Royal United Services Institute
for Defence and Security Studies

Orientações 2022

Combate ao Financiamento da Proliferação para Prestadores de Serviços de Ativos Virtuais

Kayla Izenman

Combate ao Financiamento da Proliferação para Prestadores de Serviços de Ativos Virtuais

Kayla Izenman

Orientações do RUSI, Março 2022

Royal United Services Institute
for Defence and Security Studies

191 anos de pensamento independente em matéria de defesa e segurança

O Royal United Services Institute (RUSI) é o grupo de reflexão em matéria de defesa e segurança mais antigo do mundo e o principal do Reino Unido. A sua missão é informar, influenciar e reforçar o debate público sobre um mundo mais seguro e estável. O RUSI é um instituto liderado pela investigação, que gera análises independentes, práticas e inovadoras para fazer face aos complexos desafios atuais.

Desde a sua fundação em 1831, o RUSI tem contado com os seus membros para desenvolver as suas atividades. Juntamente com as receitas provenientes da investigação, publicações e conferências, o RUSI tem mantido independência política durante os seus 191 anos de existência.

Disclaimer

Este documento de orientações destina-se aos prestadores de serviços de ativos virtuais (VASP) que pretendem criar ou desenvolver uma função de combate ao financiamento da proliferação (CFP) na sua organização. Este documento tem como objetivo fornecer um enquadramento para que os VASP apliquem e adaptem as suas próprias práticas de conformidade com o crime financeiro, mantendo-se em linha com os requisitos regulamentares internos. Este documento não constitui aconselhamento jurídico nem regulamentar e deve ser lido sempre em conjunto com a legislação nacional e as normas e orientações internacionais relevantes, devendo sempre ser procurado aconselhamento jurídico independente em matéria de sanções, combate ao crime financeiro e implementação do CFP.

Durante a redação deste documento, Kayla Izenman era investigadora no Centro de Estudos de Crimes Financeiros e Segurança (Centre for Financial Crime and Security Studies) do RUSI. Este documento representa o seu ponto de vista pessoal durante esse período e não representa p ponto de vista, nem se relaciona com o trabalho que desempenha atualmente nem o da sua entidade patronal atual.

As opiniões expressas nesta publicação são as do autor e não refletem as opiniões do RUSI nem de qualquer outra instituição.

A presente versão resulta da tradução da publicação, em língua inglesa, de Setembro de 2021.

Publicado em 2022 pelo Royal United Services Institute for Defence and Security Studies.

RUSI Guidance Paper, Março 2022. ISSN 2397-0286 (Online).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
o RUSI é uma instituição de caridade registada (N.º 210639)

Índice

Agradecimentos

Este estudo foi realizado com o generoso apoio da Fundação John D e Catherine T MacArthur (John D and Catherine T MacArthur Foundation). Agradeço a David Carlisle e Malcolm Wright pelos seus úteis comentários sobre uma versão anterior deste documento. Agradeço também a todos os que generosamente disponibilizaram o seu tempo para serem entrevistados para a investigação sobre ativos virtuais do RUSI desde 2017, assim como à equipa de publicações do RUSI pelo seu trabalho na edição destas orientações.

Acrónimos

CBC – Combate ao Branqueamento de Capitais

CDD – Acompanhamento Adequado da Relação de Negócio (customer due diligence)

CFT – Combate ao Financiamento do Terrorismo

CFP – Combate ao Financiamento da Proliferação

EDD – Vigilância Reforçada (enhanced due diligence)

GAFI – Grupo de Ação Financeira

KYC – Conheça o seu Cliente (know your customer)

BC – Branqueamento de Capitais

FP – Financiamento da Proliferação

FT – Financiamento do Terrorismo

AV – Ativo Virtual

VASP – Prestador de Serviços de Ativos Virtuais

I. Âmbito e objetivos

O FINANCIAMENTO DA PROLIFERAÇÃO (FP) de ADM é definido pelo Grupo de Ação Financeira (GAFI) como "o ato de fornecer fundos ou serviços financeiros que são utilizados, no todo ou em parte, para o fabrico, aquisição, posse, desenvolvimento, exportação, transbordo, corretagem, transporte, transferência, armazenamento ou utilização de armas nucleares, químicas ou biológicas".[1] Esta é a definição utilizada pelo GAFI, mas vale a pena salientar que não existe uma definição internacionalmente aceite de FP, e alguns têm defendido uma interpretação mais ampla que pode incluir, por exemplo, atividades que geram receitas.[2]

Os proliferadores de ADM, como a Coreia do Norte e o Irão, continuam a evadir-se a sanções financeiras orientadas. Os ativos virtuais[3] (VAs) VA) têm-se tornado cada vez mais um veículo através do qual são levantados e movimentados fundos relacionados com a proliferação. No entanto, o elevado nível de conhecimento dos proliferadores de ADM sancionados em matéria de branqueamento e angariação de fundos de AV ainda não cumpriu as medidas de conformidade, regulamentação e de aplicação da lei. Nos últimos anos, o espaço dos AV tem aumentado e melhorado em termos de práticas de conformidade, mas alguns criminosos continuam à frente.

As sanções direcionadas para o programa de armas nucleares da Coreia do Norte estão em vigor ao nível da ONU desde 2006, e têm-se expandido constantemente de modo a incluir sanções financeiras específicas contra indivíduos e entidades designadas, sanções baseadas em atividades que restringem a capacidade da Coreia do Norte para aceder ao sistema financeiro internacional e sanções setoriais direcionadas para setores específicos ou as exportações da Coreia do Norte. A ONU também mantém sanções contra determinados indivíduos e entidades iranianas e restringe as atividades relacionadas com o desenvolvimento de mísseis balísticos.[4]

---

1. Grupo de Ação Financeira (GAFI), "Combater o Financiamento da Proliferação: Um Relatório sobre a Situação do Desenvolvimento e Consulta de Políticas (Combating Proliferation Financing: A Status Report on Policy Development and Consultation)", Relatório do GAFI, Fevereiro de 2010, pág. 5.
2. Para discussões adicionais sobre a definição de financiamento da proliferação (FP), consulte Anagha Joshi, Emil Dall e Darya Dolzikova, "Guia para a Realização de uma Avaliação Nacional dos Riscos de Financiamento da Proliferação (Guide to Conducting a National Proliferation Financing Risk Assessment)", RUSI, Maio de 2019, pág. 5.
3. Nestas orientações, "ativos virtuais" refere-se a tokens de pagamento digitais, tais como Bitcoin. Para ver a definição completa, consulte a secção "Terminologia".
4. Para obter informações atualizadas sobre os requisitos de sanções da ONU relacionados com a proliferação, consulte a ONU, "Órgãos Subsidiários do Conselho de Segurança das Nações Unidas (Subsidiary Organs of the United Nations Security Council)", 2021. As sanções unilaterais, tais como as impostas pelos EUA, pela UE ou pelo Reino Unido, podem impor requisitos adicionais aos das sanções da ONU.

Desde, pelo menos, 2014, a Coreia do Norte tem apresentado um conhecimento e interesse crescente pelo cibercrime, expandindo-se mais recentemente para os AV.[5] Em 2020 e 2021, o Departamento de Justiça dos EUA acusou uma série de indivíduos por branqueamento de AV em nome da Coreia do Norte.[6] No entanto, apesar de a maior parte da atividade de AV da Coreia do Norte envolver ataques de hackers em grande escala, tais como o hack Upbit de 49 milhões de dólares em 2019 [7] ou os 275 milhões de dólares roubados à KuCoin em 2020,[8] o regime também demonstrou interesse em ataques de ransomware e na mineração de AV.[9] m geral, a Coreia do Norte está altamente avançada no domínio do cibercrime e parece cada vez mais interessada em aplicar essas competências em atividades com criptomoedas. Da mesma

5. Um dos primeiros casos de cibercrime da Coreia do Norte foi o infame ataque de hackers à Sony Pictures, o qual foi atribuído pelo Federal Bureau of Investigation dos EUA em dezembro de 2014. Consulte o Gabinete de Imprensa Naciona do FBI, "Atualização sobre a Investigação da Sony (Update on Sony Investigation)", 19 de dezembro de 2014,, <https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>, acedido em 24 de agosto de 2021.
6. Departamento de Justiça dos EUA, "Três Hackers Militares Norte-Coreanos Indicados em Esquema Amplo para Cometer Ciberataques e Crimes Financeiros em Todo o Mundo (Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe)", 17 de fevereiro de 2021; Departamento de Justiça dos EUA, "Os Estados Unidos Apresentam um Pedido para Confiscar 280 Contas em Criptomoedas Ligadas ao Ataque de Hackers a Duas Corretoras por Agentes Norte Coreanos (United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors)", 27 de agosto de 2020; Departamento de Justiça dos EUA, "Dois Cidadãos Chineses Acusados de Branqueamento de Capitais num Valor Superior a 100 milhões de dólares em Criptomoedas Resultantes do Ataque de Hackers à Corretora (Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack)", 2 de março de 2020, <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack>, accessed 24 August 2021.
7. Para obter informações sobre o ataque de hackers à Upbit, consulte Marie Huillet, "Ataque de Hackers à Upbit: Os ETH Roubados Valem Milhões e Rumam a Carteiras Desconhecidas (Upbit Hack: Stolen ETH Worth Millions on the Move to Unknown Wallets)", Coin Telegraph, 3 de dezembro de 2019, <https://cointelegraph.com/news/upbit-hack-stolen-eth-worth-millions-on-the-move-to-unknown-wallets>, acedido em 25 de agosto de 2021. O Processo do Departamento de Justiça dos EUA em 2020 contra Tian Yinyin refere-se ao ataque de hackers à Upbit como "Intrusão e Roubo de novembro de 2019 (November 2019 Intrusion and Theft)" da "Corretora 3". Departamento de Justiça dos EUA, "Dois Cidadãos Chineses Acusados de Branqueamento de Capitais num Valor Superior a 100 milhões de dólares em Criptomoedas Resultantes do Ataque de Hackers à Corretora (Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack)".
8. Para obter informações sobre o ataque de hackers à KuCoin, consulte, "O ataque de hackers à KuCoin: O Que Sabemos Até à Data e Como os Hackers Wstão a Utilizar Protocolos DeFi para Branquear Fundos Roubados (The KuCoin Hack: What We Know So Far and How the Hackers are Using DeFi Protocols to Launder Stolen Funds)", 2 de outubro de 2020, <https://blog.chainalysis.com/reports/kucoin-hack-2020-defi-uniswap>, acedido em 25 de agosto de 2021. O Relatório Final do Painel de Peritos da ONU de 2021 refere-se a uma investigação em curso sobre um "ataque de hackers contra uma corretora de criptomoedas que ocorreu em setembro de 2020", resultando no "roubo à corretora de aproximadamente 281 milhões de dólares em criptomoedas". Resolução 1718 do Comité de Sanções (DPRK), "Relatório Final do Painel de Peritos Apresentado nos Termos da Resolução 2515 (Final Report of the Panel of Experts Submitted Pursuant to Resolution 2515) (2020)", 4 de março de 2021.
9. Yosuke Onchi, "A Coreia do Norte Ataca com Ransomware para Obter Dinheiro (North Korea Ramps up Ransomware Attacks in Hunt for Cash)", Nikkei Asia, 18 de fevereiro de 2021.

forma, embora não seja o foco principal deste documento de orientação, o Irão terá começado a utilizar a mineração de AV para evitar as sanções e exportar petróleo, com uma grande parte da mineração de AV global a ocorrer neste país.[10] Devido à falta de conformidade e de regulamentação global em muitas jurisdições, os prestadores de serviços de ativos virtuais (VASP) podem representar um alvo fácil para estes agentes.

Este documento de orientação tem como objetivo aconselhar os VASP sobre o cumprimento das boas práticas quando lidam com o risco de FP e direciona os responsáveis pela conformidade para publicações relevantes que poderão contribuir para o seu trabalho (consulte o Anexo II). O documento será particularmente útil para os VASP que não pensaram anteriormente no FP ou na implementação de sanções financeiras orientadas e relacionadas com a proliferação como um crime financeiro diferente ou risco de sanções.

Embora este documento utilize estudos de caso de proliferação, centrados principalmente na Coreia do Norte, grande parte desta baseia-se em tipologias, sinais de alerta e boas práticas que podem ser encontradas noutros tipos de crimes de AV, especialmente quando são realizadas atividades ilícitas por grandes organizações criminosas que podem ter experiência e financiamento comparáveis aos de um país sancionado.

Este documento segue a estrutura geral do ciclo de conformidade, começando com pré-requisitos antes da interação com o cliente, passando em seguida para o processo de integração, seguido de monitorização contínua durante todo o relacionamento com o cliente. Depois de analisar todo o ciclo, o guia aborda indicadores de risco elevado e sinais de alerta que podem resultar em medidas de identifição e diligëncia reforçada ou na saída do cliente e conclui com requisitos de notificação após sinalização de qualquer atividade suspeita.

FATF Recomendações do GAFI para AV e VASP

A compreensão e implementação das Recomendações do GAFI para os VASP é fundamental para o cumprimento das boas práticas e este documento tem como objetivo igualar e apoiar as Recomendações do GAFI.

Embora o GAFI tenha reconhecido os riscos associados aos AV desde 2014,[11] as primeiras alterações nas suas Recomendações relacionadas com os AV foram realizadas em outubro de 2018, esclarecendo que as Recomendações são aplicáveis a atividades financeiras que envolvem AV. Em junho de 2019, o GAFI adotou uma Nota Interpretativa para a Recomendação 15,[12] a qual esclareceu melhor como as Recomendações do GAFI se aplicam aos AV e aos VASP. Isto incluiu orientações em matéria de supervisão,

10. Tom Robinson, “Como o Irão Utiliza a Mineração de Bitcoins para se Evadir às Sanções e “Exportar” Milhões de Barris de Petróleo (How Iran Uses Bitcoin Mining to Evade Sanctions and “Export” Millions of Barrels of Oil)”, Elliptic, 21 de maio de 2021.
11. GAFI, “Moedas Virtuais: Definições principais e potenciais riscos de CBC/CFT (Virtual Currencies: Definitions and Potential AML/CFT Risks)”, junho de 2014, <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> acedido em 25 de agosto de 2021.
12. GAFI, “Declaração Pública Sobre Ativos Virtuais e Prestadores Relacionados (Public Statement on Virtual Assets and Related Providers)”, 21 de junho de 2019, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html>, acedido em 24 de agosto de 2021.

monitorização, licenciamento e registo, acompanhamento adequado da relação de negócio (CDD), relatórios de transações suspeitas, medidas de monitorização das sanções e muito mais.

Em junho de 2019, o GAFI também adotou a Orientação para uma Abordagem Baseada em Riscos para Ativos Virtuais e Prestadores de Serviços de Ativos Virtuais,[13] que tem como objetivo auxiliar as autoridades nacionais no desenvolvimento de regimes regulamentares apropriados para ao AV e os VASP, e também aconselhar o setor privado sobre como cumprir estes requisitos.

Foram realizadas duas revisões da Orientação do GAFI desde sua publicação, em julho de 2020 e julho de 2021.[14] A Orientação também é atualizada periodicamente para melhorar as recomendações e permanecer atualizada de acordo com o ritmo da inovação no setor de AV e, para tal, o GAFI realiza consultas públicas sobre a Orientação.[15]

Requisitos Internacionais

Este documento de orientação tem como objetivo apresentar um conjunto de normas em linha com as mais rigorosas recomendações e regulamentos internacionais em matéria de conformidade dos AV. Contudo, deve salientar-se que não segue nenhuma regulamentação nacional específica em matéria de criptomoedas. Certifique-se de que compreende totalmente os regulamentos para as jurisdições relevantes para os VASP antes de tentar aplicar qualquer um dos conselhos indicados neste documento. Além disso, e/ou se não existir regulamentação na(s) jurisdição(ões) relevante(s), certifique-se de que compreende totalmente as Recomendações do GAFI. Consulte o Anexo I para obter informações adicionais.

13. GAFI, "Orientação para uma Abordagem Baseada no Risco: Ativos Virtuais e Prestadores de Serviços de Ativos Virtuais (Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers)", junho de 2019, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>, acedido em 24 de agosto de 2021.
14. GAFI, "Revisão de 12 meses das Normas Revistas do GAFI sobre Ativos Virtuais e Prestadores de Serviços de Ativos Virtuais (12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers)", julho de 2020, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html>, acedido em 24 de agosto de 2021; GAFI, "Segunda Revisão de 12 meses das Normas Revistas do GAFI sobre Ativos Virtuais e Prestadores de Serviços de Ativos Virtuais (Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers)", julho de 2021, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html>, acedido em 24 de agosto de 2021.
15. GAFI, "Consulta Pública sobre o Projecto da Orientação do GAFI Sobre uma Abordagem Baseada no Risco aos Ativos Virtuais e Prestadores de Serviços de Ativos Virtuais (Public Consultation on FATF Draft Guidance on a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers)", março de 2021, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html>, acedido em 24 de agosto de 2021.

II. Terminologia

ESTE DOCUMENTO DE orientação utiliza o vocabulário utilizado pelo GAFI. Por conseguinte, os termos "ativo virtual" (AV) e "prestador de serviços de ativos virtuais" (VASP) são utilizados em todo o documento.

Note que, embora o termo "VASP" seja utilizado, o âmbito deste termo é mais restrito do que o da definição do GAFI. Embora a definição do GAFI inclua qualquer empresa envolvida na troca de AV para dinheiro, AV para AV, qualquer transferência, guarda, administração de A e qualquer empresa que forneça serviços financeiros relacionados com AV,[16] este documento de orientação define VASP como uma **troca centralizada de ativos virtuais** que fornece serviços de AV para dinheiro ou AV para AV.

Do mesmo modo, o termo AV é aplicável apenas a **tokens de pagamento**, tais como Bitcoin, e não se refere a moedas estáveis (stablecoins) ou moedas digitais de bancos centrais. Neste documento, AV é equivalente aos termos "criptomoeda", "moeda virtual" ou "cripto-ativo".

As "carteiras" de AV estão disponíveis em várias formas, e este documento não discrimina entre carteiras quentes (online) e carteiras frias (offline). As carteiras mantêm as chaves privadas de um utilizador seguras e acessíveis, e são fornecidas por muitos prestadores, incluindo corretoras centralizadas.

Metodologia

Este documento foi elaborado como parte do projeto de CFP do RUSI em curso. A equipa do RUSI analisou a atividade de FP desde 2015,[17] iincluindo a continuação da investigação sobre o papel desempenhado pelos AV e outros novos sistemas de pagamento na evasão às sanções, centrando-se na sua grande maioria na Coreia do Norte.[18] Este documento baseia-se na experiência da equipa do RUSI nesta área, na investigação aprofundada e em conversas informais ao longo dos últimos três anos com as partes interessadas de setores relevantes, incluindo reguladores de VASP, forças de segurança, bancos tradicionais, bancos concorrentes (challenger banks) e universidades.

16. GAFI, "Normas Internacionais Sobre o Combate ao Branqueamento de Capitais e o Financiamento do Terrorismo e da Proliferação: As Recomendações do GAFI (International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations)", atualizado em junho de 2021, pág. 130.
17. Para mais publicações do RUSI sobre FP, consulteRUSI, "Financiamento da Proliferação (Proliferation Financing)", <https://rusi.org/explore-our-research/topics/proliferation-financing>, acedido em 24 de agosto de 2021.
18. Para informações mais detalhadas sobre a atividade de AV da Coreia do Norte, consulte David Carlisle e Kayla Izenman, "Fechar o Fosso Cripto: Orientação para combater a Atividade com Criptomoedas da Coreia do Norte no Sudeste Asiático (Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia)", Artigos Ocasionais do RUSI (abril de 2019).

III. Pré-requisitos

ESTA SECÇÃO CENTRA-SE em todos os aspetos do sistema de conformidade que deverá estar implementado antes de integrar qualquer cliente. Inclui uma equipa de conformidade eficaz e com conhecimento, avaliações iniciais do risco, uma compreensão abrangente de todos os requisitos nacionais e internacionais relevantes, formação e protocolos adequados em matéria de cibersegurança e uma política personalizada em relação às decisões de listagem de moedas.

Equipa de Conformidade

De modo a implementar adequadamente qualquer uma das seguintes orientações, os VASP devem certificar-se primeiro de que possuem a estrutura de governança e a equipa de conformidade adequadas. A estrutura organizacional de uma VASP deve garantir que a função de conformidade dispõe dos recursos, autoridade, informação e independência necessários para avaliar e gerir os riscos do combate ao crime financeiro.

Uma estrutura de governança abrangente considera todos os níveis da empresa. A administração deve ter a responsabilidade final pela supervisão e eficácia do programa contra o crime financeiro.

Um programa eficaz também requer um responsável pela conformidade, normalmente nomeado Diretor de Conformidade, que é o responsável final pela conceção e implementação do programa de conformidade, assim como por garantir a total conformidade com as obrigações regulamentares e legais. Em empresas de maior dimensão, pode existir ainda um Diretor de Conformidade das Sanções designado para garantir a supervisão e o cumprimento dos requisitos específicos das sanções.

Os funcionários de nível médio e júnior de todos os níveis da organização também devem ser informados sobre os sinais de alerta das transacções, os requisitos de monitorização e comunicação, os métodos de investigação e outros procedimentos de conformidade relevantes que se possam manifestar noutras áreas das operações comerciais dos VASP.

Algumas jurisdições regulamentadas exigem funções específicas na equipa de conformidade. A administração deve garantir que estes são tidos em consideração na constituição de uma equipa de conformidade. Todos os membros da equipa de conformidade devem receber formação periódica sobre quaisquer novas tendências de AV, ferramentas de conformidade específicas de AV e todas as regulamentações locais, nacionais e internacionais relevantes.

Avaliação do Risco

Os VASP devem realizar periodicamente uma avaliação interna do risco de modo a identificar clientes, setores ou tipos de transações que possam estar mais expostos ao branqueamento de capitais (BC)/ financiamento de terrorismo (FT)/atividade de FP, e conceber e implementar controlos para mitigar estes riscos específicos. As avaliações do risco são realizadas periodicamente por instituições financeiras em matérias semelhantes, e os VASP devem adotar igualmente esta abordagem.

As avaliações do risco devem ser registadas por escrito e estar disponíveis para inspeção pelas entidades reguladoras. As avaliações do risco são constituídas por três elementos: ameaças; vulnerabilidades e consequências.

Na área do FP, o GAFI considera que "ameaça" se refere a qualquer pessoa ou entidade que tenha anteriormente evadido, violado ou explorado sanções de FP, ou que tenha potencial para o fazer no futuro. As "vulnerabilidades" são tudo o que pode ser explorado pela ameaça, por exemplo, lacunas na regulamentação ou pontos fracos da cibersegurança. Isto inclui vulnerabilidades geográficas e específicas do setor. As "Consequências" referem-se ao resultado quando fundos ou ativos ficam disponíveis para os autores da ameaça designados, não apenas em termos de financiamento de ADM, como também no que diz respeito ao impacto final nas operações comerciais e na reputação do VASP.[19]

A linha entre as ameaças e as vulnerabilidades pode ser ténue, mas é importante compreender a interação entre as duas, juntamente com quaisquer fatores de mitigação. Ao analisar as ameaças e vulnerabilidades, tenha em consideração, pelo menos, os seguintes aspetos:

- Responsáveis por ameaças conhecidas.
- Tipologias de crime de financiamento conhecidas.
- Dimensão e complexidade do VASP.
- Produtos fornecidos e serviços prestados.
- Método de entrega dos produtos e serviços.
- Tipos de clientes.
- Localização física dos clientes.
- Localização física do VASP e regulamentos relevantes.
- Instituições relacionadas.

O resultado de uma avaliação do risco deve indicar a um VASP quais as áreas em que os riscos inerentes são particularmente elevados. O risco inerente é geralmente definido como a quantidade de risco que existe na ausência de controlos, informações que ficarão mais claras após uma avaliação abrangente do risco. Estes controlos devem ser considerados fatores mitigantes na avaliação do risco.

As potenciais consequências do FP são mais graves do que as do BC ou do FT. Os VASP devem avaliar os impactos e danos físicos, sociais, ambientais, económicos e estruturais.

Para informações adicionais sobre a realização de avaliações do risco para os VASP, consulte o Anexo I.

Cibersegurança

Além dos procedimentos de conformidade, dada a extensão dos ataques cibernéticos para financiar a proliferação, é essencial ter um foco na cibersegurança. Este inclui tanto a formação dos funcionários do VASP de todos os níveis, assim como o investimento em profissionais de cibersegurança para instalar salvaguardas apropriadas para os VASP.

19. Para informações adicionais sobre as definições destes três elementos, consulte GAFI, " Orientações sobre a Avaliação e Mitigação dos Riscos de Financiamento da Proliferação (Guidance on Proliferation Financing Risk Assessment and Mitigation)", junho de 2021, pág. 9.

Dar formação aos funcionários sobre protocolos de cibersegurança é essencial para a proteção contra hackers que trabalham em nome de proliferadores. Sabe-se que a Coreia do Norte, em especial, tem estado envolvida em esquemas de phishing complicados para se infiltrar nos VASP, tais como o seu ataque à DragonEx em 2019.

Estudo de caso 1: DragonEx (2019)

Em março de 2019, a Coreia do Norte executou um elaborado esquema de phishing que levou um funcionário da VASP DragonEx a instalar inconscientemente software malicioso num computador que continha chaves privadas da carteira do VASP, permitindo que a Coreia do Norte roubasse milhões de dólares em ativos virtuais. Os investigadores descobriram que o Lazarus, um grupo cibercriminoso da Coreia do Norte, foi responsável pelo ataque, resultando numa perda superior a 7 milhões de dólares.

O Lazarus registou dois domínios na Internet, falsificou software de negociação de AV, incorporou-lhe código malicioso e ocultou-o dentro de uma plataforma de negociação de AV automatizada que funcionou normalmente durante seis meses. Posteriormente, os atacantes enviaram o software para funcionários de vários VASP, sob o pretexto de uma promoção do produto. A equipa de apoio ao cliente da DragonEx abriu um pacote de instalação do software malicioso, através do qual os hackers conseguiram obter a chave privada da carteira do VASP e concretizar o roubo.

Fontes: Lylian Teng, "Alerta! O Grupo de Hackers Lazarus Continua a ter a Criptomoeda como Alvo Utilizando Software de Negociação Falso (Alert!, Lazarus Hacker Group Continues Targeting Crypto Using Faked Trading Software)", 8BTC, 1 de abril de 2019, <https://news.8btc.com/alert-lazarus-hacker-group-continues-targeting-crypto-using-faked-trading-software>, acedido em 24 de agosto de 2021; Chainalysis, "Enquanto as Corretoras Implementam Medidas de Segurança, os Hackers Tornam-se Mais Sofisticados (As Exchanges Beef Up Security Measures, Hackers Get More Sophisticated)", 21 de janeiro de 2020, <https://blog.chainalysis.com/reports/cryptocurrency-exchange-hacks-2019>, accessed 25 August 2021.

A formação é fundamental, assim como proteger fisicamente o VASP contra estes tipos de ataques. Os funcionários deverão frequentar sessões periódicas de formação em cibersegurança e saber o que esperar e como identificar e-mails, anexos, links e programas potencialmente suspeitos. Deverão participar nestas sessões todos os funcionários, não apenas os envolvidos no programa de conformidade. Os VASP também deverão investir especificamente numa infraestrutura de TI e de cibersegurança apropriada de modo a garantir que os atacantes não se conseguem infiltrar no sistema a partir do exterior.[20]

Requisitos para a listagem de ativos

Em virtude do crescente interesse dos agentes criminosos pelas moedas de privacidade (privacy coins), que potencialmente lhes permitem mover AV sem serem detetados, é fundamental ter em consideração

20. Para obter informações adicionais sobre as salvaguardas de cibersegurança recomendadas, consulte Cloud Security Alliance, "Orientações de Segurança para a Troca de Cripto-Ativos (Crypto-Asset Exchange Security Guidelines)", 13 de abril de 2021, <https://cloudsecurityalliance.org/artifacts/csa-crypto-asset-exchange-security-guidelines-abstract/>, acedido em 22 de agosto de 2021.

a capacidade de rastreamento da blockchain para qualquer ativo que esteja listado na plataforma de um VASP. Existem várias opções que podem ajudar a mitigar os riscos que as moedas de privacidade representam. Uma opção é simplesmente oferecer exclusivamente ativos com blockchains transparentes (ou seja, não aceitar nenhuma moeda de privacidade). Se esta não for uma solução apropriada e a listagem de moedas de privacidade for um risco aceite e fizer parte da estratégia comercial do VASP, devem ser tidas em consideração as seguintes mitigações do risco:

- Listar apenas um grupo seleto de moedas de privacidade que tenham, pelo menos, alguma medida de transparência (por exemplo, Zcash) e para as quais esteja disponível uma análise de rastreamento da blockchain.
- Permitir a utilização de moedas de privacidade apenas nos casos de transações de AV para AV (ou seja, permitir que sejam negociadas moedas de privacidade para outros AVA, mas não para dinheiro) num esforço para dificultar o “resgate de dinheiro”.
- Permitir que os clientes transacionem em moedas de privacidade apenas quando estas são submetidas a medidas de identifição e diligëncia reforçada (EDD) e quando a transação de moedas de privacidade está sujeita a limites e limiares estritos.

IV. Monitorização de sanções e de pessoas politicamente expostas (PPE)

AS SANÇÕES APLICAM-SE a todos os clientes e transações, independentemente do valor. Os VASP devem aderir plenamente às listas de sanções internacionais e nacionais relevantes de modo a evitar ter contas para os agentes designados, ou para qualquer pessoa detida, controlada, a agir em nome ou sob a direção dos agentes designados. O rastreio de sanções deve ser realizado na primeira verificação da identidade e periodicamente ao longo de toda a relação de negócio,[21] em quaisquer transações de entrada e saída, ou quando existirem adições às listas de sanções.

O Gabinete de Controlo de Ativos Estrangeiros dos EUA (US Office of Foreign Assets Control, OFAC) também incluiu previamente endereços de AV na sua lista de sanções, que devem ser sinalizados além de quaisquer nomes listados.[22] O OFAC também sancionou muitos indivíduos e grupos por atividades de evasão às sanções baseadas em AV. Recomenda-se que as listas de sanções dos EUA sejam tidas em consideração além de quaisquer listas internacionais. O OFAC incluiu especificamente endereços de AV pertencentes a agentes de branqueamento em nome da Coreia do Norte, mostrando a importância destas listas na abordagem do risco de financiamento da proliferação.

Estudo de caso 2: Tian Yinyin e Li Jiadong (2020)

Em março de 2020, o OFAC sancionou Tian Yinyin e Li Jiadong, dois cidadãos chineses que efetuam o branqueamento de AV em nome da Coreia do Norte. Estes agentes foram sancionados ao abrigo dos programas CYBER2 e DPRK3 dos EUA, e identificados como associados ao grupo de hackers Norte-Coreano, o Grupo Lazarus.

A lista do OFAC para cada indivíduo inclui não apenas as suas informações pessoais, como também todos os endereços Bitcoin associados conhecidos. Tian, por exemplo, tem oito endereços Bitcoin listados. As listas também incluem pseudónimos conhecidos, neste caso, as identificações online dos perpetradores.

21. Por exemplo, quando os dados pessoais do cliente (diretores, propriedade, detalhes de identificação) sofrerem alterações.
22. Esta prática teve início em 2018, quando o OFAC listou os endereços de AV dos agentes cibernéticos filiados ao Irão. Consulte o Departamento do Tesouro dos EUA, "O Tesouro Designa Facilitadores Financeiros de Atividade Cibernética Maliciosa Sediados no Irão e pela Primeira Vez Identifica Endereços de Moeda Digital Associados (Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses)", comunicado de imprensa, 28 de novembro de 2018, <https://home.treasury.gov/news/press-releases/sm556>, acedido em 24 de agosto de 2021.

Fonte: Para obter informações adicionais sobre as listas do OFAC, consulte Departamento do Tesouro dos EUA, "Criptomoeda para o Grupo Lazarus (Treasury Sanctions Invididuals Laundering Cryptocurrency for Lazarus Group)", 2 de março de 2020, <https://home.treasury.gov/news/press-releases/sm924>, acedido em 24 de agosto de 2021; OFAC, <https://sanctionssearch.ofac.treas.gov/Details.aspx?id=28263>, acedido em 24 de agosto de 2021.

Além das listas de sanções, todos os agentes ou grupos mencionados nos relatórios do Painel de Peritos da ONU devem ser incluídos no rastreio de sanções. Para obter informações adicionais sobre estes relatórios, consulte o Anexo I.

Os VASP também devem ter em consideração o rastreio dos meios de comunicação e a consulta de relatórios de tipologia por ONGs e pelo setor privado, incluindo empresas de análise de blockchain e empresas de cibersegurança. Estes agentes publicam periodicamente resultados tanto sobre sinais de alerta da utilização de AV pela Coreia do Norte assim como sobre indivíduos e organizações filiadas à Coreia do Norte. Da mesma forma, os VASP devem realizar o rastreio dos clientes assim como continuar a monitorizar para verificar se são (ou estão a interagir com) uma pessoa politicamente exposta (PPE).[23] Se for esse o caso, deve ser realizada uma EDD. Para orientações adicionais sobre EDD, ver infra.

23. O GAFI define uma pessoa politicamente exposta (PPE) como "um indivíduo a quem é ou foi confiada uma função proeminente" e que pode estar "em posições que podem ser abusadas com o objetivo de branquear [fundos ilícitos]". Consulte GAFI, "Orientação do GAFI: Pessoas Politicamente Expostas (Recomendações 12 e 22) (FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22))", junho de 2013, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf>, acedido em 22 de agosto de 2021.

V. Integração

A INTEGRAÇÃO É O passo seguinte do ciclo de conformidade. Os VASP têm frequentemente preocupações sobre o nível de informação a pedir aos clientes no primeiro contacto. Embora as empresas possam operar de forma diferente e as jurisdições tenham requisitos diferentes, existem alguns princípios e atividades de boas práticas comuns que irão garantir a maior probabilidade possível de detetar atividades suspeitas.

Processos de Conheça o Seu Cliente (Know Your Customer, KYC)

Os processos de KYC são padrão nos bancos e devem ser igualmente padrão nos VASP. Infelizmente, um relatório de 2020 indicou que 56% dos VASP globais têm processos de KYC fracos ou com lacunas.[24] Podem ser dados passos iniciais simples de modo a garantir que um VASP não se enquadra neste grupo.

Muitos VASP permitem a criação de contas sem verificar a identidade, mas exigem informações adicionais para enviar ou receber fundos. Alguns VASP requerem inclusive uma verificação antes da criação da conta, enquanto que outros requerem apenas KYC quando envolvem dinheiro.

As boas práticas dizem que o KYC deve ser realizado antes de os fundos serem depositados ou aceites pelo cliente, quer isto ocorra no momento da criação da conta ou imediatamente antes da primeira transação ser iniciada.

A primeira consideração é a identificação do cliente e a verificação dessa identidade. Embora as autoridades reguladoras possam exigir informações adicionais específicas, devem ser recolhidas, no mínimo, as seguintes informações dos indivíduos:

- Nome, data de nascimento e nacionalidade (verificada através de processo oficial de identificação governamental).
- Endereço verificado utilizando um documento comprovativo do endereço, tal como um extrato bancário, fatura de serviços públicos, documento fiscal emitido pelo governo, documento de seguro da casa, ou certificado ou residência, ou através de meios digitais que forneçam uma garantia razoável sobre a localização física do cliente.

Adicionalmente, devem ser recolhidas, no mínimo as seguintes informações de pessoas coletivas:

- Nome, registo, endereço e estado (verificado através número da empresa ou de documentos de registo e registos governamentais relevantes).
- Informações de identificação de membros principais da administração, incluindo pessoas autorizadas a efetuar transações na conta do cliente.

24. CipherTrace, "Relatório de risco geográfico da CipherTrace 2020: KYC de VASP por Jurisdição (CipherTrace 2020 Geographic Risk Report: VASP KYC by Jurisdiction)", outubro de 2020, pág. 4, <https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/>, acedido em 24 de agosto 2021.

- Estrutura da propriedade.

Deve ser realizado o processo de KYC (e a CDD contínua) não apenas em relação aos próprios clientes, como também em relação a quaisquer proprietários beneficiários, assim como em relação a quaisquer pessoas que atuem em nome do cliente.

Os VASP também devem garantir que os seus processos de verificação da informação são abrangentes. Isto inclui solicitar os documentos oficiais mencionados acima e garantir a sua legitimidade, assim como ter em consideração outros mecanismos de KYC, quer durante a integração quer no momento de uma transação suspeita. Estes requisitos adicionais podem incluir:

- Selfies tiradas através da própria aplicação, incluindo um teste de "vida", para provar que o rosto carregado é o de uma pessoa que está viva no momento da fotografia.
- Chamadas de vídeo.

As verificações da identidade e os testes de vida são fundamentais para uma conformidade eficaz, especialmente quando se trata de táticas utilizadas pelos agentes envolvidos no financiamento da proliferação. Em 2020, os branqueadores que movimentavam fundos em nome da Coreia do Norte não podiam cumprir os requisitos de conformidade das chamadas de vídeo num VASP, o que, idealmente, teria impedido que os fundos fossem branqueados através da plataforma.

Estudo de caso 3: 'VCE3' (2020)

Tal como no caso descrito no Estudo de Caso 2, além das sanções do OFAC, o Departamento de Justiça dos EUA acusou Tian Yinyin e Li Jiadong de branqueamento num valor superior a 100 milhões de dólares em várias criptomoedas em nome da Coreia do Norte. As moedas foram obtidas através de ataques de hackers Norte-Coreanos ao VASP e Tian e Li tentaram movimentar os fundos através de múltiplos VASP, com resultados amplamente bem sucedidos.

De modo a fornecer documentação suficiente aos VASP durante o processo de integração, Tian e Li editaram fotos de indivíduos utilizando informações pessoais identificáveis roubadas. Um VASP (referido como VCE3) não ficou satisfeito com a imagem fornecida e solicitou uma chamada de vídeo com o titular da conta, a qual foi negada. Apesar disso, o VCE3 aceitou transações de Tian e Li, recebendo quase 2 milhões de dólares dos fundos roubados na conta dos agentes criminosos. Se esta chamada de vídeo e a subsequente EDD, a criação de relatórios e/ou a recusa de serviços tivessem sido uma exigência de todos os VASP envolvidos no branqueamento, os fundos não poderiam ter sido branqueados através da plataforma.

Fonte: Departamento de Justiça dos EUA, "Dois Cidadãos Chineses Acusados de Branqueamento de Capitais num Valor Superior a 100 milhões de dólares em Criptomoedas Resultantes do Ataque de Hackers à Corretora (Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack)", 2 de março de 2020, <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack>, acedido em 24 de agosto de 2021.

Natureza e Objetivo da Relação de Negócio

Tão importante como a identificação do cliente é a natureza e o objetivo da relação de negócio. A única forma de compreender eficazmente a aparência de uma atividade suspeita relativamente a um cliente específico é compreender a aparência de uma atividade normal, ou a aparência que se espera que tenha para esse cliente. De modo a compreender plenamente a natureza e o objetivo da relação durante a integração, devem ser solicitadas ao cliente, no mínimo, as seguintes estimativas:

- Frequência expetável das transações.[25]
- Dimensão expetável das transações.
- Volume expetável de transações.

Origem e Destino dos Fundos

É essencial, como VASP, conhecer tanto a origem como o destino de quaisquer fundos que sejam movimentados através da plataforma. Em particular, quando é necessária EDD, os VASP devem reunir informações sobre a origem dos fundos de um cliente e verificar a legitimidade antes de realizar qualquer negócio em nome do cliente. Para orientações adicionais sobre EDD, consulte a secção dedicada mais abaixo no documento.

Do mesmo modo, quando um cliente está a receber fundos ou envolvido em transações, o VASP deve tentar obter informações relevantes sobre a outra parte.[26] As ferramentas de análise de blockchain podem fornecer uma melhor perceção da origem e do destino final dos fundos, e são um passo recomendado para tal.

25. Aqui, “transacção” refere-se a depósitos, levantamentos e movimentos.
26. Está em discussão a possibilidade total, em conformidade com a Recomendação 16 do GAFI. Por enquanto, as corretoras devem solicitar as informações que conseguirem obter dos clientes. Consulte GAFI, “Normas Internacionais Sobre o Combate ao Branqueamento de Capitais e o Financiamento do Terrorismo e da Proliferação: As recomendações do GAFI”, pág. 17.

VI. Monitorização do Acompanhamento Contínuo da Relação de Negócio.

APÓS A INTEGRAÇÃO, o passo seguinte é garantir a continuidade e a eficácia da CDD nos clientes existentes. Isto significa a monitorização das transações num esforço para identificar qualquer atividade invulgar, tal como um desvio da atividade de transação expetável ou antecipada, e compreender o raciocínio e o objetivo subjacente a qualquer variação que se identifique na plataforma. Atividades invulgares ou suspeitas que não possam ser explicadas pelo cliente podem indicar ligações a BC/FT/FP. Deve existir um escrutínio constante da atividade do cliente ao longo da relação de modo a garantir que a atividade é consistente com o processo de KYC realizado durante a integração, e que a natureza e objetivo do negócio se mantém consistente com o fornecido pelo cliente como parte do processo de integração e de KYC. Quaisquer alterações significativas devem ser documentadas e questionadas. As informações do processo de KYC também devem ser revistas periodicamente, com base em eventos de risco ou de ativação, tais como uma mudança de endereço.

Quaisquer clientes que sejam considerados de maior risco durante a integração ou em qualquer ponto durante o processo de CDD devem ser sujeitos a uma monitorização mais frequente e minuciosa.

Os VASP também devem garantir que todos os documentos e informações apresentados durante a integração são mantidos atualizados durante toda a relação.

Quando os clientes necessitam de EDD, a origem e o destino dos fundos identificados durante a integração deve continuar a ser consultada ao longo da relação.

Monitorização Manual Vs Automática

Qualquer sistema de monitorização de transações tem como objetivo sinalizar transações e/ou atividades suspeitas ou invulgares para análise posterior. Quaisquer atividades sinalizadas devem ser analisadas imediatamente e pelas pessoas com a formação apropriada nessa área, que então tomarão as medidas necessárias como resposta aos resultados, tais como reportar às autoridades reguladoras relevantes e/ou submeter um relatório de transação/atividade suspeita (STR/SAR). Isto pode ocorrer durante o processo de KYC, quando uma transação é iniciada e é sinalizada, ou após a transação ter ocorrido.

Embora seja possível a monitorização manual e o rastreio de blockchains, a utilização de soluções automatizadas de análise de blockchains de terceiros é altamente recomendada. A análise de blockchains permite uma compreensão mais abrangente de quaisquer padrões de comportamento, assim como a capacidade de sinalizar quaisquer endereços e carteiras de criminosos. As classificações do risco dos clientes também são significativamente mais acentuadas quando examinadas através da análise de blockchains. A análise de blockchains deve incluir o rastreio da carteira antes e depois da transação de modo a identificar a origem e o destino dos fundos. A análise de blockchains e uma melhor compreensão

dos padrões de transação, assim como a coordenação com as forças de segurança, permite que os VASP reajam rapidamente a qualquer ataque de hackers ou roubo de fundos e os congelem conforme apropriado, uma técnica que já foi utilizada anteriormente no combate ao financiamento da proliferação através de AV.

Estudo de caso 4: 'Exchange 9' (2019)

O Departamento de Justiça dos EUA abriu uma queixa de confiscação civil em agosto de 2020, identificando os ataques de hackers a VASP por agentes norte-coreanos, que branquearam fundos através de mercados não regulamentados de instrumentos financeiros chineses.

A queixa afirma que, em dezembro de 2019, um dos perpetradores tentou converter o Ethereum roubados em Bitcoin através de um VASP (Exchange 9). Os Ethereum roubados foram o fruto de um ataque de hackers a um VASP (Exchange 2) diferente, que tinha sido divulgado. Como resultado, a Exchange 9 congelou os fundos envolvidos na transação, uma vez que as moedas roubadas à Exchange 2 foram sinalizadas no seu sistema. Os fundos permanecem congelados na Exchange 9.

Fonte: Departamento de Justiça dos EUA, "Os Estados Unidos Apresentam um Pedido para Confiscar 280 Contas em Criptomoedas Ligadas ao Ataque de Hackers a Duas Corretoras por Agentes Norte Coreanos (United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors)", 27 de agosto de 2020, <https://www.justice.gov/usao-dc/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two>, acedido em 24 de agosto de 2021.

Os VASP devem investir não apenas na análise de blockchains, mas também em ferramentas de monitorização para combate ao branqueamento de capitais (CBC) que procurem comportamentos clássicos de monitorização de transações de BC/FT/FP.

Diligência reforçada (EDD)

Deve ser realizada EDD quando uma transação ou conta é sinalizada como tendo um risco particularmente elevado, ou sendo potencialmente suspeita. Podem ser encontrados indicadores específicos de risco elevado na secção seguinte. A EDD depende de uma monitorização eficaz e deve ser aplicada num sistema baseado no risco quando existem suspeitas de atividades de crime financeiro. Existem muitas razões pelas quais a EDD pode ser necessária, incluindo (mas não limitado a) quando um cliente:

- É identificado numa avaliação de risco como apresentando um risco particularmente alto para o crime financeiro.
- Tem uma estrutura de negócios desnecessariamente complexa ou obscura.
- Efetua transações com indivíduos ou entidades em jurisdições de risco elevado.
- Fornece identificação roubada ou falsa durante a integração.
- Se envolve em transações que não correspondem à natureza e ao objetivo da relação.
- Envia, recebe ou movimenta somas invulgarmente elevadas de ativos virtuais ou dinheiro.
- É uma PPE.
- Não consegue explicar adequadamente o objetivo de uma transação

Vale a pena realçar que a definição de “somas elevada” de ativos virtuais é relativa e irá depender da dimensão do VASP e da natureza da relação de negócio.

Se uma ou mais destas preocupações for identificada, deve ser iniciada a EDD. O primeiro passo é a obtenção de informações de identificação adicionais. Parte destas podem ser exigidas ao cliente e outra parte pode ser possível de verificar separadamente através de fontes abertas. No caso de uma PPE, por exemplo, seriam necessários título e detalhes sobre o cargo ocupado.

Também deve ser realizada uma verificação adversa/negativa nos meios de comunicação para criar um perfil completo. Demasiados resultados negativos nesta verificação podem indicar um cliente com o qual o risco de continuar uma relação é demasiado elevado.

As entrevistas por telefone ou vídeo também podem ser ferramentas necessárias para compreender a natureza e o objetivo das transações.

Muitos VASP também registram os endereços de IP dos clientes, assim como a localização de quaisquer caixas automáticas/bancos/outros VASP envolvidos em qualquer corretora, de modo a garantir que essas localizações correspondem à relação esperada.

As redes virtuais privadas (virtual private networks, VPN) também podem ser um indicador de risco que pode resultar em EDD em circunstâncias específicas. Embora existam utilizações legítimas das VPN para criar ambientes de negociação seguros, deve existir, pelo menos, um ponto de contacto onde uma VPN não esteja ativa, como o registro com um VASP, para que o VASP possa registar um endereço de IP genuíno.

VII. Indicadores e Sinais de Alerta de Risco Elevado

EXISTEM VÁRIOS INDICADORES e sinais de alerta de risco elevado que podem levar a EDD, STR/SAR ou mesmo ao congelamento de fundos. O GAFI, o setor privado e os reguladores nacionais listaram exaustivamente os sinais de alerta identificados com os correspondentes estudos de caso. Consulte o Anexo I para obter informações adicionais.

Utilização de Misturadores ou de Serviços de Anonimização

Os serviços de misturadores, carteiras de privacidade e CoinJoin[27] proporcionam vários tipos de ocultação das transações e aumentam a privacidade dos utilizadores. Cada um oculta o percurso da transação e torna o rastreio da blockchain cada vez mais difícil, e por vezes impossível.[28]

É essencial que os VASP tenham a capacidade de identificar transações com misturadores e carteiras de privacidade, e tratar as transações relacionadas com misturadores como apresentado maior risco na maioria dos casos.

Esta gestão do risco pode incluir:

- Criar uma lista aprovada de misturadores conhecidos e/ou de confiança ou de serviços CoinJoin com os quais os clientes têm permissão para realizar transações.
- Permitir apenas relações com misturadores de confiança sob condições específicas (sob um determinado limiar de valor).

Sabe-se que os branqueadores e hackers que trabalham em nome de proliferadores têm utilizado misturadores cada vez mais frequentemente. O Grupo Lazarus, em particular, é conhecido pelo seu interesse e utilização de serviços de mistura para ocultar o rastro das transações.

---

27. A CoinJoin é uma estratégia de anonimização que mantém as transações em criptomoeda privadas. Utiliza contratos inteligentes para misturar moedas em novas transações, onde os resultados são o mesmo número de moedas, mas de várias transações diferentes, ocultando a origem e o destino pretendido.
28. Para obter informações adicionais sobre as especificidades destas tecnologias, consulte Anton Moiseienko e Kayla Izenman, "Da Intenção à Ação: Próximos Passos na Prevenção do Abuso Criminoso da Criptomoeda" (From Intention to Action: Next Steps in Preventing Criminal Abuse of Cryptocurrency)", Artigos Ocasionais do RUSI (setembro de 2019), pág. 19–24; Andrea O'Sullivan, "O Que São Misturadores e "Moedas de Privacidade"? ('What are Mixers and "Privacy Coins)", Coin Center, 7 de julho de 2020, <https://www.coincenter.org/education/advanced-topics/what-are-mixers-and-privacy-coins/>, acedido em 24 de agosto dde 2021.

Case Study 5: Grupo Lazarus (2018)

No seu Relatório de Crime com Criptomoedas de 2020 (2020 Crypto Crime Report), a empresa norte-americana Chainalysis identificou as formas como o Grupo Lazarus tinha mudado os seus métodos de 2019 para 2020. Uma das áreas destacadas foi a crescente utilização de misturadores e carteiras CoinJoin por parte do grupo Lazarus.

De acordo com a Chainalysis, "48% dos fundos roubados pelo Lazarus foram movidos para carteiras CoinJoin" em 2019. No ataque de hackers àDragonEx (Estudo de Caso 1), por exemplo, o grupo Lazarus mudou altcoins roubados como Ethereum e Litecoin para o VASP, trocando-os por Bitcoin. Em seguida, moveram os Bitcoin para várias carteiras locais antes de mover os fundos para uma Carteira Wasabi, que mistura as moedas através do protocolo CoinJoin.

Embora o Relatório de Crime com Criptomoedas 2021 apresente outras técnicas que estão a ser utilizadas pelo grupo Lazarus, as estatísticas da Chainalysis também mostram que a utilização de misturadores pelo grupo Lazarus para branquear fundos roubados aumentou ainda mais em 2020.

Fonte: Chainalysis, "O Estado do Crime com Criptomoedas 2020 (The 2020 State of Crypto Crime)", janeiro de 2020, <https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf>, acedido em 24 de agosto de 2021; Chainalysis, "O Estado do Crime com Criptomoedas 2021 (The 2021 State of Crypto Crime)", 16 de fevereiro de 2021, <https://go.chainalysis.com/2021-Crypto-Crime-Report.html>, acedido em 2 de setembro de 2021.

VIII. Dever de Comunicação

O DEVER DE COMUNICAÇÃO pode variar significativamente entre jurisdições, embora algumas jurisdições possam ainda não exigir nenhuma notificação por parte dos VASP. No entanto, os VASP devem estar preparados para operar no mais elevado padrão - juntamente com os de outros prestadores de serviços financeiros regulamentados - e devem estar plenamente cientes dos requisitos da sua jurisdição. Os funcionários deverão reportar as atividades que considerem suspeitas, devendo ser identificado um processo claro, com os funcionários a reportar ao responsável designado que iniciará uma investigação adequada e reportará às autoridades competentes.

Este processo deverá ser claramente informado aos funcionários. Os termos relevantes deverão ser padronizados e definidos para facilitar a compreensão tanto por parte da unidade de inteligência financeira relevante como por parte do VASP. Exemplos de notificações podem incluir SAR/STR registado devido a:

- Preocupações sobre a origem dos fundos recebidos na carteira de um utilizador.
- Transações estruturadas em pequenos montantes, logo abaixo dos limiares de notificação.
- Transferências imediatas de AV para múltiplos VASP que operam noutras jurisdições, especialmente em jurisdições com regulamentos fracos em matéria de VASP.
- A carteira de um utilizador a receber fundos de endereços de AV que foram previamente sinalizados em relação a fundos roubados ou a ransomware.
- Documentos ou fotografias falsificadas ou editadas e utilizadas para fins de identificação.
- Incapacidade de um VASP em obter as informações solicitadas ao cliente, ou um cliente que se recusa a fornecer documentos CDD ou informações sobre a origem dos fundos.

Note que esta não é uma lista extensiva e deverão ser realizadas notificações sempre que os processos internos sinalizarem atividades suspeitas.[29]

29. A Autoridade Financeira das Ilhas Caimão publicou uma lista de outros possíveis sinais de alerta que desencadeariam requisitos de notificação para os VASP na sua jurisdição. Consulte Autoridade Financeira das Ilhas Caimão, "Notas Orientadoras (Alterações) sobre a Prevenção e Deteção de Branqueamento de Capitais, Financiamento do Terrorismo e Financiamento da Proliferação nas Ilhas Caimão (Guidance Notes (Amendments) on the Prevention and Detection of Money Laundering, Terrorist Financing, and Proliferation Financing in the Cayman Islands)", fevereiro de 2021, pág. 13.

IX. Considerações finais

EMBORA A CONFORMIDADE e requisitos normativos direcionados aos VASPs tenha aumentado nos últimos anos, ainda existe um progresso considerável a ser feito. É absolutamente essencial que os VASP realizem avaliações do risco e tenha uma abordagem coordenada baseada no risco para as atividades de BC/FT/FP.

O GAFI espera que os países implementem medidas preventivas semelhantes para os VASP às que requerem para as instituições financeiras tradicionais, incluindo uma supervisão apropriada do setor e requisitos de licenciamento ou registo. Embora as Recomendações do GAFI sejam direcionadas para os seus países associados, e não aos próprios VASP, a implementação das Recomendações e Orientações por parte dos países tem exigido cada vez que os VASP as cumpram, e espera-se que isto aumente. Os VASP têm agora a oportunidade de compreender o que é exigido ao setor e de cumprir proativamente caso a sua jurisdição ainda não tenha implementado as Recomendações.

Existe também uma quantidade considerável de conversações sobre a Recomendação 16 do GAFI em matéria de transferências eletrónicas, que aconselha os VASP a tratar todas as transações de AV como transferências transfronteiriças, dada a natureza sem fronteiras da tecnologia. [30] Isto exigiria a partilha de informações entre os VASP a um nível imprevisto, incluindo a detenção e o envio a outros VASP envolvidos numa transação, informações tanto sobre a origem dos fundos como sobre o beneficiário. Existem actualmente várias organizações públicas e privadas que estão a investigar soluções tecnológicas para a Recomendação 16.[31]

Os VASP devem ter como objetivo cumprir de forma proativa e estar focados numa abordagem baseada no risco de modo a mitigar eficazmente as ameaças provenientes de países com proliferação, com o objetivo de explorar o sistema para seu próprio benefício.

Uma vez que as orientações do GAFI estão a ser alteradas para incluir o FP, os VASP devem estar particularmente atentos a estes tipos de agentes. Os estudos de caso continuam a indicar a utilizaçãoo em larga escala de AV para evasão a sanções e serão certamente divulgados mais no futuro. De modo a mitigar tanto o risco para as empresas como os riscos internacionais e geopolíticos destas ações, os VASP devem aplicar o nível de conformidade mais abrangente possível, conforme ilustrado nesta orientação e nas leituras recomendadas associadas (consulte o Anexo II).

30. GAFI, “Normas Internacionais Sobre o Combate ao Branqueamento de Capitais e o Financiamento do Terrorismo e da Proliferação: As recomendações do GAFI”, pág. 77.
31. Por exemplo, consulte Ian Allison, “Os Gigantes das Criptomoedas dos EUA Criam a Primeira Versão da Ferramenta “Regra de viagens” compatível com o GAFI (US Crypto Giants Build First Version of FATF-Compliant “Travel Rule” Tool)”, CoinDesk, 25 de junho de 2021, <https://www.coindesk.com/us-crypto-giants-build-first-version-of-fatf-compliant-travel-rule-tool>, acedido em 24 de agosto de 2021.

Anexo I: Lista de verificação

A lista de verificação abaixo resume este documento de orientação. Para mais detalhes sobre qualquer um dos passos, consulte a secção apropriada no documento.

Pré-requisitos

- □ O prestador de serviços de ativos virtuais (VASP) tem uma estrutura de governança e uma equipa de conformidade adequada.
    - o A administração supervisiona e é responsável pelo programa de combate ao crime financeiro.
    - o Existe um Diretor de Conformidade (Chief Compliance Officer, CCO).
    - o Se aplicável, existe um Diretor de Conformidade das Sanções.
    - o Os colaboradores de nível médio e júnior estão informados sobre todos os procedimentos de conformidade relevantes que se podem manifestar noutras áreas de negócios do VASP.
    - o Os colaboradores recebem formação periodicamente em matéria de tendências e tipologias de CBC/FT/FP.
- □ O VASP realizou, pelo menos, uma avaliação do risco abrangente e documentada nos últimos dois anos.
    - o O VASP ativou requisitos de controlo principais para abordar áreas de risco elevado agiu com base nos resultados da avaliação do risco.
- □ O VASP tem protocolos de cibersegurança eficazes.
    - o Os funcionários participam periodicamente em sessões de formação em matéria de cibersegurança.
    - o Existe uma infraestrutura de TI e de cibersegurança adequada e abrangente.
- □ O VASP tem requisitos apropriados de listagem de ativos.

Monitorização de Sanções e de Pessoas Politicamente Expostas (PPE)

- □ O VASP realiza rastreios de sanções para todos os clientes.
- □ O VASP utiliza todo o material disponível para realizar um rastreio completo.

- O VASP adere plenamente às listas de sanções internacionais e americanas.
- O VASP monitoriza para os agentes incluídos nos Relatórios do Painel de Peritos da ONU.
- O VASP consulta os relatórios de tipologia das ONGs e também utiliza rastreio negativo nos meios de comunicação.

□ A monitorização das sanções e das PPE está implementada. O VASP monitoriza carteiras de ativos virtuais (AV) pré-transações e realiza uma monitorização contínua das transações.

- A monitorização é realizada na primeira verificação da identidade.
- A monitorização é realizada ao longo de toda a relação de negócio.

Integração

□ O VASP tem processos abrangentes de Conheça o seu cliente (know-your-customer, KYC) implementados.

- Os processos de identificação dos clientes requerem, no mínimo, o nome completo, a data de nascimento, a nacionalidade e o endereço do cliente.
- As informações pessoais dos clientes são verificadas através de documentos de identificação oficiais do governo. Os endereços são verificados utilizando um documento comprovativo do endereço ou meios digitais apropriados.
- A identificação da pessoa coletiva requer, no mínimo, o nome, o registo, o endereço, o estado, as informações de identificação dos membros da administração principais e a estrutura de propriedade da entidade.
- As informações da pessoa coletiva são verificadas utilizando o número da empresa, os documentos de registo governamentais relevantes e os registos.
- São realizados processos de KYC e CDD contínuos em quaisquer proprietários benéficos ou em pessoas que atuam em nome do cliente.
- São considerados ou implementados outros mecanismos de KYC, incluindo selfies tiradas na aplicação e chamadas de vídeo, verificados através de testes de vida.

□ O VASP compreende plenamente a natureza e o objetivo da relação de negócio.

- O cliente fornece a frequência expetável das transações.
- O cliente fornece a dimensão expetável das transações.

- O cliente fornece o volume expetável de transações.

□ O VASP compreende, na medida do possível, tanto a origem como o destino de quaisquer fundos movimentados.

Monitorização e CDD Contínua

□ Todos os documentos e informações submetidos ao VASP durante a integração são mantidos atualizados durante toda a relação.

□ O VASP tem um sistema de monitorização manual ou automático das transações.

- O VASP utiliza um sistema que permite o rastreio exaustivo de sanções.
- O VASP compreende as limitações do sistema em vigor.

□ O VASP considerou os benefícios de implementar análises de blockchains em grande escala.

□ O VASP realiza uma auditoria jurídica (acompanhamento da relação de negócio) reforçada quando uma transação ou conta é sinalizada como sendo de risco elevado.

- O VASP compreende quando e como realizar EDD.

Indicadores e Sinais de Alerta de Risco Elevado

□ O VASP gere as relações com os misturadores.

- O VASP cria uma lista aprovada de misturadores conhecidos e/ou de confiança e de serviços CoinJoin.
- O VASP apenas permite relações com misturadores de confiança sob condições específicas.

Requisitos de Notificação

- □ O VASP está ciente e compreende as Recomendações do GAFI.
- □ O VASP está ciente, compreende e cumpre toda a regulamentação jurisdicional apropriada.
- □ O VASP está ciente, compreende e cumpre os requisitos de notificação da sua jurisdição.
- □ É informado aos funcionários um processo claro sobre como notificar transações suspeitas e o que enviar especificamente ao responsável interno designado.
- □ O responsável de notificação designado sabe especificamente como notificar às autoridades competentes e como escalar uma situação.
- □ Os termos relevantes são padronizados e definidos internamente de modo a facilitar a compreensão.

Anexo II: Fontes de informação adicional

Orientações do GAFI sobre Ativos Virtuais e Prestadores de Serviços de Ativos Virtuais (FATF Guidance on Virtual Assets and Virtual Asset Service Providers)

GAFI, "Orientação para uma Abordagem Baseada no Risco: Ativos Virtuais e Prestadores de Serviços de Ativos Virtuais (Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers)", junho de 2019, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>.

GAFI, "Revisão de 12 meses: Ativos Virtuais e VASP (12-Month Review: Virtual Assets and VASPs)", julho de 2020, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html>.

GAFI, "Segunda Revisão de 12 meses das Normas Revistas do GAFI - Ativos Virtuais e VASP (Second 12-Month Review of Revised FATF Standards – Virtual Assets and VASPs)", julho de 2021, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html>.

GAFI, "Normas Internacionais Sobre o Combate ao Branqueamento de Capitais e o Financiamento do Terrorismo e da Proliferação: As Recomendações do GAFI (International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations)", junho de 2021.

Orientações Sobre a Avaliação do Risco de Financiamento da Proliferação de Prestadores de Serviços de Ativos Virtuais (Guidance on Virtual Asset Service Provider Proliferation Financing Risk Assessment)

Anagha Joshi, Emil Dall e Darya Dolzikova, "Guia para a Realização de uma Avaliação Nacional dos Riscos de Financiamento da Proliferação (Guide to Conducting a National Proliferation Financing Risk Assessment)", RUSI, Maio de 2019.

BitAML, "Criptoconformidade 101: Precisa de uma Avaliação do Risco? (Cryptocompliance 101: Do You Need a Risk Assessment?)" Em Criptomoeda, a Resposta é Sim" (In Crypto, the Answer Is Yes)", 28 de janeiro de 2019, <https://bitaml.com/2019/01/28/risk-assessment-crypto/>.

GAFI, "Orientação sobre a Avaliação e Mitigação dos Riscos de Financiamento da Proliferação (Guidance on Proliferation Financing Risk Assessment and Mitigation)", junho de 2021, <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf>.

Ministério da Justiça do Governo do Grão-Ducado do Luxemburgo, "Avaliação Vertical do Risco de BC/FT: Prestadores de Serviços de Ativos Virtuais (ML/TF Vertical Risk Assessment: Virtual Asset Service Providers)", dezembro de 2020, <https://mj.gouvernement.lu/dam-assets/dossiers/blanchiment/ML-TF-vertical-risk-assessment-on-VASPs.pdf>.

Departamento de Assuntos Internos do Governo da Nova Zelândia, "Avaliação od Risco do Setor das Instituições Financeiras (Financial Institutions Sector Risk Assessment)", Parte 19: Riscos do Setor – Prestadores de Serviços de Ativos Virtuais (Sector Risks – Virtual Asset Service Providers), dezembro de 2019, <https://static1.squarespace.com/static/5a77b9d390bade7aa2cf8692/t/600e144cc42d5b31a3ccc997/1611535442275/Financial-Institutions-SRA-2019.pdf>.

Indicadores e Sinais de Alerta de Risco Elevado

Chainalysis, "O Relatório do Crime com Criptomoedas da Chainalysisde 2021 (The Chainalysis 2021 Crypto Crime Report)", março de 2021, <https://go.chainalysis.com/2021-Crypto-Crime-Report.html>.

Elliptic, "Cumprimento de Sanções em Criptomoedas: Utilização da Análise de Blockchains para Navegar em Campos Minados (Sanctions Compliance in Cryptocurrencies: Using Blockchain Analysis to Navigate the Minefield)", maio de 2021, <https://www.elliptic.co/hubfs/downloads/Elliptic_Sanctions-Compliance-In_Crypto.pdf>.

GAFI, "Indicadores e Sinais de Alerta de Ativos Virtuais de Branqueamento de Capitais e Financiamento do Terrorismo (Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing)", setembro de 2020, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>.

Centro de Análise de Transações Financeiras e Notificações do Governo do Canadá (FinTRAC), "Indicadores de Branqueamento de Capitais e Financiamento do Terrorismo - Transações em Moeda Virtual (Money Laundering and Terrorist Financing Indicators – Virtual Currency Transactions)", dezembro de 2020, <https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/vc_mltf-eng>.

Departamento do Tesouro dos EUA, Financial Rede de Aplicação da Lei em Crimes Financeiros (FinCEN), "Aconselhamento sobre Atividades Ilícitas Envolvendo Moeda Virtual Conversível (Advisory on Illicit Activity Involving Convertible Virtual Currency)", 9 de maio de 2019, <https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf>.

Fontes Adicionais para Rastreio de Sanções

Departamento de Assuntos Estrangeiros e Sanções Comerciais do Governo Australiano, "'Austrália e Sanções (Australia and Sanctions)", <https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list>.

Serviço de Ação Externa da UE, "Lista Consolidada da Lista de Sanções (Consolidated List of Sanctions List)", <https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions>.

Governo do Canadá, “Lista Consolidada de Sanções Autónomas do Canadá (Consolidated Canadian Autonomous Sanctions List)”, <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/consolidated-consolide.aspx?lang=eng>.

Ministério da Economia, Comércio e Indústria do Japão, “‘Lista de Sanções’ (Sanctions List)”, <https://www.meti.go.jp/english/>.

Gabinete do Tesouro do Reino Unido para a Implementação de Sanções Financeiras, “Lista Sonsolidada de Sanções (Consolidated Sanctions List)”, <https://sanctionssearch.ofsi.hmtreasury.gov.uk/>.

Conselho de Segurança da ONU, “‘Lista Consolidada (Consolidated List)”, <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>.

Conselho de Segurança da ONU, “Relatórios do Painel de Peritos sobre a Resoçução 1718 do Comité de Sanções (DPRK) (Panel of Experts 1718 Sanctions Committee (DPRK) Reports)”, <https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports>.

Gabinete de Controlo de Ativos Estrangeiros dos EUA, “Pesquisa da Lista de Sanções (Sanctions List Search)”, <https://sanctionssearch.ofac.treas.gov/>.