REDPOINT EVENTURES GESTÃO DE RECURSOS E CONSULTORIA LTDA.

Política de Combate e Prevenção à Lavagem de Dinheiro
(Outubro de 2018)

I. Objetivo e Escopo da Política de Combate e Prevenção à Lavagem de Dinheiro

1. O Departamento de Compliance e Gestão de Risco da **REDPOINT EVENTURES GESTÃO DE RECURSOS E CONSULTORIA LTDA.**, sociedade limitada com sede na Cidade de São Paulo, Estado de São Paulo, na Alameda Vicente Pinzon, 54, andar 00, Vila Olímpia, CEP 04547-130, inscrita no CNPJ sob o nº 29.292.940/0001-83 ("**Redpoint**" ou "**Sociedade**"), sob responsabilidade do Sr. Fábio Schenberg Frascino, brasileiro, casado, engenheiro, residente e domiciliado na Cidade de São Paulo, Estado de São Paulo, com escritório na Alameda Vicente Pinzon, 54, andar 00, Vila Olímpia, CEP 04547-130, portador da Cédula de Identidade RG n° 18.615.664-9 SSP/SP, inscrito no CPF sob o n° 116.015.278-02, responsável por monitorar e fiscalizar o cumprimento das normas e políticas a serem observadas por todos empregados, colaboradores e administradores da Redpoint ("**Membros**"), identificando potenciais riscos e prevenindo a ocorrência de condutas antiéticas ou ilegais.

2. O objetivo desta Política de Combate e Prevenção à Lavagem de Dinheiro é assegurar um completo e eficaz conhecimento dos clientes e parceiros da Sociedade no desenvolvimento de suas atividades. Assim, a aceitação de clientes e parceiros e a manutenção do relacionamento com os mesmos deverá considerar a lisura de suas atividades, e não somente o interesse comercial e a rentabilidade que podem proporcionar à Redpoint.

3. A adequada identificação dos clientes permite o estabelecimento de parâmetros para um monitoramento eficaz de suas movimentações, auxiliando no processo de prevenção à lavagem de dinheiro e mitigando riscos de financiamento ao terrorismo. O monitoramento das movimentações realizadas pelos clientes será realizado pelo Departamento de Compliance e Gestão de Risco da Sociedade, que, por meio de acesso à base de dados, poderá avaliar, a partir de parâmetros estabelecidos, as movimentações dos clientes.

II. O que é "Lavagem de Dinheiro"

4. A "Lavagem de Dinheiro" é um processo pelo qual transgressores procuram dar aparência legítima a recursos provenientes de atividades ilícitas.

5. A lavagem de dinheiro é frequentemente usada para dissimular o produto de corrupção, sendo amplamente praticada por traficantes de drogas, criminosos de colarinho branco e terroristas.

6. O processo envolve, teoricamente, três fases ou etapas: Colocação, Ocultação e Integração.

7. A colocação, primeira fase do processo, é a introdução do dinheiro no Sistema Financeiro, esta colocação é feita de forma pulverizada, através de depósitos, compra de instrumentos negociáveis ou compra de bens, com o objetivo de dificultar a identificação da origem do dinheiro.

8. A ocultação, segunda fase do processo, os valores são movimentados de forma eletrônica, transferidos diversas vezes, com o objetivo de dificultar o rastreamento contábil dos recursos ilícitos.

9. Na integração, os valores são introduzidos definitivamente na economia formal.

III. Base Legal

10. O processo de prevenção à lavagem de dinheiro da Sociedade tem como base legal, em especial, as seguintes normas: Lei nº 9.613/98, conforme alterada; as Circulares do Banco Central do Brasil nº 3.461/09, n° 3.517/10 e n° 3.654/13; as Cartas-Circulares do Banco Central do Brasil nº 3.430/10 e 3.542/12; e a Instrução CVM nº 301/99, conforme alterada.

11. Esta política considera, ainda, o Guia de Prevenção à "Lavagem de Dinheiro" e ao Financiamento do Terrorismo no Mercado de Capitais Brasileiro da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA, entidade de autorregulação do mercado financeiro e de capitais.

IV. Princípios Gerais

12. Alguns princípios gerais a serem considerados:

(i) Nenhum Membro da Redpoint deve, em qualquer hipótese, de maneira consciente:

(a) participar de qualquer operação financeira proibida; e

(b) prestar assistência a qualquer cliente, sócio do negócio ou terceiros em violação de quaisquer leis e regulamentos de combate à lavagem de dinheiro aplicáveis. Esse princípio inclui a obrigação de evitar "cegueira deliberada", em que uma pessoa permite que uma operação obviamente ilícita passe desapercebida.

(ii) Os Membros da Sociedade devem buscar conhecer suficientemente os clientes por meio dos procedimentos de *Know Your Customer* – KYC e *suitability*, a fim de assegurar que a Redpoint conduza o negócio apenas com empresas e pessoas físicas que atendam aos padrões necessários para o cumprimento, de maneira confortável, das exigências nos termos das leis e regulamentos de combate à lavagem de dinheiro aplicáveis. Isso inclui buscar conhecer a fonte dos recursos ou patrimônio dos clientes, especialmente se o cliente realizar operações ou residir em um país sujeito a programas de sanções mantidos por diversos governos, bem como se cliente constar em lista de pessoas restritas emitida por diversos governos e pela Organização das Nações Unidas (ONU).

(iii) Todos os Membros da Sociedade, independentemente de seu cargo ou localidade, devem permanecer alerta para detectar possíveis atividades criminosas ou suspeitas e, imediatamente, denunciar operações questionáveis ao responsável pelo Departamento de Compliance e Gestão de Risco.

V. Procedimento

13. A abordagem da Sociedade com relação à prevenção de lavagem de dinheiro segue os seguintes pontos:

(i) Consultas para conhecer seus clientes (*Know Your Customer*);

(ii) Consultas para conhecer seus parceiros (*Know Your Partner*);

(iii) Abordagem baseada em risco com relação à lavagem de dinheiro;

(iv) Monitoramento contínuo de atividades suspeitas;

(v) Comunicações endereçadas ao Conselho de Controle de Atividades Financeiras – COAF;

(vi) Treinamento;

(vii) Auditoria;

(viii) Consultas a listas restritivas, sites de busca e órgãos reguladores para confirmação de informações de clientes;

(ix) Aceitação e manutenção de relacionamentos comerciais com clientes conforme análise de risco com relação à lavagem de dinheiro;

(x) Identificação, análise e documentação de situações que possam configurar indícios da ocorrência dos crimes previstos na Lei nº 9.613/98, ou que com eles se relacionem; e

(xi) Avaliação da exposição ao risco de lavagem de dinheiro e financiamento ao terrorismo na aprovação de produtos e serviços.

14. O monitoramento deverá ser realizado de forma imediata e automática, e serão consideradas transações de alto risco aquelas elencadas nas legislações e normas aplicáveis.

15. Deverá, ainda, ser realizado um processo diário e outro mensal pelos quais serão avaliados os riscos de lavagem de dinheiro nas movimentações feitas pelos clientes. Em tais processos, deverão estar incluídos o controle e verificação da origem de recursos, além da busca de informações dos clientes, como por exemplo, notícias desabonadoras e se o cliente é uma pessoa exposta politicamente ou relacionada.

VI. Consultas para Conhecer seus Clientes (*Know Your Customer*)

16. A Redpoint, quando atua como distribuidora das cotas dos próprios fundos, além de realizar o cadastro do cliente em conformidade com o Capítulo III da Instrução CVM nº 505, de 27.9.2011, solicita ao cliente cuja carteira será administrada, conforme o caso, os documentos aplicáveis a fim de conhecer o cliente. Se pessoa jurídica, a Sociedade busca ainda conhecer seus controladores e beneficiários finais. Nos casos em que não distribui as cotas do fundo sob gestão,

solicita tais informações ao administrador do fundo. O intuito dos procedimentos de consulta da Sociedade para conhecer seus clientes é:

(i) Garantir que a Redpoint saiba a verdadeira identidade de todos os clientes com quem faz negócios; e

(ii) Proteger a Sociedade dos riscos de fazer negócios com indivíduos ou entidades cuja identidade ela não possa determinar.

17. Estão listados abaixo os procedimentos principais de consultas da Redpoint para conhecer seus clientes:

(i) Identificar os clientes e seus beneficiários finais, obtendo informações sobre eles, em especial sobre os clientes que sejam considerados pessoas politicamente expostas de acordo com o artigo 3º-A e 3º-B da Instrução CVM nº 301/99, incluindo a origem de seu patrimônio;

(ii) Conhecer a origem do patrimônio do cliente;

(iii) Verificar a identidade dos clientes e de seus beneficiários finais, principalmente os que sejam pessoas politicamente expostas, por meio de documentos, dados ou informações de fontes confiáveis e independentes;

(iv) Conhecer a origem e o destino dos recursos movimentados pelo cliente;

(v) Identificar e verificar pessoas físicas nomeadas para agir em nome de clientes corporativos;

(vi) Identificar e verificar a identidade de titulares indiretos;

(vii) Obter informações sobre a finalidade e a natureza pretendida de qualquer relacionamento comercial;

(viii) Realizar análises de atividades de transações ao longo do relacionamento comercial e verificar a compatibilidade de tais transações com o perfil do cliente;

(ix) Analisar a possibilidade de veto a relacionamentos devido ao risco envolvido; e

(x) Rever periodicamente a adequação das informações dos clientes.

18. Caso os procedimentos de consulta da Redpoint para conhecer seus clientes indique elevado risco decorrente do relacionamento com determinado cliente, a Sociedade vetará o início ou a continuidade de tal relacionamento.

VII. Abordagem Baseada em Risco com Relação à Lavagem de Dinheiro

19. A Redpoint adota uma abordagem baseada em risco para focar seus esforços contra a lavagem de dinheiro onde for necessário e onde houver mais impacto. A abordagem da Sociedade baseada em risco equilibra os recursos disponibilizados com uma avaliação realista da ameaça de que a Redpoint será usada para fins de lavagem de dinheiro ou financiamento de terrorismo.

20. Os critérios utilizados para definir o grau de risco do relacionamento e das transações de determinados clientes levam em consideração os seguintes fatores:

(i) Localização geográfica das pessoas físicas ou das empresas que foram constituídas ou que sejam domiciliadas em países considerados de alto risco com relação à lavagem de dinheiro;

(ii) Risco associado ao tipo de profissão ou de atividade realizada, respectivamente, por pessoas físicas ou empresas; e

(iii) Risco associado ao tipo de serviço ou produto contratado, no caso de produtos que possuam maior risco de serem utilizados para a prática de atos ilícitos

21. A abordagem baseada em risco da Sociedade:

(i) Reconhece que a ameaça à Redpoint com relação à lavagem de dinheiro/financiamento de terrorismo varia entre clientes, jurisdições, produtos e canais de distribuição;

(ii) Permite à Sociedade fazer a diferenciação entre os clientes de forma a equiparar o risco em seus negócios particulares; e

(iii) Auxilia na criação de um sistema mais viável e eficaz.

VIII. Monitoramento Contínuo de Atividades Suspeitas

22. As obrigações da Redpoint de prevenir a lavagem de dinheiro não param quando uma conta é aberta. Os Membros devem estar continuamente alertas a qualquer coisa incomum no contexto de suas relações regulares com os clientes, e devem comunicar imediatamente qualquer transação ou atividade suspeita ao responsável ou qualquer outro membro do Departamento de Compliance e Gestão de Risco.

23. Os Membros do Departamento de Compliance e Gestão de Risco devem conduzir, de tempos em tempos, revisões independentes de atividades a fim de identificar eventuais tendências ou questões incomuns, confrontando as informações cadastrais dos clientes com as movimentações realizadas por eles, buscando a identificação de operações que possam indicar a ocorrência dos crimes previsto na Lei nº 9.613/98, ou a eles relacionados, nos termos dos artigos 6º, 7º e 7º-A da Instrução CVM nº 301/99.

24. A análises das movimentações dos clientes observarão os seguintes aspectos:

(i) Compatibilidade das transações com a situação patrimonial do cliente;

(ii) Ocupação profissional do cliente;

(iii) Beneficiários finais de cada uma das operações;

(iv) Transferências ou pagamentos a terceiros;

(v) Transações em espécie;

(vi) Pessoas politicamente expostas, de acordo com o artigo 3º-B da Instrução CVM nº 301/99; e

(vii) Procuradores e representantes legais.

IX. Consultas para Conhecer seus Parceiros (*Know Your Partner*)

25. A Redpoint identificará e avaliará seus parceiros comerciais, de acordo com o perfil e o propósito do relacionamento, buscando a prevenção contra a realização de negócios com contrapartes inidôneas ou suspeitas de envolvimento em atividades ilícitas, assegurando-se de que seus parceiros mantenham práticas de combate e prevenção à lavagem de dinheiro.

26. Tal avaliação contará com a aplicação de um questionário, ou com visitas de diligências realizadas por Membros.

X. Consultas para Conhecer seus Membros (*Know Your Employee - KYE*)

27. Desde a contratação dos Membros, a Redpoint adorará procedimentos com objetivo de: (i) garantir a aderência dos Membros aos padrões de ética e conduta, e (ii) identificar eventual envolvimento em atividades ilícitas ou de lavagem de dinheiro e financiamento do terrorismo.

28. Mesmo após a contratação, a Redpoint realizará esforços para identificar violações posteriores a partir de indícios concretos, por exemplo, uma mudança repentina no padrão econômico de seus funcionários, promovendo ações que possibilitem identificar possíveis origens ilícitas de tais recursos.

XI. Cuidados Adicionais Aplicáveis aos Administradores de Carteiras

29. A Redpoint realizará, também, o processo de identificação de contrapartes nas operações, buscando prevenir que a contraparte utilize as instituições gestoras, como a Redpoint, e/ou os fundos de investimento ou carteiras por ela geridos para atividades ilegais ou impróprias.

30. Vale ressaltar que os ativos e valores mobiliários elencados abaixo, em função de sua contraparte e do mercado nos quais são negociados, já terem passaram por processo de análise quanto à prevenção de "lavagem de dinheiro", exime a Redpoint de diligência adicional em relação ao controle da contraparte, a saber:

(i) Ofertas públicas iniciais e secundárias de valores mobiliários, registradas de acordo com as normas emitidas pela CVM;

(ii) Ofertas públicas de esforços restritos, dispensadas de registro de acordo com as normas emitidas pela CVM;

(iii) Ativos e valores mobiliários admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida;

(iv) Ativos e valores mobiliários cuja contraparte seja instituição financeira ou

equiparada; e

(v) Ativos e valores mobiliários de mesma natureza econômica daqueles acima listados, quando negociados no exterior, desde que (a) sejam admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida pela CVM, ou (b) cuja existência tenha sido assegurada por terceiros devidamente autorizados para o exercício da atividade de custódia em países signatários do Tratado de Assunção ou em outras jurisdições, ou supervisionados por autoridade local reconhecida pela CVM.

31. Para os demais ativos e valores mobiliários, como títulos e valores mobiliários objeto de distribuição privada (renda fixa ou ações), direitos creditórios, empreendimentos imobiliários etc., a Redpoint, além dos procedimentos de Identificação de Contrapartes, adotará também outros procedimentos de diligência com objetivo de evitar o envolvimento com ativos e valores mobiliários suspeitos.

XII. Comunicações Endereçadas ao COAF

32. Os Membros que se depararem com transações ou propostas de transações que possam constituir indícios de crime de lavagem de dinheiro, conforme os parâmetros indicados nesta Política de Combate e Prevenção à Lavagem de Dinheiro e nos termos dos artigos 6º e 7º da Instrução CVM nº 301/99, deverão comunicar tais transações ao Conselho de Controle de Atividades Financeiras – COAF.

33. Desta forma, a depender da situação verificada no caso concreto, a Redpoint realizará a comunicação ao COAF por meio do Sistema de Controle de Atividades Financeiras – SISCOAF, na modalidade aplicável, no termos dos artigos 6º, 7º e 7º-A da Instrução CVM nº 301/99.

34. As seguintes situações poderão configurar indícios dos crimes previstos na Lei nº 9.613/98:

(i) Realização de aplicações ou resgates em contas de investimento em fundos que apresentem atipicidade em relação à atividade econômica do cliente ou incompatibilidade com a sua capacidade econômico-financeira;

(ii) Resistência ao fornecimento de informações necessárias para o início de relacionamento ou para a atualização cadastral, oferecimento de informação

falsa ou prestação de informação de difícil ou onerosa verificação;

(iii) Abertura, movimentação de contas de fundos de investimento ou realização de aplicações e/ou resgates por detentor de procuração (em especial no caso de pessoas físicas) ou de qualquer outro tipo de mandato;

(iv) Apresentação de irregularidades relacionadas aos procedimentos de identificação e registro das operações exigidos pela regulamentação vigente;

(v) Realização de várias aplicações em contas de investimento em fundos, em uma mesma data ou em curto período, com depósitos de valores idênticos ou aproximados;

(vi) Abertura de contas de investimento em fundos em que não seja possível identificar o beneficiário final, observados os procedimentos definidos na regulamentação vigente;

(vii) Informação de mesmo endereço comercial por diferentes pessoas jurídicas ou organizações, sem justificativa razoável para tal ocorrência;

(viii) Representação de diferentes pessoas jurídicas ou organizações pelos mesmos procuradores ou representantes legais, sem justificativa razoável para tal ocorrência;

(ix) Informação de mesmo endereço residencial ou comercial por pessoas naturais, sem demonstração da existência de relação familiar ou comercial;

(x) Incompatibilidade entre a atividade econômica e o faturamento informados pelo cliente com o padrão apresentado por clientes com o mesmo perfil de risco;

(xi) Manutenção de numerosas contas de investimento em fundos, destinadas ao acolhimento de aplicações de um mesmo cliente, incompatíveis com o patrimônio, a atividade econômica ou a ocupação profissional e a capacidade financeira do cliente;

(xii) Movimentação de quantia significativa, por meio de contas de fundos, até então pouco movimentada;

(xiii) Ausência repentina de movimentação financeira em conta de fundo que anteriormente apresentava grande movimentação;

(xiv) Solicitação de não observância ou atuação no sentido de induzir funcionários da instituição a não seguirem os procedimentos regulamentares ou formais para a realização de uma aplicação ou resgate em contas de fundos;

(xv) Realização de aplicações em contas de fundos que, por sua habitualidade, valor e forma, configurem artifício para burla da identificação da origem, do destino, dos responsáveis ou dos beneficiários finais;

(xvi) Manutenção de contas de fundos, qualquer que seja o valor da aplicação, por pessoas que reconhecidamente tenham cometido ou intentado cometer atos terroristas, ou deles participado ou facilitado o seu cometimento;

(xvii) Existência de recursos em contas de fundos pertencentes ou controlados, direta ou indiretamente, por pessoas que reconhecidamente tenham cometido ou intentado cometer atos terroristas, ou deles participado ou facilitado o seu cometimento; e

(xviii) Movimentações (aplicações ou resgates em contas de investimento em fundos) com indícios de financiamento de terrorismo.

35. Os Membros deverão manter arquivados de forma adequada os registros que fundamentarem a decisão de comunicação ou de não comunicação ao COAF, pelo prazo de 5 (cinco) anos, conforme §5º do artigo 7º da Instrução CVM nº 301/99. As comunicações ou as possíveis comunicações ao COAF têm caráter confidencial e, portanto, são restritas aos funcionários envolvidos no processo de análise e não deve ser informada ao cliente.

XIII. Treinamento

36. Ao ingressar na Sociedade, todos os Membros passam por um programa de treinamento, cuja participação é atestada através da assinatura de um termo de adesão, conforme informado no Manual de Compliance da Redpoint. Por meio do programa de treinamento, os Membros terão perfeito conhecimento de todas as condutas e responsabilidades esperadas no que se refere às políticas adotadas pela Sociedade, incluindo esta Política de Combate e Prevenção à Lavagem de Dinheiro.

37. Além do treinamento recebido no momento do ingresso, o Membro receberá treinamento com periodicidade, no mínimo, anual, podendo ser inferior, conforme a área e a função desemprenhada pelo Membro, ou quando o responsável pelo Departamento de Compliance e Gestão de Risco da Redpoint julgue necessário.

38. Os treinamentos são efetuados pessoalmente para grupo ou ainda individualmente pelo responsável pelo Departamento de Compliance e Gestão de Risco da Sociedade ou alguém por ele designado ou, ainda, por empresa terceirizada especialmente contratada para esta finalidade.

XIV. Auditoria

39. As práticas e procedimentos desta Política de Combate e Prevenção à Lavagem de Dinheiro serão submetidas à auditorias internas, que analisarão e apontarão possíveis melhorias nas práticas de combate e prevenção à lavagem de dinheiro, garantindo o cumprimento das normas vigentes.

XV. Revisão

40. Ao menos uma vez ao ano, o Departamento de Compliance e Gestão de Risco da Sociedade conduzirá uma revisão completa de todo Programa de Compliance, que inclui esta política, a agenda regulatória, o programa de treinamento, as revisões de formulários e etc.

41. A partir dos resultados desta revisão, será preparado pelo Departamento de Compliance e Gestão de Risco o relatório que trata o artigo 22 da Instrução CVM nº558/15.

XVI. Responsabilidade

42. Cada Membro da Redpoint tem a responsabilidade de conhecer e seguir as políticas e procedimentos previstos neste documento. Cada pessoa com função de supervisão é também responsável por aqueles sob sua supervisão. O responsável pelo Departamento de Compliance e Gestão de Risco tem a responsabilidade de monitorar e verificar o cumprimento das políticas e procedimentos da Sociedade. O não cumprimento das políticas e procedimentos aqui previstos serão documentadas e relatadas ao responsável pelo Departamento de Compliance e Gestão de Risco para a tomada de medidas corretivas.