Rahapesu Andmebüroo tagasiside virtuaalvääringu teenuse pakkujatele

Riskikeskkond

2022. aastal oli jätkuvalt siseriiklikust kuritegevusest saadud tulu, mida on võimalik pesta, kordades väiksem, kui piiriülesest kuritegevusest saadud tulu rahapesemise oht läbi Eesti. Rahapesu Andmebüroole (RAB) laekunud ja analüüsitud info osutab, et **piiriülese rahapesu oht** on Eestis riigisisesega võrreldes märksa kõrgem ning Eesti on jätkuvalt rahapesu mõttes **transiitriik**. Eestis toimub välisriikides saadud **kriminaaltulu kihistamine** *(layering)*. 2022. aastal RABile saadetud välispäringutes on sarnaselt 2021. aastaga enamlevinud seoseks Eestiga siin avatud **kontod**, Eestis asuv **vara** või Eestis asutatud **juriidiline isik**.

Kõige haavatavamad on rahapesu ja terrorismi rahastamise vaatest jätkuvalt **pangandussektor** ja **virtuaalvääringu teenuse pakkujad** (VASPid). Eesti tegevusloaga VASPide arv on viimastel aastatel riigi kasutatud meetmete tõttu vähenenud ja hoolsusmeetmete kohaldamise kvaliteet tõusnud, kuid risk on jätkuvalt olemas ning oluline.

Endiselt on välispäringute ja teadete alusel levinuim rahapesu tüpoloogia mitmesugustest **kelmustest saadud tulu kandmine Eesti krediidiasutuse respondentkliendist välisriigi makseteenuse või virtuaalvääringuteenuse pakkuja kontole**, kust raha suunatakse koheselt edasi vastava teenusepakkuja platvormile. RABile saadeti 2022. aastal enam kui kaks korda vähem kelmuseteateid, kui aastal 2021, mis annab alust arvata, et selliste Eestiga seotud juhtumite arv eelneva aastaga võrreldes vähenes. Samas suurenes RABile esitatud **virtuaalvääringute** ja **sularahaga** seotud teadete arv. Eesti tegevusloaga virtuaalvääringu teenuse pakkujate riskid on jätkuvalt kõrged, kuid RABi prognoos, et nendega seotud välispäringute ja teadete arv kasvavad väga kiiresti, ei ole realiseerunud, suurt muutust võrreldes 2021. aastaga ei toimunud. Samas seostatakse osasid Eesti tegevusloa kaotanud VASPisid jätkuvalt Eestiga, mis tähendab jätkuvat mainekahju nende reeglitele mittevastava tegevuse Eestiga seostamise tõttu. RAB töötab jätkuvalt selle nimel, et neid riske maandada.

Rahapesu ja sanktsioonidest kõrvalehoidmise vaates kätkeb käimasolev Vene-Ukraina sõda Eesti jaoks eeskätt ohtu, et **Vene oligarhid ja kleptokraadid** püüavad kasutada Eesti finantssüsteemi ja juriidilisi isikuid sanktsioonidest kõrvalehoidmiseks, kasutades traditsioonilisi rahapesuvõtteid nagu peitumine **keerukate juriidiliste struktuuride** taha ning **vara paigutamine sularahasse, kulda või kõrge väärtusega kaupadesse.**

Terrorismi rahastamise vaatest on Eestis endiselt kõrgeim risk **edastamise** faasis. Terroristlikul eesmärgil vahendite **kogumise** ja **kasutamise** risk on madal. Siiski mängivad üha enam keskset rolli ühisrahastusplatvormid, mille puhul puudub selge ülevaade nii lõppkasutajast kui kogutud vahendite tegelikust kasutusviisist. Seonduvalt vahendite **edastamisega,** torkab kõrge riskiga silma VASPide sektor, mistõttu on RAB tunnistanud teenusepakkujate tegevuslubasid kehtetuks ning tegelenud põhjaliku teavitustööga. Kõikidest VASPidest esitab terrorismi rahastamisele viitavaid teateid siiski vaid väga väike osa turuosalistest, üksikud turuosalised. Arvestades klientide arvu ja tehingute mahtu riskiriikidega, peaks teavitamisaktiivsus olema suurem. See osutab, et teenusepakkujatel puuduvad piisavad monitooringumehhanismid, et tuvastada terrorismi rahastamisele viitavaid

ohumärke. RAB palub kõigil turuosalistel pöörata tähelepanu ebaharilikele tehingutele isikutega, kel on seos kõrgema terrorismi rahastamise riskiga riikidega.

Euroopa Komisjoni 2022. aastal valminud Euroopa Liidu ülese riskihinnangu (*Supra-National Risk Assessment*, SNRA[1]) kohaselt on **VASPide puhul nii rahapesu kui ka terrorismi rahastamise risk väga kõrge**. Virtuaalvääringu teenuse pakkujate sektoris on riskid järk-järgult suurenenud, sest kasvanud on nii klientide ja tehingute arv kui pakutavate toodete ja teenuste hulk. Peamisteks probleemideks on pakutavate toodete/teenuste puhul vähene hoolsusmeetmete kohaldamine, vastavuskontrolli ebaküpsus ning üldine rahapesu ja terrorismi rahastamise riskidest arusaamise puudulikkus. Kõige suurem riskifaktor on tehingute läbipaistmatus ning lõppkliendi identiteedi kindlakstegemise raskused. Virtuaalvääringuid kasutatakse ära terrorismi rahastamiseks, millele aitavad kaasa virtuaalvääringu rahvusvahelisus, tehingute kiirus ning võimalik anonüümsus. Virtuaalvääringuga kaasnev terrorismi rahastamise oht on seega märkimisväärne.

Alljärgnevad on peamised tüpoloogiad[2], millele palume teenusepakkujatel tähelepanu pöörata:

- **Kokkuleppemängud/kihlveod:** virtuaalvääringuid kasutatakse veebis kihlveokontode avamiseks.
- **Korruptsioon ja altkäemaks:** vara liigutamiseks kasutatakse virtuaalvääringuid ja VASPe.
- **Rahapesu võrgustik (*ML Controlled Networks, MLCN*)** – raha vahetatakse erinevates jurisdiktsioonides, erinevates valuutades või vahendajate abil. Kasutatakse kaubanduspõhist rahapesu (*Trade Based ML, TBML*), mille käigus ei kanta raha otse üle, vaid vahetatakse sularahaks, kullaks, virtuaalvaluutaks, kaupadeks jms.
- **Laste seksuaalse ärakasutamisega** (*child sexual exploitation, CSE*) seotud veebilehed pakuvad liikmetele võimalust maksta virtuaalvääringus (peamiselt Bitcoinides).
- **Investeerimispettused.**
- **Riiklike toetuste kuritarvitamine.**
- **Kaupade tarnimata jätmise pettus:** kaupleja soovib maksed ebaharilike maksevahendite kaudu (ettemaksukaardid, rahateenused (*money service*) jne), mis ei peegelda sektori tavapärast käitumist.
- **Võltsitud kaubad:** kasutatakse ebaharilikke maksevahendeid, mh VASPide kaudu, näiteks virtuaalvääringud, ettemaksukaardid ja rahasiire.
- **Ebaseaduslik kaubavahetus:** seotud ebaseadusliku looduslike liikidega kauplemisega (*wildlife trade*), tehinguid tehakse virtuaalvääringute või rahasiirde kaudu.

Chainalysise analüüsi[3] kohaselt ligi pool virtuaalvääringute mahust, mis pärines ebaseaduslikelt aadressidelt, liikus läbi suuremate vahetusplatvormide.

Eestis toimus 2022. aastal virtuaalvääringu teenuse pakkujate sektoris korrastus ning riskide maandamine. Märtsis jõustunud seadusemuudatusega karmistati nii turule sisenemise kui ka teenuse pakkumise nõudeid. Uus regulatsioon nägi ette kõrgendatud standardid IT-süsteemidele ja juhtkonna ning AML kontaktisiku pädevusele, aga ka siseauditi vajadust ning kapitalinõuete olulist suuremist.

2022. aasta lõpus Eesti tegevusluba omavate VASPide vahendatud teenuste käive oli 2022. aastal hinnanguliselt 10 miljardit eurot. Võrreldes 2021. aastaga oli käive ligi poole võrra väiksem, mis oli valdavalt tingitud mitme suure ja kõrge riskiga teenusepakkuja tegevusloa kehtetuks tunnistamisest, aga ka üldisest virtuaalvääringute väärtuse kahanemisest. Riskide vähenemisele viitab ka asjaolu, et välisriikide huvi RABi tegevusloaga teenusepakkujate vastu on veidi vähenenud. Aasta jooksul RABile esitatud 562 välispäringust ja spontaansest

[1] SNRA täistekst ning eesti- ja ingliskeelne kokkuvõte on leitavad Rahandusministeeriumi veebilehelt: https://www.fin.ee/finantspoliitika-valissuhted/rahapesu-ja-terrorismi-rahastamise-tokestamine/riskihinnangud
[2] Sama
[3] Chainalysis, https://blog.chainalysis.com/reports/crypto-money-laundering-2022/

infoedastusest (välispäringu liik) puudutas 85 virtuaalvääringu teenuse pakkujaid (15%) (2021. aastal 107 ja 16%).

Teatamiskohtuste täitmine on sektori turuosaliste poolt aasta-aastalt paranenud, kuid on jätkuvalt **ebapiisav**. Oluline osa aktiivsetest teenusepakkujatest pole RABile esitanud ühtegi teadet ja enamik teatetest on seotud kliendisuhte loomisel valeandmete esitamisega, mis näitab, et ärisuhete jälgimine on puudulik.

Vaatamata olulistele sammudele paremuse poole, pole VASPide sektori riskid veel ammendavalt maandatud. RAB analüüsis 2022. aastal teenusepakkujate (käibe alusel) suurimaid kliente ning tuvastas riskiriikide kliente ja nii rahapesu kui ka terrorismi kahtlusega isikuid. Lisaks jätkuvatele rahapesu ja terrorismi rahastamise ohukohtadele kerkivad aina enam probleemina esile teenusepakkujate suutlikkus kaitsta oma klientide vara ning andmeid, seda nii väliste rünnakute kui ka omanike pahatahtlikkuse tõttu. Samuti on tõenäoline, et varasemast enam hakkame nägema teenusepakkujate pankrotistumist virtuaalvääringute hinna olulise kukkumise tõttu.

Lisaks tasub jälgida **pesastatud teenustega** (*nested services*) seotud ohte. Pesastatud teenuste, mis on sisult korrespondentsuhe, pakkumine võimendab oluliselt riske, sest ühe kliendi „konto" varjus võib olla tuhandeid ja sadu tuhandeid järgmisi kliente, kelle tuvastamine ja tehingute seire ei ole siinse teenusepakkuja võimuses.

Alates 2022. aasta märtsi algusest kogus RAB seoses Vene-Ukraina sõjaga Eesti tegevusloaga VASPidelt andmeid nende Vene, Valgevene ja Ukraina klientide ja vahendatud teenuste käibe kohta. Andmed näitasid, et Eesti tegevusloaga VASPide, nii Vene kui ka Valgevene isikute kliendibaas, jäi stabiilseks või vähenes. Samuti vähenes Vene klientidele vahendatud teenuste käive ligi 80%. Seega riski realiseerumist, et VASPe kasutatakse sanktsioonidest kõrvalehoidmiseks või kanalina varade liigutamiseks, ei tuvastatud.

Ülevaade 2022. aastal saadetud teadetest

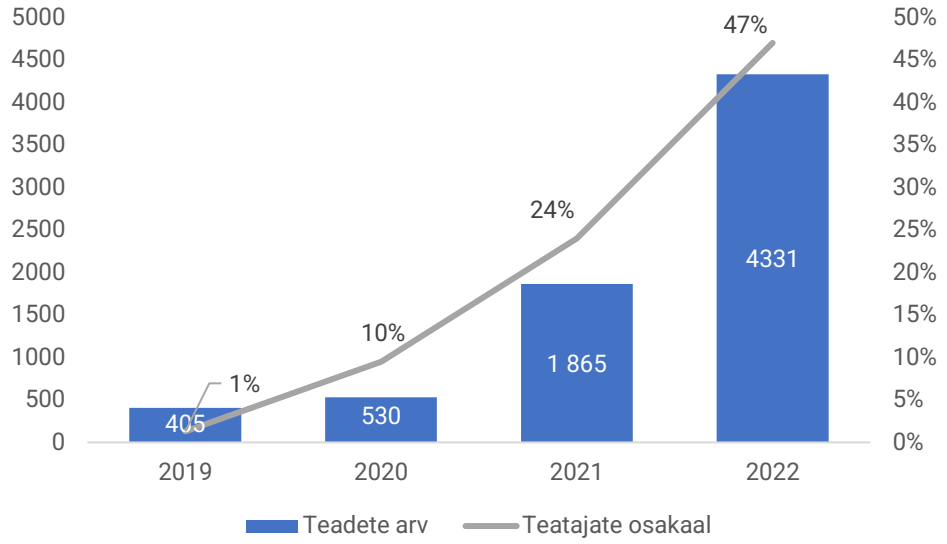
Kui 2020. aastal saatsid virtuaalvääringu teenuse pakkujad RABile 530 ja 2021. aastal 1865, siis 2022. aastal **4331** teadet, mis moodustas **29%** kõikidest teadetest (tabel 1).

Tabel 1. 2022. a RABile saadetud teadete jagunemine teataja gruppide kaupa.

Teatajagrupp	Kokku	Kokku (%)	RP	RP (%)	TFR	TFR (%)	ISR	ISR (%)	CTR	CTR (%)
Krediidiasutused	7274	*51%*	6588	*57%*	25	*8%*	657	*69%*	4	*0%*
Virtuaalvääringu teenuse pakkujad	**4331**	***30%***	**4054**	***35%***	**146**	***47%***	**112**	***12%***	**19**	***1%***
Finantseerimisasutused	1363	*10%*	400	*3%*	124	*40%*	38	*4%*	801	*58%*
Teise riigi asutused ja isikud	58	*0%*	57	*0%*		*0%*	1	*0%*		*0%*
Hasartmängukorraldajad	425	*3%*	103	*1%*		*0%*		*0%*	322	*23%*
Professionaalid	315	*2%*	139	*1%*	15	*5%*	37	*4%*	124	*9%*
Riigiasutused	148	*1%*	66	*1%*	1	*0%*	39	*4%*	42	*3%*
Muud eraõiguslikud ettevõtjad	201	*1%*	84	*1%*	1	*0%*	52	*5%*	64	*5%*
Ei ole RahaPTS kohustatud subjekt	170	*1%*	146	*1%*		*0%*	17	*2%*	7	*1%*
KOKKU	**14285**	***100%***	**11637**	***100%***	**312**	***100%***	**953**	***100%***	**1383**	***100%***

Selgitus: RP – rahapesuteade (STR, UTR ja UAR); TFR – terrorismi rahastamise teade (TFR-1 ja TFR-2); ISR – rahvusvahelise sanktsiooni kahtluse teade; CTR – sularaha teade.

2022. aastal esitas teateid **69 virtuaalvääringu teenuse pakkujat,** mis moodustas **47%** aasta lõpu seisuga tegevusluba omavatest VASPidest (joonis 1). Kuigi VASPide teatamisaktiivsus on kasvanud, esitas aasta jooksul üle 10 teate vaid **32%** VASPidest ning mitmed suurima käibega teenusepakkujad esitasid jätkuvalt vaid üksikuid teateid. Seega olgugi, et teatajate osakaal on aastate jooksul märkimisväärselt kasvanud (2021. aastal 24%), on teatajate hulk sektori riskitaset ja mahte arvestades jätkuvalt **ebapiisav**.



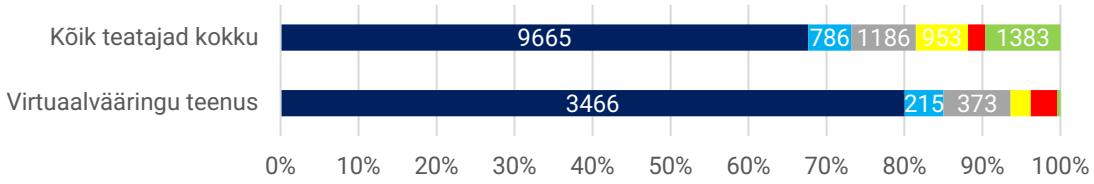
Joonis 1. Virtuaalvääringu teenuse pakkujatelt RABile 2019.–2022. aastal saadetud teadete arv ja teatajate osakaal tegevusloa omajatest.

Suurimate teatajate hulka tuleb aina rohkem virtuaalvääringu teenuse pakkujaid. Kui 2021. aastal oli teatajate esikümnes kaks VASPi, siis 2022. aastal juba viis (tabel 2).

Tabel 2. 2022. a RABle saadetud teadete esikümne jagunemine teate esitajate põhitegevusala alusel.

Teataja põhitegevusala alusel	Teateid
1. Teataja 1	4 555
2. Virtuaalvääringu teenuse pakkuja 1	**1 035**
3. Teataja 2	1 012
4. Virtuaalvääringu teenuse pakkuja 2	**996**
5. Teataja 3	867
6. Teataja 4	742
7. Virtuaalvääringu teenuse pakkuja 3	**512**
8. Teataja 5	507
9. Virtuaalvääringu teenuse pakkuja 4	**279**
10. Virtuaalvääringu teenuse pakkuja 5	**241**

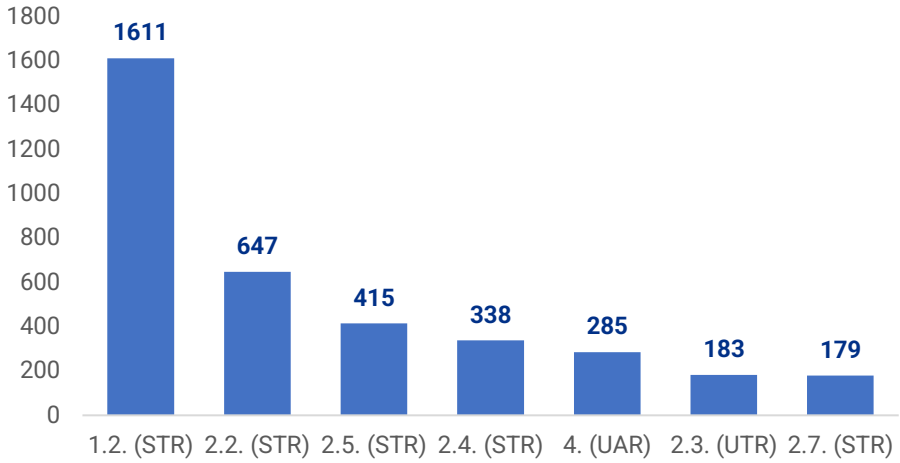
VASPid on teatajate seas olulisel kohal, eriti kuna tegemist on riskantse sektoriga ning esitatud teated võimaldavad RABil hinnata turul valitsevaid trende ning ohte. Enamik VASPide esitatud teadetest puudutas rahapesukahtlust – kahtlase tehingu teateid (**STR**) saadeti 3466, ebahariliku tegevuse teateid (**UAR**) 373 ja ebahariliku tehingu teateid (**UTR**) 215. Terrorismiga seotud teateid (**TFR**) esitati kokku 146 (joonis 2). Sanktsioonikahtlust puudutavaid teateid (**ISR**) esitati kokku 112, need olid seotud Venemaa suhtes kehtestatud sanktsioonidega. 2022. aastal laekus virtuaalvääringu teenusepakkujatelt 19 sularahateadet (**CTR**).



	Virtuaalvääringu teenus	Kõik teatajad kokku
STR	3466	9665
UTR	215	786
UAR	373	1186
ISR	112	953
TFR	146	312
CTR	19	1383

Joonis 2. Virtuaalvääringu teenuse pakkujatelt ja kõikidelt teatajatelt RABile 2022. a saadetud teadete jagunemine teate liigi kaupa.

VASPide esitatud teadete puhul võib oluliste märksõnadena tuua välja **võltsitud dokumendi, ebaselge vara päritolu, pettuse, identiteedi varguse** ja **tumeveebi**. Eelkuritegudena domineerivad kelmus ja küberkuritegevus. Sarnaselt 2021. aastaga märgiti kõige sagedamini teate saatmise põhjuseks, et esineb kahtlus isiku poolt esitatud andmete tõelevastavuses (**1.2. STR**) (joonis 3). Sageduselt järgmised põhjused isiku suhtes olid varasemalt teadaolev või hoolsusmeetmete rakendamise käigus tekkinud rahapesukahtlus (**2.2. STR**) ja isik ei esita tehingu kohta hoolsusmeetmete täitmiseks vajalikus ulatuses selgitusi või dokumente või esitatu ei ole usutav (**2.5. STR**).



Joonis 3. Virtuaalvääringu teenuse pakkujate poolt RABile 2022. a saadetud teadete enam levinud indikaatorid.

1.2. (STR)	Kahtlus isiku poolt esitatud andmete tõelevastavuses
2.2. (STR)	Isiku suhtes on varasemalt teadaolev või hoolsusmeetmete rakendamise käigus tekkinud rahapesukahtlus
2.5. (STR)	Isik ei esita tehingu kohta hoolsusmeetmete täitmiseks vajalikus ulatuses selgitusi või dokumente või esitatu ei ole usutav (RahaPTS § 42 lg 1 juhutehing ning § 43 lg 1 kliendisuhtes oleva isiku tehing)
2.4. (STR)	Rahapesukahtlus kontol tehtava tehingu korral
4. (UAR)	Ebaharilikud tehingud virtuaalvääringutega
2.3. (UTR)	Ebaharilik tehing virtuaalvääringuga
2.7. (STR)	Kahtlus, et tehingu objektiks olev vara on pettuse objekt või seda kasutatakse rahapesuks (eksiteele viidud isiku tehingud)

RAB analüüsis on teadetel oluline roll. RAB suunas 2022. aastal VASPide saadetud teadetest süvaanalüüsi **292** teadet. Lisaks siseriikliku koostööd hõlmavatele pettusekaasustele suunati 187 teadet pettuseid koondavatesse toimikutesse, kus teostati taktikalise tasandi analüüse, mille tulemusi jagati ka välisriikide õiguskaitseasutustega. Võrreldes 2021. aastaga kasvas süvaanalüüsi läinud teadete arv 284 teate võrra, peamiselt sanktsiooniteadete tõttu. RAB kasutab teadete infot lisaks juhtumianalüüsile ka oma taktikalistes ja strateegilistes analüüsides. Näiteks valmib 2023. aasta esimeses pooles sularaha uuring, mille peamiseks sisendiks on summapõhised (CTR) ja sularahaindikaatoriga rahapesuteated. Eesti uurimisasutustele edastatud materjalides kasutati **159** teates sisaldunud infot. 2022. aastal seati virtuaalvääringu teenusepakkujate teadete või välisriigi info põhjal **seitsmel** korral virtuaalvääringu teenusepakkuja kontole või kontol olevale varale käsutuspiirang, seda kolme juhtumi raames. Ühe juhtumi raames anti vara osaliselt üle ka Ameerika Ühendriikidele.

Teadete sisu, kvaliteet ja soovitused tulevikuks

VASPide teadete kvaliteet on võrreldes varasemate aastatega **tõusnud**. Näha on, et turuosalised on hakanud RABi läbiviidud infopäevadelt ja koolitustelt saadud informatsiooni rakendama. On teateid, mis on selge sisuga ning millest on näha, et kohustatud isik rakendab hoolsusmeetmeid ja esitab selgelt struktureeritud analüüsina kahtluse sisu.

VASPide teated on andnud panuse terrorismi rahastamise tõkestamisesse nii Eestis kui ka rahvusvaheliselt. Tänu sektori esitatud infole on RAB saanud teha edastusi nii uurimisasutustele Eestis kui ka välisriikide rahapesu andmebüroodele. Teateid esitanud virtuaalvääringu teenuse pakkujad on näidanud üles pigem head võimekust leida avaandmetest tehingu osapoole kohta täiendavat informatsiooni. Seega on võimalik rakendada tõhusaid meetmeid tuvastamaks kuritegevuse, rahapesu ja terrorismi rahastamise kahtlust. Virtuaalvääringu teenuse pakkujad on hakanud tehingu kirjelduse narratiivi osa struktureerima, kasutades selleks RABi soovitatud raamistikku (mis, kes, millal, kus, miks, kuidas). Struktureeritud tehingu kirjeldus aitab oluliselt kaasa tehingu kirjelduse selgusele ja põhjalikkusele.

Korrektse teate näide:

Tehingu kirjeldus: *„15.12.2022 tuvastasime, et ühe kliendi esitatud dokumendid ei olnud meie nõuetega kooskõlas. Tugevdatud hoolsusmeetmete kohaldamise käigus tuvastati järgmine teave ja punktid:*

- *ISIK 1 on x-aastane RIIGIS 1 elav inimene.*
- *ISIK 1 jagas ETH rahakotti nr WALLET 1 teise kasutajaga ISIK 2.*
- *Mõlemad kasutajad kasutasid oma elukoha kontrollimiseks sama ettevõtte (ETTEVÕTE 1) arve dokumenti, mis oli võltsitud (vt lisatud). Nende arvete summad on samad (x EUR) ja ainult nimele ja aadressile viitavad väljad on erinevad.*
- *Kasutades ülaltoodud kontodel tuvastatud sarnasusi (sama võltsitud arve; e-posti aadressi struktuur märkega "psg"; vanus), õnnestus tuvastada sama petturlik meetod järgmistel kasutajakontodel, mis registreeriti septembris-oktoobris 2022.*

/... tabel tehingute ja klientidega.../

- *Tuvastatud kasutajatega seotud petuskeem viitab suuresti rahapesu tüpoloogiale - rahamuulade kasutamine.*
- *Kasutaja peamine tehingumuster on „raha sisse ja virtuaalvääring välja“ ilma rakenduse varahaldustooteid kasutamata.*
- *Elliptic Lens (krüptoanalüütiline tööriist) ei tuvastanud riske klientide kontol.*

Kokkuvõte: Arvestades eespool nimetatud fakte ja järeldusi, otsustati sulgeda kliendi ja kõigi teiste seotud klientide kontod, mis tuvastati xx.xx.2022.“

Kommentaar: *Teate kirjeldamisel kasutatud struktuuri on hea jälgida. Teataja poolt on tuvastatud isikud, kelle käitumises märgati sarnast tegevust. Teates on väga toodud võimalik rahapesu tüpoloogia ning informatsioon kliendisuhte lõpetamise kohta. Teatega olid kaasas asjakohased ja informatiivsed hoolsusmeetmete kohaldamise käigus kogutud dokumendid.*

Siiski esineb jätkuvalt **puudusi nii teadete kvaliteedis kui mahus**. Virtuaalvääringu sektori teadete suurim puudus on **info vähesus**. Näiteks esitatakse teate sisukirjelduses üks lause, milles puudub selge indikatsioon kahtlusele. Osade teatajate puhul on arusaamatu, kuidas ettevõte hoolsusmeetmeid kohaldab ning kas vara päritolu kohta on küsitud informatsiooni. Paljude teadete probleemiks on **vormivead**, **ebapiisav tehingu ja kahtluse kirjeldus** ja **tehingu osapoolte lisamata jätmine**.

Puuduliku teate näide:

Tehingu kirjeldus: *„Kliendile on laekunud krüptoraha summas 100 000 USDT. Kliendile saadeti päring raha päritolu kohta.“*

Kommentaar: *Teade on poolik, puudusid lisatud dokumendid ning info kliendi poolt antud selgituste ning vara päritolu kohta. Lisaks on ebaselge, kas kliendisuhet jätkati.*

Oluline on teate terviklikkus. RAB soovitab lähtuda tehingu kirjelduses struktureeritud narratiivist, kasutades selleks järgmist raamistikku: **mis, kes, millal, kus, miks, kuidas**. Teadet esitades tuleb muuhulgas märkida, kas kliendisuhe peatati või mitte. Kui teates on mainitud, et kliendisuhe on plaanis üle vaadata, ootab RAB teatele jätkuteadet kliendisuhte lõpetamise otsuse kohta. Lisaks peab teade olema õigesti kategoriseeritud ning teates tuleb arusaadavalt välja tuua seos teate liigiga, näiteks sularahateadete puhul on vaja selgitada seost sularahaga.

Sarnaselt eelmisele aastale esitati ka 2022. aastal mitteõigustatult teateid märksõnaga „**KIIRE**“, peamiselt soovides saada RABilt seisukohta kliendisuhte lõpetamise kohta. „Juhend kahtlaste tehingute tunnuste kohta“[4] annab juhised, millal selliseid teateid esitada. Märksõnaga „KIIRE“ esitatakse teade kui:

- rahapesu või terrorismi rahastamise kahtluse tekkimisel kahtlust ei kõrvaldatud ning ei tohi tehingut teha ega ärisuhet luua ja tehing tuleb edasi lükata;
- on kahtlus kontode võrgustiku osas, mille eesmärgiks on vara päritolu hägustamine. Järgmine kontole või kontolt tehtav ülekanne tuleb võimalusel peatada, vormistada STR märkega „KIIRE“.
- ärisuhtes oleva isiku kontol on nn transiitkonto tunnused. Järgmine kontole või kontolt tehtav ülekanne tuleb võimalusel peatada, vormistada STR märkega „KIIRE“.
- tehingu ettevalmistamisel või tegemisel – kui kahtlust ei kõrvaldata, tuleb tehing edasi lükata ja saata teade (STR, TFR-2 märkega „KIIRE“), tehingut teha ei tohi.

Ehkki tegu on kõrgeima terrorismi rahastamise riskiga sektoriga, esitas 2022. aastal terrorismi rahastamisele viitavaid teateid siiski vaid **kriitiline vähemus turuosalistest.** 148 teenusepakkujast esitas teateid kõigest 6 ehk **4%**. See viitab asjaolule, et ülejäänud virtuaalvääringu teenuse pakkujatel puuduvad piisavad monitooringumehhanismid, et tuvastada terrorismi rahastamisele viitavaid ohumärke.

RAB uuendas 2022. aastal kahtlaste tehingute tunnuste juhendit, *sh terrorismi rahastamisele viitavate teadete esitamise süsteemi, kus eristatakse kahte tüüpi terrorismi rahastamisele viitavaid teateid: TFR-1 ja TFR-2.* ***TFR-1*** *eeldab lisaks tehingu osapoole seotusele riskiriigiga ka riskiindikaatorit,* ***TFR-2*** *eeldab konkreetsele terrorismi rahastamise kahtlusele viitavat asjaolu. Juhendis on toodud* ***terrorismi rahastamise indikaatorid*** *ehk ohumärgid, mis aitavad kohustatud isikul tuvastada analüüsi käigus tehingu või toimingu ebaharilikkust. See võimaldab anda kohustatud isikul esmase hinnangu, kas tegu võib olla potentsiaalselt terrorismi rahastamisega, ning esitada RABile vastavasisulise teate.* ***Juhendi lisana avalikustati RABi kodulehel ka kõrgema terrorismi rahastamise riskiga riikide ehk riskiriikide nimekiri****.*

Palume terrorismi rahastamise teadetes märkida ära ***konkreetne riskile osutav indikaator*** *(lisaks seotusele riskiriigiga)* ***või konkreetne kahtlusele osutav indikaator****, lisada tehingu osapooled, tehingu osapoolte sideandmed (telefon, e-posti aadress), tehingu objekt ning tehingu kuupäev. Palume lisaks dokumentide esitamisele tuua välja hinnang, kas hoolsusmeetmete kohaldamise käigus on tõendatud vara päritolu, tuvastatud tegelik kasusaaja ning kliendi või juhuti tehtavas tehingus osaleva isiku omandi- ja kontrollistruktuur.*

Peamised puudujäägid **TFR teadete** kvaliteedis on järgmised:

- Üldiselt lisavad VASPid teatele enamiku vajalikest dokumentidest. Vahel lisatakse tehingute kirjeldamiseks visualiseering plokiahela analüüsi tarkvarast, kuid jäetakse lisamata vaba teksti väljale tehingu räsi (*hash*). Tehingu räsi lisamine on oluline selleks, et RAB saaks tehingut kontrollida.
- Mõningatel juhtudel täidavad VASPid teate esitamisel tehingu kirjelduse vaid lakoonilise infoga. Ehkki on tänuväärne, et põhjalikum analüüs lisatakse eraldi failina, peab ka tehingu kirjeldus hõlmama põhipunktide piisava detailsusastmega välja toomist – RABile teate esitamisel tuleb lähtuda RABi poolt välja antud juhisest.
- Terrorismi rahastamisele viitavates teadetes on olnud ka teate valesti klassifitseerimist. Näiteks on esitatud TFR-1 teade, ehkki teenusepakkuja on tuvastanud kliendi kohta avaandmete põhjal viited terrorismile või terrorismi

[4] Rahapesu Andmebüroo, https://fiu.ee/oigusaktid-ja-juhendid/juhendid#juhend-kahtlaste-teh

rahastamisele. Niisugusel juhul tuleb esitada TFR-2 ajendiga teade, mis on kõrgema prioriteediga.
- Osadel juhtudel on teenusepakkuja toonud teates välja kavatsuse kliendisuhe lõpetada, kuid jätnud märkimata konkreetse ajaraamistiku.

TFR teadete **tüpoloogiad** on järgmised.

- 97% teadete puhul on kahtlusega haaratud summa jäänud vahemikku alla 1000 euro. Seega on enamik VASPide esitatud teadetest **väikeste summade** kohta.
- 46% teadetest on sellised, mille puhul on teavitatud **kliendisuhte algatamisest riskiriigi** kodanikuga. Enamikel juhtudel on olnud järgnevaks kliendisuhte lõpetamise põhjuseks asjaolu, et klient ei ole täiendavate hoolsusmeetmete kohaldamise käigus küsitud andmeid esitanud. Selliste teadete puhul pole teenusepakkuja tuvastanud kindlat riski, v.a seos riskiriigiga.
- 16% teadete puhul nähtub potentsiaalne **testmaksete** tegemine. Näiteks on klient teinud summas 1–20 eurot kas sissemakse või üritanud teha makset teisele osapoolele. Kui kliendilt on küsitud seejärel täiendavat infot, ei ole teenusepakkuja vastuseid saanud. See võib viidata nn testmaksete tegemisele eesmärgiga tuvastada, kui rangeid hoolsusmeetmeid konkreetne teenusepakkuja kohaldab.

ISR teadete osas oli 2022. aasta erakordne, kus esitatud teadete arv võrreldes eelneva aastaga kümnekordistus (2021. aastal oli 99 ja 2022. aastal 953). Kui VASPid esitasid 2021. aastal vaid 4 ISR teadet, siis 2022. aastal 112. Vastavalt järjest kehtestatud sanktsioonimeetmetele teavitasid VASPid esmalt **Venemaa kodanike** üle 10 000-eurostest deposiitidest ja seejärel Venemaa kodanike kontode sulgemisest. Kontode sulgemisel esitasid mõned VASPid iga kliendist Venemaa kodaniku kohta eraldi teate, mille tulemusel laekus RABile mitukümmend teadet kontode sulgemisest. Tavapärane praktika näeb ette, et sama piirangu kohaldamisel mitmele isikule võib vastavad isikud **koondada ühte teatesse** ja ei ole vaja esitada mitut teadet. Murettekitav on, et osa VASPidest, kellel on **vene klientuur**, ei ole teinud sanktsiooniteateid.

Lisaks teavitasid VASPid mittesiduva rahvusvahelise sanktsiooni (**ISR.4**) kohaldamisest olukordades, kus tuvastati, et nende klient on teinud/saanud laekumise OFAC/OFSI poolt nimekirja kantud isikult või on raha tulnud/läinud rahakotti, mis on OFAC nimekirjas välja toodud. VASPide puhul oli selliste teadete kvaliteet kohati puudulik, sest märkimata oli **sanktsiooni subjekt**.

Kokkuvõtteks, teadetest on näha, et ärisuhteid jälgitakse aina rohkem, kuid siiski on enamik virtuaalvääringu teenuse pakkujate poolt esitatud teateid kas kliendisuhte loomise käigus tuvastatu või pettuste kohta. RAB ootab VASPidelt veelgi põhjalikumat ärisuhete jälgimist ning sisukamaid teateid.

Esitatud teadete asjakohasust aitab hinnata **välispäringutele** vastamise valmisolek. VASPide puhul ei ole tihti info enne RABile välispäringu laekumist esitatud. Samuti viitab eelmainitu asjaolule, et VASPid ei suuda vajalikus ulatuses kahtlaseid tehinguid tuvastada.

Rahapesu andmebüroo järelevalve tähelepanekud

Seisuga 31.12.2022 oli Eestis kehtiv tegevusluba **148** virtuaalvääringu teenuse pakkujal, uusi taotlusi menetluses **7** ning tegevusloa muutmise taotluseid menetluses **150** (tabel 3). 15. märtsil 2022 jõustusid rahapesu ja terrorismi rahastamise tõkestamise seaduse (RahaPTS) muudatused, mis kohustasid virtuaalvääringu teenuse pakkujad viima end kooskõlla uute nõuetega 15. juuniks. Tegevusloa muutmise taotluse esitas tähtajaks 135 teenusepakkujat. Seadusemuudatuse tulemusena vähenesid turuosaliste arv, seega vähenes ka sektori käive ja klientide arv ning seda valdavalt ebapiisava hoolsuskohustusega teenusepakkujate arvelt. Aasta jooksul tunnistati kehtetuks 234 VASPi tegevusluba.

Tabel 3. Virtuaalvääringu teenuse pakkujad seisuga 31.12.2022

Tegevusala	Aktiivsed tegevusload	Ajutises loobumises	Uued taotlused menetluses	Tegevusloa muutmise taotlused menetluses
Virtuaalvääringu teenuse pakkujad	148[5]	0	7	150[6]

RAB järelevalve viis 2022. aastal läbi riskide hindamiseks **küsitluse** VASPide seas. Küsiti infot kaitseliinide, sisekontrolli, siseauditi, riskihinnangu, riskiisu, ärisuhte seire ning süsteemide, klientide, tegevuse edasiandmise ja teatamiskohustuse täitmise kohta. Lisaks lõpetas RAB 2022. aastal virtuaalvääringu teenuse pakkujate järelevalvemenetlusi, mis alustati 2021. a lõpus. Alustatud järelevalve menetlusi oli **9** ning varasemast oli pooleli veel täiendavalt **1**. Eelnevalt mainitud 10st järelevalvemenetlusest **5** lõppesid VASPi loobumisega Majandustegevuse registris (edaspidi MTR) tegevusloast. Enim tähelepanu järelevalvemenetlustest pälvisid 2022. aastal **Hodltech OÜ** ning **Garantex Europe OÜ**, mille osas avaldas RAB ka vastavad pressiteated.

Nii 2022. aastal lõppenud kui pooleliolevad menetlused sisaldavad kõik **RahaPTS** või **RsanS nõuete rikkumisi**. VASPidel on puuduseid alates organisatsiooni ülesehitusest kuni ärisuhteseireni. Järelevalvemenetluste tulemused viitavad selgelt, et ilma nõuetele vastava organisatsioonilise lahenduseta on VASPide sektoris rahapesu ja terrorismi rahastamise risk jätkuvalt väga kõrge. Virtuaalvääringu teenuse pakkujate sektoril on vaja veel enam rõhku panna enda sisemiste süsteemide efektiivsemaks muutmisele, et rahapesu ja terrorismi rahastamise risk oleks piisaval määral maandatud.

Peamised puudused, mida RAB on järelevalvemenetlustes tuvastanud, on järgmised.

- Puudulik **organisatsiooni ülesehitus** (kolm kaitseliini).
  - Huvide konflikt erinevate kaitseliinide vahel ehk funktsioonide lahususe puudused, mistõttu pole rahapesu ja terrorismi rahastamise riskid piisavalt maandatud
  - Kõigi kolme kaitseliini tegevuse eest vastutab üks isik.
  - Puudub sisekontrollisüsteem.

- Puudulikud **sisemised dokumendid** (protseduurireeglid, riskihinnang, riskiisu).
  - Sisemised dokumendid ei vasta ettevõtte reaalsele majandustegevusele ning neid ei rakendata töötajate poolt nii nagu need on kehtestatud.
  - Ettevõtte riskihinnang ja riskiisu ei vasta ettevõtte reaalsele majandustegevusele ja sellega kaasnevatele riskidele.
  - Ettevõtte riskihinnang/riskiisu ei ole kooskõlas ettevõtte protseduurireeglitega.
  - Ettevõtte ei lähene klientidele riskipõhiselt.

- Puudulik **isikusamasuse tuvastamise süsteem**.
  - Ärisuhte loomisel ei viida klientidega läbi reaalajas videointervjuud (RahaPTS § 31).
  - Luuakse ärisuhteid klientidega, kelle esitatud isikusamasust tõendavad dokumendid ei vasta nõuetele (RahaPTS § 31 lg 6).
  - Ei koostata või koostatakse puudulikult kliendi riskiprofiil (näiteks ei tuvastata kliendi tegevusala ja vara päritolu).

[5] 15.03.2022 jõustunud RahaPTS muudatuse tulemusel antud välja 1 luba, mis sisaldub 148 hulgas. Lisaks on tänase päeva seisuga üks VASP võtnud enda tegevusloa muutmise taotluse tagasi, mistõttu tänase päeva seisuga kajastub ettevõtte kehtivate lubade hulgas. Viimati mainitud tegevusloast on loobutud.

[6] VASPide muutmise menetlusi (150) on rohkem, kui kehtivaid lube, sest muutmise menetlused sisaldavad ka veel nelja vana tegevusloa muutmise taotlust (rahakotiteenuse tegevusluba ja virtuaalvääringu vahetamise teenuse tegevusluba).

- Tegelik kasusaaja jäetakse tuvastamata.

- Puudulik **ärisuhte seiresüsteem**.
  - Riskipõhise lähenemise puudumisel, ei lähtuta ärisuhte seire teostamisel reaalsetest äritegevusega kaasnevatest riskidest.
  - Puudub protsess ärisuhte seire läbiviimiseks (ei lähtuta sisemistes dokumentides kirjas olevast regulaarsusest).
  - Puudub tehniline võimekus piisaval määral teostada ärisuhte seiret.
  - Sanktsiooni tuvastamise süsteemid on puudulikud.