Rahapesu Andmebüroo

Virtuaalvääringute abil sanktsioonidest kõrvalehoidmine

24.05.2023

Lühikokkuvõte

Virtuaalvääringute abil sanktsioonidest kõrvalehoidmiseks kasutatakse kolme üldist tüpoloogiat, milleks on **otsene ehk *peer-to-peer*-mudel**, **vahendaja-mudel** ja **tingdeponeerimise mudel**. Ülevaates kirjeldatakse mainitud kolme mudelit ning tuuakse välja indikaatorid, mis viitavad sanktsioonidest kõrvalehoidmise kõrgendatud riskile. Sanktsioonidest kõrvalehoidmise riskiindikaatorid on valitud nii Eesti kui ka rahvusvahelise praktika põhjal. Ülevaate lõpus on toodud olulisemad tegurid vastavuskontrolli tagamiseks, mis aitavad riske maandada.

Sanktsioonidest kõrvalehoidmise tüpoloogiad

Otsene ehk *peer-to-peer*-mudel

Otsesed ehk *peer-to-peer* virtuaalvääringute tehingud eri osapoolte vahel on kõige vahetum viis vahendeid lihtsal viisil liigutada (joonis 1). Ehkki otsesed kanded krüptovara-aadresside vahel on idee poolest kõige lihtsakoelisem meetod, on see samas piisav võimaldamaks diskreetset äritegevust. Sellest tulenevalt on *peer-to-peer* mudel ka üks enim kasutatavaid sanktsioonidest kõrvalehoidmise meetodeid, eriti ühekordsete tehingute tegemiseks mistahes summade puhul.

Joonis 1. Otsene ehk *peer-to-peer*-mudel

Vahendaja-mudel

Vahendaja-mudel on keerukam virtuaalvääringuga kauplemise süsteem, milles krüptovarasid ostetakse, varjatakse, investeeritakse, kaubeldakse ja müüakse kindla ärikontaktide võrgustiku kaudu, kus on teiste seas esindatud näiteks nii ettevõtjad, virtuaalvääringu teenuse platvormid kui ka ettevõtted, mis vahel on riigiosalusega.

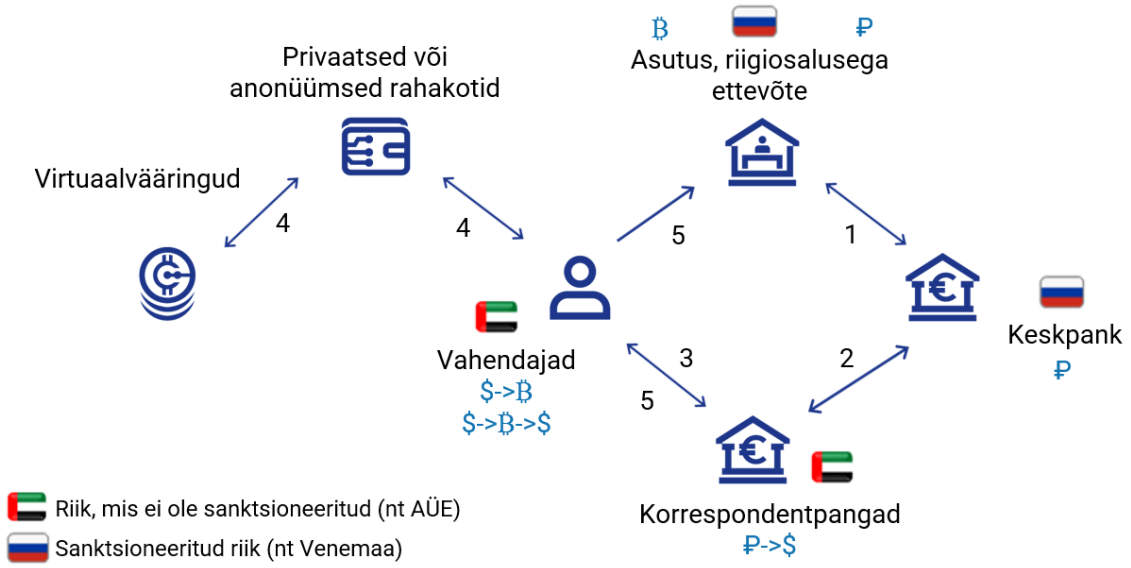
Vahendaja-mudeli üheks kõige olulisemaks komponendiks on usaldusväärne partner, kes on valmis sanktsioonidest kõrvalehoidmisele kaasa aitama. Selliseks partneriks võib olla näiteks mõni riik väljaspool Euroopa Liitu, kus Venemaa-vastaseid sanktsioone ei järgita. Niisugust käitumismustrit oli näha, kui vahetult pärast Venemaa agressiooni algust liikusid miljardite dollarite suurused virtuaalvääringu portfellid Euroopa Liidust ja teistest Venemaale sanktsioone kehtestanud jurisdiktsioonidest välja kolmandatesse riikidesse. Näiteks olid Araabia Ühendemiraatide (AÜE) virtuaalvääringu teenuse pakkujad ühed esimesed Venemaa ja Valgevene kodanike virtuaalvarade portfellide vastuvõtjad ja ümberpaigutajad.

Vahendaja-mudel koosneb mitmest vahendajate kihist, mille kaudu liigutatakse märkimisväärselt suuri summasid Venemaaga seotud rahalisi vahendeid ja virtuaalvääringut. Mudeli esimeseks lüliks on sanktsioonide all olev riik, käesoleval juhul Venemaa, kus riigil endal ning riigi osalusega ettevõtetel või riigiga seotud isikutel on arvestaval määral varasid kohalikus väärингus ehk rublades. Venemaaga seotud pankadele või keskpangale antakse järgmise sammuna korraldus edastada rahalised vahendid sanktsioone mittejärgivate ja Venemaa-sõbralike riikide (nt AÜE) korrespondentpankadele (joonis 2).

Korrespondentpank vahetab sanktsioneeritava riigi kohaliku vääringu näiteks USA dollaritesse või eurodesse ning edastab need vahendid omakorda kolmandates riikides asuvatele

vahendajatele, st isikutele, kes tegutsevad mainekates või madala profiiliga ettevõtetes. Taoline vahendajate kiht muudab raha virtuaalvääringuks ja liigutab seda mitme krüptovara-aadressi kaudu, et varjata rahaliste vahendite tegelikku päritolu ja tagada anonüümsus. Seejärel konverteeritakse virtuaalvääring taaskord tavavaluutaks (nt USA dollar) ja tagastatakse korrespondentpankade kaudu sanktsioonide all oleva riigi panka või jäetakse muudel eesmärkidel kasutamiseks osaliselt virtuaalvääringusse (nt tehingute tegemiseks ja kauplemiseks või suunatakse riigiga seotud krüptovara-aadressidele edasisteks investeeringuteks).

Vahendaja-mudel võimaldab riikide tasemel kaubanduse korraldamist ning suuremate summadega tehingute tegemist. Taolist mudelit on riiklikul tasemel eriti aktiivselt praktiseerinud Põhja-Korea.



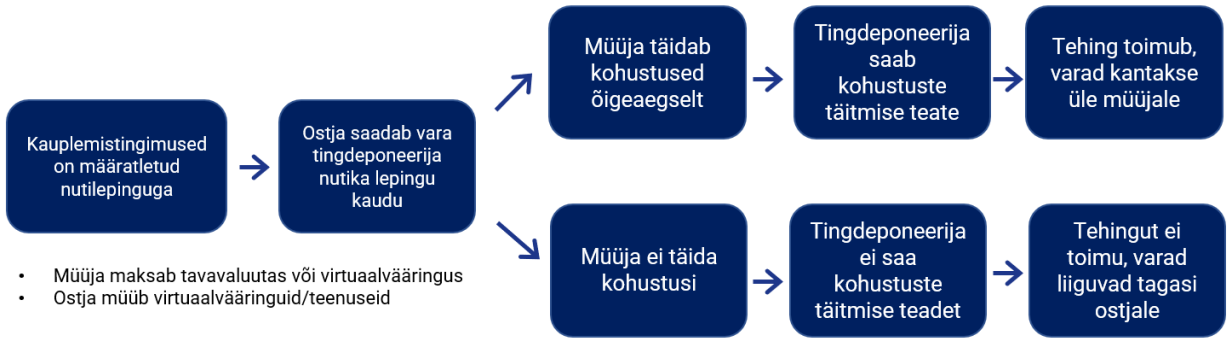
Joonis 2. Vahendaja-mudel

Tingdeponeerimise mudel

Tingdeponeerimise mudelit võib vaadelda kui vahendaja-mudeli automatiseeritud, anonüümsemat ja väiksemamahulist varianti. Tingdeponeerimise näol on tegu turukeskkonnaga, mis sobitab automaatselt kokku anonüümsed ostjad ja müüjad. Turul toimuvaid tehinguid korraldab tingdeponeerimise süsteemi vahendaja, kes tagab kauplemise turvalisuse (joonis 3).

Kauplemise tingimused on määratletud eelnevalt programmeeritud stsenaariumis (*coded script*) või nutilepinguga (*smart contract*). Taoline kaupade ja teenustega kauplemine on automatiseeritud – tehing toimub, kui ostja ja müüja täidavad tinghoiusüsteemi määratletud tingimused. Juhul kui üks osapooltest või kumbki osapool etteantud tingimusi ei täida, liiguvad tehinguks deponeeritud vahendid ostjale ja müüjale tagasi ning tehing jääb toimumata.

Taolist tingdeponeerimise süsteemi on kinnisvaratehingute teenuse pakkumisel kasutanud aktiivselt Venemaal tegutsev Sberbank. Süsteemi saab edukalt kasutada aga ka paljude teiste kaupade ja teenuste vahetamisel virtuaalvääringute vastu. Siiski sõltub selliste tehingute edukus tingdeponeerimise teenust pakkuvast vahendajast, kes võib samuti sanktsioonide alla sattuda või kehtestada turul olevatele müüjatele ja ostjatele reeglid vastavalt riskiisule.



Joonis 3. Tingdeponeerimise mudel

Sanktsioonist kõrvalehoidmise riskiindikaatorid

Järgnevalt on välja toodud kõige levinumad sanktsioonidest kõrvalehoidmise riskiindikaatorid, mida võib täheldada kõigi kolme eespool toodud sanktsioonidest kõrvalehoidmise mudeli juures

Kliendiportfell koosneb **ainult privaatsusmüntidest** või moodustab portfellis sisalduvate privaatsusmüntide väärtus kliendi **koguvarast suure osakaalu**.	Privaatsusmüntide aktiivne kasutamine võib viidata soovile varjata vara päritolu ja vahendite liikumist, et takistada sanktsiooninimekirja lisatud isiku tuvastamist.
Klient **ei soovi või ei suuda anda teavet** portfellis olevate või olnud **privaatsusmüntide päritolu** kohta.	Privaatsusmündid võivad pärineda sanktsiooninimekirja lisatud isikult või puudutada sanktsioneeritud kaubaga seotud tehinguid.
Klient esitab **konto avamisel ebatäpset või mittetäielikku teavet**. Klient ei reageeri päringutele või **keeldub uuendamast** klienditundmise põhimõtte meetmete rakendamiseks vajalikku infot.	Isikutuvastust võimaldava teabe kogumine aitab välistada võimalust, et kliendi näol on tegemist sanktsiooninimekirja lisatud isikuga, teabe andmisest keeldumine viitab katsele identiteeti varjata.
Klient ei reageeri virtuaalvääringu teenuse pakkuja esitatud päringule või **keeldub** andmast täiendavat infot **kontol toimunud tehingute kohta**.	Soov varjata tehingu asjaolusid võib viidata, et tehingu osapool on lisatud sanktsiooninimekirja või võib tehing olla seotud sanktsioneeritud kaubaga.

Krüptovara-aadressid on toodud ära olulistes **kontrollnimekirjades**, näiteks USA rahandusministeeriumi välisvarade kontrolli ameti (OFAC) nimekirjas või õiguskaitsealases teabes.	Nn mustas nimekirjas olevad aadressid on suurema tõenäosusega seotud sanktsiooninimekirja lisatud isikutega. Sanktsiooni kohaldamine OFACi nimekirja lisatud isikute suhtes ei ole Eestis seadusest tulenev kohustus, kuid nimekirja lisatud osapooled on kõrgema riskiga ning neil võib olla otsene seos ka ELi sanktsioneeritud osapooltega.
Virtuaalvääringu teenuse platvormile registreerub **lühikese ajaperioodi** mitu klienti, kasutades **sama aadressi, mobiilseadet, telefoninumbrit, IP-aadressi** vm.	Sanktsiooninimekirja lisatud isik või ettevõte võib luua samast asukohast eri kontosid ja liigutada väiksemate summade kaupa mitme kasutaja kaudu rahalisi vahendeid, et identiteeti varjata.
Klient üritab **logida** virtuaalvääringu teenuse platvormile, kasutades selleks **IP-aadressi** või **VPNi**, mis on seotud **sanktsioneeritud jurisdiktsiooniga**.	Sanktsioneeritud jurisdiktsioonist oma kontole logimine ja VPNi kasutamine viitavad sanktsioonidest kõrvalehoidmise või rikkumise kõrgendatud riskile.
Virtuaalvääringu teenuse platvorm saab **teistelt teenusepakkujatelt kliendi vahendite** kohta **ebatavalisi või tihedaid päringuid**.	Taolised päringud viitavad kliendi kõrgemale riskitasemele, klient või tema omanduses olev virtuaalvääring võib olla seotud sanktsioonidega.
Ülekanded mitmele aadressile. Tehingute eesmärk näib olevat varjata vara päritolu või vahendite plaanitud kasutust.	Sanktsiooninimekirja lisatud isik võib tahtlikult üritada vara päritolu varjata ning raskendada vahendite liikumise jälgimist plokiahelas.
Kliendi tehingud toimuvad **samal kellaajal**. Tehakse ülekanded, vahetades tavavaluutat virtuaalvääringuks ning seejärel virtuaalvääringut tagasi tavavaluutasse.	Selline tehingute tegemise muster viitab, et klient kasutab läbimõeldud meetodit, mille eesmärk võib olla varjata vara päritolu ja raskendada vahendite liikumise jälgimist plokiahelas.
Klient saab virtuaalvääringuid börsiväliselt aadressilt, tehes kohe laekumise järel mitu kiiret tehingut eri virtuaalvääringute vahel (vahetades ühte virtuaalvääringu teiseks), millele järgneb tehing, kus vahendid kantakse virtuaalvääringu teenuse platvormilt edasi mõnele teisele aadressile.	Taoline tegevus võib viidata sanktsiooninimekirja lisatud isiku katsele püüda varjata vara päritolu ja raskendada vahendite liikumise jälgimist plokiahelas. Lihtsamad plokiahelaanalüüsi tarkvarad tuvastavad konkreetse virtuaalvääringuga aset leidnud tehingutest keskmiselt vaid neli viimasena aset leidnud tehingut või toimingut.

Suur ülekannete maht ja sagedased tehingud eri tüüpi virtuaalvääringute vahel.	Suuremate summade liigutamine viitab kõrgemale sanktsioonidest kõrvalehoidmise ohule, kannete tegemine eri virtuaalvääringutes võib aga viidata püüdele varjata vara päritolu ja raskendada vahendite liikumise jälgimist plokiahelas.
Klient annab virtuaalvääringu teenuse platvormile kasutajakonto registreerimisel **anonüümse e-posti aadressi**, mis pärineb **krüpteeritud meiliteenusest**.	Krüpteeritud e-posti aadressi kasutamine on tavaklientide hulgas ebatavaline ning viitab kliendi soovile jääda anonüümseks, millest tulenevalt on ka kõrgem sanktsioonidest kõrvalehoidmise oht.
Raha või virtuaalvääringut liigutatakse (lisatakse või võetakse välja) aadressile, mille juures on plokiahela analüüsi käigus tuvastatud otsesed või kaudsed seosed kahtlaste allikatega, sealhulgas näiteks **tumeveeb**, ***mixing/tumbling*-teenused** ja **lunaraha/küberkuritegevus**.	Krüptovara-aadressi seos nimetatud kahtlaste allikatega suurendab riski, et tehingute taga võib olla sanktsiooninimekirja lisatud ettevõte või isik, kes kasutab kahtlasi allikaid oma tegevuse ja identiteedi varjamiseks.
Enne kliendi aadressini jõudmist või vahetult **pärast** sealt **vahendite väljavõtmist** liigub virtuaalvääring väga **lühikese aja jooksul** läbi suure hulga eri aadresside.	Virtuaalvääringu kiire liigutamine paljude aadresside kaudu muudab rahaliste vara päritolu tuvastamise keerulisemaks. Taoliste tehingute taga olla sanktsiooninimekirja lisatud isik, kes soovib identiteeti varjata.
Virtuaalvääring läbib ***mixing/tumbling*-teenuseid** ja see kantakse üle mitmele aadressi, kus virtuaalvääring vahetatakse tavavaluutaks.	Taoliste teenuste kasutamine viitab soovile vahendite päritolu varjata ning raskendada vahendite liikumise jälgimist plokiahelas.
Virtuaalvääring pärineb börsiväliselt virtuaalvääringu teenuse pakkujalt, mis reklaamib teenuseid privaatse ja anonüümsena.	Sanktsioonidest kõrvalehoidmise eesmärgil valitakse suurema tõenäosusega vahendajaks anonüümsusele orienteeritud teenusepakkuja.
Krüptovara-aadressi on mainitud **ühisrahastusplatvormil või sotsiaalmeedias** seonduvalt üleskutsega **toetada Venemaa sõjategevust** või mõnda **muud sanktsioonide** all olevat riiki.	Seos taoliste veebilehtedega on üks selgemaid viiteid sanktsioonide rikkumisele. Enamikul juhtudel on osalisteks eraisikud, kes toetavad otseselt Venemaa sõjategevust Ukrainas.

Virtuaalvääringu ostmiseks kasutatud **vara päritolu pole teada**.	Info puudumine vara päritolu kohta tõstab oluliselt sanktsioonidest kõrvalehoidmise riski, eriti juhul, kui tegemist on ka kõrge rahalise väärtusega tehinguga.
Kliendile tuleb sageli **ülekandeid mitmelt maksevahendajatelt**, mis asuvad kõrge riskiga jurisdiktsiooniks ja/või mille **klienditundmise põhimõtte meetmed** ja **isikutuvastuse protseduurid** võivad olla keskmisest **nõrgemad.** Klient kasutab **ülekannete tegemisel** selliseid maksevahendajaid.	Sanktsiooninimekirja lisatud isikud kasutavad virtuaalvääringu teenuse pakkujale sissemakse tegemiseks eelistatult maksevahendajaid, kuna nende klienditundmise põhimõtte meetmed on võrreldes traditsiooniliste pankadega reeglina oluliselt leebemad.
Kliendi tehingud algatatakse või saadetakse **IP-aadressidelt**, mis viitavad asukohale **Venemaal, Valgevenes** ja rahapesuvastase töökonna (**FATF**, *Financial Action Task Force*) mõistes **puudulike meetmetega jurisdiktsioonis**, sanktsioneeritud jurisdiktsioonis. Samuti võib olla tegu kahtlaseks märgitud IP-aadressiga.	Nimetatud jurisdiktsioonidest pärinevad tehingud on kõrgema riskiga ning suurema tõenäosusega seotud sanktsioonidest kõrvalehoidmise ja nende rikkumisega.

Lisaks eespool toodud riskiindikaatoritele tuleks virtuaalvääringu teenuse pakkujatel kindlasti pöörata tähelepanu ka viimastel aastatel üha aktuaalsemaks muutunud **Põhja-Korea küberkuritegevusest tulenevatele ohtudele**. ÜRO raporti kohaselt oli Põhja-Korea küberkuritegevuse teel tekitatud kahju 2022. aastal rekordiline, täpsemalt sai riik küberkuritegevuse tulemusena virtuaalvääringuid ligi nelja miljardi dollari väärtuses. On teada, et Põhja-Korea kasutab küberkuritegevuse teel saadud vahendeid tuumaprogrammi rahastamiseks. Sageli kasutavad Põhja-Korea häkkerid ära just virtuaalvääringu teenust pakkuvate platvormide turvanõrkusi, valides sihtmärgiks teenusepakkujaid, kes ei rakenda klientide vara hoiustamiseks asjakohaseid turvameetmeid.

Olulisemad tegurid tõhusa vastavuskontrolli tagamiseks

Juhtkonna toetus vastavuskontrolli süsteemile

Juhtkonna pühendumus sanktsioonide järgimisele on vastavuskontrolli süsteemi eduka toimimise üks olulisemaid tegureid. Juhtkonna toetus on tähtis, kuna aitab tagada, et sanktsioonide järgimise süsteem saaks piisavalt ressursse ja oleks integreeritud ettevõtte igapäevategevusse piisaval määral. Juhtkonna avalik toetus soodustab vastavuskontrolli süsteemi kasutamist, motiveerib sanktsioonide järgimisega tegelevat personali ning edendab vastavuskontrolli kultuuri kogu organisatsioonis.

Süsteemi katsetamine ja auditeerimine

Tagamaks sanktsioonide vastavuskontrolli süsteemi töökindluse ja tõhususe tuleb regulaarselt süsteemi testida. Selle jaoks tuleks kasutada laiapõhist ja objektiivset testimis-

või auditeerimisviisi, mis annaks hinnangu süsteemi toimimise kohta: millised aspektid vajavad parandamist, võttes arvesse pidevalt muutuvat riskitaset ja sanktsioonikeskkonda.

Olenevalt ettevõtte suurusest ja tegevusala keerukusest tuleb auditeerida sanktsioonide vastavussüsteemi nõuetelevastavust kas organisatsioonisiseselt või kaasates auditeerimisprotsessi välised audiitorid.

Riskianalüüs ja sisemised protseduurireeglid

Tahtmatu äritegevuse eest sanktsiooninimekirja lisatud isikutega aitavad pakkuda kaitset riskianalüüs ja sisemised protseduurireeglid, mis tagavad tegevuse vastavuse seaduses sätestatud tingimustele. Riskianalüüs peab olema kohandatud konkreetsele ettevõttele, võttes arvesse kliendibaasi, partnereid, tooteid ja teenuseid, tarneahelat, tegutsemispiirkonda ning otseseid ja kaudseid puutepunkte teiste jurisdiktsioonide ja potentsiaalsete sanktsioneeritud isikutega. Riskide hindamisel võib olla vajalik hinnata, kas tehingupartneritel on piisavad vastavuskontrollimehhanismid.

Sisemised protseduurireeglid peavad lähtuma riskianalüüsist. Tõhusad protseduurireeglid aitavad kohaldada hoolsusmeetmeid ning tuvastada potentsiaalsed riskile viitavad tegurid. Sisemised protseduurireeglid hõlmavad tihtipeale valdkonnapõhiste tööriistade kasutamist, sh tehingute sõelumisel, seirel ja edasisel uurimisel. Klienditundmise põhimõtte meetmeid tuleb rakendada nii kliendisuhte alguses kui ka kogu äritegevuse vältel tuvastamaks isikud, kes võivad üritada varjata vara päritolu, omanikke või tegelikke kasusaajaid.

Töötajate koolitamine

Sanktsiooniteemaline koolitusprogramm töötajatele on ettevõtte sanktsioonide vastavussüsteemi toimimise seiskohast üks olulisemaid komponente, millega on võimalik tagada õigeaegne sanktsioonirikkumise tuvastamine. Organisatsioonisisese koolitusprogrammi sisu ja ulatus määrateletakse lähtuvalt konkreetse ettevõtte suurusest, selle tegevuse keerukusest ja riskianalüüsist. Koolitusprogramm peab vastama ettevõtte eripäradele ehk arvestama pakutavate toodete, teenuste, klientide, partnerite ja tegutsemispiirkonnaga ning olemas kooskõlas proportsionaalsuse põhimõttega. Hästi väljatöötatud koolitusprogramm arvestab konkreetse ametikoha vajadusi. Niisugune koolitus tagab, et ettevõtte töötajad oleksid kursis sanktsioonide kohaldamise konkreetse vastutusalaga ning et ettevõte tervikuna suudaks tagada sanktsioonide efektiivse järgimise.

Allikad

FINTRAC, Money laundering and terrorist financing indicators — Virtual currency transactions, June 2021, https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/indicators-indicateurs/vc_mltf-eng#s1

FinCen, FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts), March 7, 2022, https://www.fincen.gov/news/news-releases/fincen-advises-increased-vigilance-potential-russian-sanctions-evasion-attempts

OFAC, Sanctions compliance guidance for the virtual currency industry, October 2021, https://ofac.treasury.gov/media/913571/download?inline

SUERF, Is it easy to hide money in the crypto economy? The case of Russia, SUERF Policy Brief, No 506, Jan 2023, https://www.suerf.org/suer-policy-brief/59935/is-it-easy-to-hide-money-in-the-crypto-economy-the-case-of-russia

United Nations, Panel of Experts established pursuant to Security Council resolution 1874, June 2022, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/N2225209.pdf