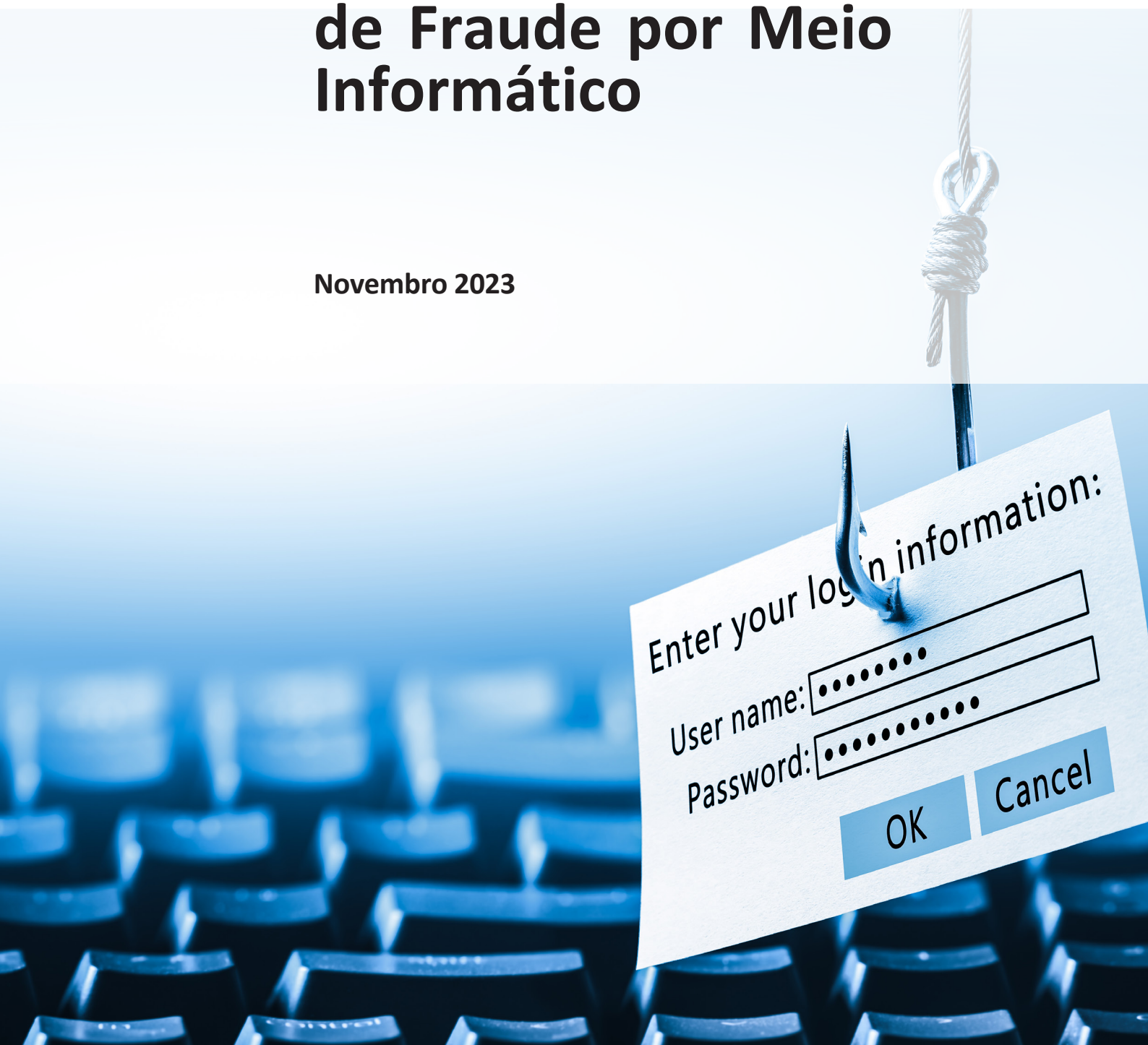
Fluxos Financeireos Ilícitos Provenientes de Fraude por Meio Informático

Novembro 2023



O Grupo de Ação Financeira Internacional (GAFI) é um organismo intergovernamental independente que desenvolve e promove políticas para proteger o sistema financeiro mundial contra o branqueamento de capitais, o financiamento do terrorismo e o financiamento da proliferação de armas de destruição massiva. As recomendações do GAFI são reconhecidas como normas globais de combate ao branqueamento de capitais (ABC) e ao financiamento do terrorismo (CFT). Para mais informações sobre o GAFI, visite www.fatf-gafi.org. O presente documento e/ou qualquer mapa nele incluído são sem prejuízo do estatuto ou da soberania de qualquer território, da delimitação de fronteiras e limites internacionais e do nome de qualquer território, cidade ou zona.

O objetivo do Grupo Egmont de Unidades de Informação Financeira (Egmont Group) é proporcionar um fórum para as unidades de informação financeira (UIF) em todo o mundo, a fim de melhorar a cooperação na luta contra o branqueamento de capitais e o financiamento do terrorismo, e promover a execução de programas nacionais neste domínio. Para mais informações sobre o Grupo Egmont, consultar: www.egmontgroup.org

O papel da Interpol consiste em permitir à polícia dos 195 países membros trabalhar em conjunto para combater a criminalidade transnacional e tornar o mundo um lugar mais seguro. Mantemos bases de dados mundiais que contêm informações policiais sobre criminosos e crimes e prestamos apoio operacional e forense, serviços de análise e formação. Estas capacidades de policiamento funcionam a nível mundial, em apoio a quatro programas globais: criminalidade financeira e corrupção; combate ao terrorismo; cibercrime; e crime organizado e emergente.

Referência para citação:

FATF – Interpol - Egmont Group (2023), *Illicit Financial Flows from Cyber-Enabled Fraud*, FATF, Paris, France, FATF – Interpol - Egmont Group (2023), Illicit Financial Flows from Cyber-Enabled Fraud, FATF, Paris, France, www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/iIllicit-financial-flows-cyber-enabled-fraud.html

Índice

Lista de Siglas

AML/CFT	Combate ao branqueamento de capitais/ financiamento do terrorismo
ATM	Caixa automático/Multibanco
BEC	E-mail empresarial comprometido
CDD	Diligência quanto à clientela/dever de diligência relativo à clientela
CEF	Fraude por meio informático
APNFD	Atividades e Profissões Não Financeiras Designadas
IF	Instituição Financeira
UIF	Unidade de Informação Financeira
IBAN	Número internacional de conta bancária
IP	Protocolo de Internet
LEA	Autoridades de aplicação da lei
BC	Branqueamento de capitais
MLA	Auxílio judiciário mútuo
PSP	Prestador de serviços de pagamento
PPP	Parceria público-privada
COS	Comunicação de operação suspeita
FT	Financiamento do terrorismo
TBML	Branqueamento de capitais mediante operações comerciais
VA	Ativo virtual
VASPs	Prestadores de serviços de ativos virtuais
IBAN	Número internacional de conta bancária virtual
VPN	Rede privada virtual
VoIP	Voz sobre protocolo de Internet

Sumário Executivo

A fraude por meio informático (*Cyber-enabled fraud*, CEF) é um crime organizado de caráter transnacional em crescimento. Os grupos criminosos de CEF encontram-se, muitas vezes, bem estruturados em subgrupos distintos, com áreas de especialização criminal, incluindo o branqueamento de capitais (BC). Estes subgrupos podem também estar livremente organizados e descentralizados em diferentes jurisdições, o que dificulta os esforços para investigar a atividade da CEF. Verificou-se que os grupos de CEF estão ligados a outros tipos de criminalidade, nomeadamente o tráfico de seres humanos e o trabalho forçado nos *call centres* de CEF, bem como ao financiamento da proliferação relacionado com atividades informáticas ilícitas por parte da República Popular Democrática da Coreia (RPDC).

As associações criminosas relacionadas com o BC e os facilitadores profissionais estão envolvidas no processo de CEF-BC. A rede de contas de BC envolve, normalmente, o recurso a ""mulas de dinheiro" (*money mules*), mas também pode incluir empresas de fachada ou empresas legítimas. As redes de BC envolvem ainda diferentes tipos de instituições financeiras (IF), incluindo bancos, prestadores de serviços de pagamento e de remessas e prestadores de serviços de ativos virtuais (VASPs). Para ocultar ainda mais o rasto financeiro dos seus ganhos ilícitos, os criminosos utilizam uma combinação de várias técnicas de BC, em particular, o recurso ao numerário, o branqueamento de capitais mediante operações comerciais (TBML) e serviços não licenciados.

Com a ajuda da digitalização, a tecnologia permitiu que criminosos da CEF desenvolvessem e aumentassem a escala, o âmbito e a velocidade das suas atividades ilícitas. Utilizam várias ferramentas e técnicas para enganar as vítimas ou aproveitar-se do seu estado psicológico e emocional para extrair o máximo de fundos possível. Os grupos da CEF estão a explorar os desenvolvimentos tecnológicos para tornar mais fácil e mais rápido o branqueamento do produto dos seus crimes. Os serviços virtuais, como a abertura remota de contas *online*, também permitem que os criminosos criem facilmente contas no estrangeiro e aí procedam ao BC, sendo as transações financeiras executadas a velocidades quase instantâneas. Os criminosos estão a recorrer às redes sociais e às plataformas de mensagens para recrutar "mulas de dinheiro" além-fronteiras em grande escala, sendo rápidos a explorar as vulnerabilidades que surgem através de novas instituições e produtos financeiros digitais, bem como de setores não tradicionais, como o comércio eletrónico, redes sociais e plataformas de *streaming*.

As jurisdições têm de responder de forma mais eficaz. Para tal, devem:

- Adotar iniciativas para aumentar as denúncias por parte das vítimas e melhorar a comunicação de operações suspeitas;
- Analisar eficazmente os volumosos fluxos de informação, para combater a CEF; e
- Dada a natureza transversal da CEF, é necessário implementar mecanismos de coordenação interna sólidos para a combater e prevenir de forma holística a CEF e o BC conexo.

O local onde ocorre a prática das infrações subjacentes à CEF tende a ser diferente do local onde ocorre o processo de BC. Os produtos do crime podem ser branqueados rapidamente através de uma rede de contas, que muitas vezes abrange várias jurisdições e instituições financeiras. As jurisdições devem colaborar

multilateralmente para intercetar, de forma eficaz e expedita, os produtos da CEF branqueados além-fronteiras. Para o efeito, as jurisdições devem alavancar e sustentar os mecanismos multilaterais existentes (e futuros) (como o I-GRIP da INTERPOL e o projeto BEC do Grupo Egmont) para uma cooperação internacional rápida e intercâmbio de informações, de forma a combater mais eficazmente a CEF.

Por último, o relatório inclui uma lista de indicadores de risco, bem como requisitos e controlos úteis em matéria de luta contra a fraude, que podem ser úteis para as entidades do setor público e privado detetarem e prevenirem a CEF e o BC conexo.

1. Introdução

1. As fraudes e os esquemas *online* têm dominado o panorama da cibercriminalidade. Se não forem controlados, estes fenómenos irão aumentar em sofisticação e representarão uma ameaça e um risco maiores à medida que mais grupos de criminalidade organizada se dedicarem a esta atividade ilícita e aproveitarem as oportunidades oferecidas pelas novas tecnologias, como a inteligência artificial generativa.[1]

2. Durante a Presidência de Singapura, o GAFI adotou uma nova iniciativa destinada a combater os fluxos financeiros ilícitos provenientes de fraudes por meio informático. O presente relatório é o resultado de um projeto conjunto entre o Grupo Egmont, o GAFI e a INTERPOL, primeiro que estas três organizações desenvolveram conjuntamente, refletindo um forte compromisso coletivo para combater o crime organizado transnacional e as suas redes.

1.1. Âmbito de aplicação

3. O presente relatório centra-se no financiamento ilícito resultante de fraudes que são viabilizadas ou conduzidas em ambiente informático que i) envolvem criminalidade transnacional, com intervenientes e fluxos de fundos transfronteiriços e ii) envolvem técnicas enganosas de engenharia social (ou seja, manipulação das vítimas para acederem a informações confidenciais ou pessoais). Reconhecendo as muitas variações deste tipo de fraudes, o presente relatório centra-se nos seguintes tipos de atividades criminosas (fraude por meio informático, CEF):

   - **Fraude com e-mails comerciais comprometidos (BEC)**: as vítimas recebem instruções por e-mail que aparentam ser dos seus clientes ou fornecedores, pedindo-lhes que transfiram fundos para novas contas de pagamento.
   - **Fraude de *phishing***: as vítimas são enganadas para revelarem informações confidenciais, como dados pessoais, detalhes bancários ou credenciais de *login* de contas. O criminoso utilizará então a informação para retirar o dinheiro das contas bancárias das vítimas, abrir novas contas ou efetuar transações fraudulentas.
   - **Fraude de falsificação de identidade nas redes sociais e nas telecomunicações**: inclui cenários em que as vítimas são contactadas através de aplicações móveis ou de redes sociais por criminosos que fingem ser funcionários públicos, familiares ou amigos, explorando a componente emocional das vítimas para as levar a efetuar pagamentos, a dar o acesso às contas ou a realizar operações financeiras, como um pedido de empréstimo ou abertura de uma conta para receber fundos com origem criminosa.
   - **Fraude no comércio *online*/em plataforma de comércio**: as vítimas são ludibriadas por anúncios falsos ou consultores online para plataformas inexistentes ou falsas (fraudulentas) de comércio ou investimento relacionados com ativos fiduciários ou virtuais.

[1] Ver também Fundo Monetário Internacional (Agosto 2023) *Fintech Note: Generative Artificial Intelligence in Finance: Risk Considerations*.

- **Fraude romântica *online***: as vítimas são levadas a enviar dinheiro para criminosos após serem convencidas de que estão numa relação romântica.
- **Fraudes de emprego**: ofertas de emprego falsas em plataformas de redes sociais que levam as vítimas a efetuar pagamentos aos burlões sob vários pretextos, como por exemplo, o pagamento antecipado da compra de mercadorias para aumentar as vendas de uma plataforma comercial ou uma taxa de garantia para assegurar um emprego.

4. O financiamento ilícito relacionado com o *ransomware* e outros crimes cometidos por *malware* não é abrangido pelo âmbito de aplicação do presente relatório. Os leitores devem consultar o relatório do GAFI sobre a luta contra o financiamento do *Ransomware* (março de 2023) para mais informações sobre este fenómeno, bem como informações sobre o branqueamento através de ativos virtuais e prestadores de serviços de ativos virtuais (VASPs) e ainda, sobre os desafios e as boas práticas para a redução dos riscos. Esta informação é relevante, uma vez que os ativos virtuais e os VASPs são por vezes explorados para branquear o produto da CEF.

1.2. Objetivos e estrutura

5. O presente relatório visa reforçar a compreensão do risco das autoridades competentes relativamente à ameaça colocada pela CEF. O relatório baseia-se no trabalho já realizado pelo GAFI e por outros organismos internacionais (incluindo o Grupo Egmont, a Europol e a INTERPOL) e procura identificar desenvolvimentos significativos e emergentes que sejam relevantes para uma melhor compreensão do risco.

- Os **capítulos 2 e 3** do relatório abordam o atual ambiente de risco operacional em relação à CEF, fornecendo informações sobre os riscos, técnicas e tendências da CEF e do branqueamento de capitais conexo (BC), incluindo o impacto e vulnerabilidades da digitalização e das novas tecnologias.
- Os **capítulos 4 e 5** do relatório identificam as boas práticas e as soluções operacionais utilizadas pelas jurisdições para superar os desafios, enfrentar e no combate e desmantelamento da CEF e BC conexo, incluindo mecanismos de cooperação internacional e de recuperação de ativos.

1.3. Metodologia

6. Este projeto foi codirigido por peritos de Singapura (em nome do GAFI), da UIF de Hong Kong/China (em nome do Grupo Egmont) e da INTERPOL. Além disso, as seguintes jurisdições e entidades contribuíram para o trabalho como parte da equipa de projeto: Azerbaijão, Brasil, Bélgica, Canadá, China, Conselho da Europa, Comissão Europeia, Europol, Alemanha, Grupo Intergovernamental de Ação contra o Branqueamento de Capitais na África Ocidental (GIABA), Índia, Itália, Israel, Japão, Malásia, México, Comité de Peritos para a Avaliação das Medidas de Branqueamento de Capitais e Financiamento do Terrorismo (MONEYVAL), Paquistão, Portugal, Arábia Saudita, Togo, Reino Unido e Estados Unidos.

7. As conclusões do relatório baseiam-se:

- Numa revisão da literatura existente e do material de fontes abertas sobre este tópico. Tal inclui dados e investigação efetuados pelo Grupo Egmont e pela INTERPOL.

- Num pedido de informação à Rede Global do GAFI e ao Grupo Egmont, que incluem mais de 200 jurisdições e 170 UIFs, respetivamente, sobre os riscos, os quadros de aplicação da lei e estratégias, bem como sobre mecanismos de cooperação e coordenação nacionais e internacionais. No total, a equipa de projeto recebeu contributos de mais de 80 delegações.
- Em discussões e perspetivas partilhadas na reunião conjunta de peritos do GAFI (abril de 2023) e no Fórum Consultivo do Setor Privado (maio de 2023), incluindo um compromisso específico com o setor privado.

2. Contexto de risco: Fraude por meio informático (CEF)

2.1. Ameaça crescente de Branqueamento de capitais (BC)

8. A CEF aumentou significativamente a nível internacional. Embora não exista uma estimativa completa da magnitude e escala globais da CEF, muitas jurisdições reportam um crescimento consistente nos últimos anos. As receitas ilícitas provenientes da CEF são frequentemente transferidas para jurisdições estrangeiras. Estas receitas poderão então ser posteriormente branqueadas através dos sistemas financeiros de jurisdições terceiras.

9. De acordo com o Relatório de 2022 da INTERPOL sobre a Tendência da Criminalidade Global[2], os esquemas *online* são uma das tendências da cibercriminalidade mais frequentemente consideradas como representando ameaças "elevadas" ou "muito elevadas" a nível mundial. A maioria das jurisdições que forneceram informações para este projeto reconhecem os riscos de BC decorrentes da CEF nas suas avaliações de risco nacionais. As regiões com menos recurso ao numerário e mais baseadas no digital (por exemplo, onde a maior parte da intermediação financeira é feita através de serviços *online*), são supostamente mais vulneráveis aos riscos de BC associados a este crime, embora a natureza transnacional da CEF signifique que os criminosos podem facilmente visar as vítimas independentemente das fronteiras internacionais. A caixa *infra* reúne várias fontes de informação[3] permitindo uma visão regional do cenário de ameaça da CEF.

Caixa 1. 2.1. Ameaça crescente de BC: tendências regionais da CEF

África: Em África, a rápida digitalização do setor financeiro abriu uma variedade de oportunidades para os criminosos perpetrarem a CEF provocando um forte aumento na fraude bancária *online*, incluindo *phishing*, furto de identidade e esquemas de ativos virtuais. O aumento das perdas financeiras devido a tais crimes representa uma ameaça acrescida de BC. Por exemplo, na África Ocidental, a CEF é alegadamente considerada uma importante fonte de rendimentos que tem subjacentes a prática de crimes.

Américas: A CEF foi identificada como um risco crescente ou emergente. Uma jurisdição assinalou o aumento das comunicações da CEF, ano após ano, observando que o risco relacionado com o BC iria também aumentar de forma equivalente. Uma outra relatou que a fraude de investimento em ativos virtuais aumentou mais de 180% entre 2021 e 2022, com os criminosos a aproveitarem o entusiasmo e a publicidade em torno dos ativos virtuais.

Ásia-Pacífico: As jurisdições identificaram a CEF como tendo um risco de BC elevado ou significativo. Por exemplo, uma jurisdição mencionou que a maioria das comunicações de fraude contém alguma forma de CEF assinalando um correspondente aumento do BC. Uma outra jurisdição

2 Ver INTERPOL (2022) *Global Crime Trend Summary Report*

3 Inclui informação e dados fornecidos pelas jurisdições, bem como relatórios da INTERPOL e da Europol.

destacou o papel dos atores transnacionais na fraudação das vítimas através de uma grande quantidade de aplicações de investimento ilegais. A pandemia da COVID-19 acelerou a digitalização dos serviços e comportamentos dos cidadãos privados, dos governos e das empresas da região. Consequentemente, a CEF e o BC associados aumentaram, esperando-se que mantenha o crescimento.

Caraíbas: A região é altamente suscetível à CEF e ao branqueamento conexo, tendo-se registado um aumento da fraude global relacionada com CEF nos últimos cinco anos. O crescente setor dos ativos virtuais na região das Caraíbas também potencia vulnerabilidades, nomeadamente devido à presença de VASPs, incluindo *mixers*, que podem ser utilizados indevidamente para branquear fundos ilícitos que voltam aos grupos de criminalidade organizada, incluindo de CEF.

Europa: A CEF é geralmente avaliada como apresentando um risco de BC. Muitas jurisdições notaram um grande aumento desta atividade, com a CEF considerada como representando uma grande ameaça. A utilização dos ativos virtuais é geralmente observada para o branqueamento do produto da CEF (em especial no que se refere à fraude de comércio *online* relacionada com ativos virtuais, como por exemplo, ofertas iniciais de moedas fraudulentas).

Médio Oriente e Norte da África (MENA): Consistente com as tendências em outras regiões do mundo, o MENA viu as taxas de digitalização acelerarem durante a pandemia, enquanto governos, empresas e cidadãos transferiam massivamente as suas atividades para o ambiente *online*. Fraudes financeiras online, incluindo *phishing*, fraude com identidade e esquemas *online*, são classificadas como ameaças elevadas. A região MENA também é vulnerável ao BC na medida em que os países membros do CCG [Conselho de Cooperação do Golfo], em particular, servem como importantes centros de transbordo para o comércio global e atividades financeiras.

10. A digitalização e o desenvolvimento de novas tecnologias são os principais motores do crescimento da CEF. Os serviços digitais são hoje parte integrante da vida quotidiana e das funções públicas. Consequentemente, mais cidadãos (incluindo grupos vulneráveis) estão a participar em atividades *online*. Ao mesmo tempo, a digitalização significa que as jurisdições estão cada vez mais ligadas, com informação e fundos s circularem rapidamente através das fronteiras. Estes dois fatores alteraram radicalmente o panorama criminal e criaram um ambiente de ameaças crescentes de CEF.

11. A pandemia da COVID-19 acelerou a transição das atividades financeiras pessoais para a abertura de contas, pagamentos e concessão de empréstimos *online*. Atividades fraudulentas como esquemas por telefone e correio eletrónico; fraudes bancárias, relacionadas com idosos e no domínio dos cuidados de saúde (por exemplo, relacionadas com equipamentos de proteção individual e outros produtos de saúde) e esquemas fraudulentos em matéria de investimentos aumentaram significativamente através da internet com a utilização de *smartphones*, correio eletrónico e redes sociais. Estas mudanças nos comportamentos financeiros também tiveram impacto no panorama BC, incluindo uma maior utilização de plataformas bancárias e de pagamentos digitais e de transações à

distância (ver também a secção "Impacto da digitalização e das novas tecnologias na página 24).[4]

12. O uso cada vez mais predominante de *smartphones*, tecnologia (com novas ferramentas e aplicações em constante evolução), assim como transações financeiras à distância, aumentaram massivamente a vulnerabilidade dos utilizadores. O recurso a tecnologia que que intensifica o anonimato, como as VPN (Rede Privada Virtual) e *Onion Router*[5], pode proporcionar aos criminosos um anonimato significativo no desenvolvimento das suas atividades ilícitas. Aproveitando a tecnologia, os criminosos podem aumentar a escala, o âmbito e a velocidade das suas atividades criminosas. Observa-se que os criminosos estão inclusivamente a adotar um modelo de "Crime como um serviço"[6], que também diminui significativamente as barreiras à entrada de grupos de CEF, com uma maior especialização em diferentes aspetos deste crime, distribuído por diferentes subgrupos (ver secção 2.2 infra).[7]

13. Em muitos casos, as os grupos de criminosos organizados expandiram ou adaptaram as suas atividades de modo a integrarem a CEF, utilizando as técnicas existentes para o branqueamento dos seus outros fundos obtidos ilegalmente.

4 Ver GAFI (Maio 2020) *COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses* and (December 2020) *Update: COVID-19-Related Money Laundering and Terrorist Financing Risks*.

5 Também conhecido como TOR, trata-se de um *software* de fonte aberta que permite aos utilizadores navegarem na Internet de forma anónima.

6 É aqui que ocorre a divisão do trabalho, com grupos criminosos a desenvolverem e a oferecerem um nicho de capacidades, competências e aptidões criminosas a outros.

7 Ver Europol (Julho 2023) *Internet Organised Crime Threat Assessment (IOCTA) 2023*; e INTERPOL (2022) *Financial and cybercrimes top global police concerns, say new INTERPOL report*

Caixa 2. Rede criminosa comum de BC utilizada para CEF e outros crimes

Uma rede de BC realiza jogos de azar *online* e operações de CEF no edifício da sua empresa na Zona Económica Especial do País A (SEZ). O complexo alberga cerca de dez empresas que exploram, elas próprias, jogos de apostas *online* e realizam operações de CEF ou que arrendam o espaço a terceiros para os mesmos fins. A rede, que inclui alegadas empresas legítimas nas regiões fronteiriças do país vizinho B, é liderada por nacionais do País B que utilizam contas bancárias na moeda do seu País para facilitar a transferência de dinheiro da ZEE para o País C, onde se encontram os principais investidores da empresa. Os dólares americanos da ZEE são branqueados através de trocas cambiais no País B, sendo o dinheiro convertido na moeda do País B e então transportado para o País C. Do lado C da fronteira, o dinheiro é então transferido para os investidores da empresa.

Fonte: Transnational Organized Crime, Casinos and Money Laundering in Southeast Asia: A Threat Analysis (UNODC, 2022)

2.2. Características criminais da CEF

Elementos da CEF

14. Com base na experiência das jurisdições, os criminosos que praticam a CEF poderão recorrer a um ou mais dos seguintes elementos para enganar as vítimas na realização de uma transferência fraudulenta. Diferentes variantes de CEF podem combinar os elementos acima referidos de diferentes maneiras.

- Extração de informações (por exemplo, através de *phishing*);
- Fraude ou engenharia social e apelo a emoções vulneráveis (por exemplo, fingindo ser outra pessoa ou entidade e usando-a para gerar urgência, medo ou confiança, ou recorrendo a falsas alegações para ganhar dinheiro facilmente); e
- Suporte ou plataforma *online* (que pode ser utilizado para comunicação ou para as vítimas transacionarem em casos de fraude de comércio *online*).

15. Uma vítima pode não ser enganada apenas por um tipo de CEF; em última análise, o objetivo é induzir uma transferência de fundos, e os criminosos usarão uma variedade de técnicas para o conseguir. Os criminosos são criativos e podem envolver-se ou fazer a transição para outros tipos de CEF se o esquema inicial começar a falhar. Por exemplo, uma vítima de fraude de *phishing* ou de usurpação de identidade nas redes sociais poderia ser convencida a realizar investimentos num esquema de fraude, pelo mesmo criminoso, tirando partido da "confiança" já criada através do esquema de fraude inicial.

Caixa 3. As mesmas vítimas, várias infrações

O *pig butchering* é uma combinação de burla romântica e fraude de investimento. Com este *modus operandi*, os criminosos criam uma relação de confiança com a vítima e convencem-na a investir as suas poupanças em produtos em plataformas fraudulentas de negociação de criptomoedas. O esquema é praticado ao longo do tempo, resultando na perda de grandes quantias.

Após as vítimas perceberem que estão a ser lesadas, os criminosos contactam-nas frequentemente, fazendo-se passar por advogados ou agentes de autoridade oferecendo ajuda na recuperação dos seus fundos, em troca de uma taxa.

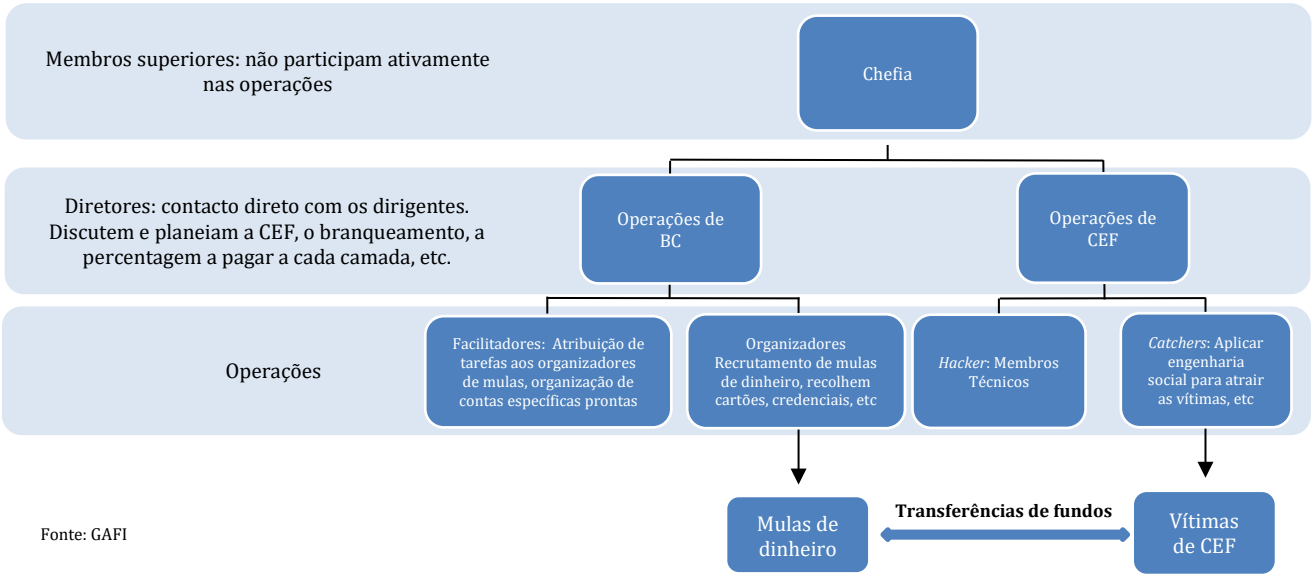
Fonte: Europol (2023), Internet Organised Crime Threat Assessment (IOCTA) 2023

Estrutura criminosa organizada

16. A CEF e o BC conexo são frequentemente executados por grupos ou associações criminosas organizadas transnacionais. Embora as suas estruturas possam variar, as associações de CEF funcionam frequentemente como organizações hierárquicas (veja o exemplo na Figura 1). Podem igualmente ser organizados de forma mais flexível, com os membros a aderir e a sair, conforme seja necessário. Estas associações também podem estar organizadas em subgrupos distintos com áreas especializadas de competência criminosa (por exemplo, segundo os elementos da CEF acima referidos (extração de informação, fraude social; utilização de conhecimentos técnicos como a criação de uma plataforma *online* ou BC). Em muitos casos, estas associações de CEF são descentralizadas e nunca comunicam pessoalmente (fazendo-o, por exemplo, através de canais codificados *online*), o que dificulta a investigação por parte das autoridades.

17. Além disso, associações os grupos da CEF são regularmente compostos por profissionais qualificados e tecnicamente competentes, permitindo uma abordagem cada vez mais sofisticada da CEF e do branqueamento de lucros ilícitos. As jurisdições referiram como os grupos da CEF podem recrutar intencionalmente indivíduos que trabalham em setores profissionais (incluindo IF), para serem utilizados como fontes de dados e informação permitindo a execução, com êxito, da CEF e facilitando o BC. Para mais informações sobre a forma como as associações de CEF estruturam e operam o BC, ver a secção 2.3 abaixo.

Figura 1. Exemplo de estrutura criminosa de CEF



Fonte: GAFI

Ligações a outros tipos de criminalidade

18. Além do BC, os grupos de CEF podem estar ligados a outras formas de criminalidade. Os crimes comuns incluem atividades associadas ou necessárias à execução da CEF, incluindo atividades de crime informático, como o *hacking* para obter informações pessoais, o desenvolvimento e a venda de *software* criminoso, a falsificação de documentos, etc. Parte dos produtos do crime pode ser auto-branqueada pelas associações de CEF através da compra de novos equipamentos e no desenvolvimento de ferramentas tecnológicas ainda mais avançadas.

Caixa 4. Operação "*Falcon*"

Três suspeitos foram detidos em Lagos, na Nigéria, em 2020, na sequência de uma investigação conjunta da INTERPOL-Group-IB e da Polícia Nigeriana que investiga crimes informáticos. Acreditava-se que cidadãos nigerianos eram membros de um grupo mais alargado de crime organizado responsável pela distribuição de *malware*, pela realização de campanhas de *phishing* e por extensos esquemas fraudulentos de E-mail empresarial comprometido. Os suspeitos terão desenvolvido *links* de *phishing*, domínios e campanhas de email em massa fazendo-se passar por representantes de organizações. Em seguida, usaram essas campanhas para disseminar 26 programas de *malware, spyware* e ferramentas de acesso remoto.

Estes programas eram utilizados para se infiltrarem e monitorizarem, os sistemas de organizações e de vítimas, antes de lançarem esquemas e desviarem fundos. De acordo com o Group-IB, acredita-se que o gangue prolífico tenha comprometido empresas governamentais e do setor privado em mais de 150 países desde 2017. O Group-IB também conseguiu determinar que o gangue está dividido em subgrupos com vários indivíduos ainda a monte.

Investigações paralelas de BC revelaram que os suspeitos também utilizaram contas bancárias estrangeiras e de ativos virtuais no Reino Unido, nos Estados Unidos e na Tailândia para receber pagamentos das vítimas. Os três suspeitos foram acusados pela prática de atividades ilícitas, nomeadamente por fraude e branqueamento de capitais. Um veículo de luxo foi confiscado e as contas dos suspeitos foram congeladas e perdidas a favor do Estado (*undergoing forfeiture*) em tribunal.

Fonte: Nigeria

19. Há também uma ligação crescente entre a CEF e o tráfico de seres humanos, em que as vítimas são atraídas através de anúncios de trabalho falsos para *call centers online* e forçadas a cometer a CEF em escala industrial. Tal permite que os grupos da CEF aumentem a diversidade geográfica das vítimas *online* que podem escolher como alvo (já que as vítimas traficadas podem ser exploradas devido ao seu conhecimento de línguas e conhecimentos culturais). Também pode aumentar a sofisticação dos centros de CEF através do tráfico de profissionais qualificados, como trabalhadores de tecnologia da informação ou "executivos de vendas digitais" (*digital sales executives*)[8]. Esses *call centers* operavam, por vezes, nos fusos horários das vítimas pretendidas recorrendo a espaços arrendados para operações criminosas temporárias, o que lhes permitia rapidamente realocar e mudar endereços IP para evitar a deteção das autoridades.[9]

8 Ver INTERPOL, (Junho 2023) *INTERPOL issues global warning on human trafficking-fueled fraud*

9 Ver INTERPOL (Julho 2023) *Operational Analysis Online Scams and Human Trafficking in South East Asia / Update 2 – From Regional to Global Threat*; apenas disponível a autoridades de polícia nacionais.

Caixa 5. Operação "*Storm Makers*"

Na Operação *Storm Makers* as autoridades realizaram ações policiais contra associações criminosas organizadas que se acredita estarem a facilitar a passagem de homens, mulheres e crianças asiáticos através das fronteiras para exploração. A operação desencadeou 121 detenções em 25 países, provocando 193 novas investigações.

Através da Operação *Storm Makers*, as polícias da Malásia e do Camboja trabalharam em estreita colaboração num caso que envolveu 15 homens e uma mulher atraídos para o Camboja com a promessa de um salário lucrativo para trabalhar num *call center*. À chegada, porém, foram presos e forçados a trabalhar 14 horas por dia como burlões.

Nota: Para mais detalhes, consultar INTERPOL (Maio 2022) *121 arrests in operation against migrant smuggling and human trafficking*

Fonte: INTERPOL

20. A maioria das jurisdições não encontrou provas substanciais indiciadoras de atividades de financiamento do terrorismo relacionadas com a CEF. No entanto, houve algumas observações em que elementos de atividades e de financiamento terroristas foram associados a agentes criminosos de CEF. Por exemplo, as comunicações de operações suspeitas (COS) de uma jurisdição sugerem que o produto de CEF estavam a ser transferidos, em alguns casos, para áreas/jurisdições de conflito específicas conhecidas por atividades relacionadas com o terrorismo.

21. Há também ligações ao financiamento da proliferação, com o crime informático a ser identificado como uma importante fonte de rendimentos ilícitos da República Popular Democrática da Coreia (RPDC). As atividades informáticas ilícitas incluem a venda de informações pessoais recolhidas ou a disponibilização de ferramentas e serviços de pirataria e *phishing,* que podem ser utilizados por outros criminosos para cometer a CEF.[10]

10 Ver Conselho de Segurança das Nações Unidas (Março 2023) *S/2023/171 Letter dated 3 March 2023 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council*

Caixa 6. Utilização de ferramentas de *phishing* da RPDC para praticar a CEF com o objetivo de financiamento de programas de armamento

De acordo com as informações disponibilizadas pelo Painel de Peritos das Nações Unidas, trabalhadores das tecnologias da informação (IT) da República Popular Democrática da Coreia, RPDC ligados ao Departamento da Indústria das Munições, têm estado a obter moeda estrangeira vendendo aplicações de *phishing* e operando em múltiplos servidores e endereços de Protocolo de Internet no estrangeiro.

Em julho de 2020, quatro cidadãos da RPDC foram detidos pelas autoridades na China e extraditados. Um deles atestou que associações criminosas adquiriram informações pessoais de cidadãos da RPDC, bem como aplicações de *phishing* de voz a um trabalhador de IT da RPDC.

Os grupos criminosos enganaram as vítimas de forma a fazerem *download* dessas ferramentas para furtar mais informações às mesmas. Posteriormente, apresentaram-se como funcionários de IF para levar as vítimas a enviar dinheiro.

Nota: Para mais detalhes, ver Conselho de Segurança das Nações Unidas (Setembro 2022) *S/2022/668 Letter dated 2 September 2022 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council*

Fonte: Painel de Peritos das Nações Unidas e da Coreia do Sul

2.3. Técnicas e tipologias de BC

Estrutura das redes de BC

22. Quando o produto do crime de branqueamento é gerado a partir de vários tipos de CEF, os criminosos têm de ser rápidos e eficientes. As jurisdições têm observado o envolvimento de grupos de BC profissionais, bem como de terceiros enquanto facilitadores profissionais, nomeadamente advogados, contabilistas, consultores fiscais, secretários de empresas e banqueiros. Os grupos de BC profissionais podem fazer parte do grupo criminoso de CEF ou de uma organização descentralizada separada que fornece serviços de BC segundo o modelo "crime como um serviço" (redes BC profissionais).

Caixa 7. Rede QQAAZZ

A rede criminosa QQAAZZ publicitou os seus serviços como um serviço global de contas piratadas [*bank drops*] em fóruns de crime informático online de língua russa, onde criminosos informáticos se reúnem para oferecer ou procurar as competências ou os serviços especializados necessários para a realização de diversas atividades de crime informático. A rede QQAAZZ tinha aberto e mantido centenas de empresas fictícias e contas bancárias pessoais em instituições financeiras em todo o mundo, que eram usadas para receber dinheiro de criminosos informáticos da CEF. Os fundos foram então transferidos para outras contas bancárias controladas pela rede QQAAZZ e, por vezes, convertidos em criptomoeda, utilizando serviços "de desagregação" concebidos para ocultar a origem inicial dos fundos. Após pagar até 50%, a rede QQAAZZ devolveu o saldo dos fundos furtados à sua clientela criminosa.

Em novembro de 2020, uma operação internacional das autoridades policiais que envolveu 16 países resultou na detenção de 20 indivíduos suspeitos de pertencerem à rede QQAAZZ, que tentou branquear dezenas de milhões de euros em nome dos principais criminosos informáticos do mundo. Foram efetuadas cerca de 40 buscas domiciliárias na Letónia, Bulgária, Reino Unido, Espanha e Itália, tendo sido instaurado um processo penal contra os detidos pelos Estados Unidos, Portugal, Reino Unido e Espanha.

Fonte: Portugal e Europol

23. Normalmente, as receitas da CEF são rapidamente branqueadas através de uma rede de contas. Estudos de casos mostram que estas redes podem ser complexas estendendo-se através de várias fronteiras e instituições financeiras, embora tal possa variar segundo o nível de sofisticação do grupo criminoso.[11]

24. As redes de contas de BC relacionadas com a CEF envolvem tipicamente não só indivíduos como pessoas coletivas.

- As **"mulas de dinheiro" individuais** (*money mules*) são frequentemente recrutadas por recrutadores também são conhecidos como "*herders"* através de vários meios, incluindo ofertas de emprego e anúncios, bem como interações nas redes sociais. As "mulas de dinheiro" podem ser conscientemente cúmplices no branqueamento de fundos ou estarem a trabalhar de forma involuntária (tendo sido enganadas), podendo ter-lhes sido oferecido incentivos ou pagamentos para manusearem os fundos ilícitos. É desafiante tentar identificar o "*herder*" das "mulas de dinheiro" que recruta tanto participantes voluntários como involuntários, ou determinar a origem de fundos fraudulentos. Algumas jurisdições assinalaram casos de recrutamento de estrangeiros sem aparente ligação com a jurisdição, tendo estes indivíduos sido orientados para a criação de "conta-mula", quer através de viagens físicas, quer através da abertura de contas virtuais.

11 Para mais informação sobre a utilização de "mulas de dinheiro" por branqueadores e redes profissionais, consultar GAFI (julho 2018) *Professional Money Laundering*

Caixa 8. Recrutamento das "mulas de dinheiro": Oferta de Emprego

A Sra. RS é uma dona de uma loja de conveniência (*sari sari*) tendo sido recrutada pelo Sr. O para o que ela achava ser uma oferta de emprego legítima. O Sr. O é um cidadão nigeriano que foi detido em 2019 por, alegadamente, ter utilizado um esquema multimilionário de fraude romântica online, o que resultou em mais de 8 milhões de PHP (cerca de 129 000 euros) de perdas para as vítimas.

O Sr. O prometeu à Sra. RS uma parcela por cada transação bancária que realizasse. No total, a Sra. RS realizou 83 transações no valor de PHP 3,6 milhões (cerca de EUR 58.000) ao longo de um período de seis meses. Todas as transações foram realizadas em numerário (ou seja, depósitos em dinheiro, levantamentos em caixas eletrónicos e ao balcão). O Sr. O foi finalmente detido, tendo sido apanhado numa armadilha, com a colaboração da Sra. RS.

Fonte: Filipinas

- As **empresas de fachada** são controladas pelos criminosos que pratica a CEF, que recorrem geralmente a "testas de ferro" ou administradores nomeados. As "mulas de dinheiro" individuais recrutadas podem também ser instruídas para atuarem como "testas de ferro", e abrirem contas de empresas numa tentativa de ocultar o património de origem criminosa. Algumas jurisdições observaram que as empresas de fachada usavam endereços de empresas virtuais[12] para ofuscar o mais possível as suas atividades criminosas. Nos casos de fraude no comércio online, os criminosos podem utilizar estas empresas fictícias para abrir contas virtuais em pontos de venda junto de empresas de serviços comerciais para processar os pagamentos e transferências das vítimas.

12 Endereços de empresas virtuais são endereços físicos reais que alguns prestadores de serviços disponibilizam para receção de correio e encomendas postais.

Caixa 9. Empresas de fachada utilizadas na fraude em plataformas de comércio online

Foram enviadas à UIF da Turquia várias COS relativas a um esquema de fraude online no qual as vítimas foram contactadas para fazer investimentos em divisas através de telefone ou de redes sociais. Por trás desse esquema havia uma rede de 209 empresas, que branqueavam o produto do crime entre si. As empresas tinham contabilistas comuns, tendo sido constituídas na mesma data e liquidadas após um curto período de tempo.

A análise efetuada pela UIF da Turquia revelou que as empresas fictícias atuaram igualmente em três subgrupos distintos com base nas transferências de fundos recorrendo a terceiros cúmplices a elas associados. Verificou-se que cerca de 10 mil milhões de TRY (Lira Turca - cerca de 336,7 milhões de euros) foram adquiridos de forma fraudulenta e branqueados.

- Cento e trinta e cinco empresas receberam 9,6 mil milhões de TRY (cerca de 323,2 milhões de euros) em dinheiro proveniente de fraudes através de empresas de pagamentos. Para facilitar a receção das transações das vítimas, estas empresas criaram contas POS virtuais. 100 milhões de TRY (cerca de 3,4 milhões de euros) foram retirados em numerário e cerca de 6 mil milhões de TRY (cerca de 202 milhões de euros) foram transferidos para uma empresa que comercializa ouro.
- Cinquenta e nove empresas receberam 700 milhões de TRY (cerca de 23,6 milhões de euros) em resultado de proveitos. 200 milhões de TRY (cerca de 6,7 milhões de euros) foram retirados em numerário e os outros foram transferidos para VASPs após terem sido branqueados através de contas mantidas por terceiros cúmplices.
- Vinte e três empresas receberam 875 milhões de TRY (cerca de 29,5 milhões de euros) em resultado de proveitos. 220 milhões de TRY (cerca de 7,4 milhões de euros) foram retirados em numerário, tendo os outros sido transferidos para VASPs após terem sido branqueados através de contas mantidas por terceiros cúmplices.

Fonte: Turquia

- As **empresas legítimas,** à semelhança das "mulas de dinheiro", podem também receber produtos da CEF (por exemplo, como investimento ou oportunidade de negócio) sendo instruídas a redirecionarem os fundos ou a reembolsá-los para uma conta separada e controlada por criminosos. Em alguns casos, observou-se que as empresas legítimas aceitavam voluntariamente tais "oportunidades de negócio", particularmente em tempos de crise económica. O envolvimento de empresas legítimas fornece uma fachada adicional dificultando a deteção de atividades ilícitas.

25. Há semelhanças na forma como as "mulas de dinheiro" funcionam nas redes de BC, quer para efeitos de CEF, quer para outros tipos de crimes. No entanto, as jurisdições observaram algumas diferenças que podem ser mais relevantes para as "mulas de dinheiro" relacionadas com a CEF.

- **Método de recrutamento:** As "mulas de dinheiro" da CEF têm maior probabilidade de virem atuar online, inclusive através de anúncios de emprego de empresas falsas ou através de correio eletrónico não solicitado. Os criminosos também podem explorar as condições económicas e mascará-las como uma oportunidade de emprego legítima para "dinheiro fácil". As vítimas da CEF (por exemplo, através de fraude romântica) podem frequentemente ser enganadas e atuar como "mulas de dinheiro". Em alguns casos, as vítimas do tráfico de seres humanos (como os migrantes ou trabalhadores ilegais) são também utilizadas para abrir essas contas**.**
- **Utilização das contas:** As "mulas de dinheiro" ligadas a CEF são utilizadas como titulares de contas junto de instituições financeiras, uma vez que os fundos fraudulentos podem ser recebidos e enviados rapidamente através de métodos de pagamento eletrónicos, em vez de transferências físicas ou depósitos de numerário, o que se deve à forma como as vítimas são defraudadas (isto é, através de transferências de fundos). Dada a conveniência que os serviços bancários digitais oferecem na movimentação de fundos, as pessoas visadas provavelmente possuem um nível básico de conhecimento ou proficiência em computadores e tecnologia.

Caixa 10. Vítima de Fraude romântica que se tornou "mula de dinheiro"

Entre abril e maio de 2022, uma idosa que abriu a sua conta bancária para receber a sua pensão, recebeu dois pagamentos num montante superior. Uma das remessas era de uma conta bancária nacional, enquanto a segunda era de uma vítima supostamente estrangeira.

Uma investigação subsequente das autoridades eslovacas permitiu concluir que a mulher comunicou com um indivíduo através das redes sociais tendo sido vítima de uma fraude romântica. A idosa forneceu as suas credenciais bancárias online ao autor da fraude, sendo a sua conta bancária utilizada para branquear outros produtos do crime. Parte do dinheiro recebido foi convertido em criptomoeda através de uma plataforma VASPs estrangeira.

Fonte: Eslováquia

Tipologias e técnicas de BC

26. O local onde ocorre a CEF (ou seja, onde a vítima se encontra) é frequentemente diferente do local onde ocorre o branqueamento do produto da CEF, sendo que as redes de "mulas de dinheiro" podem abranger várias jurisdições. Os grupos da CEF apercebem-se de que as IF ou as autoridades competentes podem já ter identificado contas com atividades fraudulentas antes do branqueamento, o que poderia resultar na interceção dos produtos do crime antes de os mesmos poderem entrar nas respetivas contas. Para aumentar as hipóteses de sucesso, os criminosos poderão efetuar "testes", realizando operações de pequeno valor para que possam alterar o destino dos fundos se esses testes falharem.

27. O tipo de conta usada como primeiro nível para receber os produtos da CEF, depende normalmente do tipo de CEF, de forma a assegurar a fachada de legitimidade. Também foram observadas alterações ao longo do tempo no que diz respeito ao tipo de conta de primeiro nível. Por exemplo, em casos de fraude com e-mails empresariais comprometidos, BEC (*Business Email Compromise)*, os grupos da CEF passaram da utilização de contas de pessoas singulares à utilização de contas empresariais para reduzir o risco de deteção.

Quadro 1. Relação entre o tipo de CEF e a conta de primeiro nível

Tipo de CEF	Tipo de conta de primeiro nível
Fraude com BEC	Empresarial (por ex., empresas de fachada ou recentemente constituídas)
Fraude de Phishing	"mulas de dinheiro" individuais
Fraude de representação nas redes sociais	"mulas de dinheiro" individuais
Fraude com comércio ou plataforma de comércio online	Empresarial (por ex., empresas de fachada ou recentemente constituídas)
Fraude romântica online	"mulas de dinheiro" individuais
Esquemas de emprego	"mulas de dinheiro" individuais

Nota: Esta tabela tenta distinguir algumas tendências gerais baseadas na experiência das jurisdições sobre os tipos de contas de primeira camada por tipo de CEF. No entanto, tal pode não se aplicar a todos os casos.

28. Uma vez aberta uma conta pelo grupo de CEF, os fundos adquiridos fraudulentamente são rapidamente processados para entrar na rede BC. Posteriormente, são

colocados em circulação através de uma série de transações "passagem direta" (*pass-through*) através de contas nacionais ou estrangeiras, controladas por "mula de dinheiro" /" testa de ferro" ou pelo grupo de CEF. Neste último caso, as "mulas de dinheiro" disponibilizam as suas credenciais bancárias, cartões e t*okens* ou conferem uma procuração ao grupo de CEF para permitir que este controle diretamente as contas. O envolvimento de facilitadores profissionais no processo, incluindo a outorga da procuração, confere legitimidade às transações facilitando a ocultação do crime.

29. Para evitar a deteção e manter o anonimato, os grupos de CEF utilizam várias técnicas e mecanismos: por exemplo, o *smurfing*; a movimentação entre várias contas de diferentes prestadores de serviços financeiros de envio ou de pagamento; a conversão para outros tipos de ativos financeiros (por exemplo, dinheiro eletrónico*, e-money*,[13] cartões pré-pagos, ativos virtuais). Essas técnicas e mecanismos poderão aumentar o tempo necessário para que as UIF e as autoridades tenham acesso aos dados financeiros necessários entre fronteiras, setores e instituições, para assim localizarem, protegerem e finalmente, recuperarem os produtos ilícitos. Algumas "mulas de dinheiro" poderão permitir que as suas contas sejam utilizadas apenas por um período de tempo específico e limitado, o que dificulta a identificação destas atividades, por parte das IF.

[13] A moeda eletrónica/e-money é uma representação digital da moeda fiduciária utilizada para transferir eletronicamente o valor denominado em moeda fiduciária. A moeda eletrónica é um mecanismo de transferência digital para a moeda fiduciária, ou seja, transfere eletronicamente valores que têm existência legal; GAFI (Junho 2014) *Virtual Currencies key Definitions and Potential AML/CFT Risks*

Caixa 11. Empresas de fachada, contas bancárias e ativos virtuais

Foram feitas várias denúncias junto da Polícia Indiana de que uma aplicação móvel estava a ser usada para enganar as pessoas a coberto de uma plataforma de investimento para "*mining*" de criptomoeda. A aplicação prometia uma participação nos lucros obtidos com esse investimento. A empresa tinha convidado as vítimas a reforçar os investimentos no esquema e, a partir daí os levantamentos/pagamentos pararam. O site e a aplicação ficaram inacessíveis, e os operadores da aplicação deixaram de responder aos investidores. Várias autoridades que investigaram as queixas apresentadas pelos clientes em diferentes partes do país, solicitaram informações à UIF Indiana no âmbito deste caso. A análise efetuada pela UIF Indiana identificou duas entidades que operam através da *Google Play Store*, tendo subsequentemente sido excluídas desta plataforma. Outras 34 entidades foram identificadas como estando ligadas às duas anteriores. Das 36 entidades, 28 entidades tinham estrangeiros como administradores.

A Direção de Fiscalização (*Enforcement Directorate*, ED) da Índia também iniciou investigações paralelas de BC que revelaram uma conspiração criminosa em larga escala e o envolvimento de várias entidades fictícias na operação de aplicações/sites fraudulentos semelhantes, para enganar as pessoas e para dissimular os produtos do crime. Após a verificação realizada apurou-se que entidades não existiam no endereço registado. Seguindo o rasto financeiro das operações, verificou-se que várias destas entidades também operavam em apostas ilegais e empréstimos. Os montantes ilícitos recolhidos junto das vítimas foram transferidos para contas de várias entidades fictícias e parte do produto do crime acabou por ser convertida em ativos virtuais. Foram encontrados e congelados produtos do crime sob a forma de saldos disponíveis nas contas bancárias de várias entidades fictícias, no valor de 865 milhões de INR (9,9 milhões de euros).

Fonte: India

30. As jurisdições comunicaram ainda a utilização de outros tipos de técnicas de BC, destinadas a ofuscar a ligação entre os diferentes grupos de criminosos de CEF e de BC.

- **Numerário:** vários estudos de casos mostram o levantamento de numerário por parte de "mulas de dinheiro" e grupos de CEF. O movimento de numerário fora das IF pode ser difícil de acompanhar. O numerário pode ser levantado em ATM após ser branqueado através de uma rede de BC, permitindo assim aos criminosos evitar o contacto direto com as IF. Estes fundos podem ser movimentados transnacional por correios de dinheiro, sendo depois depositados para posterior branqueamento. O produto do crime pode também ser utilizado para a compra de objetos de valor e instrumentos que possam depois ser novamente vendidos a dinheiro, tais como cartões pré-pagos ou metais preciosos.

Box 11. Levantamento de numerário e compra de ouro e cartões de combustível

Em março de 2023, um contabilista de uma empresa chinesa foi vítima de uma fraude bancária de falsificação de identidade. Foi adicionado a um grupo numa aplicação de mensagens sob o pretexto de ter de ser realizada uma inspeção anual da conta da empresa.

Os criminosos no grupo de mensagens posteriormente fizeram-se passar por representantes legais e acionistas da empresa e solicitaram à vítima que transferisse 7,8 milhões de RMB (cerca de 996 000 euros) para duas contas empresariais controladas pelo grupo criminoso. As investigações policiais mostraram que os fundos foram transferidos para 26 contas bancárias secundárias, sendo depois retirados em numerário em balcões bancários ou ATM, transferidos para plataformas de pagamento de terceiros ou usados para comprar ouro e cartões de combustível.

Fonte: China

- **BC baseado no comércio/serviços (*trade-based money laundering, TBML)*:** Existem várias técnicas de BC baseadas no comércio/serviços que os criminosos podem utilizar para transferir os produtos do crime para o exterior.[14] No que se refere aos produtos da CEF, algumas jurisdições observaram que os criminosos utilizam técnicas de BC com base no TBML, tais como faturação fictícia ou falsa, prática de atos ilícitos para adquirir bens de elevado valor ou facilmente comercializáveis (i.e., peças para veículos, bilhetes, artigos de uso doméstico, etc.). Por exemplo, algumas jurisdições relataram transferências fraudulentas para empresas legítimas que vão desde conhecidas marcas de luxo ou eletrónica, a pequenas empresas locais para a compra de bens. Estes bens podem ser transferidos para o exterior e convertidos em numerário para uma maior circulação e integração. As empresas comerciais fora do regime ABC/CFT podem não estar alerta ou ter conhecimentos suficientes para efetuar a verificação da identidade ou o controlo das transações - sendo inadvertidamente exploradas por criminosos. O fornecimento de faturas excessivamente onerosas ou fictícias para serviços de IT ou de consultoria pode também fazer parte das técnicas BC adotadas.

14 Ver também FATF – Egmont Group (Dezembro 2020) *Trade-based Money Laundering: Trends and Developments*; e FATF (Julho 2018) *Professional Money Laundering*

Box 12. A CEF, as "mulas de dinheiro" e o TBML

As autoridades irlandesas prenderam um indivíduo-chave, a pessoa MS, num esquema de branqueamento de produtos de fraude romântica e de e-mails comerciais comprometidos (BEC) entre a Irlanda e a Nigéria, através de TBML. As investigações ainda se encontram a decorrer. Até à data, as autoridades consideram que o sistema de branqueamento envolve, pelo menos, 60 nomes e 64 contas bancárias.

Neste esquema, os produtos das referidas fraudes são inicialmente transferidos para as contas bancárias de "mulas de dinheiro" irlandesas, sucedendo-se o levantamento em numerário, seguindo de transferências para contas irlandesas diretamente ligadas ou detidas pela pessoa MS. Muitas das contas vinculadas à Pessoa MS foram abertas sob identidades falsas.

Uma empresa nigeriana (controlada por um nigeriano que se acredita estar sedeado nos EUA), encomendou bens a empresas europeias ou chinesas legítimas, que comercializavam artigos que podem ser adquiridos e enviados para revenda, incluindo álcool, roupas, eletrónica e produtos farmacêuticos. As contas irlandesas da Pessoa MS efetuariam o pagamento das faturas relevantes, sendo as mercadorias finalmente expedidas para a empresa cúmplice da Nigéria.

Num caso, uma empresa farmacêutica alemã recebeu fundos superiores a 1,7 milhões de euros como pagamento dos bens adquiridos pela empresa nigeriana. Estes fundos foram localizados, sendo reconduzidos ao produto de fraudes de BEC e da fraude romântica, ocorridas na Europa e nos EUA, sendo provenientes de várias contas ligadas ou detidas pela Pessoa MS ou diretamente das vítimas. Estes bens foram finalmente enviados para a Nigéria.

Fonte: Irlanda

- **Remetentes e VASPs não licenciados ou não registados:** o produto dos atos criminosos pode ser transferidos para fora da jurisdição utilizando prestadores de envio de dinheiro clandestinos ou de serviços de *hawala* com pouco ou nenhum controlo ABC/CFT. Quando estão envolvidos Ativos Virtuais, os sindicatos criminosos podem explorar os VASPs sedeados em jurisdições com controlo ABC/CFT fraco ou inexistente.
- **Técnicas de anonimato acrescido para Ativos Virtuais:**[15] O uso de carteiras não hospedadas, transações diretas P2P (*Peer-to-Peer*), *peel chains* e operações de alto risco são os métodos preferidos para branquear rapidamente os Ativos Virtuais ligados a CEF de uma jurisdição, sendo frequentemente combinados com outros. Os criminosos estão também a utilizar cada vez mais ATM de Bitcoins para transferir valores e ocultar a identidade de quem controla os fundos, inclusive apresentando documentos

15 Estas técnicas estão exploradas em pormenor em: FATF (Março 2023) *Countering Ransomware Financing*

de identificação falsos ou alterados, tais como documentos identificativos, números de telefone ou datas de nascimento diferentes aquando do depósito ou levantamento de fundos. Utilizam igualmente técnicas de ofuscação, incluindo a utilização de serviços de *mixers* e *tumblers*, ativos virtuais de anonimato acrescido (também denominadas moedas de privacidade, como por exemplo a Monero) e serviços financeiros descentralizados (DeFi).

Caixa 13. BC complexo distribuído por vários setores

Uma organização criminosa estrangeira que se dedicava aos crimes do tipo fraude romântica enganou cerca de 70 vítimas japonesas. Aproximadamente 3 milhões de dólares foram transferidos para várias "contas-mula" no Japão. Um cidadão japonês, agindo como angariador local das "mulas de dinheiro", branqueou os fundos enviando-os para o Gana, onde o grupo fraudulento estava sedeado. O japonês acabou por ser preso graças à cooperação do Gana, via INTERPOL.

Os fundos das "contas-mula" foram posteriormente transferidos para a conta do angariador japonês. A análise das COS revelou que os fundos foram branqueados através de três canais pelo angariador japonês:

- Foram feitas transferências para uma conta bancária detida pelo angariador japonês no Gana, onde os fundos foram levantados entregues, em mão, ao líder do grupo, que ainda se encontra a monte. Ao fazer as transferências, o japonês apresentou faturas fictícias ao seu banco japonês, tendo declarado que as mesmas se destinavam a uma atividade comercial legítima (compra de grãos de cacau).
- Alguns fundos foram convertidos em ativos virtuais através de um VASP no Japão.
- Os fundos também foram transferidos para o Gana através de um banco clandestino ligado à comunidade ganesa no Japão.

Fonte: Japão

Impacto da digitalização e das novas tecnologias no BC

31. As novas tecnologias proporcionaram novos benefícios e oportunidades aos consumidores. Há uma profunda mudança no sentido da digitalização dos serviços financeiros, que acelerou durante a pandemia da COVID-19. A redução da utilização de numerário e o aumento da atividade online resultaram em novos instrumentos e processos inovadores. A cadeia de pagamentos financeiros está também a tornar-se cada vez mais dinâmica e fragmentada, com uma maior diversidade de prestadores de serviços a oferecerem serviços de pagamento e de transações (ver também a secção 3.1 abaixo).

32. No entanto, o desenvolvimento tecnológico também é aproveitado pelas associações criminosas, que exploram estas oportunidades para melhorar exponencialmente as suas técnicas de BC. As transações financeiras são cada vez mais executadas a velocidades quase instantâneas (como as VPN), tornando-se difícil para as autoridades identificar os criminosos reais que executam estas transações de BC em operações sucessivas e rapidíssimas.

33. A digitalização aumentou a facilidade e a velocidade com que as contas para BC podem ser criadas, expandindo ao mesmo tempo o alcance externo dos grupos de CEF. Algumas jurisdições notaram o aumento dos processos virtuais remotos em duas áreas: abertura de contas e criação de empresas, facilidades exploradas pelos criminosos.

Caixa 14. Escalada através da digitalização

Uma análise da UIF detetou uma rede alargadamente composta por 147 indivíduos e 276 contas bancárias, em oito bancos. Estes indivíduos tinham cedido a sua identidade digital, concebida para identificação do utilizador em plataformas governamentais e outras plataformas online, aos grupos criminosos. Estes grupos utilizaram então a identidade digital para abrir contas bancárias remotamente e exercer controlo direto sobre estas "contas-mula", a fim de branquear os produtos da CEF. A UIF detetou a rede através da identificação de elementos comuns, tais como transações bancárias, dados (informações de contacto estrangeiras e ID de dispositivos), bem como detalhes de contacto (correio eletrónico, telefone).

Estas informações foram transmitidas ao Comando Antifraude (*Anti-Scam Command* (AScom), Singapore's), uma unidade dedicada ao combate da CEF e BC conexos, no seio da Polícia de Singapura. As investigações da AScom acabaram por resultar na detenção de seis indivíduos e na acusação de três indivíduos pelo seu papel no esquema criminoso.

Fonte: Singapura

34. Os criminosos podem expandir rapidamente a magnitude (muitas vezes transnacional) de uma rede de "mulas de dinheiro", utilizando ferramentas digitais para aumentar o recrutamento externamente. As redes sociais e as aplicações *Voice over Internet Protocol* (VoIP) também foram identificadas como meios preferidos neste processo de recrutamento. Tradicionalmente, pode haver um certo grau de atrito no processo de branqueamento através das redes de "mulas de dinheiro", devido ao tempo necessário para que estas recebam e cumpram as instruções fornecidas pelos grupos criminosos. Esses períodos de espera foram significativamente reduzidos com o uso de plataformas de mensagens instantâneas, por parte dos grupos de CEF.

35. Cada vez mais os criminosos podem furtar identidades através de várias técnicas e ferramentas tecnológicas, incluindo *phishing*, aquisição, ou enganar as vítimas que acabam por declarar voluntariamente a sua identidade. Por vezes, podem utilizar falsas identidades ou identidades sintéticas, que envolvem uma combinação de elementos de

identidade reais e falsos ao mesmo tempo, para criar contas de forma fraudulenta. Os criminosos criam e controlam diretamente as contas, utilizando estas identidades furtadas ou falsificadas, tornando-se mais difícil de rastrear as atividades de BC, uma vez que os titulares das contas podem nem sequer ter conhecimento do seu envolvimento.

36. Uma delegação assinalou os riscos das *deepfakes* serem potencialmente utilizadas para apropriação fraudulenta de contas. Com a ajuda de algoritmos de *learning*, um criminoso pode criar uma *deepfake* da voz ou imagem de alguém, podendo usá-la para se fazer passar por essa pessoa ao telefone ou em sistemas de autenticação biométrica. As *deepfakes* também podem ser usadas em combinação com técnicas de engenharia social para levar as vítimas a cederem as credenciais das suas contas. A tecnologia *deepfake* ainda é relativamente nova, o que significa que o risco de controlo de contas *deepfake* é ainda limitado. No entanto, poderá representar um risco significativo no futuro, se a tecnologia continuar a desenvolver-se, e se tornar mais amplamente disponível.

Caixa 15. Furto remoto de identidade para controlo direto

Numa série de fraudes relacionadas com *phishing*, as vítimas foram enganadas por criminosos que as convenceram a instalar ferramentas de acesso remoto nos seus computadores. Em muitos dos casos, foram criadas contas em VASPs no nome das vítimas sem o seu conhecimento. Os criminosos fizeram-no utilizando dados furtados através das referidas ferramentas de acesso remoto. Suspeita-se que os criminosos tenham enganado as vítimas através do processo de verificação online de abertura de conta, recorrendo ao uso das ferramentas de acesso remoto para ocultar as interfaces reais.

As vítimas acabaram por transferir fundos para estas contas de VASPs. Os criminosos puderam assim utilizar diretamente estas contas de VASPs para posterior branqueamento. No total, estima-se que as vítimas tenham perdido mais de 600 000 euros através desta série de fraudes.

Fonte: Áustria

3. Outras vulnerabilidades emergentes de BC

37. As medidas preventivas que decorrem para as IF, APNFD e VASPs, ao abrigo dos Padrões do GAFI (Recomendações 9 a 23), constituem uma base que permite evitar que os produtos ilícitos da CEF entrem nos setores financeiro e outros. Esta secção centra-se nas vulnerabilidades de BC emergentes e que podem ser exploradas por grupos de CEF.

3.1. Riscos decorrentes das instituições financeiras digitais[16]

38. A evolução dos pagamentos financeiros deu origem a novas instituições financeiras digitais, como os prestadores de serviços de pagamento (PSP), os prestadores de serviço de emissão de moeda eletrónica, etc. As IF tradicionais dispõem de mais recursos, o que pode resultar em controlos relativamente mais robustos, em comparação com estas instituições financeiras digitais mais recentes, onde os criminosos procurarão explorar as vulnerabilidades, por forma a branquear fundos.

39. A rede de pagamentos também pode ser fragmentada. Podem existir várias relações financeiras entre estas instituições, por exemplo, com várias instituições de pagamentos que transacionam entre si ou que fornecem contas a pequenos prestadores, que, por seu turno, prestam outro tipo de serviços financeiros (ver também caixa 17 abaixo). Esta fragmentação pode aumentar as dificuldades de identificação de transações entre vários tipos de instituições na "cadeia de pagamentos". Poder-se-ão também colocar desafios no sentido de assegurar a disponibilidade imediata de informações básicas sobre o ordenante e o beneficiário das transferências ao longo da cadeia de pagamentos[17].

40. Em conformidade com os padrões do GAFI, deve existir uma supervisão regulamentar sólida relativamente às instituições financeiras mais recentes, incluindo o licenciamento ou registo adequados, por forma a impedir que os criminosos ou os seus associados controlem estas entidades. As autoridades reguladoras deverão assegurar que todas as instituições que realizem transações são objeto de uma supervisão suficiente, já que têm a responsabilidade de realizar ou assegurar a devida vigilância da clientela (CDD) e o acompanhamento das transações, tanto a nível de beneficiários.

16 O presente relatório também reconhece os riscos de BC decorrentes de ativos virtuais e VASPs. Para obter mais informações sobre os riscos e desafios regulamentares relacionados com os VASPs, consultar GAFI (Março 2023) *Countering Ransomware Financing* as well as (Junho 2023) *Virtual Assets: Targeted Update on the Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*.

17 O GAFI está também a considerar potenciais revisões da Recomendação 16 (relativa às transferências eletrónicas), a fim de ter em conta a evolução recente e futura da arquitetura dos sistemas de pagamentos.

Caixa 16. Abuso do sector dos PSP

A análise efetuada pelas autoridades de supervisão francesas no primeiro semestre de 2021 identificou os principais PSP utilizados para receber transferências eletrónicas fraudulentas. Estes ofereciam normalmente "serviços bancários", tendo alguns deles filiais em França com a única finalidade de disponibilizar IBAN franceses, com uma presença física mínima.

A análise revelou que estes PSP tinham cerca de 200 vezes mais riscos do que as outras instituições. A maioria tinha sistemas de verificação de identidade e monitoração de transações inadequados. Os criminosos abriam contas com uma identidade falsa, podendo rapidamente verificar se algumas das contas abertas estariam a ser monitorizadas pelo PSP, tentando primeiro realizar transações de pequenos montantes e depois alterar o destino dos fundos, se necessário. De seguida, transferiam rapidamente os fundos para uma ou várias contas. A divisão dos montantes entre várias contas permitia que os criminosos contornassem as restrições impostas pelo PSP em relação aos seus serviços, com limites de levantamento de numerário ou permanência abaixo do limite de monitorização de operações definido internamente pelo PSP.

Fonte: França

3.2. Abuso de IBANs virtuais[18]

41. Outro exemplo de como a inovação financeira pode ser explorada para fins da CEF é o uso de IBAN virtuais/vIBAN. Existem diversas instituições que emitem vIBAN para clientes, incluindo bancos e PSPs. Embora os vIBAN sejam utilizados de diversas maneiras legítimas, como facilitar e classificar pagamentos, várias jurisdições assinalaram o abuso dos vIBAN como uma ferramenta utilizada para atividades de branqueamento relacionadas com a CEF.

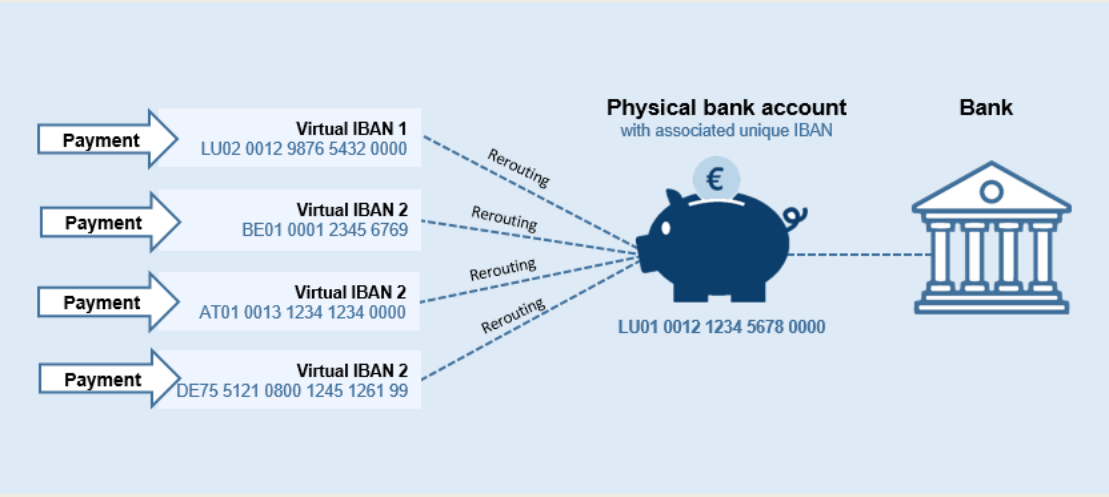
18 Para mais informações sobre os riscos e desafios associados aos vIBANs, ver: (Junho 2023) *Europol Financial Intelligence Public Private Partnership (EFIPPP) Threat Intelligence Information on Virtual IBANs (available only to EFIPPP members).*

Caixa 17. O que é um vIBAN?

Os vIBAN são funcionalmente idênticos aos IBAN convencionais, na medida em que podem ser utilizados para enviar e receber pagamentos à escala mundial. Têm uma aparência idêntica à sua versão tradicional, sendo também compostos por um número de caracteres alfanuméricos até ao máximo de 34. Assim, funcional e visualmente, são indistinguíveis dos IBAN regulares.

A principal diferença entre os IBAN comuns e os virtuais reside na correspondência de contas. Um IBAN comum corresponde numa proporção de 1:1 a uma conta bancária, o que significa que existe apenas uma única conta bancária física ligada a cada número IBAN individual. Por conseguinte, se uma pessoa utilizar o IBAN para efetuar um pagamento, os fundos acabarão automaticamente na conta bancária a que o IBAN está ligado.

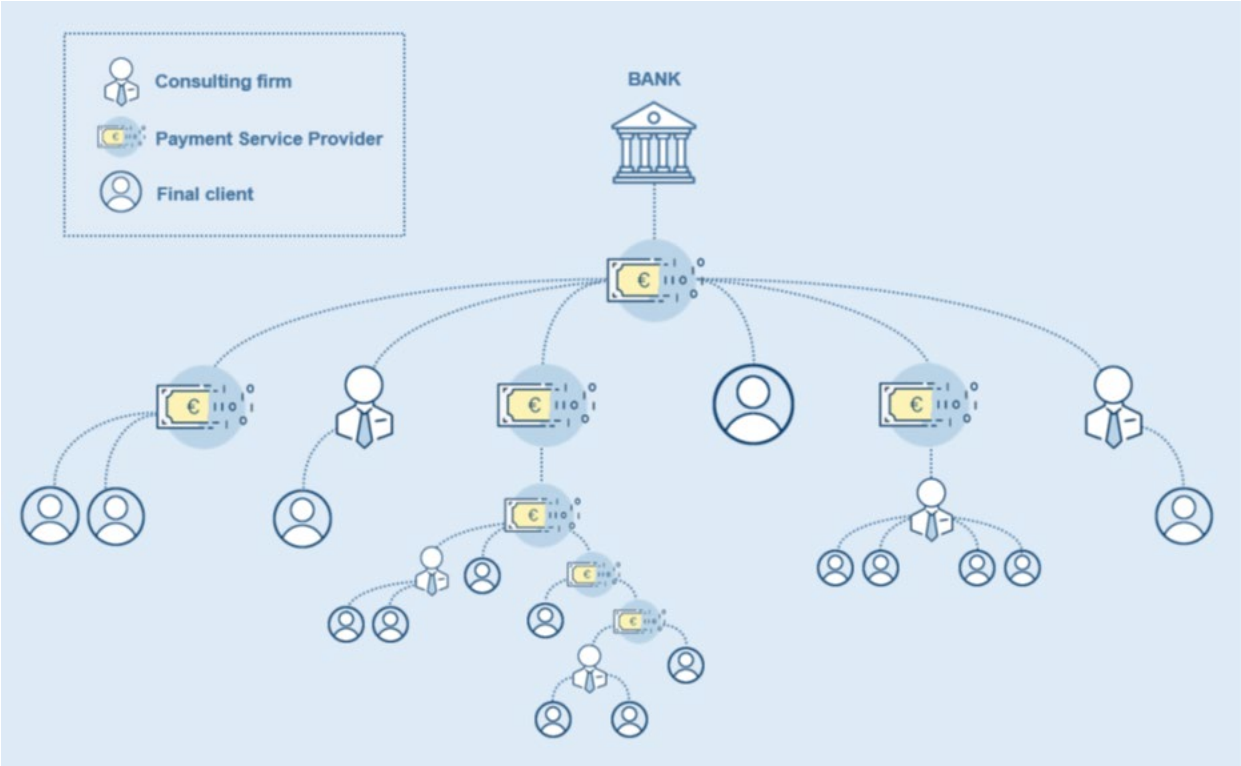
Por outro lado, um IBAN virtual que não corresponde a uma conta num banco físico. Trata-se de números de referência emitidos pelos bancos que permitem que os pagamentos recebidos sejam reencaminhados para um IBAN físico, que está ligado a uma conta bancária física. Os titulares de vIBAN podem ter vários IBAN virtuais únicos, que redirecionam e centralizam todos os pagamentos numa única conta bancária física, como se pode ver na Figura 3.



Fonte: Parceria Público-Privada Europol de Inteligência Financeira

42. Uma vez que os IBAN e os vIBAN são aparentemente idênticos, os criminosos usam-nos para enganar as vítimas e levá-las a pensar que estão a transferir fundos para uma conta bancária, quando, em vez disso, poderá ser um vIBAN utilizado para creditar uma carteira eletrónica. Acresce que os vIBAN podem ser reemitidos pelo cliente de uma instituição financeira, em especial se o cliente for outra instituição financeira, tornando difícil, quer a identificação do país de origem do vIBAN, quer a localização da conta principal.

Figura 2. Rede em cascata de fornecedores de vIBAN que emitem e reemitem vIBAN



Fonte: Parceria Público-Privada Europol de Inteligência Financeira

43. Em suma, os criminosos podem usar os vIBAN para mascarar informações sobre beneficiários efetivos e obscurecer o movimento de dinheiro ilícito, dificultando a identificação da verdadeira conta principal e da instituição financeira emitente, bem como o acompanhamento adequado das transações. Em última análise, tal resulta em desafios enfrentados pelas autoridades competentes para localizar as contas físicas e congelar os fundos (uma vez que os vIBAN são meramente números de referência emitidos pelos bancos e não contas reais que possuem saldos físicos). Como boa prática, algumas jurisdições trabalham com bancos que emitem vIBAN por forma a identificar rapidamente a instituição de pagamento ligada a essas contas principais sempre que é identificado um caso de CEF.

Caixa 18. vIBAN utilizados para cometer a CEF

Entre fevereiro e março de 2023, a UIF Luxemburgo recebeu várias comunicações das chamadas fraudes "Olá mãe", em que as vítimas receberam mensagens do WhatsApp de um número de telefone desconhecido, mas local, de burlões que fingiam ser seus filhos. As vítimas receberam mensagens de texto em luxemburguês através de números de telemóvel luxemburgueses, com a inclusão de um IBAN luxemburguês.

Durante a investigação deste caso, a UIF Luxemburgo descobriu que os IBAN fornecidos pelos autores das fraudes eram vIBAN. Estes vIBAN foram emitidos por uma instituição bancária luxemburguesa para um prestador de serviços de pagamento sedeado no Luxemburgo que oferece cartões de crédito pré-pagos a clientes europeus. Estes cartões de crédito pré-pagos podem ser carregados transferindo dinheiro para os IBAN virtuais que os criminosos pretendiam utilizar para posterior branqueamento.

Dos seis vIBAN identificados utilizados nas fraudes, a UIF Luxemburgo conseguiu bloquear ou recuperar 40 000 EUR dos 55 000 EUR de fundos obtidos com as fraudes. A ação da UIF Luxemburgo foi facilitada pela cooperação entre a UIF e o banco emissor dos vIBAN, que permitiu identificar rapidamente a instituição de pagamento onde estava registada a conta subjacente do cliente final.

Fonte: Luxemburgo

3.3. Setores não tradicionais

44. Muitas jurisdições destacaram a importância de trabalhar com setores não tradicionais, incluindo plataformas de redes social, comércio eletrónico, telecomunicações e prestadores de serviços de Internet no combate ao branqueamento derivado da CEF. Embora estes setores não tradicionais não sejam regulados em termos de ABC/CFT, os mesmos possuem informações úteis que podem ajudar as investigações de BC, especialmente quando são utilizados para perpetrar a CEF e recrutar "mulas de dinheiro". As plataformas de redes sociais, bem como os prestadores de serviços de telecomunicações e Internet, podem fornecer informações forenses digitais cruciais, incluindo endereços IP, números de telefone, endereços de e-mail, etc., ajudando a identificar os autores dos crimes. Nos casos em que são utilizados sítios Web ou anúncios fraudulentos para a CEF, estes setores também possuem informações sobre transações financeiras e pagamentos relacionados com os criminosos (por exemplo, informações sobre pagamentos para alojamento de sítios Web, anúncios).

45. A experiência e estudos de casos de várias jurisdições também têm mostrado como o comércio eletrónico ou as redes sociais, *o streaming* ou as plataformas de jogos podem ser usados como um meio de branquear o produto da CEF. O uso generalizado das redes sociais, *streaming* ou plataformas de jogos permite que os utilizadores recebam doações, presentes, *tokens* ou créditos de espectadores e do público. Os criminosos podem tirar partido da ausência de requisitos ABC/CFT e utilizar tais plataformas para branquear o produto do crime.

Caixa 19. Produtos de práticas ilícitas de *Phishing* através das redes sociais e plataformas de *streaming*

Foi possível descobrir que 19 contas bancárias tinham sido debitadas no âmbito de um ataque de *phishing* dirigido a clientes de certos bancos. A análise efetuada pela UIF alemã revelou que as transações eram efetuadas através de contas de pagamento detidas por dois utilizadores. Esses fundos foram enviados posteriormente para uma rede social e uma plataforma de *streaming*, sendo os fundos usados para recarregar as contas de utilizador mantidas na plataforma de *streaming* com "moedas", (servindo como uma espécie de moeda nativa entre os utilizadores da plataforma) que podem ser usadas para comprar presentes virtuais. Esses presentes podem ser transferidos para criadores de conteúdos que podem converter essas moedas em moeda normal, e daí retirar o valor monetário equivalente.

As investigações ainda decorrem. Os dados de endereço IP mostraram que as transações fraudulentas foram realizadas através dos mesmos endereços IP de login. A análise da UIF aponta para um criminoso comum que estará a branquear uma grande parte do produto do *phishing* através das redes sociais e da plataforma de *streaming*, para posteriormente fazer a conversão e retirar o dinheiro correspondente.

Fonte: Alemanha.

4. Respostas e estratégias operacionais nacionais

46. Este Capítulo aborda, em primeiro lugar, as principais fontes de informação das quais as jurisdições dependem para detetar e investigar a CEF. Exploram-se, em seguida, as estruturas de coordenação e cooperação internas e a forma como as jurisdições utilizam estas estruturas para investigar e prevenir a CEF e o BC conexo.

4.1. Principais fontes de deteção

47. Com base na experiência das jurisdições e do conhecimento de estudos de casos, existem duas fontes primárias de informação para a deteção e investigação de BC relacionada com a CEF: denúncia da vítima e comunicações de operações suspeitas (COS).

48. As jurisdições também dispõem de várias iniciativas para estimular as comunicações e assim maximizar a quantidade total de informações a que podem ter acesso para uma atuação efetiva. Utilizando estas informações e dados, as autoridades competentes utilizam estratégias e instrumentos digitais para analisar e identificar *clusters* criminosos para uma aplicação mais eficaz e direcionada.[19]

Denúncia das vítimas

49. A denúncia das vítimas é uma importante fonte de informação para detetar e investigar o produto de atividades ilícitas relacionadas com a CEF. Em certas fraudes, como as BEC, as vítimas normalmente descobrem relativamente rápido que foram objeto de fraude (por exemplo, quando a respetiva e legítima contraparte começa a pedir pagamentos em falta). Noutro tipo de casos de CEF, como fraudes de investimento, fraudes românticas ou *phishing*, as vítimas poderão aperceber-se, após algum tempo, que foram defraudadas.

50. A denúncia em tempo oportuno por parte da vítima é importante para permitir às autoridades competentes agir rapidamente no sentido de rastrear o produto de atividades ilícitas, podendo assim aumentar a probabilidade de sucesso nos resultados da aplicação da lei. As vítimas podem comunicar as suas suspeitas de crime, quer às agências policiais, incluindo unidades dedicadas que lidam com denúncias de fraude, quer às respetivas instituições financeiras, prestadores de serviços de pagamento e VASPs, quando suspeitem da ocorrência de transações ilícitas nas suas contas. Algumas jurisdições assinalaram que as vítimas podem também recorrer a organismos financeiros de proteção dos consumidores em vez de se dirigirem aos organismos responsáveis pela aplicação da lei.

51. No entanto, é muito provável que a CEF não seja denunciada pelas vítimas, especialmente quando estas sofreram apenas perdas insignificantes. Fatores emocionais, como constrangimento ou medo, podem levar as vítimas a decidir não efetuas as denúncias.

52. Como boa prática para fomentar a denúncia por parte das vítimas, algumas jurisdições criaram plataformas específicas para este tipo de fraude, incluindo portais on-line, que, oferecerem um formato estruturado de comunicação, permitindo normalizar a recolha de dados, facilitar a análise de comunicações e possibilitam a identificação de tendências

[19] Para mais informações sobre como as UIF e as autoridades podem aproveitar a transformação digital para maior eficácia de análise e investigação ABC/CFT, consultar Confidential Reports on Digital Transformation of AML/CFT for Operational Authorities: Egmont Group-FATF (October 2021) *Detection of Suspicious Activities and Analysis of Financial Intelligence (Phase 1);* and FATF (Maio 2022) *Law Enforcement Authorities and Information Exchange (Phase 2).*

e padrões criminosos. As plataformas podem também incluir ferramentas úteis ao nível de prevenção e assistência à vítima de CEF.

Caixa 20. "Action Fraud" do Reino Unido

O organismo de luta antifraude*, Action Fraud,* é o centro nacional de denúncias de fraudes e crimes cibernéticos do Reino Unido. Proporciona um ponto central de contacto para a tratamento de fraudes e crimes online com origem em transações financeiras através da Internet e é gerido pela Polícia da Cidade de Londres, juntamente com o Serviço Nacional de Informações sobre Fraude (NFIB). O site *Action Fraud* disponibiliza vários recursos públicos de sensibilização para a prevenção da criminalidade, bem como para proteção e apoio às vítimas.

O *Action Fraud* também gere um portal online de comunicações para as vítimas que funciona 24 horas/dia, 7 dias/semana. As comunicações via o *Action Fraud* são transmitidas ao NFIB, que faz a avaliação e análise em diferentes partes do país no sentido de identificar os autores das práticas criminosas. Essas comunicações são depois enviadas às forças policiais locais competentes do Reino Unido para investigação. O NFIB também utiliza essas comunicações para desativar contas bancárias, sites e números de telefone usados pelos autores das fraudes.

Fonte: Reino Unido

Comunicações de Operações Suspeitas

53. Dada a possibilidade de não haver participação por parte das vítimas, as COS são uma fonte de deteção independente crucial para os fluxos financeiros relacionados com a CEF.

54. Com base em dados recolhidos junto das UIF, a maioria das COS relacionadas com a CEF foram enviadas pelo setor bancário. Os bancos devem continuar a reforçar as suas capacidades de deteção da CEF e do BC conexos, uma vez que os *modi operandi* dos grupos da CEF estão em permanente evolução. Os dados revelaram também que os serviços de transferência de valores (MVTS) e os VASPs enviam menos COS. Relativamente aos VASPs, o mesmo pode ficar a dever-se ao facto de, em algumas jurisdições, o setor não estar totalmente regulamentado, em conformidade com as normas do GAFI[20].

55. É importante assegurar uma análise atempada das COS relacionadas com a CEF, dada a possível de dissipação dos produtos da mesma. Algumas UIF implementaram um sistema de priorização para filtrar o elevado volume de COS, concentrando-se nas de maior risco, o que inclui as COS relacionadas com a CEF. Outras dão formação aos seus funcionários sobre os riscos de BC relacionado com a CEF, capacitando-os para que possam filtrar e a classificar as COS relacionadas. Todas estas medidas facilitam a análise oportuna da UIF, permitindo um seguimento rápido dos incidentes relacionados com a CEF.

20 Ver também GAFI (Junho 2023) *Virtual Assets: Targeted Update on the Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*.

Caixa 21. Priorização e *clustering* de COS relacionadas com a CEF

A UIF do Chile recebeu mais de 1.500 COS em 2021 e 2022 relacionadas com um esquema de fraude numa plataforma de comércio online. Para lidar com tal volume de COS, a UIF aplicou técnicas de *clustering* na análise, tendo sido possível descobrir alguns padrões de atuação.

A UIF aplicou uma ferramenta de *mining* de texto, usando palavras-chave e frases conhecidas detetadas. Através desde meio foi possível identificar *clusters* geográficos que permitiam uma referenciação direcionada para o Ministério Público. O *clustering* permitiu às investigações descobrir que os fundos eram levantados em ATM, sendo entregues aos criminosos de nível superior dentro do grupo criminal organizado.

Fonte: Chile

56. Para além da deteção, as jurisdições também procuraram sensibilizar e melhorar as comunicações. Muitas jurisdições emitiram Orientações relacionadas com a CEF e/ou realizaram ações de formação, quer para os profissionais das instituições financeiras, quer paras outros setores, a fim de promover a sensibilização para as tendências mais recentes da CEF e para as tipologias de BC. Aconselha-se também a consulta do **Anexo A** com a compilação de indicadores de risco que possam ajudar a melhorar a deteção da CEF. As UIF de outras jurisdições desenvolveram documentos de análise estratégica sobre a CEF. Todas estas iniciativas visam reforçar a deteção e a prevenção da criminalidade relacionada com a CEF e com as atividades de BC associadas.

Caixa 22. Análise estratégica sobre as "mulas de dinheiro" relacionadas com a CEF

Uma análise estratégica efetuada pela UIF espanhola procurou compreender um perfil de uma "mula de dinheiro": contas bancárias abertas por um único indivíduo em três ou mais instituições financeiras num período de 20 dias. Com base em informações do Registo de Contas Bancárias (RCB), entre dezembro de 2020 e fevereiro de 2022, o estudo revelou cerca de 40 000 outras contas bancárias ligadas a cerca de 10 000 pessoas. 15% das contas bancárias identificadas tiveram coincidências nas bases de dados da UIF espanhola. Estas contas foram classificadas como de alto risco, tendo sido lançado um estudo-piloto em colaboração com quatro instituições financeiras para reforçar o conhecimento sobre o perfil de risco associado a estas contas.

O estudo-piloto visava prevenir a CEF e outras possíveis fraudes, bem como melhorar a cooperação com o setor privado. Destinava-se igualmente a reforçar a capacidade das instituições financeiras para detetar lacunas nos seus sistemas e para obter mais informações sobre a CEF, a fim de detetar e prevenir criminalidade subsequente. Em última análise, o estudo também resultou na implementação de um sistema de

verificação cruzada que alavanca o RCB para detetar de forma proactiva redes o BC relacionadas com a CEF.

Fonte: Espanha

4.2. Coordenação e colaboração nacionais

Coordenação entre autoridades competentes

57. Dada a natureza transversal da CEF, existe uma clara necessidade de uma forte coordenação interna entre as agências. Algumas jurisdições abordaram a coordenação através de uma abordagem estratégica de todo o governo que orienta as políticas relacionadas com a CEF de uma jurisdição. Para tal criam um organismo multifuncional abrangente, composto por ministérios-chave nos setores judicial, policial, regulatório e de informação-comunicação. A abordagem coordenada permite que as jurisdições identifiquem as principais vulnerabilidades e definam respostas políticas holísticas em todos os setores-chave.

58. A coordenação de operações a nível nacional pode também envolver agências técnicas para reforçar a deteção e a investigação. Tal inclui:

- Desenvolvimento de canais de comunicação entre as UIF, a polícia e os magistrados do Ministério Público para garantir a elaboração centralizada de comunicações, a simplificação da troca de informações e provas, bem como instruções para o congelamento e apreensão de ativos. Pode incluir também a utilização de uma triagem automatizada de dados para ajudar a identificar possíveis questões de interesse, bem como identificar rapidamente uma autoridade adequada para a investigação. Esta coordenação reduz a duplicação de esforços das autoridades, uma vez que os criminosos da CEF podem atingir vítimas em diferentes locais de uma jurisdição (ver secção abaixo, sobre a definição adequada de responsabilidade).
- Utilização de peritos em cibercriminalidade, em especial no que se refere a intrusões na rede e outros crimes de infraestrutura técnica, bem como agências de proteção da privacidade. Tal reflete a natureza multifacetada da CEF e a relevância das provas forenses digitais (tais como endereços IP, identificadores ligados a domínios da Internet, etc.) na identificação dos grupos de CEF e posteriores investigações de BC.

Caixa 23. Centro conjunto de Coordenação da Cibercriminalidade

A Polícia Federal Australiana (*Australian Federal Police*, AFP) lidera o Centro Conjunto de Coordenação da Cibercriminalidade (*Policing Cybercrime Co-ordination* Centre, JPC3). Os membros da JPC3 incluem polícia federal e estadual, analistas governamentais, incluindo a AUSTRAC, e parceiros do setor, como analistas de bancos australianos.

O JPC3:

- Coordena a resposta policial da Austrália a crimes cibernéticos de alto volume e alto nível de danos par, para maximizar o impacto no ambiente criminal;
- Fomenta a partilha de informações e visa o desenvolvimento em toda a Commonwealth, na Polícia Estadual e Territorial e na indústria;
- Coordena as *task forces* conjuntas com a polícia e com os parceiros do setor para combater as ameaças prioritárias de cibercrime;
- Providencia a coordenação nacional no que diz respeito ao reforço das capacidades através de uma qualificação cruzada, de formação conjunta e do desenvolvimento de instrumentos de colaboração; e
- Divulga junto da indústria e do público atividades de prevenção, sensibilização e comunicação de forma consistente a nível nacional.

O JPC3 tem uma capacidade de prevenção que é exercida junto da indústria e no domínio público na luta contra a cibercriminalidade. Para sustentar de forma efetiva o JPC3, a AUSTRAC tem também uma equipa financeira de cibercrime, que se concentra especificamente em fornecer informações financeiras sobre crimes informáticos e praticados com recurso a meios informáticos num nexo financeiro, o que inclui o BC fruto de fraudes com recurso a meios informáticos.

Em janeiro de 2020, a AFP criou a Operação DOLOS, que é uma *task force* de várias agências[1] liderada pela AFP e combate aos cibercriminosos transnacionais que cometem ou facilitam o BEC. A operação DOLOS trabalha com privados australianos e pequenas e médias empresas que foram alvo de BEC, intercetando o fluxo de produtos ilícitos de e para os grupos de BEC. Desde o início da Operação DOLOS, a *task force* desenvolveu novas técnicas que levaram à redução de prejuízos tanto para os privados como para as empresas. Entre 1 de julho de 2022 e 30 de junho de 2023, a operação DOLOS impediu que mais de 30,6 milhões de AUD fossem perdidos por vítimas australianas e estrangeiras, perturbando o modelo financeiro utilizado pelos criminosos.

Fonte: Austrália

1 A task-force inclui vários serviços policiais estatais e territoriais, serviços de informação e cibersegurança, a UIF, bem como o setor financeiro.

Parcerias operacionais com o setor privado

59. As jurisdições também procuram colaborar com o setor privado através de parcerias público-privadas (PPP). Essas PPP podem ajudar a melhorar os esforços de deteção, identificação de redes BC ocultas através do intercâmbio tático de informações, bem como melhorar a resposta a nível da recuperação de ativos operacionais.

Caixa 24. Projeto: Ações rápidas para prevenir Fraudes

A UIF do Sri Lanka lançou um projeto denominado "Ações Rápidas para Prevenir Fraudes" (*Rapid Actions to Prevent Scams*, RAPS), para agir imediatamente quando uma vítima relata a ocorrência de uma potencial CEF. O objetivo é interromper as fraudes no sistema financeiro do Sri Lanka, nomeadamente a CEF, reunindo as UIF e os *compliance officers* das IF para detetar rapidamente atividades ilícitas em contas utilizadas por criminosos e seus cúmplices.

O mecanismo envolve a identificação das credenciais dos autores de fraudes com base nas queixas públicas recebidas, credenciais essas que são partilhadas com os compliance officers das IF. Com base nessas informações, as instituições financeiras monitorizam as atividades das contas de potenciais autores de fraudes e tomam as medidas adequadas para interromper o uso do sistema financeiro e prevenir qualquer fraude.

Além disso, as informações acerca dos autores das fraudes são partilhadas com a polícia do Sri Lanka para que os possa investigar.

Fonte: Sri Lanka

60. Tendo em conta aumento significativo da CEF, bem como o risco associado de BC, muitas jurisdições criaram centros de resposta centralizados em autoridades locais ou reguladores para intensificar as ações contra a CEF e aumentar a sensibilização do público (ver também a secção sobre unidades anti-CEF infra). Como boa prática, representantes das IF e dos VASPs poderiam ser alocados a esses centros de resposta centralizados, proporcionando o acesso, quase em tempo real aos dados financeiros e rastreando as várias entidades e setores financeiros, além de acelerar a capacidade das autoridades competentes de intercetar e congelar fundos.

Caixa 25. Co-localização de funcionários bancários

A Arábia Saudita criou uma Sala de Operações Conjuntas *(Joint Operations Room,* JOR) para os bancos. A JOR tem a tarefa de acompanhar e monitorizar casos de fraude financeira a que os clientes bancários possam estar expostos. A JOR reúne todos os bancos e instituições financeiras para resolver casos confirmados de fraude financeira.

A JOR é acolhida pelos bancos da Arábia Saudita com o objetivo de facilitar esforços conjuntos para a estabilidade do setor bancário. A JOR funcional 24 horas por dia, 7 dias por semana, e visa proporcionar uma cooperação e integração rápidas e eficazes entre todos os bancos sauditas, a fim de limitar o desenvolvimento de casos de fraude, bem como dar uma resposta rápida às queixas apresentadas e, sempre que possível, tomar medidas imediatas para evitar atos fraudulentos.

Fonte: Arábia Saudita

61. Estas parcerias proporcionam também uma plataforma útil para o intercâmbio de boas práticas, tipologias comuns e desenvolvimento de medidas recomendadas para interromper a atividade ilícita.

Caixa 26. Parceria Público-Privada de Informação Financeira da EUROPOL

A Parceria Público-Privada de Informação Financeira da EUROPOL (*Europol Financial Intelligence Public Private Partnership,* EFIPPP) é o primeiro mecanismo transnacional de partilha de informações entre os setores público e privado para ABC/CFT. A EFIPPP autoridades policiais, UIFs e entidades privadas de vários países da UE e de países terceiros.

O Grupo de Trabalho Ameaças e Tipologias no âmbito da EFIPPP desenvolvem diversos trabalhos relativos a vários tópicos relacionados com a CEF e os seus diferentes *modi operandi*, incluindo BEC, fraude no investimento, "contas-mulas", IBAN virtuais e criptoativos. Embora o objetivo da EFIPPP seja a criação de relatórios estratégicos de tipologias, também funciona como plataforma para discutir a facilitação da cooperação operacional entre os seus membros.

Fonte: Europol

62. A composição das PPP pode variar. Muitas jurisdições continuam a centrar-se nos intervenientes tradicionais (em especial bancos e outras instituições financeiras), mas existe um envolvimento crescente de APNFD, VASPs e outros setores não tradicionais (por exemplo, operadores de telecomunicações e fornecedores de serviços de Internet). A composição específica dependerá dos propósitos e objetivos da PPP.

Caixa 27. Cooperação com o setor das telecomunicações

Nos últimos anos, a China continuou a promover o reforço do combate e da gestão da fraude nas telecomunicações e, em 1 de dezembro de 2022, implementou oficialmente a "*Lei de Combate à Fraude na Rede de Telecomunicações da República Popular da China*", que conferiu fortes salvaguardas para o combate e contenção de atividades de fraude nas telecomunicações, tendo os atos criminosos relacionados sido eficazmente combatidos.

A lei reúne as autoridades do setor público (incluindo autoridades policiais, agências financeiras, de telecomunicações e de informação da internet), bem como as IF (bancos e prestadores de serviços de pagamento não bancários), os operadores de telecomunicações e os prestadores de serviços Internet para a criação de um sistema de alerta precoce e de dissuasão. Este sistema identifica as potenciais vítimas, através de um alerta precoce, permitindo a adoção de medidas dissuasivas, adequadas e atempadas.

As IF também podem utilizar este sistema para abrir contas bancárias, contas de pagamento e fornecer serviços de pagamento e liquidação. O sistema é utilizado para melhorar os processos de vigilância da clientela (*due diligence*) e permite às IF tomar medidas de mitigação do risco de exposição a atividades fraudulentas.

Fonte: China

4.3. Estratégias úteis de repressão nacionais

63. Esta secção explora algumas boas práticas e estratégias úteis que têm sido utilizadas pelas jurisdições. Em geral, estas estratégias utilizam as fontes de informação referidas na secção 4.1 para identificar, investigar e prevenir a CEF e o BC relacionado, de forma mais eficaz.

64. Estas estratégias envolvem normalmente várias agências e entidades do setor privado. Tal significa que é normalmente necessária uma forte coordenação e cooperação a nível interno para as implementar (como referido na secção 4.2).

Definição adequada da responsabilidade

65. Muitas jurisdições comunicaram um aumento das perdas e do volume de casos de CEF nos últimos anos. Embora alguns casos individuais possam envolver pequenas perdas, o volume de tais fraudes significa que o total do produto do crime acumulado, por cada grupo criminoso, é potencialmente elevado.

66. Várias jurisdições indicaram que o grande volume de CEF reportado torna urgente a definição da responsabilidade de investigação. Como boa prática, as jurisdições que dispõem de várias agências de combate à fraude ou à cibercriminalidade com supervisão sobre os casos de CEF procuraram identificar a autoridade ou autoridades competentes para tratar os mesmos. Outras jurisdições introduziram legislação destinada a consolidar investigações complexas que envolveram múltiplas vítimas do mesmo grupo, de tal forma que uma única autoridade competente tem supervisão sobre toda a investigação. Estas iniciativas evitam a duplicação de esforços das diferentes autoridades competentes e impedem que os casos sejam ignorados, além de abordarem a natureza transnacional do crime.

Caixa 28. Uso da tecnologia para definir a responsabilidade da investigação

A Polícia de Hong Kong (*Hong Kong Police Force*, HKPF) criou o *e-Crime Processing and Analysis Hub* (*e-Hub*) em setembro de 2022, com o objetivo de aumentar a eficácia no tratamento do crime tecnológico e das queixas relacionadas com a fraude. O *e-Hub* usa um sistema informático avançado para realizar análises de correlação entre os tipos comuns de fraude cibernética, e identificar *clusters* de casos.

Em 2022, o número de casos de fraude aumentou 45,1%, para 27 923 casos, representando quase 40% do número total de crimes. Quase 80% dos casos de fraude estavam relacionados com a CEF. Mais vítimas têm denunciado a CEF online e a maioria dos casos denunciados por e-mail estão correlacionados, sendo, muitos deles, do mesmo grupo criminoso. Os casos correlacionados são atribuídos a uma única equipa de investigação para investigação consolidada, permitindo uma melhor coordenação dos recursos.

Usando algoritmos de *cluster*, o *e-HUB* pode identificar padrões e semelhanças nos dados que podem não ser imediatamente evidentes, permitindo uma compreensão mais profunda do âmbito e da natureza dos casos. Tal inclui tipos comuns de ferramentas digitais criminosas, as contas de "mulas de dinheiro" utilizadas, e como a CEF é planeada, executada e ocultada.

Fonte: Hong Kong China

Unidades Específicas de combate à CEF e do BC relacionado

67. Com o objetivo de fortalecer as capacidades de ABC/CFT face à evolução do panorama criminoso, muitas jurisdições criaram uma unidade ou grupo de trabalho específico para investigar a CEF e BC conexos. Essas jurisdições alocaram recursos adicionais para fortalecer as capacidades em investigação financeira, recolha de informações e formação das autoridades, bem como o desenvolvimento de capacidades para o setor privado. Estas unidades centralizadas consolidam o conhecimento de forma transversal a todas as autoridades, tornando-as mais capazes de intercetar as operações de CEF, rastrear os fundos branqueados e recuperar os produtos ilícitos relacionados.

68. As jurisdições partilharam que os benefícios de tal organização são múltiplos. A consolidação de todos os casos de CEF por parte de uma única unidade permite uma melhor análise de dados e das ligações da rede para identificação dos grupos. Pode ainda servir de ponto único de contacto para as partes interessadas do setor privado e para os seus homólogos estrangeiros e ajudar a desenvolver relações estratégicas a longo prazo. Isto melhora os esforços de intervenção das autoridades, permite a monitorização das linhas telefónicas, a remoção de *monikers* e anúncios online suspeitos, e melhora os resultados da recuperação de ativos.

Caixa 29. Centro Nacional de Resposta a Fraude

O Centro Nacional de Resposta a Fraudes da Malásia (*Malaysia's National Scam Response Centre*, NSRC) constitui uma resposta multifacetada que reúne uma variedade de recursos e capacidades do Centro Nacional de Combate ao Crime Financeiro, da *Royal Malaysia Police* (RMP), do Banco Central e de outras entidades do setor público e privado.

O NSRC serve como um centro de informações sobre as fraudes recebidas de diversas fontes e utiliza a análise da rede para identificar as "mulas de dinheiro" e de práticas de branqueamento. As entidades do setor privado, incluindo as instituições financeiras, rastreiam os fundos, de nível em nível, de forma a chegarem às "contas-mula". A RMP investigará mais profundamente o caso, e adotará as medidas convenientes, como a emissão de uma ordem de congelamento das contas.

Fonte: Malásia

Melhorar o acesso às informações financeiras

69. Devido ao volume e à rapidez dos casos de CEF, o acesso atempado à informação financeira e bancária é crucial para acelerar a investigação e o rastreio dos produtos de CEF. Algumas jurisdições têm utilizado tecnologia para acompanhar o rápido fluxo do produto da CEF, colaborando muitas vezes com o setor privado no processo. Outras recorrem a registos centrais ou desenvolvem bases de dados para simplificar o processo de recuperação de informações. Essas boas práticas geralmente baseiam-se na criação de uma plataforma centralizada que reúne várias partes interessadas para um intercâmbio mais rápido de informações.

- **Recuperação de informações com base nas tecnologias:** Para permitir que as instituições financeiras forneçam rapidamente informações relevantes às autoridades policias, seria útil que as autoridades competentes de uma jurisdição chegassem a acordo relativamente aos campos de dados relevantes para as suas investigações. A emissão de vários pedidos, cada um deles exigindo uma resposta personalizada por parte da instituição financeira em causa, poderá ser moroso para o setor privado. Como boa prática, as autoridades policiais de algumas jurisdições desenvolveram um modelo normalizado que inclui campos de dados pré-acordados que são solicitados às instituições financeiras. Os pedidos podem então ser agregados, enviados a instituições financeiras em lotes e legíveis por máquinas. As instituições financeiras podem também fornecer digitalmente respostas aos pedidos legais das autoridades, permitindo uma análise mais eficiente dos dados.

Caixa 30. Utilização da automatização de processos robóticos para acelerar o acesso aos registos financeiros das instituições financeiras

O acesso atempado às informações bancárias e financeiras é fundamental para uma interceção eficaz e para a recuperação de ativos. Singapura está a utilizar a automatização de processos robóticos (RPA) para obter informações bancárias numa fração do tempo anterior.

As instruções são agora enviadas eletronicamente aos bancos através de um modelo normalizado. Os bancos automatizam o processo de recuperação de informações financeiras e, em seguida, enviam-nas de volta às autoridades policiais por via eletrónica. Os dados eletrónicos também podem ser imediatamente usados para análise por parte das autoridades policiais.

O processo reduziu o tempo de recuperação até 97%, conduzindo a investigações mais eficientes. A informação é agora disponibilizada num formato digital, pronta para análise. Para os bancos, esta iniciativa resultou numa economia significativa de custos ao eliminar os fluxos do trabalho manual. Do mesmo modo, permitiu aos Bancos a extração de dados através dos seus processos automatizados, que podem ser utilizados para melhor a deteção das redes BC ocultas.

Fonte: Singapura

- **Facilitação do rastreamento de ativos entre as IF**: As transferências e troca de contas entre várias IF aumentam os esforços de identificação por parte das autoridades policiais, dado que é necessário tempo para recolher informação junto das respetivas IF; analisar as diversas camadas de transações, de forma a identificar a origem e o destino final dos fundos. Este processo pode ser desafiante dada a velocidade das transações. As boas práticas incluem o desenvolvimento de plataformas para facilitar a deteção rápida e o intercâmbio de informações entre diferentes IF, a fim de intercetar o produto de atos ilícitos.

Caixa 31. Comunicação de Fraude Financeira Informática pelo cidadão e Gestão do Sistema *Citizen Financial Cyber Fraud Reporting and Management System* (CFCFRMS)

O CFCFRMS é um sistema online desenvolvido pelo Centro de Coordenação do Cibercrime Indiano para uma rápida comunicação de fraudes financeiras informáticas e para impedir o fluxo do produto de fraudes nos setores financeiros. O sistema integrou autoridades em todo o país e entidades financeiras (isto é, bancos, carteiras, agregadores de Pagamento, portais de pagamento, plataformas de comércio eletrónico, etc.) para trabalharem em conjunto e tomarem medidas imediatas relativamente às queixas apresentadas ao CFRMS. Atualmente, todas as

autoridades do Estado e do Território da União e 243 entidades financeiras estão incluídas neste sistema.

Uma vez que uma vítima comunique uma fraude a uma autoridade, os dados relativos ao beneficiário da operação fraudulenta são registados e enviados para o sistema CFRMS sob a forma de um *ticket*. Este *ticket* é encaminhado para a entidade financeira em questão (banco, carteira de pagamento, etc.), que o verá no painel do seu sistema. A entidade verificará se os fundos objeto de fraude ainda se encontram na conta, procedendo então, ao bloqueio dos mesmos. Se os fundos tiverem sido dissipados para outra entidade, o *ticket* ser-lhe-á remetido. O processo é repetido até que o dinheiro seja intercetado. Se o dinheiro for levantado, os dados do levantamento são preenchidos pela IF para posterior ação das autoridades.

O sistema tem sido muito eficaz, evitando que as transações fraudulentas cheguem às mãos dos autores das fraudes. Desde o seu início, em abril de 2021, o sistema conseguiu intercetar mais de 6,02 mil milhões de INR (cerca de 66,1 milhões de euros).

Fonte: India

- **Utilização dos registos centrais**: Os registos dos bancos centrais permitem às autoridades policiais um acesso rápido às informações bancárias básicas e ajudam a acelerar as investigações da CEF. As informações permitem que as autoridades policiais responsáveis verifiquem quais os bancos em que o suspeito detém contas ou a identidade do titular das mesmas. Este procedimento auxilia no processo de recuperação de informações, permitindo que as autoridades dirijam, em tempo útil, o foco das suas investigações e se concentrem apenas nas instituições financeiras nas quais o suspeito mantém contas.

Caixa 32. Identificação de "contas-mula" ocultas

Em Malta, foi apresentada uma COS relativa a uma suposta "mula de dinheiro", após a verificação da realização de uma série de transações suspeitas com diferentes beneficiários. Os fundos foram transferidos para vários bancos locais e internacionais com ligações a uma suspeita de fraude romântica.

As pesquisas efetuadas através do Registo Nacional de Contas do Banco Central permitiram à UIF identificar imediatamente outra conta ativa detida pela presumível "mula de dinheiro" num banco diferente. A UIF conseguiu estabelecer rapidamente um quadro global e o foco de análise financeira necessários. Em última análise, esta situação ajudou a UIF a identificar rapidamente os aspetos comuns com outras instâncias de branqueamento para outros indivíduos estrangeiros.

Fonte: Malta

- **Desenvolvimento de bases de dados para a partilha de informação a nível do setor privado**: No caso de redes BC profissionais, poderá haver um conhecimento ou suspeita relativamente a muitas "contas-mula" como parte de esquemas anteriores (por exemplo, as fraudes românticas, lotaria e propostas de emprego) ou de situações de furto de identidade. Também há sobreposições semelhantes nos dados e processos usados para identificar fraudes e para identificar redes de "mulas de dinheiro". Como boa prática, algumas jurisdições têm procurado centralizar dados transversais às bases de dados antifraude e ABC, no sentido de identificar redes BC mais profundas em várias IF, a fim de prevenir fraudes e promover a recuperação de ativos.

Caixa 33. Base de dados centralizada a nível privado

O Brasil aprovou recentemente uma resolução que torna obrigatória uma base de dados que centraliza informações sobre fraudes (incluindo as tentativas de fraude) por todas as instituições financeiras e de pagamentos. Esta base de dados é implementada pelo Banco Central do Brasil (BCB) e prevê-se que entre em funcionamento em novembro de 2023.

A Resolução estabelece que a partilha de informações sobre fraudes (incluindo as tentativas fraude) é obrigatória para as instituições financeiras e de pagamentos e define quais as informações mínimas que devem ser partilhadas. Estão incluídas, a identificação das pessoas envolvidas na fraude (incluindo as "mulas de dinheiro"), a instituição ou instituições financeiras envolvidas e a(s) conta(s) utilizada(s). O sistema visa facilitar a partilha de informações entre o setor privado, com o objetivo de prevenir e combater a fraude, bem como de recuperar o produto da fraude.

Fonte: Brasil

Identificar e dissuadir as "mulas de dinheiro"

70. Tal como foi referido anteriormente, as "mulas de dinheiro" desempenham um papel importante nas redes de BC relacionadas com a CEF, sendo recrutadas de diversas formas. Consoante o modo como são recrutadas e se foram enganadas ou exploradas inadvertidamente, podem ter diferentes níveis de conhecimento e envolvimento no esquema de CEF subjacente (ver secção 2.3 supra).

71. Consequentemente, as autoridades competentes podem enfrentar desafios no que se refere a acusações de BC. Pode ser difícil obter provas suficientes que demonstrem a intenção criminosa da "mula de dinheiro" em cometer BC (ou seja, nível de conhecimento de sua participação nono processo de branqueamento). Para tal, algumas jurisdições introduziram legislação para reduzir a *mens rea* exigível na infração de BC, como por exemplo o "conhecimento" e/ou a "suspeita".

Caixa 34. Artigo 9(3) da Convenção de Varsóvia do Conselho da Europa

Uma das questões subjacentes à acusação efetiva da infração BC é a necessidade de provar *mens rea* - ou seja, que o branqueador tinha conhecimento de que os fundos com que lidava eram produto do crime. Em casos complexos de BC em que estejam envolvidos branqueadores profissionais, é frequente o arguido negar categoricamente que sabia que os fundos eram produto do crime. Por conseguinte, demonstrar consciencialização dos atos praticados pelo arguido é uma das tarefas mais difíceis de provar na tipologia do crime de BC.

Tendo em conta as dificuldades em provar o *mens rea*, os autores da Convenção de Varsóvia introduziram novos elementos no artigo 9.º, onde é apresentada a infração de BC. Para além dos elementos já consagrados nas Convenções de Viena e de Palermo, o artigo 9.º da Convenção de Varsóvia, no seu n.º 3, vai mais longe, estabelecendo que a infração BC ocorre mesmo quando o autor da infração apenas suspeitasse ou deveria ter presumido que a origem dos fundos era criminosa.

Fonte: MONEYVAL

72. Outras jurisdições abordaram o desafio apresentado pelas "mulas de dinheiro", de forma geral através da educação pública e da sensibilização para o potencial recrutamento. Campanhas globais nas redes sociais, como a *#DontbeaMule*, apoiada pela Europol e pela *#YourAccountCrime* da INTERPOL, podem servir como plataformas úteis para coordenar a consciencialização internacional relativamente às atividades das "mulas de dinheiro", especialmente quando os fundos podem ser facilmente branqueados no exterior. A colaboração com o setor privado pode maximizar o efeito e os resultados de tais esforços de sensibilização. As autoridades podem também utilizar os mecanismos de deteção existentes (COS e denúncias das vítimas) para identificar potenciais "mulas de dinheiro" que possam ter lidado com receitas de CEF. A sensibilização e advertências direcionadas podem levar a que essas potenciais "mulas de dinheiro" não repitam tais comportamentos no futuro. Os registos passados de ações de sensibilização ou advertências podem ser utilizados como elementos de prova úteis para determinar a intenção criminosa de BC, em caso de reincidência.

4.4. Prevenção e rutura / desmantelamento

73. Dada a rapidez com que os fundos são dissipados, muitas jurisdições têm trabalhado para explorar iniciativas no sentido de impedir que a CEF e BC relacionados ocorram. Tal abordagem permitirá limitar a atuação dos grupos de CEF e reduz significativamente a dedicação de recursos a jusante, desde a investigação à gestão das vítimas.

Educação pública e sensibilização

74. Pode adotar-se uma abordagem preventiva através da educação do público e do reforço da vigilância contra a exploração, incluindo campanhas nacionais de conscientização que defendam a alfabetização cibernética. De modo a atingir este objetivo, algumas jurisdições utilizaram a tecnologia para implementar campanhas de informação aos cidadãos, a fim de os ajudar a detetar operações fraudulentas, aumentar a sensibilização para os indicadores e incentivar a denúncia por parte das vítimas.

Caixa 35. Utilização da tecnologia para a educação pública relativa a CEF

A Polícia de Hong Kong (*Hong Kong Police Force*,HKPF) lançou, em setembro de 2022, um motor de busca para os esquemas e armadilhas fraudulentos, o *Scameter*. A aplicação visa ajudar o público a identificar tais situações online.

Quando o público se depara com chamadas suspeitas e vendedores online, solicitações de amizade não solicitadas, mensagens de recrutamento arbitrárias, sites de investimento suspeitos de serem fraudulentos e similares pode inserir no *Scameter* o nome ou número da conta de origem, número da conta de pagamento, número de telefone, endereço de e-mail, URL, etc.

Os dados e a classificação do *Scameter* provêm de várias fontes fidedignas, incluindo comunicações públicas à polícia, informações fornecidas por organizações, base de dados de números de telefone suspeitos, bem como a base de dados e a análise em tempo real das empresas de segurança da informação.

Fonte: Hong Kong China

Segurança e controlos antifraude para resultados ABC/CFT

75. As experiências dos setores público e privado começam a mostrar que os processos antifraude e ABC são complementares. Tal inclui a utilização de tecnologia para ajudar os utilizadores a rejeitarem automaticamente a receção de mensagens fraudulentas, num trabalho conjunto com o setor privado para mitigar proativamente as tendências emergentes da fraude, através da criação de funcionalidades de segurança de contas, controlos e regras, bem como mensagens em programas antivírus alertando para potenciais sites de *phishing* (ver **Anexo B** que compila bons exemplos de como os reguladores financeiros adotaram requisitos antifraude juntamente com controlos ABC/CFT).

76. Outra boa prática é incentivar as instituições financeiras a adotarem o controlo das transações em tempo real para identificar e prevenir, de imediato, atividades fraudulentas ou ilícitas. Ao monitorizar informações invulgares sobre o titular da conta (por exemplo, endereços físicos, de IP e de e-mail, números móveis, etc.) e transações em tempo real, as IF podem identificar, investigar e comunicar rapidamente qualquer atividade pouco comum ou suspeita.

77. A monitorização de transações em tempo real, envolvendo o uso de softwares e algoritmos sofisticados para monitorizar transações financeiras, é considerado útil para detetar e prevenir a CEF. Dado o excesso de informações causado pela digitalização, a CEF pode ser difícil de detetar através de processos manuais. O acompanhamento das transações em tempo real pode ajudar as IFs a identificar e investigar os padrões de atividade suspeita em várias contas ou transações, mesmo que essas contas ou transações não estejam diretamente ligadas, impedindo a criminalidade futura.[21]

[21] Para mais informação de como a tecnologia pode ser utilizada para fins de ABC/CFT, ver também GAFI (Julho 2021) *Opportunities and Challenges of New Technologies for AML/CFT*

Remoção de instrumentos criminosos

78. Uma vez que a CEF também pode ser perpetrada através de setores não tradicionais (ver secção 3.3 supra), algumas jurisdições reforçaram a prevenção e os controlos antifraude nesses setores. Tal inclui fazer face aos instrumentos da CEF, como o encerramento das linhas móveis e das páginas Web fraudulentas utilizadas por criminosos, a filtragem de mensagens de *phishing* e de ligações Web maliciosas, etc.

Caixa 36. Remoção de sites suspeitos e campanhas de *phishing*

Na Arábia Saudita, as agências de aplicação da Lei e as autoridades reguladoras adotam uma abordagem colaborativa com os fornecedores de telecomunicações para melhorar substancialmente a sua capacidade de prever, prevenir, detetar e responder a eventos fraudulentos de forma eficaz. Para combater os instrumentos criminosos, a Autoridade Nacional de Cibersegurança da Arábia Saudita impôs requisitos rigorosos a nível de proteção de marcas, focando-se na luta contra sites de clones e mensagens de *phishing* em plataformas sociais. Além disso, o Banco Central da Arábia Saudita (*Saudi Central Bank*, SAMA) estabeleceu estruturas robustas de segurança cibernética e combate à fraude, definindo requisitos básicos de controlos obrigatórios para as entidades reguladas. Este quadro visa proteger proactivamente contra ameaças emergentes de fraude, assegurando assim a estabilidade e a salvaguarda do setor financeiro do Reino.

Um aspeto crucial destes requisitos nacionais e regulatórios é o controlo proativo dos instrumentos criminosos por parte das organizações. Isso envolve uma vigilância contínua de potenciais atividades fraudulentas, como sites suspeitos e campanhas de *phishing* através de tecnologias sofisticadas e medidas de proteção de marcas implementadas pelas organizações. Quando detetadas, estas atividades são prontamente comunicadas às autoridades competentes. A comunicação atempada garante uma ação rápida para investigar e encerrar operações criminosas, evitando novos danos e reduzindo o impacto de eventos fraudulentos.

Fonte: Arábia Saudita

Prevenção da dissipação de bens

79. Muitas jurisdições concluíram que um dos aspetos mais desafiadores das investigações da CEF é a rapidez com que o respetivo produto pode ser branqueado. Existe um consenso relativamente ao facto de ser crucial que as autoridades competentes possam intervir rapidamente para chegar ao produto dos crimes antes destes serem dissipados das várias contas bancárias. As jurisdições implementaram diversas medidas para recuperar mais eficazmente os ativos associados à CEF (ver secção 5.1 abaixo).

80. Poderá igualmente haver vantagens em envolver representantes-chave do setor financeiro privado para facilitar e incentivar uma interceção proactiva dos fundos ilícitos assim que é recebida uma comunicação de fraude de uma vítima, antes da mesma ser contactada pelas autoridades competentes. Podem também, ser necessárias trocas de

informação entre IFs nacionais e estrangeiras ou prestadores de serviços de pagamento (ver também a caixa 41 abaixo).

Caixa 37. Relatório do Grupo Egmont sobre a Fraude BEC

Em julho de 2019, o Grupo Egmont publicou um relatório destinado a alertar as UIF e respetivas jurisdições para a ameaça crescente que a fraude BEC representa através da partilha de cenários-chave e indicadores de risco associados à BEC. O relatório identificou ainda como as instituições financeiras (IF) podem desempenhar um papel importante na identificação, prevenção e comunicação da fraude BEC, promovendo uma maior comunicação e colaboração entre as suas unidades internas ABC, empresas, prevenção da fraude e Cibersegurança.

Para auxiliar na investigação de incidentes BEC e na recuperação de fundos das vítimas, as IF beneficiárias que tenham tido informação de que uma transferência fraudulenta foi executada numa das contas dos seus clientes (por exemplo, uma mensagem de devolução SWIFT), foram aconselhadas a não efetuar quaisquer transações que pudessem levar à perda de fundos, devendo contactar a autoridade policial ou a UIF para avaliar a validade da transação recebida.

Fonte: Grupo Egmont

5. Cooperação internacional e recuperação de ativos

81. Como referido anteriormente, a jurisdição onde ocorre a CEF (ou seja, onde a vítima está geralmente localizada) tende a ser diferente da jurisdição onde os produtos do crime são branqueados. Isto pode gerar a alguns desafios no que toca a investigações transnacional e na cooperação internacional eficaz para obter informações e provas, desmantelar os grupos de CEF e recuperar o produto do crime. Por exemplo, uma determinada jurisdição em que os produtos da CEF tenham sido branqueados, pode ter dificuldades em identificar todas as vítimas relacionadas com uma conta de BC, dado que esses fundos podem estar distribuídos por várias jurisdições.

82. A natureza descentralizada da CEF aumenta ainda mais a complexidade. Pode haver desfasamentos nas prioridades de cooperação internacional das jurisdições, por exemplo, nos casos em que as vítimas da Jurisdição A transferem fundos para a Jurisdição B, mas as vítimas da Jurisdição B estão na Jurisdição C (ou seja, A pode priorizar a colaboração com B, mas B pode priorizar a cooperação com C). A necessidade de envolver várias partes interessadas e parceiros, públicos e privados, no exterior também dificulta a identificação e o rastreamento de fundos ilícitos.

    - Os grupos de CEF utilizam diversos de serviços financeiros e tipos ativos. As transações podem ser realizadas quase instantaneamente, a nível transnacional, entre diferentes fornecedores e setores, tornando difícil localizar e determinar origem das transferências de fundos.
    - É provável que as provas forenses digitais relevantes estejam disseminadas por diferentes jurisdições, o que dificulta a construção um panorama completo do funcionamento das organizações criminosos e de como operam. Acrescem as características voláteis das provas forenses digitais, que podem ser facilmente dissipadas se não forem preservadas rapidamente.

83. A cooperação formal, incluindo a assistência jurídica mútua, demora normalmente muito tempo. Dada a natureza rápida dos crimes digitais e das atividades conexas do BC (em que as provas podem ser rapidamente dissipadas se não preservadas), a cooperação formal pode, por isso, ser bastante menos eficaz. Para continuarem a ser céleres na assistência transnacional e nos esforços para travar a atividade criminosa da CEF, as autoridades competentes dependem cada vez mais de mecanismos informais de cooperação através da partilha de informação diretamente com os seus homólogos estrangeiros. Tal pode ocorrer a nível policial ou das UIF através de vários canais, incluindo o Egmont Secure Web, a INTERPOL I-24/7, bem como outras redes informais, como a *Camden Asset Recovery Inter-Agency Network* (CARIN) e as agências regionais *Asset Recovery Inter-Agency Networks* (ARIN).

Caixa 38. Interceção do produto da CEF através de redes multilaterais informais

Para combater o aumento da CEF, as autoridades francesas de investigação utilizam ativamente redes informais, entre as quais a sub-rede *European Asset Recovery Office* (ARO) da *Camden Asset Recovery Inter-Agency Network* (CARIN) para uma cooperação internacional eficaz e recuperação de ativos relacionados.

O GRA francês (*French ARO*) trabalha em estreita colaboração com os membros destas duas redes, o que permite o intercâmbio rápido de informações pelas várias jurisdições entre autoridades legais e UIF especializadas na deteção, apreensão e confisco de ativos criminosos, especialmente em casos de emergência, em que os pedidos são respondidos no prazo de oito horas. Esta cooperação permite a rápida preservação dos fundos na conta de destino inicialmente identificada e em todas as outras contas subsequentes.

Em 2022, por exemplo, o GRA francês contactou o GRA eslovaco (*Slovak ARO*), relativamente a uma transferência bancária fraudulenta de 1 875 000 euros em detrimento de uma empresa francesa vítima, tendo solicitado que os fundos fossem congelados na conta bancária beneficiária na Eslováquia. As trocas entre os dois GRA resultaram no congelamento dos fundos e permitiram às autoridades eslovacas obter todas as informações necessárias para elaborar e executar um pedido de congelamento judicial. No final, o montante de 1 874 907 libras esterlinas foi congelado e subsequentemente devolvido à empresa vítima.

Fonte: França

84. A fim de maximizar a eficácia na investigação de BC relacionado com a CEF e na recuperação do produto do crime, a cooperação deve ter uma incidência multilateral e não bilateral. Esta secção analisa os desafios e boas práticas em relação à cooperação internacional através de dois resultados operacionais: i) recuperação de ativos e ii) execução e ação penal.

5.1. Recuperação de Ativos

85. Um desafio fundamental na recuperação de ativos da CEF é o ritmo rápido do branqueamento. Para mitigar este desafio, existem programas multilaterais de "resposta rápida" criados por vários organismos para rastrear e recuperar os produtos da CEF, incluindo o INTERPOL *Global Rapid Intervention of Payments* (I-GRIP), o Projeto BEC do Grupo Egmont e, dos EUA, a*Financial Fraud Kill Chain*. A experiência destes organismos mostra geralmente que a intervenção é mais eficaz no prazo de 24 a 72 horas após uma transação fraudulenta. Essas boas práticas reduzem o risco de que os fundos se dissiparem em vários níveis subsequentes, o que restringe drasticamente o âmbito da investigação de BC, e facilita a recuperação de produtos ilícitos.

Caixa 39. "Financial Fraud Kill Chain" e Equipa de Recuperação de Ativos

A *Financial Fraud Kill Chain* (FFKC) foi criada pelo FBI e pelo FinCEN (UIF dos EUA) em 2016, em resposta ao aumento dos esquemas de e-mails comerciais comprometidos. A FFKC tenta ajudar a recuperar as transferências internacionais enviadas como parte de esquemas de fraude, aproveitando as relações do FinCEN com o Grupo Egmont de Unidades de Informação Financeira. Este processo só pode ser implementado se a transferência fraudulenta preencher os seguintes critérios: 1) se a transferência for igual a USD 50 000 ou superior; 2) se a transferência for internacional; 3) se tiver sido iniciado um processo de devolução de fundos via SWIFT; e 4) se a transferência tiver ocorrido nas últimas 72 horas.

Em 2018, o *Internet Crime Complaint Center* (IC3) do FBI criou a Equipa de Recuperação de Ativos (*Recovery Asset Team*, RAT) para lidar com vulnerabilidades em transferências domésticas. A RAT simplifica a comunicação com as instituições financeiras e auxilia o FBI no terreno, com o congelamento de fundos para a transferências domésticas fraudulentas. Até à data, a RAT registou alguns êxitos notáveis, congelando 73% dos fundos declarados ao IC3 como fraudulentos (433,3 milhões de dólares de 590,62 milhões de dólares). De acordo com o exemplo deste caso americano, este programa pode, em alguns casos, identificar rapidamente as contas de 2º nível e congelar os fundos, possibilitando uma recuperação total.

Fonte: Estados Unidos

86. Estes programas multilaterais visam duas coisas: recolher o nível mínimo de informação exigido para a ação policial e transmitir essa informação às "mãos certas". Para garantir uma resposta transnacional eficaz, todos os elos das redes multilaterais estão igualmente de acordo sobre as regras e procedimentos de governação. Embora estas redes multilaterais sejam normalmente de natureza global, as iniciativas regionais podem também ser úteis para mitigar os desafios, baseando-se na colaboração regional já estabelecida.

Caixa 40. Projeto Anti-Fraude Multijurisdicional

Dada a natureza transnacional da fraude, foi desenvolvida uma iniciativa regional no âmbito do *Financial Intelligence Consultative Group* (FICG)[1], denominada Projeto Anti-Fraude Multijurisdicional. Esta iniciativa é coliderada pelas UIF da Malásia, Indonésia e Singapura e visa detetar, localizar e recuperar fundos para as vítimas.

Foi criado um mecanismo de resposta que envolve transações transnacionais entre os países membros do FICG. Este projeto ajudará os membros do FICG a partilhar informação financeira de forma rápida e fácil, em apoio a ações rápidas das autoridades para combater a fraude e recuperar o dinheiro furtado.

Fonte: Malásia

1 O FICG é um organismo regional de UIF do Sudeste da Ásia, Nova Zelândia e Austrália.

Recolha e troca transnacional de informações: "Recolher o nível mínimo de informação"

87. Onde a CEF é considerada um crime grave nos termos do direito interno, deve ser criminalizado como crime subjacente ao BC, nos termos da Recomendação 3 do GAFI. Além disso, ao contrário das formas tradicionais de fraude praticadas entre conhecidos, em que é difícil distinguir a fraude de potenciais litígios entre devedores e credores civis, é relativamente mais fácil estabelecer a criminalidade *prima facie* nos casos da CEF, em que a fraude ocorre tipicamente entre não conhecidos. Tal mitiga a necessidade de um longo pedido de assistência para articulação e definição do nexo criminoso, como normalmente é exigido para outros tipos de crimes (que não são universalmente reconhecidos como crimes subjacentes).

88. Como boa prática, os vários programas de resposta rápida utilizam modelos para acelerar a recolha e o intercâmbio de informações. Os modelos permitem a rápida recolha de um nível mínimo de informação necessário para estabelecer a criminalidade. Ajudam a dirigir os esforços das unidades de resposta no terreno para os tipos vitais de provas ou informações que devem ser obtidos nas fases iniciais de uma queixa-crime. Tais modelos também atenuam os desafios em matéria de qualidade das informações trocadas e melhoram a resposta transnacional das autoridades.

89. Para além de um resumo para descrever o crime da CEF, os modelos procuram geralmente obter os dados básicos necessários para avançar com os esforços de deteção de fundos. A padronização dos pedidos permite que as jurisdições requeridas processem rapidamente quaisquer pedidos recebidos, acelerando a capacidade das autoridades para intercetar fundos ilícitos que entraram na sua jurisdição.

90. Os campos de dados dos modelos podem incluir informações sobre o ordenante e a conta do beneficiário, bem como informações sobre a transação (data, hora, montantes transferidos). A fim de reforçar a eficácia, os modelos poderiam também incluir informações sobre o destino seguinte dos fundos, se estes já tiverem saído da conta do beneficiário. Pode também ser útil minimizar quaisquer restrições impostas às jurisdições na divulgação de quaisquer informações que estejam a ser trocadas com as autoridades competentes relevantes a nível interno, aquando da sua receção.

Caixa 41. INTERPOL I-GRIP

A INTERPOL desenvolveu o sistema *INTERPOL Global Rapid Intervention of Payments* (I-GRIP), que é um mecanismo global de interrupção de pagamentos que permite aos países membros enviar e processas os pedidos para acompanhar, intercetar ou congelar provisoriamente o produto da CEF. Conhecido como I-GRIP, o mecanismo foi originalmente apresentado como *Anti-Money Laundering Rapid Response Protocol* (ARRP) em 2022, tendo sido lançado oficialmente em novembro de 2022, graças a muitos casos bem-sucedidos de interrupção de pagamentos durante a fase-piloto.

O I-GRIP facilita a rápida comunicação entre os gabinetes centrais nacionais da INTERPOL (*INTERPOL National Central Bureaus*, GCN), a fim de evitar a transferência de bens ilícitos suspeitos entre os países membros. Os pedidos apresentados via I-GRIP devem incluir detalhes suficientes com base nos quais o GCN destinatário pode atuar, tais como, a data da transação, a moeda e o montante, os números de conta e os nomes das instituições financeiras das contas do beneficiário e do remetente.

Fonte: INTERPOL

91. Além disso, campos de dados padronizados em modelos permitem que organizações internacionais com recursos centralizados os analisem facilmente e maximizem os esforços de investigação e recuperação de ativos. Por exemplo, a INTERPOL utiliza as informações trocadas através dos seus canais para criar uma base de dados interna, o ficheiro de análise criminal (*Financial Criminal Analytical* File, FINCAF), para facilitar a análise de informações com dimensão transnacional sobre diversas formas de crimes financeiros e para identificar ligações entre os casos e investigações transnacionais, ameaças, tendências criminais e redes criminosas (ver também caixa 45 abaixo).

92. Para acelerar as ações de recuperação de ativos, algumas jurisdições permitiram que as vítimas estrangeiras apresentassem queixas de CEF diretamente junto das suas autoridades locais, inclusive através da sua plataforma de comunicações online, para preenchimento direto dos campos de dados necessários para a ação respetiva (ver seção supra sobre Comunicação das Vítimas). Tal elimina mais um nível de comunicação e permite às autoridades competentes tomar rapidamente quaisquer medidas disponíveis contra transações suspeitas efetuadas sobre contas beneficiárias nas suas jurisdições.

Poderes necessários para atuar: "as Mãos Corretas"

93. Dado que a rapidez é essencial, qualquer informação recolhida deve, de preferência, ser diretamente entregue a autoridades já dotadas de poderes e competências adequadas para a deteção e recuperação de ativos. Tal permite a adoção imediata de medidas provisórias após a receção de um pedido para evitar o branqueamento ou a dissipação de ativos. Proporciona ainda às autoridades o tempo vital necessário para prosseguir as suas investigações, desenvolver e recolher provas e dar seguimento aos pedidos formais de auxílio judiciário mútuo.

Caixa 42. Pedido de adiamento por parte da entidade obrigada

A UIF de Itália recebeu de uma entidade obrigada um pedido de adiamento de quatro transferências eletrónicas suspeitas no montante de 490 000 euros. As transações foram ordenadas por uma empresa italiana de comércio grossista de vestuário, a favor de várias empresas de um país do extremo leste asiático.

A entidade obrigada tinha considerado as quatro transações como suspeitas, uma vez que os fundos eram provenientes de transferências recebidas que estavam a ser alvo de pedidos de devolução pelo banco remetente, por alegadamente os fundos terem sido enviados ao abrigo de uma "fraude CEO" por parte de uma empresa vítima da Europa Ocidental. A UIF de Itália recebeu igualmente uma informação internacional espontânea proveniente da UIF do referido país da Europa Ocidental. A empresa italiana foi igualmente alvo de uma comunicação à UIF por uma possível ligação a esquemas de fraude de IVA que envolviam o referido país asiático, através de um outro país da Europa de leste, o que apontava para mais ligações entre a CEF e outros tipos de criminalidade organizada.

As transações foram suspensas com êxito. Tal permitiu às autoridades estrangeiras emitir uma ordem de apreensão com vista à recuperação dos fundos em Itália.

Fonte: Itália

94. No entanto, essa interação direta pode comportar desafios devido às diferenças entre os quadros legislativos e de execução das jurisdições. Algumas boas práticas para mitigar estes desafios incluem o estabelecimento de mecanismos de coordenação nacionais para facilitar a transmissão de pedidos às autoridades competentes, bem como o aproveitamento dos canais de colaboração público-privados e a capacidade das IF para adotarem voluntariamente medidas provisórias, uma vez informados de transações suspeitas por parte das autoridades competentes.

Governança e Regras: "o Acordo Coletivo"

95. A governança e as regras aplicáveis aos quadros multilaterais oferecem garantias e o compromisso de reconhecerem mutuamente a atividade criminosa e de agir rapidamente assim que são recebidas informações. Isso ajuda a ultrapassar o desafio que possa existir de incompatibilidade de prioridades entre as agências internacionais, uma vez que as condições para aceder e prestar assistência foram previamente acordadas. Como boa prática, essas regras e critérios devem ser claros e facilmente compreendidos.

96. Os princípios acima referidos aplicam-se quer aos mecanismos formais de cooperação internacional, quer aos mecanismos informais. Como bom exemplo, o Regulamento (UE) 2018/1805 do Parlamento Europeu e do Conselho permite o reconhecimento mútuo das decisões estrangeiras de apreensão e de perda. Este mecanismo de aplicação direta permite uma intervenção transnacional rápida.

97. A partilha rápida de informações não deve ser feita em detrimento da proteção de dados e da confidencialidade. A fim de garantir a segurança das informações transmitidas, as

estruturas multilaterais utilizam normalmente os canais de comunicação seguros existentes, como os fornecidos pela INTERPOL, pela Europol e pelo Grupo Egmont. Estes canais de comunicação seguros permitem que estes quadros multilaterais se expandam facilmente, uma vez que evitam a necessidade de desenvolver canais de comunicação bilaterais.

Caixa 43. A Equipa de Projeto BEC do Grupo Egmont

Para enfrentar a crescente e grave ameaça que o BEC representa para as instituições financeiras e seus clientes, 11, as UIF lançaram a *Equipa de Projeto BEC do Egmon*t, Equipa do Projeto (*Egmont BEC Project Team),* que se concentrou na análise das tendências, indicadores e metodologias de BEC, bem como na partilha dos principais resultados com as UIF. As tipologias financeiras comuns de BEC e os estudos de casos mostram que uma reação rápida para deter e seguir as transferências é a forma mais eficaz de combater este tipo de crime.

Como tal, a Equipa de Projeto[1] estabelece protocolos entre as autoridades policiais e as UIFs, e entre as UIFs internacionais, no sentido de acompanhar e congelar os produtos de BEC:

- Ao receber uma COS relacionada com fluxos transnacionais suspeitos de BEC, a UIF recetora desenvolve um pedido de "resposta rápida" à UIF de destino;
- O pedido deve conter dados e informações básicos acordados, necessários ao intercâmbio de medidas de execução;
- À UIF de destino solicita-se que tome (sempre que possível) medidas imediatas para suspender e recuperar o produto do crime, idealmente no prazo de 72 horas após a sua ocorrência.

O projeto BEC é alavancado na plataforma segura do Grupo Egmont para as comunicações para trocar os pedidos de "resposta rápida".

Fonte: Grupo Egmont

1 Os membros da equipa de projeto são atualmente: AUSTRAC (Austrália), BFIU (Bangladesh), CTIF-CFI (Bélgica), TRACFIN (França), GHFIU (Gana), HFIU (Hungria), IMPA (Israel), SIC (Líbano), FIU Luxemburgo, UPWBNM (Malásia), FinCEN (EUA) e Europol.

5.2. Repressão e exercício da ação penal

98. Além da recuperação de ativos, a natureza transnacional da CEF também resultou em dificuldades ao longo de todo o processo de execução, desde a recolha de informações e investigação até à recolha de provas para efeitos de ação penal. A evolução da tecnologia aumentou a velocidade das transações e facilitou as operações fragmentadas transnacionais. Aumentou também o tempo e os esforços necessários para que as autoridades policiais rastreiem e identifiquem os criminosos.

Recolha de provas digitais

99. Embora não estejam exclusivamente relacionadas com o BC, as provas forenses digitais podem fornecer pistas críticas para as autoridades policiais direcionarem as suas investigações de BC. A disponibilidade generalizada e a facilidade de utilização dos serviços de ocultação de identidade, como as VPNs, complicam ainda mais os esforços para localizar os principais autores de CEF.

100. Infelizmente, não existe atualmente um regime global único que regule a duração da retenção de dados digitais, incluindo no que se refere aos prestadores de serviços técnicos. Várias jurisdições destacaram o risco significativo de dissipação de provas digitais. Os atrasos nos mecanismos formais de cooperação representariam um desafio para a rápida obtenção de provas digitais.

101. Existem diversas boas práticas que podem mitigar esses desafios.

- **Utilizar canais informais** para inicialmente reunir e proteger informações. Seguidamente, são utilizados canais de cooperação formais para obter os elementos de prova e as declarações necessários à preparação dos processos judiciais**.**
- **Convenções e instrumentos de investigação**, como a Convenção sobre Cibercriminalidade, também conhecida como Convenção de Budapeste, permitem a rápida conservação de dados eletrónicos e a transmissão de informações espontâneas, o que ajuda a acelerar a identificação dos reais autores da CEF. A Convenção de Budapeste estabelece igualmente uma rede 24 horas por dia, 7 dias por semana, que assegura assistência imediata em matéria de investigação para a prestação de aconselhamento técnico, recolha de provas, conservação de dados, etc.
- **Cooperação direta** com prestadores de serviços estrangeiros para obter as provas forenses necessárias, como, por exemplo, informações sobre subscritores, sem passar pelo processo de auxílio judiciário mútuo. De acordo com uma jurisdição, a cooperação voluntária direta de um prestador de serviços estrangeiro é o mecanismo mais eficaz para recolher provas digitais relevantes.[22]

[22] Ver também Conselho da Europa (Julho 2020) *Budapest Convention on Cybercrime: benefits and impact in practice* para mais informação sobre a cooperação voluntária com prestadores de serviços estrangeiros.

Caixa 44. A Convenção de Budapeste

A Convenção de Budapeste estabelece poderes processuais para: conservação expedita dos dados armazenados, preservação expedita e divulgação parcial de dados de tráfego, injunção, busca e apreensão de dados informáticos, recolha de dados de tráfego em tempo real e interceção de dados de conteúdo. A Convenção prevê também um regime rápido e eficaz de cooperação internacional.

O Segundo Protocolo Adicional à Convenção sobre a Cibercriminalidade sobre o reforço da cooperação e da divulgação de provas eletrónicas constitui igualmente uma base jurídica para a divulgação de informações relativas ao registo de domínios, bem como para a cooperação direta com os prestadores de serviços para obtenção de informação sobre assinantes, meios eficazes para obter informações sobre os mesmo, assim como dados de tráfego, cooperação imediata em situações de emergência, instrumentos de assistência mútua, e salvaguardas relativas à proteção de dados pessoais.

Fonte: Conselho da Europa

Ação conjunta de Fiscalização

102. As equipas de investigação conjuntas transnacionais [*JIT – Joint Investigation Teams*] envolvem um acordo jurídico entre autoridades competentes de duas ou mais jurisdições para efeitos de realização de investigações criminais. Estas podem facilitar a partilha de informações e a deteção financeira das fraudes transnacionais. A partilha de informações ocorre tipicamente ao abrigo de vários enquadramentos e acordos (por exemplo, o Eurojust, o Grupo de Ação Comum sobre Cibercrimes apoiado pela Europol).

103. As JITs constituem igualmente um importante de coordenação ponto para a ação coerciva multilateral contra a CEF, dado que se está perante operações transnacionais e descentralizadas. Com a redução das barreiras das operações criminosas, os grupos de CEF podem facilmente relocalizar-se, criando novos centros de operações digitais remotamente. Por conseguinte, é necessária uma ação de coordenação para erradicar, simultaneamente, os vários subgrupos (que podem estar a trabalhar em várias jurisdições).

Caixa 45. Ação conjunta contra fraude ao investimento em larga escala [1]

A Sérvia, juntamente com a Áustria, a Bulgária e a Alemanha e com o apoio da Eurojust, participou com sucesso em operações contra dois grupos de criminalidade organizada suspeitos de fraude em larga escala no comércio eletrónico. As autoridades sérvias prenderam cinco suspeitos e revistaram nove locais, apreenderam cinco apartamentos, três carros, um montante considerável de dinheiro e equipamento informático. Mais de 30 contas bancárias sérvias foram também colocadas sob vigilância. Além disso, quatro suspeitos foram detidos na Bulgária, enquanto 2,5 milhões de euros foram congelados na conta bancária de uma empresa envolvida no esquema de fraude na Alemanha.

Com base nas informações recolhidas durante a operação, as autoridades iniciaram rapidamente outra operação contra uma empresa em Belgrado, dois dias depois, detendo um suspeito e apreendendo servidores, mais equipamento informático e documentos.

Neste caso, as autoridades sérvias recorreram, nomeadamente, ao artigo 26.º da Convenção de Budapeste (informação espontânea) para partilhar informação com outros parceiros. A Eurojust continuou a apoiar as investigações através do financiamento de uma equipa de investigação conjunta (JIT), bem como organizando uma reunião de coordenação nas suas instalações em Haia e uma videoconferência.

Fonte: Sérvia; Conselho da Europa (julho de 2020) Convenção de Budapeste sobre Cibercriminalidade: benefícios e impacto na prática

1 Para mais informação, ver também "press release" da Eurojust (Abril 2020), disponível em: www.eurojust.europa.eu/news/action-against-large-scale-investment-fraud-several-countries

104. Há também desafios associados a uma ação conjunta.

- **Obstáculos jurídicos** poderão restringir o intercâmbio informal de informações, mesmo no âmbito de equipas de investigação conjuntas. Uma jurisdição compartilhou a necessidade de continuar a depender dos pedidos de assistência legal mútua (MLA) para poder trocar informações, o que pode prejudicar a eficácia e a envolvência. Podem igualmente existir limites quanto à informação que pode ser partilhada, nomeadamente no que se refere à granularidade das informações sobre transações financeiras.
- **Capacidades e prioridades desiguais** podem também dissuadir as jurisdições de participarem em ações conjuntas. Como referido anteriormente, as prioridades internas podem não estar alinhadas com a ação conjunta e as jurisdições podem ter dificuldade no equilíbrio destes interesses face às restrições em matéria de recursos, apesar do aumento da CEF.

105. Além das JIT, as operações conjuntas organizadas por organizações multilaterais, como a INTERPOL, constituem também um importante ponto de coordenação das ações multilaterais contra a CEF. Embora estas operações possam ser mais informais do que as

JIT na ausência de acordos jurídicos formais, podem ainda constituir uma plataforma importante para as jurisdições relevantes combaterem conjuntamente a CEF.

Caixa 46. Operação HAECHI da INTERPOL

Desde 2020, a INTERPOL realiza uma operação anual denominada HAECHI que visa crimes financeiros com recurso a meios informáticos e BC associado e que que permite o intercâmbio de informações entre jurisdições participantes. Nos termos do recente HAECHI III (2022), em que participaram 30 jurisdições, foram detidos quase 1 000 suspeitos e bloqueadas 2 800 contas bancárias e de ativos virtuais, relacionadas com o produto do crime, no valor de 130 milhões de dólares. Através do HAECHI III, a INTERPOL coordenou inúmeros casos entre os países membros para combater conjuntamente a CEF.

A Operação HAECHI também serviu de plataforma para a FINCAF, que recolhe informações de diferentes fontes e identifica ligações entre investigações em curso em diferentes países membros. A FINCAF está estruturada por forma a incluir dados e outras informações relativas a quaisquer tipos de criminalidade financeira e infrações de dimensão transnacional. A INTERPOL utiliza a FINCAF para trabalhar com os países membros no sentido de reforçar a resposta tática global ao crime organizado internacional, como a CEF. A FINCAF é uma ferramenta importante que fornece a melhor informação sobre atividades criminosas transnacionais, organizações criminosas, suas estruturas de grupo, papéis individuais e pessoas chave, *modi operandi* e transações financeiras fraudulentas.

Fonte: INTERPOL

Colaboração público-privada

106. A colaboração público-privada pode estender-se para além das fronteiras nacionais, o que pode permitir melhores resultados, tendo em conta o alcance transnacional da CEF. Tal como as PPP nacionais, essa colaboração pode abranger tipologias ou uma partilha estratégica, bem como a coordenação operacional. A composição dessas parcerias dependeria igualmente dos objetivos e poderia incluir os setores tradicionais pertinentes ABC/CFT, bem como os não tradicionais.

Caixa 47. Ação "Money Mule" Europeia

A Ação *Money Mule ("*Mulas de dinheiro*")* Europeia é uma operação internacional baseada na partilha de informação entre o setor público e o setor privado para combater crimes complexos modernos.

Em 2022, com a coordenação contínua da Federação Bancária Europeia, cerca de 1 800 bancos e instituições financeiras apoiaram a aplicação da lei nesta ação, juntamente com serviços de transferência de dinheiro online, bolsas de criptomoeda, empresas Fintech e KYC e empresas multinacionais de tecnologia informática.

A operação incluía as autoridades de 25 jurisdições[1] e foi ainda apoiada pela Europol, Eurojust e INTERPOL. Foram identificadas 8 755 "mulas de dinheiro", juntamente com 222 angariadores. No total, foram intercetados 17,5 milhões de euros de fundos, com 2 469 "mulas de dinheiro" detidas.

Fonte: Europol

Austrália, Áustria, Bulgária, Colômbia, Chipre, República Checa, Estónia, Grécia, Hungria, Singapura, Hong Kong (China), Irlanda, Itália, Moldávia, Países Baixos, Polónia, Portugal, Roménia, República Eslovaca, Eslovénia, Suécia, Suíça, Espanha, Reino Unido e Estados Unidos.

6. Conclusão e áreas prioritárias

107. A CEF é perpetrada por grupos transnacionais de crime organizado. É expectável que a escala e magnitude da CEF aumentem com a tendência crescente de digitalização e serviços virtuais em todo o mundo. As jurisdições devem também estar cientes das vulnerabilidades adicionais em vários setores, incluindo as instituições financeiras digitais e os setores não tradicionais, e que os criminosos podem explorar para melhorar as técnicas de CEF e BC através de uma digitalização crescente.

108. As jurisdições devem concentrar-se na eliminação de barreiras, a fim de acelerar e reforçar a colaboração entre vários setores e entidades, tanto a nível nacional como internacional. Devido à natureza descentralizada da CEF e ao branqueamento conexo, as informações e os elementos de prova financeiros vitais estão frequentemente fragmentados em diferentes locais. Esta situação complica os esforços para investigar e desmantelar os grupos de CEF, bem como para rastrear e recuperar o produto do crime.

109. A CEF pode ter um impacto financeiro significativo e negativo nas vítimas. Mas o impacto não se limita às perdas monetárias; pode ter implicações sociais e económicas devastadoras. As conclusões do presente relatório indicam três domínios prioritários em que as jurisdições devem agir para combater de forma mais eficaz a CEF e o branqueamento de capitais conexo: reforço da coordenação interna; apoio à colaboração multilateral e reforço da deteção e prevenção.

Áreas prioritárias para combater eficazmente a CEF e o BC conexo

Reforçar a coordenação interna entre os setores público e privado

- As jurisdições devem desenvolver mecanismos de coordenação que reúnam as autoridades competentes relevantes para combater a CEF e o branqueamento de produtos do crime conexos de forma holística. Tal inclui peritos técnicos em cibercriminalidade, bem como setores não tradicionais, como as plataformas de redes sociais, o comércio eletrónico, os fornecedores de serviços de telecomunicações e de Internet. As jurisdições devem também alavancar parcerias público-privadas para melhorar a deteção e as investigações e acelerar as respostas operacionais em matéria de recuperação de bens.
- Uma boa prática envolve a criação de uma unidade centralizada específica que possa tirar partido das informações pertinentes e coordenar ações em vários setores públicos e privados, incluindo investigações, recuperação de bens e prevenção da fraude.

Apoio à colaboração internacional multilateral

- A fim de melhorar os resultados da recuperação de bens e evitar a dissipação das receitas relacionadas com a CEF, as jurisdições devem trabalhar em conjunto para intercetar rapidamente as receitas da mesma. A experiência operacional mostra que a intervenção é geralmente mais eficaz no prazo de 24 a 72 horas após um incidente de CEF. É necessária uma abordagem global unificada para detetar e recuperar eficazmente o produto dos crimes, que são branqueados e distribuídos por várias jurisdições.
- Para o efeito, as jurisdições devem mobilizar e apoiar os mecanismos multilaterais existentes (e futuros) (como o I-GRIP da INTERPOL e o Projeto BEC do Grupo Egmont) para uma rápida cooperação internacional e intercâmbio de informações no combate à CEF. Esses mecanismos multilaterais também permitem às jurisdições colaborar e desmantelar coletivamente os grupos transnacionais de CEF.

Reforçar a deteção e a prevenção

- A fim de melhorar a deteção, as jurisdições devem assegurar a facilidade de denúncia por parte das vítimas, por exemplo, através de plataformas específicas que permitam uma denúncia simplificada. As jurisdições devem também colaborar com o setor privado para melhorar a comunicação de transações suspeitas.
- As jurisdições devem promover a sensibilização e a vigilância contra a CEF através da educação pública, incluindo a partilha de sinais de alerta de CEF e o reforço da cibe literacia. A prevenção desempenha um papel fundamental na redução da rentabilidade global dos grupos de CEF. As jurisdições podem também colaborar com o setor privado para apoiar as

estratégias de prevenção de CEF, como é o caso da proteção dos consumidores e a remoção de instrumentos criminosos.

Anexo A: Indicadores de risco de CEF

Os seguintes potenciais indicadores de risco baseiam-se na experiência e nos dados recebidos de jurisdições de toda a rede global do GAFI, do Grupo Egmont e do setor privado. Estes indicadores visam melhorar a deteção de operações suspeitas relacionadas com a CEF. A lista é ainda categorizada sob várias perspetivas, desde a abertura de conta até à monitorização das transações. Os indicadores podem ser relevantes para as entidades reguladas, incluindo IF, VASPs, APND e outras instituições financeiras e de pagamento.

A existência de um indicador único em relação a um cliente ou transação não pode, por si só, justificar a suspeita de uma infração de CEF, nem um único indicador fornecerá necessariamente uma indicação clara dessa atividade. No entanto, poderá levar a um acompanhamento e uma análise mais aprofundados, conforme adequado.

Padrões de transações

- Operações rápidas ou imediatas, de valor elevado ou reduzido após a abertura de uma conta, incompatíveis com a finalidade da conta.
- Levantamentos ou transferências de numerário rápidos ou imediatos, de montantes avultados, após a receção de uma transferência de fundos, de modo que a conta fique sem fundos.
- Transações frequentes e de grande dimensão que são inconsistentes com o perfil económico do titular da conta (por exemplo, transferências internacionais súbitas, levantamentos de numerário efetuados através de cartões de pagamento em caixas automáticas estrangeiras, grandes compras de ativos virtuais ou bens a exportar para o estrangeiro, ou pagamentos a favor de MVTS [Serviços de transferência de dinheiro ou valores] estrangeiros não licenciados).
- Transferências de fundos de e para jurisdições de alto risco de BC.
- Transações elevadas frequentes com empresas recentemente estabelecidas e/ou cujas atividades principais não são coerentes com as atividades realizadas pelo beneficiário, ou têm um objetivo geral.
- Pequeno pagamento a um beneficiário que, uma vez concluído com êxito, é rapidamente seguido de pagamentos de maior valor ao mesmo beneficiário.
- Compras de valor arredondado que são frequentes e/ou em montantes elevados, que podem indicar compras com cartão de oferta.

Instruções e observações sobre transações do cliente

- Um cliente requer pagamentos adicionais, imediatamente após um pagamento bem-sucedido, para uma conta por ele não utilizada em momentos anteriores, para pagar aos seus fornecedores/vendedores. Tal comportamento pode ser coerente com uma tentativa criminosa de emitir pagamentos adicionais não autorizados, após ter tomado conhecimento de que um pagamento fraudulento foi bem-sucedido.
- As instruções de transação aparentemente legítimas de um cliente contêm uma linguagem vernacular, prazos e montantes diferentes das instruções de transação previamente verificadas.
- As instruções de transação incluem marcas, afirmações ou linguagem que designam o pedido de transação como «urgente», «secreto» ou «confidencial».
- Um cliente apresenta mensagens/e-mails mal formatadas (erros ortográficos e/ou gramaticais) como justificação de uma transação.
- Instruções de transação para o pagamento direto a um beneficiário conhecido; no entanto, as informações sobre a conta do beneficiário são diferentes das anteriormente utilizadas.
- O beneficiário previsto na descrição da operação e o nome do titular da conta tal como conhecido pelo banco beneficiário, são inconsistentes.
- Transferências ordenadas por pessoas singulares (alegados investidores) sem experiência financeira e conhecimentos especializados, a favor de empresas (em muitos casos estabelecidas em jurisdições de alto risco) com motivos para pagamentos relacionados com investimentos e produtos financeiros.
- Contrapartes não condizentes com o nome da firma/empresa da conta podem ser utilizadas para o movimento de grandes montantes a nível internacional (por exemplo, a empresa declarada como uma empresa de mobiliário efetuou múltiplas transferências importantes para uma empresa designada como empresa de comércio de petróleo).
- Transações realizadas com desfasamento com o fuso horário do dispositivo.

Suspeita relativamente ao perfil do titular da conta

- O titular da conta não está disposto ou não está em condições de passar nas verificações de CDD [procedimentos de vigilância da clientela].
- O titular da conta não está familiarizado com a origem dos fundos que transitam pela sua conta, ou refere estar a fazê-lo por conta de outrem.
- Alterações frequentes dos nomes das pessoas coletivas/empresas em nome individual utilizando expressões e terminologia estrangeiras.
- O cliente demonstra ter conhecimentos inadequados sobre a natureza, o objeto, o montante ou a finalidade da(s) transação(ões) ou relacionamento, ou fornece explicações irrealistas, confusas ou incoerentes, que levam a suspeitar que o cliente está a agir como "mula de dinheiro".

Suspeita na identidade do utilizador da conta

- O utilizador tenta ocultar a sua identidade utilizando uma identificação partilhada, falsificada, furtada ou alterada (endereço, número de telefone, correio eletrónico).
- Alterações frequentes dos dados de contacto, números de telefone e endereços de correio eletrónico após a abertura da conta.
- Endereços de correio eletrónico que não parecem compatíveis com o nome do titular da conta ou um padrão de endereços eletrónicos semelhantes observados em várias contas.
- Irregularidades nos dados relativos ao perfil do cliente, tais como credenciais partilhadas (partilhadas, por exemplo, por dois ou mais utilizadores) com outras contas.
- Anomalias identificadas através do comportamento online, tais como hesitação na introdução de dados, demora na digitação, sinais de automatização, múltiplas tentativas falhadas de início de sessão, etc.
- Contas relativas a entidades que seria de esperar já não estarem ativas na jurisdição (por exemplo, conta de estudantes estrangeiros passada a outros quando terminados os estudos).
- Endereços IP ou coordenadas GPS provenientes de jurisdições de alto risco de branqueamento de capitais.
- Utilização de VPNs, dispositivos comprometidos (como os dispositivos IOT – *Internet Of Things*) e empresas de alojamento virtual que possam ocultar o endereço IP de um utilizador.
- Vários endereços IP ou dispositivos eletrónicos associados a uma única conta online.
- Endereço IP estático único ou dispositivo eletrónico associado a várias contas de vários titulares de contas.
- Acesso remoto a uma conta através de "portas de computador" usadas por aplicações como o *TeamViewer,* etc., o que impede a visualização do verdadeiro dispositivo e localização.
- Contas acedidas num teclado excessivamente rápido ou navegação que sugere um possível *control bot.*

Informações adversas sobre o titular da conta

- Existência de notícias negativas relevantes e verificáveis sobre clientes ou contrapartes, por exemplo, conta detida por uma vítima anterior, conhecida ou presumida, de burla, "mula de dinheiro" ou aquisição de identidade.
- Comunicação de fraude ou pedido de devolução proveniente de uma instituição correspondente, ou de outras bases de dados, relativas a fraude de terceiros.
- Presença de pedidos de devolução de transferências eletrónicas.
- Presença de informações adversas fornecidas pelas UIF ou pelas autoridades de polícia sobre as pessoas envolvidas numa transação.

Transações com ativos virtuais

- Envio/receção de grandes volumes de ativos virtuais ou de baixos valores, com elevada frequência, para endereços de carteiras não alojadas ou endereços associados a mercados na *darknet*, plataformas de material referente a abusos sexuais de crianças, mercados de *cyber exploit*, grupos de *ransomware*, serviços de *mixing/tumbling*, jurisdições de alto risco, sites de jogo e autores de fraudes.
- Limites diários de financiamento excedidos em caixas eletrónicos de Bitcoin.
- Ausência de documentos comprovativos da origem dos ativos virtuais ou do dinheiro convertido em criptoativos.
- Transferências de ativos virtuais para carteiras relacionadas com atividades ilegais na *dark web* (por exemplo, terrorismo, pornografia infantil, estupefacientes, etc.).
- Transações que envolvam mais do que um tipo de ativos virtuais, em especial as que asseguram um maior anonimato.
- Atividade transacional anormal com ativos virtuais de carteiras associadas à plataforma *peer-to-peer* sem uma explicação comercial lógica.

Outros

- Incompatibilidade entre o número de conta e o nome do titular da conta.
- O utilizador é visto ao telefone ou acompanhado por alguém através do circuito fechado de televisão (CCTV) e está a receber instruções ou a ser orientado durante a transação.
- Empresas beneficiárias que gerem sítios na Internet prestando serviços de comércio/investimento, em muitos casos não autorizados ou listados pela autoridade supervisora nacional.

Anexo B: Aproveitamento das sinergias entre os controlos de combate à fraude e ao BC/FT

O presente anexo compila alguns bons exemplos da forma como os reguladores financeiros adotaram requisitos antifraude juntamente com os controlos ABC/CFT, alguns dos quais visando a capacidade de registo, acesso e controlo remotos de contas "mula de dinheiro" por parte dos criminosos.

Tais exemplos incluem medidas variáveis relacionadas com a verificação dos clientes e a monitorização das transações.

Estes controlos poderão ser úteis às IF, VASPs e outras instituições financeiras e de pagamento.

- Implementação de processos rigorosos de *Know-Your-Customer* (KYC) ou *Know-Your-Business*, características biométricas durante o processo de integração digital, etc., e identificação de um dispositivo móvel ou seguro para autenticar transações bancárias online (outros dispositivos estarão bloqueados ou sujeitos a medidas reforçadas de redução dos riscos).
- Definição de um período de carência para a primeira inscrição nos serviços bancários online ou de dispositivos seguros (ou seja, o conjunto completo de serviços bancários não estará imediatamente disponível no momento da abertura), limitando o número ou o valor das transações financeiras do cliente.
- Identificação de um leque de transações expectáveis (número de transações, montantes, tipos de contrapartes, países envolvidos) para auxiliar na deteção de transações suspeitas, bem como reforçar as regras de identificação de fraudes e desencadear o bloqueio preventivo de transações ilícitas.
- Utilização de serviços de «verificação do beneficiário», que permitem ao ordenante/pagador/devedor de uma ordem de transferência verificar se o beneficiário/aquele que recebe um pagamento/credor mencionado nas mensagens de pagamento corresponde ao nome do titular da conta.
- Limitação quanto à realização de comunicações por correio eletrónico e redes sociais com os clientes apenas a informações gerais, indicando explicitamente que não deve ser trocada qualquer identificação ou dados pessoais com a IF/VASPs por correio eletrónico.
- Implementação de software de reconhecimento de voz e suporte de inteligência artificial na comunicação com os clientes, a fim de garantir a sua verdadeira identidade.
- Definição de mecanismos de autenticação multifator para a verificação dos clientes e para a realização de transações financeiras, adicionando ou ativando os beneficiários utilizando diferentes canais.
- Autenticação da identidade do utilizador durante a configuração remota e impedir que os criminosos obtenham acesso a múltiplas contas, utilizando informações sobre "contas-mula" ou contas de vítimas através:

- Do reforço da fiabilidade do processo de identificação de clientes por recurso a provas de vida (ou seja, garantir a existência de um ser humano vivo e genuíno), nomeadamente se um indivíduo está a ser objeto de engenharia social durante as verificações; ou
- Da Monitorização dos endereços IP utilizados para conexão com sites bancários online etc., incluindo a deteção da utilização de instrumentos de acesso remoto e do ataque *Man-in-the-Browser*.

- Alargamento dos tipos de dados que as entidades recolhem e analisam sobre os clientes, incluindo, por exemplo, números de telemóvel, endereços IP, coordenadas GPS, identificação do dispositivo, etc. Para efeitos de prevenção da fraude, as IF podem repetir essa identificação utilizando uma abordagem baseada no risco (por exemplo, realizar estes controlos quando são detetados comportamentos anómalos).
- Implementação de um sistema de monitorização das transações em tempo real baseado no risco, a fim de assegurar que qualquer atividade anormal possa ser rapidamente detetada, investigada e, se for caso disso, comunicada através do envio de uma comunicação de operações suspeitas. A sofisticação do sistema de monitorização deve ser proporcional ao volume e à natureza das transações tratadas pela IF.

www.egmontgroup.org | www.interpol.int | www.fatf-gafi.org

Novembero 2023

Fluxos Financeiros Ilícitos Provenientes de Fraude por Meio Informático

O presente relatório analisa os métodos utilizados nos crimes com recurso a meios informáticos, as suas ligações a outros crimes e a forma como os seus autores poderão explorar as vulnerabilidades das novas tecnologias. Destaca ainda exemplos de respostas operacionais e estratégias nacionais que tiveram êxito na luta contra o crime com recurso a meios informáticos. O relatório identifica igualmente indicadores de risco e requisitos e controlos antifraude que podem ser úteis às entidades dos setores público e privado na deteção e prevenção do crime com recurso a meios informáticos, bem como do branqueamento de capitais conexo.