pelo cliente.

Exemplos relacionados à negociação

- Operações ou instruções que não têm qualquer finalidade legítima aparente e/ou parecem não tem uma lógica comercial;
- Operações, instruções ou atividades que envolvem complexidade aparentemente desnecessária ou não constituem a maneira mais lógica, conveniente ou segura de fazer negócios;
- Operações solicitadas pelo cliente estão fora do leque normal de serviços normalmente solicitados ou fora da experiência da BlackRock com relação ao cliente específico (por exemplo, mudar de negociação somente de alto rendimento para predominantemente blue chips), sem qualquer explicação razoável;
- O tamanho ou o padrão das operações é inconsistente com qualquer padrão que surgiu anteriormente sem uma explicação razoável;
- Um cliente que entrou em relacionamento comercial utiliza o relacionamento para uma única operação ou por apenas um período de tempo bem curto sem uma explicação razoável;
- O uso extensivo de trusts ou contas no exterior, empresas ou estruturas em circunstâncias em que as necessidades do cliente sejam incompatíveis com a utilização desses serviços;
- Operações de investimento incomuns sem aparente motivo lucrativo discernível;
- Pagamentos que excedem o valor devido (resultante de pagamento a maior);
- Pagamentos que são recebidos de partes ou fontes imprevistas (quando a BlackRock possuir uma conta bancária do cliente no registro verificado);
- Subscrições acompanhadas por um rápido resgate sem qualquer explicação lógica;
- Um cliente se envolve em uma negociação pré-acordada ou outra negociação não competitiva com relação a determinados valores mobiliários, contratos de futuro ou contratos de câmbio alavancados; e
- Operações de valores mobiliários ocorrem em diversas jurisdições e em jurisdições específicas que não aplicam ou aplicam de maneira insuficiente as recomendações da FATF ou, por outro lado representam risco mais elevado.

Exemplos relacionados à liquidação/custódia/transferências

- Fornecimento de garantia na forma de caução ou garantia sem qualquer motivo plausível discernível por terceiros desconhecidos para a BlackRock que não possuam qualquer relacionamento próximo identificável com o cliente;

- Pagamento por meio de cheques de alto valor de terceiros endossados em favor do cliente na liquidação de valores mobiliários adquiridos;
- Aumento repentino na intensidade de operações, sem um motivo plausível, no que anteriormente era uma conta de negociação de cliente relativamente inativa, em particular, se envolverem grandes subscrições e pagamentos em dinheiro;
- Um cliente utiliza repetidamente um fundo mútuo como um local de manutenção temporária dos recursos de diversas fontes sem uma finalidade comercial clara (incluindo de investimento);
- Compras frequentes de cotas de fundos mútuos seguidos de grandes resgates, particularmente se o investimento solicitar que os recursos do resgate sejam transferidos para terceiros não relacionados ou para uma conta bancária estrangeira em um país que não seja o país de residência do investidor;
- O envolvimento de empresas no exterior em cujas contas sejam realizadas diversas transferências, especialmente quando elas forem destinadas para um paraíso fiscal e para contas no nome de empresas no exterior das quais o cliente possa ser um acionista;
- Conta de não residente com movimentações na conta muito grandes e subsequentes transferências de recursos para centros financeiros no exterior;
- Transferências de e para jurisdições de alto risco sem uma explicação razoável, que não sejam compatíveis com os negócios ou interesses comerciais declarados do Cliente;
- Encaminhamento desnecessário de recursos ou outros bens de/para terceiros ou por meio de contas de terceiros;
- Um cliente transmite ou recebe transferências de recursos sem informações de identificação normais, ou de forma que possa indicar uma tentativa de encobrir ou ocultar o país de origem ou destino, ou a identidade do cliente que esteja enviando os recursos, ou o beneficiário para o qual os recursos foram enviados;
- As transferências de recursos não incluem informações sobre o originador, ou a pessoa em nome da qual a operação é realizada ou quando a inclusão dessas informações seria esperada;
- Solicitações frequentes para alterar a situação das instruções de liquidação;
- Grande número de transferências eletrônicas de e para a conta;
- As transferências não indicam a identidade da parte solicitante ou o número da conta da qual originou a transferência;
- Diversas operações pela mesma contraparte em pequenos valores relacionados ao mesmo valor mobiliário, cada um adquirido em dinheiro e, depois, vendido em uma operação, com os recursos posteriormente creditados em uma conta diferente da conta original; e
- Qualquer transação na qual a contraparte na operação seja desconhecida ou quando a natureza, o tamanho ou a frequência pareça incomum.

Anexo C: Formulário de Apresentação de Atividade Potencialmente Suspeita e Formulário de Encaminhamento de Atividade Suspeita.

Envie por e-mail o formulário preenchido para o head regional da equipe de Crimes Financeiros listados abaixo. Anexe em seu e-mail toda a documentação comprobatória relevante.

Mantenha este relatório confidencial. A equipe de Crimes Financeiros fará o acompanhamento com você caso informações adicionais sobre este encaminhamento sejam necessárias.

Lisa Belle lisa.belle@blackrock.com

Parte responsável pelo encaminhamento

Seu nome:	**Seu departamento:**
Seu cargo:	**Data do relatório:**
Seu endereço de e-mail:	

Informações sobre o cliente

Nome do cliente:	
Endereço do cliente:	**Código da carteira da BlackRock do cliente:**
Detalhes do produto:	

Motivo para a Encaminhamento

Sumarize abaixo os motivos pelos quais você está encaminhando esse caso para a equipe de Crimes Financeiros. Inclua o máximo de detalhes, conforme necessários, para substanciar sua preocupação. Limite a sua descrição somente aos fatos e evite usar linguagem editorial ou conclusiva. A equipe de Crimes Financeiros avaliará e determinará se a atividade encaminhada é ou não suspeita.