7.6. Virtuālās valūtas pakalpojumu sniedzēji

Saskaņā ar Novēršanas likuma 20.panta pirmo daļu, likuma subjekts pēc darījuma attiecību uzsākšanas vai veicot gadījuma rakstura darījumus, balstoties uz noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas risku novērtējumu, pastāvīgi veic klienta darbību un darījumu uzraudzību, lai pārliecinātos, vai darījumi nav uzskatāmi par aizdomīgiem.

Virtuālās valūtas pakalpojumu sniedzējiem ir pienākums izpildīt minētas Novēšanas likumā noteiktās prasības un nodrošināt uz risku balstītu klientu darbību un darījumu uzraudzību.

Novēršanas likuma subjektam, kas darbojas kriptoaktīvu jomā, darījumu uzraudzības kontekstā jāņem vērā, ka tie tiek izmantoti dažādām noziedzīgām darbībām, tostarp noziedzīgi iegūtu līdzekļu legalizācijai, visizplatītākais līdzeklis, kas tiek izmantots šādām darbībām ir kriptovalūtu biržas. Lai konstatētu aizdomīgus darījumus kriptoaktīvu jomā var izmantot FATF apkopotos aizdomīgu aktivitāšu indikatorus kriptoaktīvu jomā, kas tiek saukti arī par "Sarkanajiem karogiem" (*red flags),* kuriem Novēršanas likuma subjektam ir jāvērš uzmanība nodrošinot darījumu uzraudzību.

Saskaņā ar FATF 2020. gada ziņojumu[1] "Sarkanie karogi" ir sagrupēti vairākās grupās, ņemot vērā personu veicamās darbības, minētās grupas ir šādas:

- Neparasti darījumu modeļi;
- Ģeogrāfiskie riski;
- Aizdomīgu lietotāju profili;
- Anonimitāte;
- Līdzekļu avots;

<u>Neparasti darījumu modeļi</u>

Neparasti darījumu modeļi, kas saistīti ar kriptovalūtu darījumu apmēru, biežumu vai veidu, var liecināt par nelikumīgi iegūtu līdzekļu legalizācijas darbībām, tostarp:

- Klienti, kas īsā laika posmā, piemēram, 24 stundu laikā, veic vairākus lielu summu pārskaitījumus;
- Darījumu summu strukturēšana tā, lai tās nepārsniegtu ziņošanas robežvērtības;
- Kriptovalūtu tūlītēja pārsūtīšana vairākiem kriptoaktīvu pakalpojumu sniedzējiem, tostarp tiem, kas reģistrēti vai darbojas citās valstīs;
- Bieži liela apjoma pārskaitījumi no vairākiem kontiem uz vienu kontu;
- Tūlītēja noguldījumu izņemšana bez darījumu vēstures, it īpaši, ja no jaunatvērtajiem kontiem tiek izņemtas lielas summas;

[1] https://www.fatf-gafi.org/en/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html

- Jauni lietotāji veic lielu sākotnējo iemaksu, lai izveidotu jaunas attiecības ar kriptoaktīvu pakalpojumu sniedzēju, kas neatbilst klienta profilam;
- Ievērojamu fiat valūtas summu konvertēšana kriptovalūtā bez saprotama ekonomiskā pamatojuma.

Ģeogrāfiskie riski

Personas, kas ir iesaistītas noziedzīgos nodarījumos, tostarp noziedzīgi iegūtu līdzekļu legalizācijā, izmanto valstis ar nepietiekamu regulējumu noziedzīgi iegūtu līdzekļu legalizācijas novēršanas jomā. Šajā sakarā jāpievērš uzmanība šādiem darījumiem:

- Kriptovalūtas līdzekļi tiek pārskaitīti uz biržām vai pakalpojumu sniedzējiem, kas atrodas reģionos, kuros ir nepilnīgs vai vispār nepastāv AML regulējums, tostarp klienta padziļinātas pārbaudes vai "pazīsti savu klientu" pasākumi neatbilsts starptautiskām AML prasībām;
- Klienti, kas nosūta vai saņem līdzekļus no biržām, kas atrodas citās valstīs, nevis tajā, kurā klients dzīvo vai darbojas;
- Klienti, kas izveido birojus vai pārvieto tos uz valstīm, kurās nav regulējuma attiecībā uz darbu ar kritoaktīviem vai tas nav ieviests.

Anonimitāte

Personām, kas ir iesaistītas noziedzīgos nodarījumos, kriptoaktīvus padara pievilcīgākus dažādas tehnoloģiskās iespējas, kas palielina anonimitāti. Darījumos ar kriptoaktīviem ir iespējams izmantot dažādas tehnoloģijas, kas ir unikālas tikai kriptoaktīviem, piemēram, *peer-to-peer* apmaiņas vietnes, sajaukšanas vai miksēšanas pakalpojumi vai kriptoaktīvi ar paaugstinātu anonimitāti. Šādu tehnoloģiju izmantošana sarežģi tiesībaizsardzības iestāžu izmeklēšanu un var liecināt par nelikumīgām darbībām. Tomēr ne vienmēr minēto vai līdzīgu tehnoloģiju izmantošana liecina par noziedzīgiem nodarījumiem. Tādēļ virtuālās valūtas pakalpojumu sniedzējiem darījumi ar jaunu tehnoloģiju izmantošanu ir jāizvērtē individuāli. Šāda veida darbību indikatori ir šādi:

- Klienti, kuri pārvieto līdzekļus no publiskām blokķēdēm uz biržām, kur līdzekļi tiek nekavējoties konvertēti privātuma monētās;
- Klienti, kas darbojas kā nelicencēti pakalpojumu sniedzēji kriptoaktīvu jomā *peer- to- peer* apmaiņas tīmekļa vietnē;
- Lietotāji, kuri regulāri veic augstvērtīgus darījumus *peer – to peer* kriptobiržās, īpaši nelicencētās;
- Bieži vai liela apjoma darījumi platformās, kas piedāvā kriptoaktīvu sajaukšanas pakalpojumus, lai slēptu līdzekļu izcelsmi;

- Klienti, kuri bieži veic augstvērtīgus darījumus platformās, kas neatbilst starptautiskajiem standartiem attiecībā uz "pazīsti savu klientu" (KYC) vai klienta uzticamības pārbaudes (CDD) procedūrām;
- Vairāki darījumi, kuros iesaistīti kriptoakīvu bankomāti, kas bieži atrodas apgabalos ar zināmu finanšu noziegumu risku;
- Starpniekserveru vai citu pakalpojumu izmantošana, kas paredzēti, lai slēptu IP adreses un domēnu nosaukumus, reģistrējoties apmaiņai.

Aizdomīgu lietotāju profili

Uzņēmumiem "pazīsti savu klientu" posmā ir jāpārtrauc darījumu attiecības ar klientu, ja tā identifikācijas dokumenti ir nepilnīgi vai nepietiekami, vai ja ir aizdomas, ka tie ir viltoti. Turklāt ir jāpievērš uzmanība personu uzvedībai, ir dažādi aizdomīgi uzvedības veidi, kas pakalpojumu sniedzējiem būtu jāņem vērā kā "sarkanie karogi":

- Darījumi, kas veikti no neuzticamām IP adresēm vai domēniem, kuri atšķiras no valsts, kurā klients darbojas vai dzīvo;
- Vairāki kriptoaktīvu maki, kurus kontrolē viena un tā pati IP adrese;
- Regulāra kriptoaktīvu izmantošana, kas saistīta ar krāpniecisku rīcību vai Ponzi shēmām;
- Klienti, kuri bieži maina savu kontaktinformāciju un identifikācijas informāciju;
- Klienti, kas izmanto vairākas IP adreses, lai veiktu darījumus vai piekļūtu kriptogrāfijas platformām;
- Klienti, kuri bieži veic darījumus ar vieniem un tiem pašiem sūtītājiem vai saņēmējiem, radot ievērojamus ieguvumus vai zaudējumus;
- Sūtītāji, kuriem nav izpratnes par kriptoaktīvu jomu (tostarp, bet ne tikai, vecāka gadagājuma cilvēkiem), tomēr tie joprojām veic regulārus vai augstvērtīgus darījumus;
- Klienta kriptoaktīvu pirkumi pārsniedz tā oficiālos ienākumus.

Līdzekļu avots

Finansējuma avoti var identificēt daudzas nelikumīgi iegūtu līdzekļu legalizācijas operācijas. Piemēram:

- Līdzekļi, kas saistīti ar kontiem, kuri saistīti ar zināmām nelikumīgām darbībām, piemēram, krāpšanu, izspiedējprogrammatūru, izspiešanu, tumšā tīkla tirgiem (*darknet*) vai nelegālām azartspēļu vietnēm;
- Kriptoaktīvu maki, kas savienoti ar vairākām kredītkartēm, ar kurām izņem ievērojamas fiat valūtas summas;

- Līdzekļi, kas iegūti no sākotnējiem monētu piedāvājumiem (ICO), kas var būt krāpnieciski, trešo pušu sajaukšanas pakalpojumi vai platformas, kas neatbilst AML standartiem;
- Būtiski noguldījumi, kas tiek tieši konvertēti privātuma monētās vai izņemti citā fiat valūtā.

Katrā no kategorijām noziedzīgu darbību konstatēšanai nepietiek tikai ar viena indikatora konstatēšanu, bieži tieši vairāku augstāk minēto indikatoru klātbūtne darījumos bez loģiska izskaidrojuma rada aizdomas par varbūtējām noziedzīgām aktivitātēm, tādēļ, lai rīkotos, nepieciešams konstatēt vairākus "sarkanos karogus" vienlaicīgi. Vairāku indikatoru klātbūtnei jāveicina turpmāka darījumu uzraudzība, pārbaude un ziņošana vajadzības gadījumā.

Būtiski ņemt vērā, ka noziedzīgi iegūtu līdzekļu legalizācijas "sarkanie karogi" un pazīmes attīstās un mainās, jo personas, kuras īsteno noziedzīgas darbības sava labuma gūšanai, atrod arvien jaunus veidus un metodes attiecīgo noziedzīgo darbību īstenošanai. Vadlīnijās ietverto pazīmju uzskaitījums nav uzskatāms par izsmeļošu, kā arī norādāms, ka katra pazīme pati par sevi neliecina par noziedzīgām darbībām.