Rahapesu Andmebüroo tagasiside virtuaalvääringu teenuse pakkujatele

Rahapesu ja terrorismi rahastamise riskipilt ning finantssanktsiooni kohaldamine aastal 2023

Piiriülese rahapesu oht on Eestis riigisisesega võrreldes jätkuvalt märksa kõrgem. Kõrgema rahapesu riskiga olid Eestis **virtuaalvääringu teenuse pakkujad** (VASPid) ja **äriühingute teenuse pakkujad** (CSPd), pangandussektori riskitase oli keskmine. Eestis toimub välisriikides saadud **kriminaaltulu kihistamine** *(layering)*, kuid digitaliseerumise tulemusena on rahapesuetappe (eriti paigutamist ja kihistamist) praktikas üha keerulisem eristada. Seda ka kelmuste puhul, mis olid 2023. aastal Eestis levinuimad eelkuriteod. 2023. aastal RABi avatud toimikutes olid jätkuvalt enamlevinud seoseks Eestiga siin avatud **kontod** või Eestis asutatud **juriidiline isik**, mida kasutati eelkõige kihistamisfaasis vara liigutamiseks. Kurjategijad eelistavad endiselt **sularaha** anonüümsuse tõttu, mida see pakub. 2023. aastal olid võrreldes eelnevate aastatega selgelt rohkem RABil pildis **sanktsioonidest kõrvalehoidumisega seotud juhtumid**.

Kuigi Eesti pangandussektori riskitase on pärast suuri rahapesuskandaale astutud maandamismeetmete tõttu oluliselt vähenenud, on riskitase endiselt keskmine, sest pankade välismaksete käive on suur ning pangakontosid kasutatakse palju kelmuse skeemides (põhjalikumalt allpool). 2023. aastal oli Eesti krediidiasutustes äriühingute, kodumajapidamiste ja finantseerimisasutuste laekuvate piiriüleste maksete maht 100,4 miljardit eurot (kasv võrreldes 2022. aastaga 1,02%) ja makstavate piiriüleste maksete maht 101,2 miljardit eurot (kasv 0,14%). Kuna enamik Eesti krediidiasutustest on oma kliendibaasi pärast rahapesuskandaale põhjalikult puhastanud, kasutavad kurjategijad välisriikide teenusepakkujaid. RABi analüüsitud juhtumites kasutatakse palju Leedu maksekontosid, mis viitab, et rahapesu kahtlusega raha on liikunud Leedus avatud kontodele.

Riigi võetud meetmete tõttu on VASPide turg suuresti korrastunud. Kui 2019. aasta lõpu seisuga kehtis Eestis enam kui 1200 ja 2022. aasta alguses 148 virtuaalvääringu teenuse tegevusluba, siis 2023. aasta lõpus 53. Ka VASPide hoolsusmeetmete kohaldamise kvaliteet on tõusnud. Siiski on sektoris rahapesu risk jätkuvalt kõrge, sest teateid saatis 2023. aastal vähem kui pool turuosalistest, järelevalvetegevus on näidanud, et VASPidel on puudujääke oma riskide hindamisel (riskihinnang ja riskiisu dokumendid ei ole kooskõlas tegelikkusega, probleeme on klientide isikusamasuse tuvastamisega) ning plokiahela analüüsifirmade andmed näitavad, et osa Eesti tegevusloaga VASPide tehingutest on jätkuvalt seotud kõrge riskiga platvormidega (*high risk exchange*). Samuti seostatakse virtuaalvääringu voogusid jätkuvalt kuritegeliku tegevusega, Eestis peamiselt pettustega. 2023. aasta lõpus Eesti tegevusluba omavate VASPide vahendatud teenuste käive oli 2023. aastal 20 miljardit eurot. 2024. aastal rakenduv regulaarne VASPide aruandlus võimaldab tulevikus sektori riskipilti veelgi paremini mõista.

CSPde risk on jätkuvalt kõrge. RAB on tuvastanud juhtumeid, kus CSPd ei rakenda kõrge riskiga, rahapesukahtlusega või sanktsiooni subjektideks olevaid kliente teenindades hoolsusmeetmeid ning on jätnud teavitamiskohustuse täitmata. Suur osa (ligi 2/3) neist pakub mitteresidentidele äriühingute teenuseid. Paljud CSPdest on „multiteenusepakkujad“ ja

pakuvad oma klientidele lisaks äriühingute teenustele ka raamatupidamis- ja nõustamisteenuseid. CSPde kogukäive on suurusjärgus 80 miljonit eurot, äriühinguteenustega seotud käive 25 miljonit eurot. Paljude CSP-de töötajate arv on väike, seda ka suure käibega teenusepakkujate puhul, mistõttu esineb risk, et nad ei suuda vajalikul määral rakendada rahapesu tõkestamise hoolsusmeetmeid.

RABile saadetud välispäringute, teadete, analüüsitud juhtumite ning teiste õiguskaitseasutuste info alusel on jätkuvalt **levinuimad rahapesu eelkuriteod erinevad kelmused** ning seoseks Eestiga on kelmusest saadud vara kandmine Eesti krediidiasutuses avatud kontole. Kelmused on levinud kogu maailmas ning tegu ei ole Eesti eripäraga. 2023 EFECTA-s[1] nenditakse, et selgelt on täheldatav *online* kelmuste osakaalu tõus ning pettuse liikide mitmekesistumine.

Kelmuse juhtumites oli 2023. aastal selgelt näha VASPide turu korrastumise tulemust ja riskide vähenemist. Suur osa VASP-idega seotud välispäringutest, mille õiguskaitseasutused said, puudutasid VASPe, millel pole enam Eesti tegevusluba.

Lisaks kelmustele, kuid märksa vähem, tulid 2023. aastal RABi analüüsitud juhtumites rahapesu eelkuritegudena esile maksu- ja narkokuriteod, vähem nägi RAB ebaseaduslikule majandustegevusele, omastamisele ja korruptsioonile viitavat kahtlust. Neid kuritegusid menetlevad teised õiguskaitseasutused (MTA, PPA), kuid enamasti ilma rahapesu kvalifikatsioonita.

Hoolimata elektrooniliste maksevõimaluste võidukäigust ja uutest tehnoloogiatest on **sularaha** jätkuvalt kurjategijate seas eelistatud[2]. 2023. aastal valmis RABis analüüs „Sularahaga seotud rahapesu ja terrorismi rahastamise riskid Eestis“[3], mis näitas, et võrreldes pandeemia-aastatega, on Eestis tõusnud suurte mitmete sularahaintensiivsete teenuste (valuutavahetus, investeerimiskulla müük ja hasartmänguteenused) sularahatehingute maht ja koos sellega rahapesuohu tase. Piiriüleste e-raha ja makseasutuste Eesti makseagentide sularahaga seotud maksetehingud on jätkuvalt kõrge rahapesuohuga. Osalt on riskid kandunud teistesse jurisdiktsioonidesse, eelkõige Leetu. RABile saadetud sularahateadetest on näha „sula(rahas)tamise“ tüpoloogiat, kus välisriigi e-raha või makseteenuse osutaja makseagenti kasutatakse vahendite sularahas väljavõtmiseks või sissepanemiseks, „sulatamine“ toimub eeskätt suunaga välisriikidest Eestisse. Sularahaintensiivsed teenusepakkujad saadavad RABile väga vähe kahtluspõhiseid sularahateateid ning viitab nende teenusepakkujate haavatavusele rahapesu (ja ka terrorismi rahastamise) vaatest.

Terrorismi rahastamise vaatepunktist on Eestis endiselt kõrgeim risk **edastamise** faasis, terroristlikul eesmärgil vahendite kogumise ja kasutamise risk on madal. 2023. aastal esitati RABile märkimisväärne hulk teateid, mis puudutasid terrorismi rahastamise riski või kahtlust isiku puhul, kes ei resideeru Eestis, kuid kasutab tehingus Eesti turuosalisi. See ilmestab, et terrorismi rahastamise vastane võitlus on olemuselt rahvusvaheline ning mõnes teises riigis tegutseva isiku kohta võib vajalikku infot koguda just Eesti turuosaline.

Konkreetsetest sündmustest mõjutas terrorismi rahastamise riskipilti kõige enam **Hamasi-Iisraeli konflikt**. See väljendus hoogsamas annetuste ja toetuste kogumises tsiviilisikute kaitseks konfliktipiirkonnas (mis ei ole terrorismi rahastamine), aga ka katsetes edastada vahendeid Hamasiga seotud osapooltele. Näiteks proovisid teiste riikide kodanikud ja residendid Eesti krediidiasutustes avatud kontode kaudu teha (annetus)makseid Palestiina

---

[1] The Other Side of the Coin. European Union Financial and Economic Crime Threat Assessment (EFECTA). Europol, 2023, https://www.europol.europa.eu/cms/sites/default/files/documents/The%20Other%20Side%20of%20the%20Coin%20-%20Analysis%20of%20Financial%20and%20Economic%20Crime%20%28EN%29.pdf

[2] Why cash is still king. A strategic report on the use of cash by criminal groups. Europol, 2015.

[3] Sularahaga seotud rahapesu ja terrorismi rahastamise riskid Eestis. Rahapesu Andmebüroo, 2023, https://fiu.ee/media/955/download.

heategevusorganisatsioonidele, meediaväljaannetele või otse Gaza sektoris asuvate isikute pangakontodele. 2023. aastal avaldas RAB lühiuuringu terroriorganisatsiooni Hamas rahastamismudelitest[4]. Hamasi-Iisraeli konflikti mõju terrorismi rahastamise riskikeskkonnale on suure tõenäosusega märkimisväärne ka 2024. aastal.

Eesti terrorismi rahastamise alane haavatavus tuleneb ka avatud majanduskeskkonnast, mis võimaldab lihtsalt ettevõtteid luua. Siinkohal on oluline CSPde keskne roll terrorismi rahastamise riski indikaatorite tundmisel. Lisaks on haavatavuse tegureid asjaolu, et kuigi islamiäärmusluse rahastamist osatakse ära tunda, on üldine teadlikkus muudest rahvusvahelistest äärmuslusideoloogiatest, sealhulgas vägivaldse paremäärmusluse eri vormidest, veel Eesti ühiskonnas üldiselt, aga ka turuosaliste seas madal.

Eestit, kui EL-i piiririiki ja Venemaa naabrit, mõjutab tugevalt **Venemaa sõjaline agressioon Ukrainas**. Alates Vene-Ukraina täiemahulise sõja algusest 24.02.2022 oli EL seisuga 31.12.2023 vastu võtnud 12 sanktsioonipaketti, mis sisaldavad ulatuslikke finants-, majandus- ja kaubandussanktsioone, et nõrgestada Venemaa majandust ning kärpida riigi sõjapidamise võimekust. Finantssanktsiooni vaatest laienes 2023. aastal vastu võetud sanktsioonipakettidega eelkõige nende isikute ring, kelle suhtes kehtib vahendite ja majandusressursside kättesaadavaks tegemise keeld. Märkimisväärne oli ka mitme Venemaa suurema panga ja Venemaa Rahapesu Andmebüroo (*Rosfinmonitoring*) juhi sanktsiooninimekirja lisamine. Külmutatud vahendite hulk Eesti krediidiasutustes ning Maksu- ja Tolliametis kasvas 2023. aastal. Kui 2023. aasta esimeses kvartalis oli külmutatud vahendeid veidi enam kui 18 miljonit eurot, siis 2023. aasta lõpuks rohkem kui 33 miljonit eurot.

2023. aasta märksõnadeks oli **sanktsioonist kõrvalehoidmine** ning **mitme sanktsiooni liigiga põimitud olukorrad**. RABile esitatud sanktsiooni teadetest (ISR) oli näha, et kohustatud isikud, aga ka riigiasutused on hakanud rohkem tähelepanu pöörama sanktsioonist kõrvalehoidumise analüüsile. Sanktsioonist kõrvalehoidumise juhtumites püütakse kasutada Eesti finantssüsteemi ja juriidilisi isikuid. RABi analüüs näitab, et maksed Venemaa ja Eesti vahel on oluliselt vähenenud ning peamised finantssanktsiooni rikkumise riskid seostuvad olukordadega, kus finantssanktsiooni subjektile tehakse kättesaadavaks mitte vahendeid (nt raha), vaid majandusressursse (nt kaupu).

Peaasjalikult on tegu juhtumitega, kus Eesti ettevõtted jätkavad vahekehade kaudu koostööd Venemaa äripartneritega, kellega enne Ukraina sõja algust tehinguid tehti, kasutades selleks kolmandates riikides registreeritud läbipaistmatu taustaga ettevõtteid. Nimelt näidatakse kolmandates riikides registreeritud ettevõtteid selliste kaupade saajatena, mida on keelatud Venemaale viia. Tegelikkuses võidakse kaup aga kolmandast riigist re-eksportida Venemaale. Kauba Venemaale viimisel, varjates seejuures kauba lõppkasutajat, võidakse rikkuda mitte ainult kauba piirangut, vaid teha majandusressursse kättesaadavaks finantssanktsiooni subjektile, rikkudes sellega finantssanktsiooni. Erinevad sanktsiooni liigid (kauba keeld, teenuse keeld ja finantssanktsioon) on omavahel tugevalt põimunud.

VASPide riskikeskkond

Chainalysise[5] andmetel oli 2023. aastal illegaalsete aadresside kaudu saadetud summa kokku **24,2 miljardit dollarit**, mis on üle 10 miljardi vähem kui 2022. aastal. Ka illegaalse summa osakaal kogu krüptovara mahust langes 0,42%lt 0,34%ni. Üha enam tehakse tehinguid kasutades *stablecoine*. Usutakse, et krüptotalv on läbi saamas ning varsti algab kasvufaas.

[4] Terroriorganisatsiooni Hamas rahastamismudelid. Rahapesu Andmebüroo, 2023, https://fiu.ee/media/1032/download.
[5] Chainalysis, https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/

2023. aasta suurim trend seoses ebaseadusliku rahaga oli **sanktsioonidega**[6] **seotud maksed**. Kokku oli neid 14,9 miljardit dollarit, mis on ligi 62% kogu kuritegeliku vara aasta mahtust. Krüpto kelmuste ja häkkimiste kasumid langesid 2023. aastal märkimisväärselt. Kelmused on kõige edukamad, kui krüptoturul läheb hästi ning inimesed soovivad kiirelt rikastuda, kuid hetkel on trendiks pigem **armukelmused**, kus panustatakse inimeste emotsioonidele. Häkkimine on samuti vähenenud, sest DeFi protokollid on oma turvalisust tugevdanud ning suudetakse ebatavalisi väljuvaid rahavooge kiiremini tuvastada. **Lunavararünnakud** ja **tumeveeb** on kaks valdkonda, kus suudeti vastupidiselt trendidele kasumeid suurendada. Ilmselt on lunavara ründajad jõudnud ennast ettevõtete küberturvalisuse tugevdatud meetmetega kurssi viia. Tumeveebi suhtes oli eelnev langus seotud Hydra sulgemisega, kuid nüüd on kasumid juba 2021. aasta tipu taseme juures tagasi.

Riskide vähenemisele viitab asjaolu, et välisriikide partnerasutuste huvi RABi tegevusloaga teenusepakkujate vastu on veidi langenud. Aasta jooksul RABile esitatud 552 välispäringust ja spontaansest infoedastusest puudutas 44 (8%) virtuaalvääringu teenuse pakkujaid (2022. aastal 85 ja 15%). Seejuures on oluline märkida, et välisriikide päringutel ning teabeedastustel on tavapäraselt ajaline viide ning oluline osa hõlmatud teenusepakkujatest on tegevusloa kaotanud.

Lisaks rahapesu ja terrorismi rahastamise ohukohtadele kerkib aina enam probleemina esile teenusepakkujate suutlikkus kaitsta oma klientide vara ning andmeid, seda nii väliste rünnakute kui ka omanike pahatahtlikkuse tõttu. Näiteks langes 2023. aastal üks suur teenusepakkuja rünnaku ohvriks, mille tagajärjel tekitati ettevõttele üle mitmekümne miljoni euro väärtuses kahju.

Oluliseks probleemikohaks on jätkuvalt **pesastatud teenused** (*nested services*). 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 **1. jaanuarist 2024** on vastavalt rahandusministri määrusele Eestis tegutsevad virtuaalvääringu teenuse pakkujad kohustatud edastama Eesti Pangale ja Rahapesu Andmebüroole regulaarselt andmeid oma tegevuse, hoolsusmeetmete, osutatud teenuste ning varade ja kohustuste kohta. Aruanded tuleb esitada kvartaalselt, **hiljemalt 20. kuupäeval pärast kvartali lõppu** läbi Eesti Panga andmekogumisportaali.*

RAB avaldas 2023. aasta algul lühiuuringu „**Virtuaalvääringute abil sanktsioonidest kõrvalehoidmine**[7]". Uuringus on välja toodud virtuaalvääringute abil sanktsioonidest kõrvalehoidmiseks kasutatavad kolm üldist tüpoloogiat. Ülevaates kirjeldatakse mainitud kolme mudelit ning tuuakse välja indikaatorid, mis viitavad sanktsioonidest kõrvalehoidmise kõrgendatud riskile. Samuti kirjeldatakse olulisemaid tegureid vastavuskontrolli tagamiseks, mis aitavad riske maandada.

Novembris saatis RAB Eesti tegevusloaga turuosalistele välja ettekirjutuse, millega koguti kõigilt Eestis tegevusluba omavatelt virtuaalvääringu teenuse pakkujatelt andmeid ettevõtte poolt osutatavate teenuste, nende mahtude ja klientide kohta. Teabe kogumise eesmärk oli Eestis tegutsevate VASPide tegevusest tulenevate ohtude ja haavatavuse väljaselgitamine, et hinnata virtuaalvääringu teenuse pakkumisega kaasnevaid riske ning töötada välja meetmed nende maandamiseks. Riskide mõistmine aitab RABil planeerida riskipõhist järelevalvet.

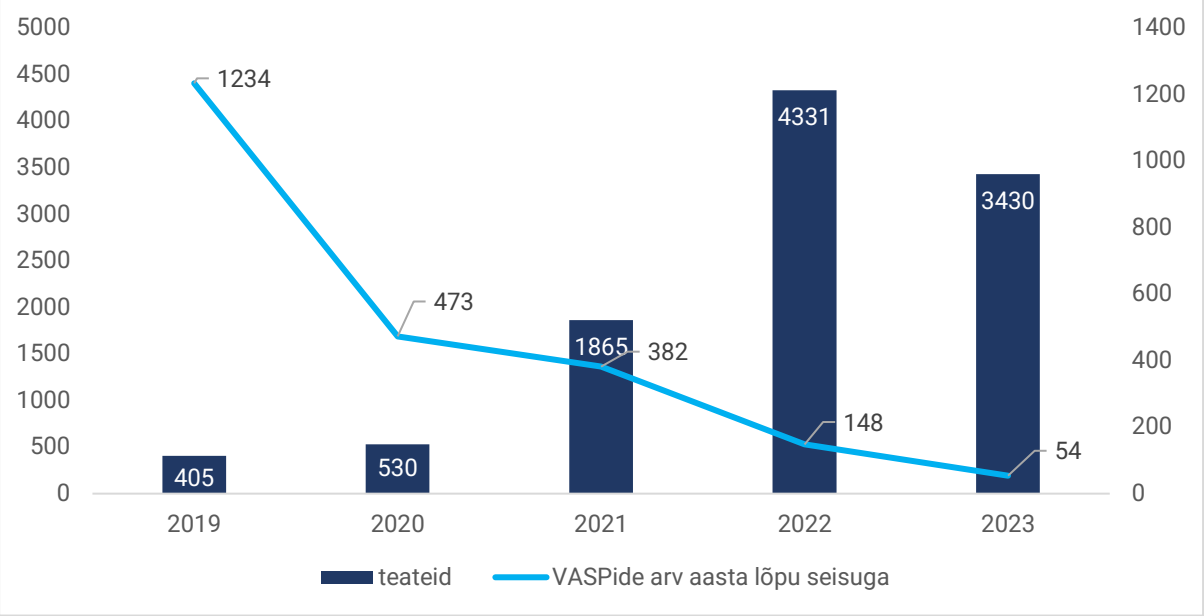
[6] Enamik oli seotud OFACi sanktsioonidega
[7] RAB, https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvaaringute-a

Soovitame kõigil turuosalistel osaleda RABi korraldatavatel infotundidel. Praktika näitab, et kohustatud isikute teadete kvaliteet on pärast infotundidel osalemist paranenud. RAB korraldas 2023. aastal VASPidele 7 infotundi[8].

Ülevaade 2023. aastal saadetud teadetest

Teatamiskohtuste täitmine on sektori turuosaliste poolt aasta-aastalt paranenud, kuid on jätkuvalt **puudujääke**, seda nii teatamisaktiivsuses kui ka teadete sisukuses. 2023. aastal vähenes RABile saadetud teadete arv, kuid samuti vähenes tegevusluba omavate VASPide arv, mistõttu teadete arvu langus on osaliselt mõistetav. Siiski ei saatnud **üle poole teenusepakkujatest** RABile **ühtegi teadet.**

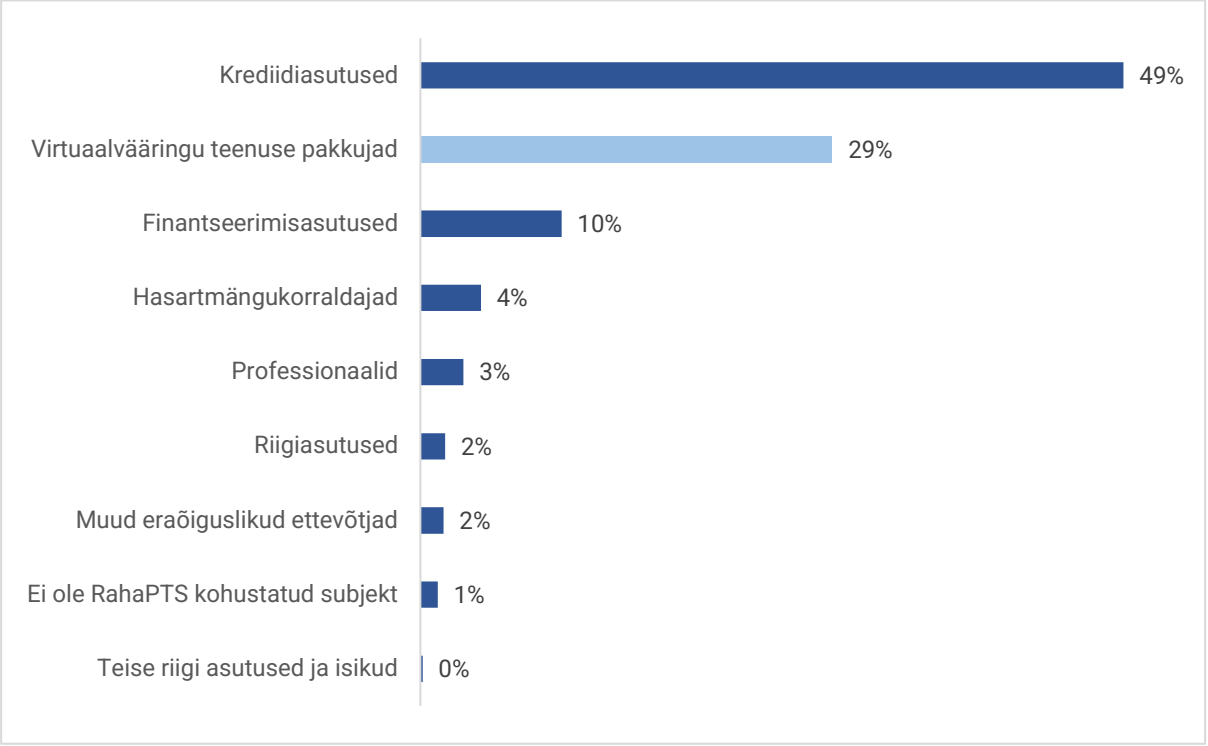
2023. aastal esitas teateid 44 virtuaalvääringu teenuse pakkujat. Neist **24 oli 2023. aasta lõpu seisuga tegevusluba,** mis moodustas **44%** aasta lõpu seisuga tegevusluba omavatest VASPidest (2022. aastal 47%). VASPide arv on alates 2020. aastast langustrendis ning vähenes 2023. aastal 64% (joonis 1). Aasta jooksul esitas üle 10 teate vaid **41%** VASPidest ning mitmed suure käibega teenusepakkujad esitasid jätkuvalt vaid üksikuid teateid. Teatajate osakaal oli ka 2023. aastal sektori riskitaset ja mahte arvestades **ebapiisav**.



Joonis 1. Virtuaalvääringu teenuse pakkujatelt RABile 2019.–2023. aastal saadetud teadete ja VASP tegevusloaga ettevõtete arv.

Alates 2020. aastast kuni 2022. aastani kasvas virtuaalvääringu teenuse pakkujate teadete arv märkimisväärselt. 2023. aastal toimunud teatamise aktiivsuse langus on osaliselt selgitatav turuosaliste arvu vähenemisega. Kui 2020. aastal saatsid virtuaalvääringu teenuse pakkujad RABile 530, 2021. aastal 1865 ja 2022. aastal **4331** teadet, siis 2023. aastal langes teadete arv ligi tuhande võrra **3430** teateni. VASPide teated moodustasid **29%** kõikidest teadetest (joonis 2).

[8] Infotundide kohta leiab infot RABi kodulehelt uudiste alt ja sotsiaalmeediast.



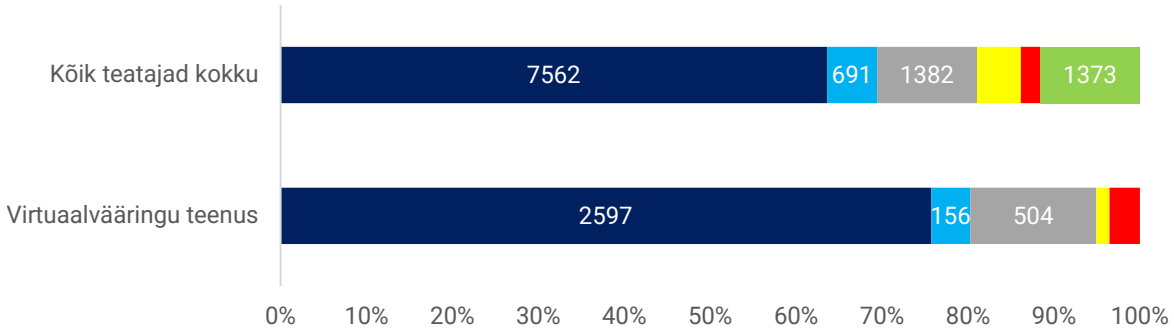
Joonis 2. 2023. a RABile saadetud teadete jagunemine teataja gruppide kaupa.

Mitmed VASPid kuulusid ka 2023. aastal suurimate teatajate hulka. 2023. aastal oli teatajate esikümnes 4 VASPi, mis on võrreldes 2022. aastaga 1 võrra vähem, kuid siiski hea tulemus.

Tabel 2. 2023. a RABile saadetud teadete esikümne jagunemine teate esitajate põhitegevusala alusel.

Teataja põhitegevusala alusel	Teateid
1. Teataja 1	2 652
2. Teataja 2	1 100
3. Teataja 3	1 057
4. Teataja 4	608
5. Virtuaalvääringu teenuse pakkuja 1	**599**
6. Teataja 5	557
7. Virtuaalvääringu teenuse pakkuja 2	**435**
8. Virtuaalvääringu teenuse pakkuja 3	**384**
9. Teataja 6	373
10. Virtuaalvääringu teenuse pakkuja 4	**344**

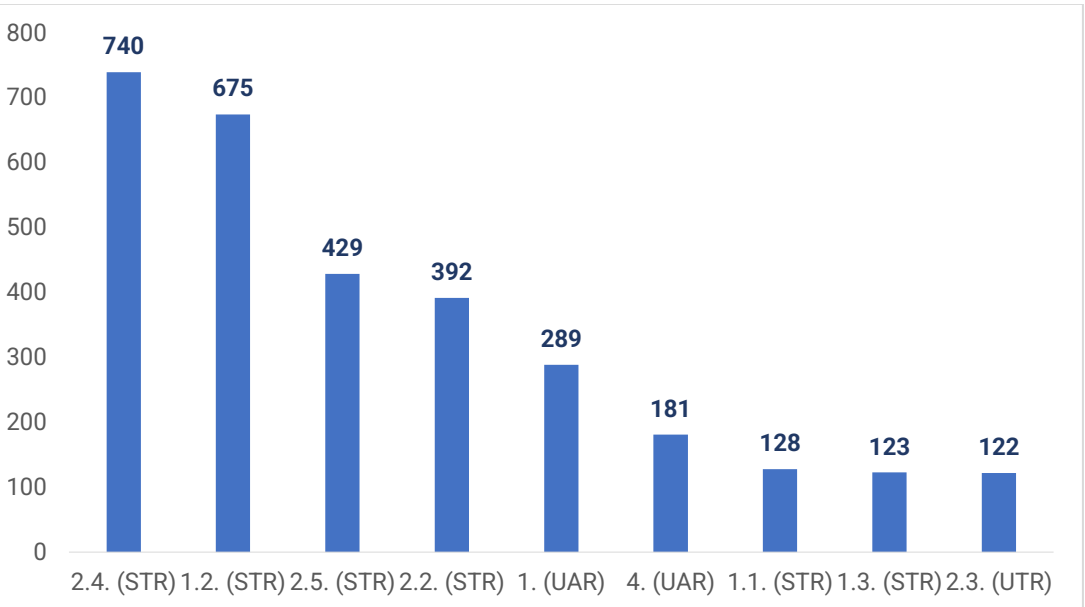
VASPid on teatajate seas olulisel kohal, eriti kuna tegemist on kõrge riskiga sektoriga ning esitatud teated võimaldavad muu hulgas RABil hinnata turul valitsevaid trende ning riske. Enamik VASPide esitatud teadetest puudutas rahapesukahtlust – kahtlase tehingu teateid (**STR**) saadeti 2597, ebahariliku tegevuse teateid (**UAR**) 504 ja ebahariliku tehingu teateid (**UTR**) 156. Terrorismiga seotud teateid (**TFR**) esitati kokku 121 (joonis 3). Sanktsioonikahtlust puudutavaid teateid (**ISR**) esitati kokku 52, millest enamus olid seotud Venemaa suhtes kehtestatud sanktsioonidega. 2023. aastal ei laekunud virtuaalvääringu teenusepakkujatelt ühtegi sularahateadet (**CTR**).



	Virtuaalvääringu teenus	Kõik teatajad kokku
STR	2597	7562
UTR	156	691
UAR	504	1382
ISR	52	606
TFR	121	273
CTR	0	1373

Joonis 3. Virtuaalvääringu teenuse pakkujatelt ja kõikidelt teatajatelt RABile 2023. 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. Kõige sagedamini märgiti teate saatmise põhjuseks, et esineb rahapesukahtlus kontol tehtava tehingu korral (**2.4. STR**) (joonis 4). Sageduselt järgmised põhjused isiku suhtes olid kahtlus isiku poolt esitatud andmete tõelevastavuses (**1.2. STR**), isik ei esita tehingu kohta hoolsusmeetmete täitmiseks vajalikus ulatuses selgitusi või dokumente või esitatu ei ole usutav (**2.5. STR**) ja varasemalt teadaolev või hoolsusmeetmete rakendamise käigus tekkinud rahapesukahtlus (**2.2. STR**).



Joonis 4. Virtuaalvääringu teenuse pakkujate poolt RABile 2023. a saadetud teadete enam levinud indikaatorid.

2.4. (STR) Rahapesukahtlus kontol tehtava tehingu korral

1.2. (STR) Kahtlus isiku poolt esitatud andmete tõelevastavuses

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)
2.2. (STR)	Isiku suhtes on varasemalt teadaolev või hoolsusmeetmete rakendamise käigus tekkinud rahapesukahtlus
1. (UAR)	Isiku ebaharilik käitumine
4. (UAR)	Ebaharilikud tehingud virtuaalvääringutega
1.1. (STR)	Isiku suhtes on varasemalt teadaolev või hoolsusmeetmete rakendamise käigus tekkinud rahapesukahtlus
1.3. (STR)	Krediidi- või finantseerimisasutus keeldub isikuga kliendisuhtesse asumisest vastavalt RahaPTS § 42 seoses hoolsusmeetmete täitmise võimatusega
2.3. (UTR)	Ebaharilik tehing virtuaalvääringuga

RAB analüüsis on VASPide teadetel oluline roll. 2023. aastal VASPide saadetud teadetest suunati süvaanalüüsi **32** teadet. Võrreldes 2022. aastaga vähenes analüüsi läinud teadete arv 260 teate võrra, selline suur muutus toimus peamiselt rahapesukahtlaste tehingute (STR) ja sanktsiooniteadete (ISR) tõttu. RAB kasutab teadete infot lisaks üksikjuhtumite analüüsile ka oma taktikalistes ja strateegilistes analüüsides. Eesti uurimisasutustele edastatud materjalides kasutati **152** teates sisaldunud infot. VASPide teadetest saadud infot on mitmel korral RAB edastanud ka välisriikide rahapesu andmebüroodele. 2023. aastal seati VASPide teadete põhjal **18** korral virtuaalvääringu teenusepakkuja kontole või kontol olevale varale käsutuspiirang.

Teadete sisu, kvaliteet ja soovitused tulevikuks

VASPide teadete kvaliteet on võrreldes varasemate aastatega **paranenud**, kuid siiski esineb jätkuvalt **puudusi.** Tõeliselt sisukaid teateid esitatakse vähe. Peamiselt on teate esitamise tinginud kas võltsitud dokumendi/ identiteedivarguse kahtlus või antakse teada kliendisuhte lõpetamisest, sest õiguskaitseasutused on kliendi vastu huvi tundnud ning klient ei vasta päringutele, mis näitab, et kohustatud isiku poolt jooksev **ärisuhete jälgimine on puudulik**. See viitab, et süsteemid ei ole piisavalt head või töötajad kogenud, et tuvastada rahapesu ja sellega seotud kahtlust. Erandiks on paar VASPi, kes edastavad sisukaid teateid, kust nähtub põhjalik analüüs, hoolsusmeetmete kohaldamine ning riskipõhine lähenemine. RAB rõhutab, et **ei piisa, kui VASPid johtuvad kahtlastest tehingutest teatamisel ainult plokiahela analüüsitarkvara pakkujate monitooringusüsteemidest, vaid nad peavad arvestama konkreetsete klientidega seotud riske ning nende tehingute vastamist klientide poolt esitatud andmetele**.

> *Teateid esitades palume järgida RABi poolt välja antud juhist. Juhised esitatava teate täitmiseks ja kahtlaste tehingute tunnuste kohta leiab RABi kodulehelt.*
>
> *RAB soovitab lähtuda tehingu kirjelduses struktureeritud narratiivist, kasutades selleks järgmist raamistikku: **mis, kes, millal, kus, miks, kuidas**.*

RAB pöörab jätkuvalt tähelepanu, et VASPide 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. Oluline on teate **terviklikkus.** Teadet esitades tuleb muuhulgas märkida, kas kliendisuhe peatati või mitte ning kas varad külmutati või mitte. Kui teates on mainitud, et kliendisuhe on plaanis üle vaadata, ootab RAB teatele jätkuteadet, kui kliendisuhte otsustatakse lõpetada.

Teade peab olema **õigesti kategoriseeritud** ning teates tuleb arusaadavalt välja tuua seos teate liigiga, näiteks sularahateadete puhul on vaja selgitada seost sularahaga. Näiteks üks levinumaid eelkuritegusid kelmus peaks olema saadetud kui STR 2.7, aga tihti esitatakse teade ekslikult kui UAR 1 või 4.

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.

Positiivne on, et mõne VASPi puhul on hästi välja toodud tehingute ja kliendikontaktidega seonduvad meta-andmed (nt IP-aadressid, MAC-aadressid jmt). Sellised andmed on RABi analüüside jaoks väga väärtuslikud.

Korrektse teate näide

Tehingu kirjeldus: *VASP sai välisriigi x politseilt taotluse kuritegevuse ennetamiseks või avastamiseks. Õiguskaitseasutuse taotluse olemus oli "tõsine ja organiseeritud kuritegevus". Nõutud teave oli seotud Isikuga x, kes oli uuritavas juhtumis huvi all seoses narkootikumide tarnimise ja rahapesuga.*

VASP tuvastas samale nimele vastava konto (rahakoti aadress: xxx).

Konto ülevaatuse käigus tuvastati järgmine teave:

1) Konto profiil:

Kasutaja üritas mitu korda edutult kinnitada oma kontot elukohatõendiga. Viimane tegevus kasutaja VASPi kontol toimus 2022. aasta septembris.

2) Konto tegevus:

Sisselogimised mitmest riigist peale elukoha (Riik y) viitavad VPN-i kasutamisele.

Kasutaja deponeeris fiati ja kasutas VASPi krüptovahetusteenuseid, et hoida ligi 1,5 aastase perioodi jooksul kahte erinevat tüüpi krüptovaluutat (XRP ja BTC).

3) Avalike allikate analüüs (OSINT):

Internetiotsing annab mitu tulemust kasutaja ebasoodsa meediateabe kohta (nime ja vanuse vastavus), mis tõendab tõsiste kuritegelike tegevustega seotud suurt riski. Järgmistes artiklites kirjeldatakse üksikasjalikult isiku osalust sellistes kuritegudes nagu mõrvakatse ja rünnak raskendavatel asjaoludel:

Artikkel 1, Artikkel 2, …

Kokkuvõte: Arvestades ülaltoodud asjaolusid ja leide, otsustati xx.xx.2023 Isiku x konto sulgeda ning teavitada sellest juhtumist RABi vastavalt RABi juhendis toodud kahtlase tegevuse tunnustele.

Kommentaar: *Teates oli selgelt ja kontsentreeritult välja toodud kahtluse sisu, kliendi ja tema tegevusega seotud ohuindikaatorid, kasutatud avalikud allikad ja rakendatud meetmed (sh konto sulgemine). Teade päädis edastusega välisriigile.*

TFR teateid esitasid 2022. aastal vaid üksikud VASPid. 2023. aastal VASP tegevusloaga teenusepakkujate arv küll vähenes, kuid TFR teateid esitavate teenusepakkujate ring laienes. 2023. aastal esitas terrorismi rahastamise teateid ligikaudu viiendik teenusepakkujatest (võrdluseks, et aasta varem esitas tegevusloaga teenusepakkujatest teateid vaid 2,5%.). Kolmandik teadetest kategoriseeriti kui TFR-2. See tähendab, et teataja jaoks esines konkreetne terrorismi rahastamise kahtlus, mitte vaid risk.

Terrorismi rahastamisele viitavate teadete esitajate arv kasvas sektoris ligi kaks korda. Lisaks tõhusamale järelevalvetegevusele võib see muu hulgas olla märk ka sektori teadlikkuse tõusust, tõhusamast hoolsusmeetmete kohaldamisest, paremast tehingute jälgimisest ja analüüsitööriistade oskuslikumast kasutamisest.

Virtuaalvääringu teenuse pakkujate hea kvaliteediga teated on andnud otsese panuse terrorismi rahastamise tõkestamisesse nii Eestis kui ka rahvusvaheliselt. Tänu sektori esitatud infokildudele on RAB saanud teha olulisi edastusi nii uurimisasutustele Eestis kui ka välisriikide rahapesu andmebüroodele.

Teateid esitanud virtuaalvääringu teenuse pakkujad näitavad üles head võimekust leida avalikest allikatest tehingu osapoole kohta täiendavat informatsiooni. Enamik virtuaalvääringu teenuse pakkujad esitab tehingu kirjelduses selge ja põhjaliku ülevaate, kasutades selleks RABi soovitatud raamistikku (mis, kes, millal, kus, miks, kuidas).

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

- Sektori suurust, mahtu ja kõrget riskitaset arvestades oli virtuaalvääringu teenuse pakkujate arv, kes terrorismi rahastamisele viitavaid teateid esitasid, sel aastal juba lähemal ootuspärasele. 2023. aastal esitas terrorismi rahastamise teateid ligikaudu viiendik teenusepakkujatest. Siiski võib see viidata asjaolule, et ülejäänud VASPidel puuduvad piisavad monitooringumehhanismid, et tuvastada terrorismi rahastamisele viitavaid ohumärke.
- Korduma kippusid TFR teated, kus esines varasem kokkupuude OFACi sanktsioneeritud üksusega, nt Iraani vahetusplatvormiga, mis on Eestile mittesiduv sanktsioon. Riskiisust tuleneva OFACi sanktsiooni kohaldamise korral, millega võib kaasneda ka kliendisuhte lõpetamine, ei ole RABile TFR teate esitamine vajalik. Niisugusel juhul on tulnud ette ka teate valesti klassifitseerimist: TFR-1 asemel ekslikult TFR-2.
- Samuti esitati teateid, kus kokkupuude potentsiaalse terroristliku üksusega oli kaudne (plokiahela analüüsi järgi *indirect exposure*). RABi hinnangul tuleb niisugusel juhul vaadelda muid asjaolusid kogumis (hoolsusmeetmete kohaldamise käigus saadud info, avalikud allikad, andmebaasid) ning hinnata ka vaheastmete arvu. Teate peab esitama, kui tegu on olnud otsese tehinguga (*direct exposure*) või kui kaudne kokkupuude on toimunud kuni mõne vaheastmega.
- Osa plokiahela analüüsi tarkvarasid kasutavad kategoriseeriat „tolm" (*dust*), kuhu liigitatakse mikroskoopilised kokkupuuted, mis n-ö päris kokkupuuteks ei kategoriseeri. Sellisel juhul ei ole terrorismi rahastamisele viitava teate esitamine põhjendatud.
- Kui teade liigitub RABi kahtlaste tehingute tunnuste juhendi järgi (vt TFi osa lk 19–22) terrorismi rahastamise kahtluseks (TFR-2), siis on kohustus hoida tehingut ja vahendeid kinni seni, kuni RAB annab tagasisidet. Kui tegu on terrorismi rahastamise riskiga ja esinevad viited terrorismi rahastamisele (juhendi järgi TFR-1), võib teataja tegutseda vastavalt riskiisule.
- Tehingu kirjelduse lahtrist peavad selguma tehingu põhiasjaolud. Ei piisa ainult lisatud failist. Sealhulgas peab tehingu kirjelduse lahtris olema välja toodud, 1) milline krüptoaadress kuulub VASPi kliendile ja 2) mis on tehingu räsi (*hash*).
- TFR-1 juures tuuakse välja küll riskiriigi seos ja indikaator, kuid jäetakse märkimata ebaharilikkusele viitav asjaolu, mille tõttu teade esitati. RAB soovitab tutvuda kahtlaste tehingute tunnuste juhendeid[9] saatvate täiendavate selgitustega.

ISR teadete arv vähenes võrreldes 2022. aastaga ning oli ligi poole võrra väiksem kui sõja esimesel aastal (2022. aastal oli 953 ja 2023. aastal 606). Eriti muret tekitav on asjaolu, et VASPide puhul vähenes perioodi lõpus teadete arv oluliselt. Kui VASPid esitasid 2021. aastal vaid 4 ISR teadet ja 2022. aastal 112, siis 2023. aastal oli vastav number 52. Teateid esitas 2023. aastal vaid 12 VASPi. Peamiselt teavitasid VASPid OFAC/OFSI sanktsioonidest – kui kliendi tehingul oli kokkupuude USA OFACi või UK OFSI poolt kehtestatud sanktsioonide all oleva teise krüptoplatvormiga.

Tegevusvaldkonda silmas pidades peaks teadete arv kõrgem olema. Teadete arvu üheks vähenemise põhjuseks on see, et ühe teatega esitati teade kümnete tehingute kohta, mis potentsiaalselt oleks võinud kõik olla eraldi teated. Samuti võeti 2023. aastal vastu vaid kolm sanktsioonipaketti ning uusi subjekte lisati nimekirjadesse vähem kui aasta varem.

[9] RAB, https://fiu.ee/oigusaktid-ja-juhendid/juhendid#juhend-kahtlaste-teh

RAB ootab sügavamat analüüsi kontrolli kriteeriumi tuvastamise osas. VASPid peavad analüüsima ka seda, kas sanktsiooni subjekt võib mingit ettevõtet või muud osapoolt kontrollida ning seeläbi tuleb ka selle ettevõte või osapoole suhtes sanktsiooni kohaldada.

VASPide puhul on läbivaks probleemiks veel teadete esitamine vale indikaatori alt. Enamasti esitavad VASPid Eestile mittekohalduva sanktsiooni rikkumisega seotud teated indikaatori ISR 1–3 alt, aga need peaks esitama indikaatoriga ISR 4 ehk mittesiduva rahvusvahelise sanktsiooni kohaldamine. Lisaks esineb palju puudusi teadete vormi täitmisel ehk jäetakse täitmata peaaegu kõik teate kohustuslikud väljad ja esitatakse enda raportid. Siinkohal eeldab RAB lisaks VASPi enda raportile ka teate vormi nõuetekohast täitmist, kus tuuakse välja sanktsiooni subjekt, režiim ja kohaldatud meede ning selle aeg.

Sektoris toimunud ning toimuvad **teatamiskohustust puudutavad edasiminekud on märkimisväärsed, kuid arenguruumi veel jagub**. Ootused teadete arvule, sisukusele, vormilisele kvaliteedile ning teatajate arvule on suuremad. Jätkuvalt on murettekitav, et mõned suured teenusepakkujad esitavaid vaid üksikuid teateid. Ebapiisavat teavitamisaktiivsust ilmestab ka asjaolu, et RAB tegeleb regulaarselt Eesti VASPide ja/või tema klientidega seotud kaasustega, kus info ei laeku mitte asjassepuutuvalt turuosaliselt, vaid kolmandalt osapoolelt või tuvastab RAB selle proaktiivselt, enda analüüsi pinnalt.

Rahapesu Andmebüroo järelevalve tähelepanekud

2023. aastal ühtegi uut VASPide järelevalvet ei alustatud, kuid tegevuslubade menetlemine paljastas mitmeid kitsaskohti turuosaliste organisatsioonilistes lahendustes. Peamised puudused, mis nähtusid tegevusloamenetluste ning varasemalt alustatud järelevalvemenetluste pinnalt, on järgmised:

- **Riskihinnangu terviklikkus**

  VASPide riskihinnangud ja muud sisemised dokumendid ei peegelda ettevõtte tegevusega kaasnevaid tegelikke riske. Riskidokumentides tuleb hinnata **kõiki** neid riske, mis tegevusega **otseselt** kaasnevad. Riskihinnangu eesmärk on tuvastada, hinnata ning analüüsida ettevõtte tegevusega kaasnevaid nii rahapesu ja terrorismi rahastamise, rahvusvahelise sanktsiooni rikkumise kui ka massihävitusrelvade leviku rahastamise riske. See tähendab, et riskihinnang peab sisaldama neid kõiki asjaolusid, mitte ainult rahapesu ja terrorismi rahastamise riskide analüüsi.

- **Riskihinnangu ja riskiisu mittevastavus ettevõtte tegeliku tegevuse ja riskidega**

  VASPid ei kajasta ja/või ei uuenda riskihinnangus ja riskiisus kõiki riske, mis nende tegevusega tegelikult kaasneb. Kui ettevõtte tehingute maht või arv, klientide arv, pakutavate teenuste maht või töötajate arv suureneb või kui laieneb geograafiline tegevus, siis vastavalt sellele tuleb ettevõttel üle vaadata ka riskihinnang ja riskiisu. Eelnevalt nimetatud asjaolud on otseselt seotud rahapesu, terrorismi rahastamise ja finantssanktsioonidega seotud riskidega.

- **Riskihinnangu ja riskiisu dokumendid ei ole omavahel kooskõlas**

  Kui ettevõtte riskihinnang on puudulik, ei ole ettevõte võimeline määratlema ka korrektset riskiisu, sest riskiisu eeltingimuseks on nõuetele vastav riskihinnang. Seetõttu jäävad ettevõttel määramata kvalitatiivsel ja kvantitatiivsel tasemel (mõõdetavad) riskid, mida kohustatud isik on valmis oma äritegevuses võtma või mida ta soovib vältida seoses rahapesu, terrorismi rahastamise ja finantssanktsioonide riskidega. Tuleb tihti ette, et ettevõte on oma riskiisus määratlenud, milliseid riske ta võtab, kuid riskihinnangus ei ole üldse vastavaid riske analüüsitud.

- **Isikusamasuse tuvastamine**

  on RAB on järelevalvetes tuvastatud mitmeid VASPide klientide isikusamasuse tuvastamisega seotud probleeme. Euroopa Nõukogu ekspertkomitee Moneyval raporti kohaselt peavad VASPid panema varasemast enam ressurssi kliendi isikusamasuse tuvastamisele, kuid VASPid tihti ei tea, kes on nende tegelikud kliendid. Tuleb meeles pidada, et tegemist on kõrge riskiga sektoriga ning suur osa VASPide klientidest on mitteresidendid, kellega kaasneb suurem rahapesu ja terrorismi rahastamise risk.

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.