LIETUVOS BANKAS
EUROSISTEMA

Nuolatinės kliento dalykinių santykių ir operacijų (sandorių) stebėsenos apžvalga

Analizė ir tyrimai

2022 / Nr. 15

Serija „Analizė ir tyrimai“
2022 / Nr. 15

ISSN 2538-9386 (ONLINE)

Nuolatinės kliento dalykinių santykių ir operacijų (sandorių) stebėsenos apžvalga

Dokumentą parengė
Finansinių paslaugų ir rinkų priežiūros departamento
Pinigų plovimo prevencijos skyrius
Pasiteirauti:
info@lb.lt
+370 800 50 500

Gedimino pr. 6, LT-01103 Vilnius
www.lb.lt

TURINYS

Santrumpos ir kiti paaiškinimai

EK	Europos Komisija
ES	Europos Sąjunga
EEE	Europos ekonominė erdvė
EBI rizikos veiksnių gairės	Europos bankininkystės institucijos 2021 m. kovo 1 d. gairės pagal Direktyvos (ES) 2015/849 17 straipsnį ir 18 straipsnio 4 dalį dėl deramo klientų tikrinimo ir veiksnių, į kuriuos kredito ir finansų įstaigos turėtų atsižvelgti vertindamos su atskirais dalykiniais santykiais ir vienkartiniais sandoriais ir (ar) operacijomis susijusią PPTF riziką, kuriomis panaikinamos ir pakeičiamos Gairės JC/2017/37
FNTT	Finansinių nusikaltimų tyrimo tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos
FRD	finansų rinkos dalyvis
FATF	Finansinių veiksmų darbo grupė kovai su pinigų plovimu ir teroristų finansavimu
IT	informacinės technologijos
KYC	deramo kliento tikrinimo informacija
nurodymai	FRD skirti nurodymai, kuriais siekiama užkirsti kelią pinigų plovimui ir (arba) teroristų finansavimui, patvirtinti Lietuvos banko valdybos 2015 m. vasario 12 d. nutarimu Nr. 03-17 „Dėl Finansų rinkos dalyviams skirtų nurodymų, kuriais siekiama užkirsti kelią pinigų plovimui ir (arba) teroristų finansavimui, patvirtinimo“
OEDD	sustiprintas didelės PPTF rizikos grupės klientų patikros ir stebėsenos procesas dalykinių santykių metu (angl. *ongoing enhanced due diligence*)
operacijos	mokėjimo operacijos ir (arba) sandoriai
PEP	politiškai pažeidžiami (paveikiami) asmenys
PPTF	pinigų plovimas ir (ar) teroristų finansavimas
PP	pinigų plovimas
PPTFP	pinigų plovimo ir (ar) teroristų finansavimo prevencija
pranešimai FNTT	pranešimas apie įtartinas pinigines operacijas ar sandorius FNTT
PPTFPĮ	Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymas
stebėsena	nuolatinė kliento dalykinių santykių ir operacijų (sandorių) stebėsena
TF	teroristų finansavimas
VSD	Lietuvos Respublikos valstybės saugumo departamentas

1. APŽVALGOS TIKSLAS

Lietuvos bankas, atlikdamas rizikos vertinimu pagrįstą priežiūrą, pastebi, kad FRD kyla klausimų, susijusių su stebėsenos įgyvendinimu praktikoje. Šioje apžvalgoje trumpai apžvelgiamas stebėsenos organizavimo ir įgyvendinimo tikslas, stebėsenos modelio (sistemos) ir sprendimų nustatymas ir jų sąveika, atskirų stebėsenos sprendimų, įskaitant stebėsenos scenarijus, pritaikymas pagal FRD verslo modelį ir turimą klientų portfelį, stebėsenos sprendimų, įskaitant automatinius scenarijus, periodinė peržiūra ir testavimas. Šioje apžvalgoje siekiama trumpai pristatyti ir galimus stebėsenos sprendimus didesnės PPTF rizikos atvejais, automatinės stebėsenos sistemos sugeneruotų įspėjimų (angl. *alerts*) peržiūros ir išsamesnių vidaus tyrimų vykdymo proceso geriausią patirtį bei praktinių netinkamai vykdytų vidaus tyrimų pavyzdžių.

Apžvalgoje remiamasi Lietuvos Respublikos teisės aktų nuostatomis, tarptautinių organizacijų, kitų priežiūros institucijų ir Lietuvos bankui vykdant priežiūros funkcijas pastebėta finansų įstaigų geriausia patirtimi.

2. STEBĖSENOS ORGANIZAVIMO IR ĮGYVENDINIMO PAGRINDAS BEI TIKSLAS

PPTFPĮ 29 straipsnio 1 dalies 3 punkte nurodyta, kad FRD privalo nustatyti vidaus kontrolės procedūras, susijusias su dalykinių santykių ir (arba) operacijų stebėsenos organizavimu. PPTFPĮ 9 straipsnio 16 dalyje įtvirtinta pareiga FRD vykdyti nuolatinę kliento dalykinių santykių stebėseną, įskaitant sandorių, kurie buvo sudaryti tokių santykių metu, tyrimą, siekiant užtikrinti, kad vykdomi sandoriai atitiktų FRD turimas žinias apie klientą, jo verslą, rizikos pobūdį ir lėšų šaltinį. PPTFPĮ 16 straipsnio 2 dalyje numatytas reikalavimas FRD nustačius, kad jų klientas atlieka įtartiną piniginę operaciją ar sandorį, nepaisant piniginės operacijos ar sandorio sumos, tą operaciją ar sandorį sustabdyti (išskyrus atvejus, kai dėl piniginės operacijos ar sandorio pobūdžio, jų atlikimo būdo ar kitų aplinkybių to padaryti objektyviai neįmanoma) ir ne vėliau kaip per 3 darbo valandas nuo piniginės operacijos ar sandorio sustabdymo apie šią operaciją ar sandorį pranešti FNTT. PPTFPĮ 17 straipsnio 1 dalyje įtvirtinta pareiga FRD atkreipti dėmesį į tokią veiklą, kuri dėl savo pobūdžio gali būti susijusi su PPTF, o ypač į sudėtingus ar neįprastai didelius sandorius ir visas neįprastas sandorių struktūras, kurios neturi akivaizdaus ekonominio ar matomo teisėto tikslo, dalykinius santykius ar piniginės operacijas su klientais iš trečiųjų valstybių, kuriose pagal tarptautinių tarpvyriausybinių organizacijų oficialiai paskelbtą informaciją PPTF prevencijos priemonės yra nepakankamos ar neatitinka tarptautinių standartų. To paties straipsnio 2 dalyje nurodyta, kad FRD privalo išnagrinėti tokių operacijų ar sandorių vykdymo pagrindą bei tikslą, tyrimo rezultatus įforminti raštu ir spręsti dėl pranešimo apie įtartiną operaciją ar sandorį perdavimo FNTT.

Nurodymų VIII skyriuje papildomai išsamiau aprašyti FRD taikomi stebėsenos reikalavimai (plačiau žr. kituose skyriuose).

EBI rizikos veiksnių gairių 4.72–4.75 punktuose nurodyta, kad FRD turėtų užtikrinti, jog jų sandorių stebėsenos metodas būtų veiksmingas ir tinkamas. Veiksminga operacijų stebėsenos sistema pagrįsta naujausia informacija apie klientą ir turėtų suteikti FRD galimybę patikimai nustatyti neįprastus ir įtartinus sandorius bei neįprastų struktūrų sandorius. FRD turėtų užtikrinti, kad jų taikomos procedūros yra skirtos pažymėtiems (angl. *flagged*) sandoriams peržiūrėti nedelsiant. Kokios stebėsenos procedūros yra tinkamos, priklausys nuo FRD veiklos pobūdžio, dydžio ir sudėtingumo, nuo FRD patiriamos PPTF rizikos. EBI rizikos veiksnių gairėse nurodyta, kad FRD turėtų koreguoti stebėsenos intensyvumą ir dažnumą laikydamiesi rizika grindžiamo metodo (angl. *risk based approach*). Kiekvienu atveju FRD turėtų nuspręsti, kuriuos sandorius jie stebės realiuoju laiku (momentinė stebėsena), o kuriuos – *ex post* (retrospektyviai). FRD turi nuspręsti, ar operacijas FRD stebės rankiniu būdu, ar naudos automatizuotą operacijų stebėsenos sistemą. Atkreiptinas dėmesys, kad daug operacijų vykdantys FRD turėtų apsvarstyti galimybę įdiegti automatizuotą operacijų stebėsenos sistemą. Kaip nurodyta EBI rizikos veiksnių gairių 4.75 punkte, be atskirų operacijų stebėsenos realiuoju laiku bei retrospektyviai ir nepriklausomai nuo taikomo automatizavimo lygio, FRD turėtų reguliariai atlikti visų apdorotų operacijų imties retrospektyvias peržiūras ir nustatyti tendencijas, kurios galėtų padėti

įvertinti riziką ir išbandyti, o prireikus vėliau pagerinti savo operacijų stebėsenos sistemos patikimumą ir tinkamumą.

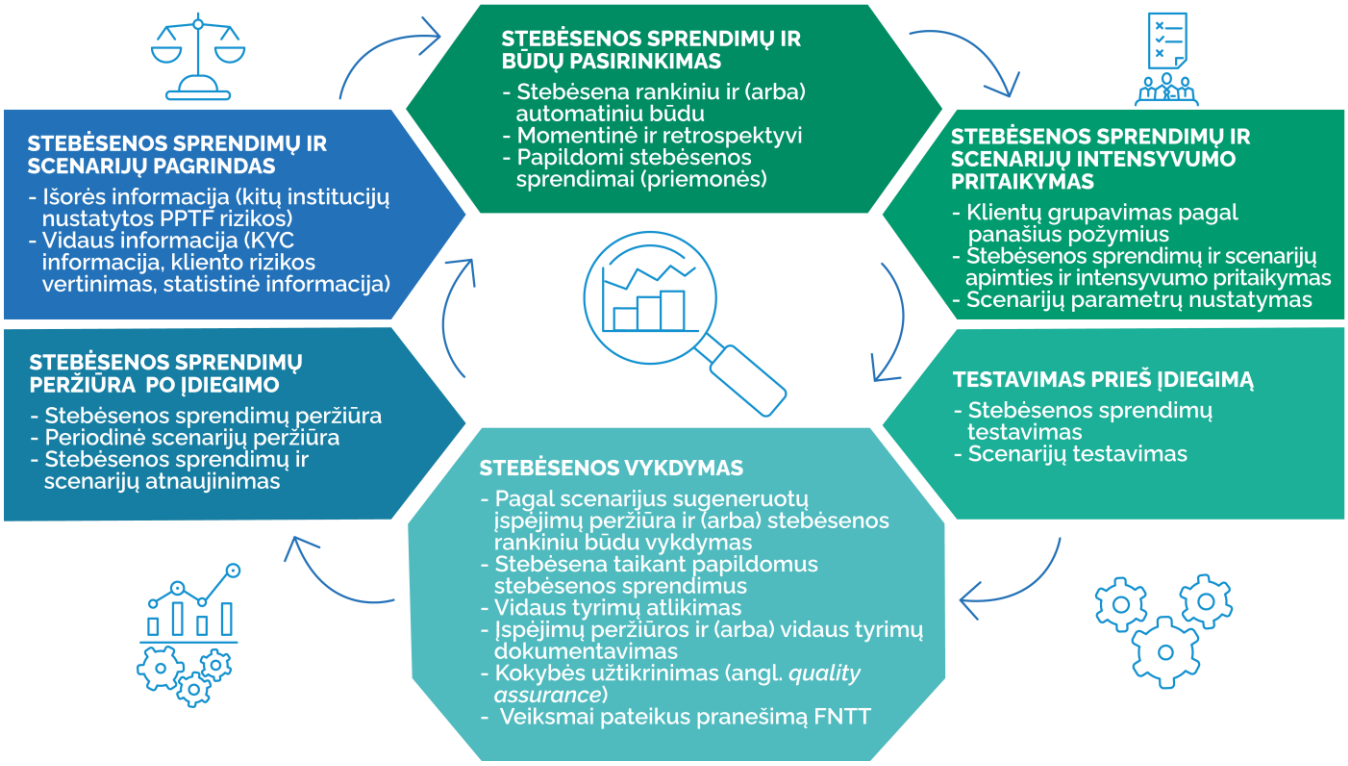
Pirmiausia pažymėtina, kad stebėsenos sprendimai, būdai bei FRD darbuotojų pareigos ir privalomi atlikti veiksmai vykdant stebėseną turėtų būti aiškiai reglamentuoti FRD vidaus kontrolės procedūrose. Be to, praktikoje atliekami stebėsenos procesai turėtų atitikti FRD vidaus kontrolės procedūrose nustatytus procesus. Pavyzdžiui, neturėtų būti situacijų, kai FRD, atsižvelgdamas į įvairias PPTF grėsmes, sukuria stebėsenos modelį ir konkrečius stebėsenos sprendimus bei priemones įtvirtina savo vidaus procedūrose, tačiau praktikoje šie FRD procedūrose nustatyti sprendimai dėl darbuotojų trūkumo ar kitų priežasčių nėra taikomi.

Pabrėžtina, kad FRD, vykdydami stebėseną, turėtų vadovautis rizika grindžiamu metodu. Rizika grindžiamas metodas reiškia, kad FRD privalo daugiausia dėmesio ir išteklių skirti toms sritims, kurios kelia didžiausią PPTF riziką. FRD, vykdydami stebėseną, privalo gebėti pagrįsti pasirinktą stebėsenos modelį, konkrečius stebėsenos sprendimus ir taikomas priemones.

Gerai, veiksmingai ir efektyviai veikiantis stebėsenos modelis yra pagrįstas optimaliais stebėsenos sprendimais, kurie parinkti atsižvelgiant į FRD veiklos mastą ir verslo modelį. FRD nustatytas stebėsenos modelis privalo būti pagrįstas FRD žiniomis tiek apie egzistuojančias PPTF rizikas, tiek apie kylančias naujas rizikas (angl. *emerging risks*), tiek geru FRD supratimu apie savo klientų bazę, nes tai leidžia geriau atpažinti neįprastą kliento veiklą ir įvertinti, ar tokia kliento veikla galėtų būti pagrįstai laikoma įtartina. Siekiant turėti veiksmingą stebėsenos modelį, labai svarbus FRD klientų portfelio grupavimas, kuriuo remiantis būtų kuriami stebėsenos scenarijai ir diegiami papildomi stebėsenos sprendimai, kurie vėliau turėtų būti testuojami, nuolat peržiūrimi bei atnaujinami.

Kitas ne mažiau svarbus žingsnis yra praktinis stebėsenos vykdymas ir stebėsenos metu surinktos informacijos panaudojimas ne tik siekiant FRD geriau suprasti savo klientų portfelį, bet ir stebėsenos modelio bei taikomų sprendimų tobulinimo tikslais. Atitinkamai padaryta išvada, kad visi šie procesai yra tarpusavyje glaudžiai susiję ir turi vienas kitą nuolat papildyti (žr. 1 pav.).

1 pav. Stebėsenos sistemos ciklas



Pažymėtina, kad teisės aktuose imperatyviai nenustatyta pareiga FRD taikyti automatinę stebėseną. FRD pasirinktas stebėsenos organizavimo modelis ir būdas turi būti proporcingas FRD veiklos mastui ir gebėjimui užtikrinti tinkamą PPTF rizikų valdymą. Dažnu atveju FRD (kurių veiklos mastas yra didesnis ir FRD neturi pakankamai galimybių operacijų peržiūrėti neautomatizuotu būdu) turėtų įvertinti automatinės stebėsenos sistemos, kuri generuos įspėjimus apie neįprastas ir (arba) įtartinas operacijas įdiegimą. Siekdami nustatyti tokias operacijas, FRD turėtų nustatyti ir suprasti neįprastos ir (arba) įtartinos veiklos požymius (angl. *red flags*) ir juos įtraukti į naudojamus automatinės stebėsenos sistemos scenarijus (angl. *business rules*). Pažymėtina, jog tuo atveju, kai FRD pasirenka taikyti vien tik stebėsenos rankiniu būdu sprendimus, lygiai taip pat turėtų užtikrinti, kad turi pakankamai darbuotojų tokiai stebėsenai vykdyti, kad operacijas peržiūri laiku, operacijų peržiūrą vykdo struktūruotai, remdamiesi pasirinktomis taisyklėmis (pvz., nustatytais kriterijais, kokios operacijos turi būti išsamiau peržiūrimos retrospektyviai), kodėl pasirinkti būtent tokios taisyklės bei privalo periodiškai peržiūrėti ir vertinti tokių taisyklių ir kriterijų veiksmingumą. Taip pat turėtų užtikrinti tiek retrospektyvią (jau įvykdytų operacijų analizę), tiek momentinę (prieš įvykdant kliento operaciją ir (arba) operacijos atlikimo metu) stebėseną.

3. STEBĖSENOS SPRENDIMŲ IR SCENARIJŲ PASIRINKIMO BEI NUSTATYMO PAGRINDAS

Nurodymų reikalavimai
60. FRD privalo užtikrinti, kad kliento dalykinių santykių ir (arba) operacijų (sandorių) stebėsenos procesas yra organizuojamas atsižvelgiant į FRD atlikto visos veiklos PPTF rizikos vertinimo rezultatus. Tai reiškia, kad, identifikavęs didesnės rizikos sritis (pvz., klientai iš didelės rizikos šalių, klientų veikla susijusi su didesne PPTF rizika, FRD siūlomo produkto specifika sudaro palankesnes sąlygas pinigų plovimui ar teroristų finansavimui ar kt.), FRD privalo pritaikyti stebėsenos intensyvumą, apimtį, scenarijus ir nustatyti atitinkamus stebėsenos kriterijus, kad galėtų laiku ir efektyviai aptikti ir nustatyti kliento atliekamas įtartinas operacijas ar sandorius. 63. FRD privalo turėti veiklos mastą ir pobūdį atitinkančias priemones, kurios užtikrina veiksmingą dalykinių santykių ir operacijų (sandorių) stebėseną.

Nurodymuose įtvirtintas reikalavimas kyla iš to, kad FRD visos veiklos PPTF rizikos vertinimo procese turėtų atsispindėti visos PPTF rizikos, aktualios konkrečiam FRD. Įprastai informacija, naudojama atlikti visos veiklos PPTF rizikos vertinimą, apima tiek išorės, tiek FRD vidaus informaciją. Šaltinius, kuriais rekomenduojama remtis nustatant stebėsenos sprendimus ir diegiant konkrečius stebėsenos scenarijus, galima suskirstyti į dvi pagrindines grupes: išorės ir vidaus. Pirmiausia atkreiptinas dėmesys, kad šių šaltinių panaudojimas neturi būti vienkartinis veiksmas. Priešingai, procesas, kurio metu peržiūrimi FRD naudojami stebėsenos sprendimai, įskaitant konkrečius scenarijus, ir atitinkamai įvertinamas poreikis stebėsenos sprendimus papildyti arba koreguoti, siekiant veiksmingai valdyti PPTF riziką, turi būti tęstinis ir pasikartojantis.

Toliau pateikiamas pavyzdinis išorės ir vidaus šaltinių, kuriais FRD turėtų remtis nustatydamas stebėsenos procesus, sąrašas. Šis sąrašas sudarytas remiantis EBI rizikos veiksnių gairių 1.29–1.32 punktais ir geriausia patirtimi, tačiau pažymėtina, kad pateikiamas sąrašas nėra baigtinis (žr. 2 pav.).

2 pav. Pavyzdinis išorės ir vidaus šaltinių sąrašas

Išorės šaltiniai	FRD vidaus šaltiniai
• EK PPTF rizikos vertinimas • Lietuvos nacionalinis PPTF rizikos vertinimas • FNTT pinigų operacijų ar sandorių įtartinumo atpažinimo kriterijai • FNTT PPTFP metinė ataskaita • VSD grėsmių nacionaliniam saugumui vertinimas • EBI gairės ir rekomendacijos • FATF rekomendacijos ir perspėjimai • Interpolo, Europolo ir (ar) vietinių teisėsaugos institucijų skelbiami perspėjimai ar tipologijų analizės • Tarptautinių ar kitų priežiūros institucijų gairės, geriausia patirtis • ES parengtas didelės PPTF rizikos valstybių sąrašas • FATF parengtas didelės rizikos valstybių sąrašas	• FRD visos veiklos PPTF rizikos vertinimas • Kylančios naujos rizikos • Klientų portfelio ar teikiamų paslaugų pokyčiai • FRD klientų deramo tikrinimo metu surinkta informacija • Individualus klientų PPTF rizikos vertinimas • Klientų portfelis (pagal klientų ekonominės veiklos grupes (segmentus)) • Vidaus ar išorės auditų rekomendacijos • Darbuotojų darbo kokybės patikros rezultatai • Aktuali klientų elgesio (operacijų) statistinė informacija • FRD žinios ir profesinė patirtis • Atliktų vidaus tyrimų analizės rezultatai • Pateiktų pranešimų FNTT analizė

FRD, pasirinkdami stebėsenos sprendimus (priemones) ir nustatydami stebėsenos scenarijus, pirmiausia turėtų atsižvelgti į **išorės šaltinius**. Pagrindiniai išorės šaltiniai yra EK PPTF rizikos vertinimas[1] (SNRA) ir 2020 m. nacionalinis PPTF rizikos vertinimas[2] (NRV). Juos atliekant PPTF rizikos nustatomos ir vertinamos ES ir Lietuvos Respublikos mastu. Atliekant šiuos PPTF rizikos vertinimus, išskiriamos atskiriems finansų sektoriams (pvz., bankų, kredito unijų, elektroninių pinigų ir mokėjimo įstaigų (EPĮ ir MĮ), finansų maklerio ir valdymo įmonių ir t. t.) ir ne finansų sektoriams (pvz., azartinių lošimų, nekilnojamojo turto, tauriųjų metalų, patikos bendrovių administratorių, ne pelno organizacijų, laisvųjų prekybos zonų ir t. t.) būdingos PPTF rizikos. Kalbant apie ne finansų sektoriui būdingas PPTF rizikas, tai ypač aktualu, jeigu FRD aptarnauja klientus iš šių sektorių. Pavyzdžiui, 2020 m. paskelbtame NRV išskirtas stebėsenos scenarijų, skirtų teroristų finansavimo atvejams nustatyti, trūkumas; nurodyta, kad EPĮ ir MĮ sektoriuje kai kurios įstaigos nevykdo retrospektyvios stebėsenos; taip pat išskirtos įvairios PPTF rizikos, susijusios su fiktyviomis paslaugomis ir fiktyviomis įmonėmis. FRD diegiant stebėsenos sprendimus, įskaitant konkrečius stebėsenos scenarijus, rekomenduojama atsižvelgti į FNTT nustatytus pinigų operacijų ar sandorių įtartinumo atpažinimo kriterijus[3], FNTT periodiškai skelbiamus perspėjimus bei metines FNTT veiklos PPTF prevencijos srityje ataskaitas[4], kuriose išsamiau aprašomos stebimos tipologijos, susijusios su pinigų plovimu ir (ar) teroristų finansavimu. FRD nustatant stebėsenos priemones, aktuali kasmet skelbiamoje VSD grėsmių nacionaliniam saugumui vertinimo ataskaitoje pateikiama informacija[5].

Apžvelgiant į kitus išorės šaltinius, paminėtina, kad tiems FRD, kurie veikia ne tik Lietuvoje, tačiau ir kitose valstybėse, turi klientų, kurie reziduoja ne Lietuvoje, vykdo tarptautinius mokėjimus, yra aktualios pasaulinės

[1] 2019 m. EK PPTF rizikos vertinimas (*Report from the Commission to the European Parliament and the Council*)

(https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union_-_annex.pdf).

[2] 2020 m. nacionalinis PPTF rizikos vertinimas (http://www.fntt.lt/data/public/uploads/2020/05/final-nra_lt_v3.pdf).

[3] Galimo pinigų plovimo ir įtartinų piniginių operacijų ar sandorių atpažinimo kriterijų sąrašas, patvirtintas Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2014 m. gruodžio 5 d įsakymu Nr. V-240 „Dėl Galimo pinigų plovimo ir įtartinų piniginių operacijų ar sandorių atpažinimo kriterijų sąrašo patvirtinimo" (https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/13a1a7307fef11e49386e711974443ff/asr).

[44] FNTT Pinigų plovimo ir teroristų finansavimo prevencijos ataskaitos (http://www.fntt.lt/lt/pinigu-plovimo-prevencija/veikla/ataskaitos/73).

[5] https://www.vsd.lt/gresmes/metiniai-gresmiu-vertinimai/

PPTF rizikos, todėl labai svarbu atkreipti dėmesį į tarptautinių institucijų, tokių kaip FATF, Interpolo, Europolo, skelbiamus pranešimus, periodiškai atliekamus organizuoto nusikalstamumo Europoje grėsmės vertinimus (angl. *Serious and Organised Crime Threat Assessment,* SOCTA)[6], kitų valstybių (pvz., Jungtinės Karalystės policijos, Jungtinės Karalystės privačiojo ir viešojo sektorių partnerystės (*Joint Money Laundering Intelligence Taskforce,* JMLIT), JAV Finansinių nusikaltimų tyrimo tinklo (*Financial Crimes Enforcement Network,* FinCEN) skelbiamas įvairias tipologijų analizes ar perspėjimus, be to, labai naudingos *Egmont* grupės skelbiamos tikrų bylų analizės ir tipologijos[7]. Rekomenduojama įvertinti ir Jungtinių Tautų narkotikų kontrolės ir nusikalstamumo prevencijos biuro (UNODC) skelbiamas analizes ir pranešimus[8].

Visi šie išorės šaltiniai leidžia atsižvelgti į operacijų geografines kryptis, klientų įsisteigimo arba rezidavimo valstybes, pilietybes, regionui būdingas tipologijas, kaip, pavyzdžiui, tranzitinės sąskaitos, fiktyvios įmonės, socialinės inžinerijos sukčiavimas, pinigų mulai (angl. *money mules*)[9]. Pažymėtina, kad, remiantis EBI rizikos veiksnių gairėmis bei FATF[10] rekomendacijomis, tiek momentinės, tiek retrospektyvios operacijų stebėsenos taisyklės turėtų būti peržiūrimos ir koreguojamos atsižvelgiant į EK (viršnacionalinį), nacionalinį ir FRD visos veiklos PPTF rizikos vertinimą bei FRD darbuotojų, vykdančių PPTF prevencijos funkcijas, pastebėjimus. Vadovaujantis Europos Tarybos Kovos su pinigų plovimu ir terorizmo finansavimu priemonių įvertinimo ekspertų komiteto (*Moneyval*) 2018 m. ataskaita[11] ir EK rizikos vertinimu, pagrindinės rizikos, į kurias FRD svarbu atkreipti dėmesį, yra grynųjų pinigų, nerezidentų vykdomos operacijos, tarpininkų kontrolė, tarpvalstybinės operacijos, sukčiavimas (įskaitant elektroninį), dokumentų padirbinėjimas, fiktyvios įmonės, prekyba narkotikais, mokesčių vengimas, kontrabanda ir kt. Remiantis UNODC informacija, pagrindinės pastebimos nusikalstamų veikų tipologijos yra prekyba narkotikais, nelegali prekyba ginklais, prekyba žmonėmis, kyšininkavimas ir korupcija, mokesčių vengimas, reketas, kibernetinis sukčiavimas. Panašiai nurodyta ir SOCTA vertinimo ataskaitoje, kurioje nurodoma, kad apie 80 proc. nusikalstamų grupuočių, veikiančių ES, yra susijusios su prekyba narkotikais, organizuotais turtiniais nusikaltimais, akcizo sukčiavimais (pvz., pasitelkiant cigarečių, alkoholio gamybą arba kontrabandą), prekyba žmonėmis, internetiniais ir kitais sukčiavimais arba neteisėta imigracija (apie 40 proc. jų susiję su prekyba narkotikais). Ataskaita naudinga ir vertinant atskirų ES valstybių keliamą geografinę riziką, nes joje pateikti narkotikų įvežimo į ES maršrutai iš Afrikos, Artimųjų Rytų, Azijos. Taip pat pateikiamas ES valstybių sąrašas, kuriose daugiausia pagaminama sintetinių narkotikų ir pan. Be to, ataskaitoje pažymima, kad Europoje tam tikros tipologijos kiekvienais metais vis plečiasi (pvz., kokaino įvežimas į ES iš Lotynų Amerikos, kibernetiniai nusikaltimai, seksualinis vaikų išnaudojimas internete, nusikaltimai, susiję su atliekų utilizavimu). Šioje ataskaitoje pažymima, kad nusikaltėliai naudojasi korupcija (nuo žemiausių iki aukščiausių viešojo administravimo sluoksnių). Apie 80 proc. nusikalstamų grupuočių naudojasi juridiniais asmenimis siekdami vykdyti pinigų plovimą, apie pusė nusikalstamų grupuočių įsteigia savo bendroves pinigų plovimo tikslais, o apie 80 proc. tarptautinės prekybos vyksta tiesiogiai atliekant mokėjimo pavedimus tarp klientų sąskaitų (t.y. be papildomo kredito įstaigų tarpininkavimo suteikiant banko garantijas, akredityvus), todėl labai svarbu gilinti žinias prekybos finansavimo tipologijoje (angl. *trade-based money laundering*) ir atitinkamai taikyti stebėsenos sprendimus. Toje pačioje ataskaitoje nurodoma, kad organizuotų nusikalstamų grupių naudojami pinigų plovimo būdai varijuoja nuo paprasčiausių – investavimo į nekilnojamąjį turtą arba aukštos vertės prekes – iki sudėtingesnių pinigų

[6] https://www.europol.europa.eu/socta-report

[7] 2014–2020 m. bylų analizė (https://egmontgroup.org/en/filedepot_download/1661/125), 2011–2013 m. bylų analizė (https://egmontgroup.org/en/filedepot_download/1661/33), 2015 m. 100 bylų analizė su nurodytais įtartinumo kriterijais (https://www.jfiu.gov.hk/info/doc/21-100casesgb.pdf).

[8] https://www.unodc.org/documents/money-laundering/Model_Provisions_Final.pdf.

[9] FNTT Pinigų plovimo ir teroristų finansavimo prevencijos ataskaitos (https://www.fntt.lt/lt/pinigu-plovimo-prevencija/veikla/ataskaitos/73).

[10] FATF rekomendacijos „Anti-Money Laundering and terrorist Financing Measures and Financial Inclusion" (http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf).

[11] *Moneyval* ataskaita, 2018 „Anti-money laundering and counter-terrorist financing measures Lithuania" (https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/Moneyval-Mutual-Evaluation-Report-Lithuania-2018.pdf).

plovimo būdų, pvz., per prekybos finansavimą naudojant daug skirtingų bendrovių (įskaitant fiktyvių[12]), per verslus, kuriuose vyrauja grynieji pinigai, ir pan.

Labai svarbu akcentuoti, kad šiuose šaltiniuose nurodyta informacija turėtų būti panaudojama ne tik priimant sprendimus dėl stebėsenos priemonių ar scenarijų, tačiau yra nepakeičiama vykdant vidaus tyrimus, rengiant vidaus tyrimams naudingas instrukcijas, gaires, tipologijų apžvalgas, mokymų medžiagą darbuotojams ir supažindinant darbuotojus su įtartinos veiklos požymiais.

Diegiant stebėsenos sprendimus (priemones) ir naujus stebėsenos scenarijus, FRD reikėtų atsižvelgti į **vidaus informaciją, statistiką ir duomenis**, susijusius su konkrečiu FRD, pavyzdžiui, FRD verslo modeliu, klientų portfeliu, klientų vykdomos veiklos pobūdžiu, tikslinėmis klientų grupėmis ir jų specifika, mokėjimų pobūdžiu, klientų rezidavimo valstybėmis, valstybėmis, kurių piliečiai yra FRD klientai, atliekamų mokėjimo operacijų kryptimis pagal užsienio valstybes, teikiamomis paslaugomis, siūlomais produktais ir paslaugų teikimo kanalais. Nustatyti PPTF riziką įstaigoje padeda tinkamai ir išsamiai atliktas visos veiklos PPTF rizikos vertinimas[13] (toliau – rizikos vertinimas). Tinkamai atliktas rizikos vertinimas, kaip nurodyta pirmiau, yra vienas iš pagrindinių vidaus dokumentų, kurio pagrindu sprendžiama dėl stebėsenos modelio ir konkrečių taikytinų FRD stebėsenos sprendimų ir priemonių. Rizikos vertinimo pagrindu kuriami ir (arba) atnaujinami stebėsenos scenarijai ir atitinkamai užtikrinamas veiksmingas scenarijų įgyvendinimas praktikoje.

Rinkdamiesi stebėsenos sprendimus, FRD papildomai turėtų atsižvelgti ir į kylančias naujas rizikas, pavyzdžiui, kai dėl tam tikrų įvykių pasaulyje (regione) padidėja PPTF rizika (pvz., atsiradus pirmiesiems ženklams dėl COVID-19 pandemijos ir su ja susijusių veiksnių, kurie lėmė padidėjusią sukčiavimo riziką dėl negautų prekių, paslaugų, investicinio sukčiavimo ir t. t., taip pat migrantų (iš Baltarusijos) ar karo pabėgėlių krizę ir galimas rizikas, įskaitant papildomas sankcijas valstybėms) arba įvyksta tam tikri FRD klientų portfelio ar teikiamų paslaugų pasikeitimai (pvz., paslaugos pradedamos teikti klientams, kurie vykdo didesnės PPTF rizikos ekonominę veiklą (virtualiojo turto keityklos, išvestinių priemonių *Forex* valiutų rinkoje brokeriai, azartiniai lošimai ir pan.) arba paslaugos pradedamos teikti naujoje geografinėje teritorijoje, kuriai būdingos specifinės PPTF rizikos ar nusikalstamos veikos tipologijos). Remdamiesi Nurodymų 38 punktu, FRD privalo įvertinti kylančią naują PPTF riziką ir atitinkamai taikyti papildomas priemones šiai rizikai suvaldyti, įskaitant FRD nustatytų stebėsenos sprendimų ir priemonių peržiūrą ir (arba) atnaujinimą. FRD turėtų atsižvelgti ir į atnaujintas EBI rizikos veiksnių gaires, kuriose daug dėmesio skiriama tiek visos veiklos PPTF rizikos vertinimui, tiek kylančių naujų rizikų nustatymui.

Papildomai pažymėtina, kad tinkamą visos veiklos PPTF rizikos ir individualų kliento PPTF rizikos vertinimą pirmiausia reikėtų pradėti nuo veiksmingai įgyvendinamo deramo klientų tikrinimo, t.y. KYC, principo. Būtent tinkamas ir veiksmingas deramas klientų tikrinimas gali padėti suprasti ne tik FRD kylančias PPTF rizikas, tačiau ir geriau suprasti kliento vykdomą veiklą, jos pobūdį bei operacijų stebėsenos vykdymo metu nustatyti, ką galima laikyti kliento neįprasta operacija, taip pat ir vertinant, ar kliento elgesys gali būti laikytinas įtartinu. Pažymėtina, kad informacijos apie klientą rinkimas neturėtų būti formalus, nes klientas teikdamas informaciją gali nurodyti ir išgalvotą ar klaidinančią informaciją, todėl svarbu įvertinti, ar informacija dėl dalykinių santykių tikslo ir numatomo pobūdžio atitinka kliento nurodytą ekonominę veiklą ir kitų panašaus ekonominio profilio klientų nurodytą veiklą bei operacijų pobūdį, o esant neatitikimų arba nematant aiškaus ekonominio pagrįstumo ir logikos, reikėtų informaciją su klientu pasitikslinti. Atitinkamai dalykinių santykių metu ši kliento informacija turi būti nuolat atnaujinama ir palyginama su faktine kliento vykdoma veikla.

FRD tinkamai nustatę klientų tapatybę ir surinkę informaciją apie savo turimus klientus, visų pirma, galėtų pasirinkti veiksmingus stebėsenos sprendimus (būdus) ir nustatyti atitinkamus scenarijų parametrus

---

[12] Lietuvos banko ir FNTT fiktyvių įmonių nustatymo gairės (https://www.fntt.lt/lt/pinigu-plovimo-prevencija/fiktyviu-imoniu-veiklos-pozymiu-nustatymo-gaires/4112).

[13] Lietuvos bankas 2021 m. vasario 11 d. paskelbė apžvalgą, kaip tinkamai atlikti visos veiklos pinigų plovimo ir teroristų finansavimo rizikos vertinimą (https://www.lb.lt/lt/naujienos/lietuvos-banko-apzvalgoje-kaip-tinkamai-atlikti-visos-veiklos-pinigu-plovimo-ir-teroristu-finansavimo-rizikos-vertinima).

(operacijų sumą, skaičių, laikotarpį), kuriuos viršijus tam tikros klientų operacijos būtų laikomos neįprastomis ir gali būti reikalinga atlikti išsamesnius vidaus tyrimus bei iš kliento prašyti papildomos informacijos ar mokėjimo operacijas pagrindžiančių dokumentų. Todėl FRD diegiant ir tobulinant stebėsenos modelį, atskirus sprendimus, įskaitant stebėsenos scenarijus ir jų parametrus, labai svarbu remtis turima statistine informacija apie FRD klientus, klientų grupes ir jų segmentus (plačiau žr. 4.1 ir 4.2 skirsniuose).

Galiausiai svarbu akcentuoti, kad tuo atveju, kai FRD automatinę stebėsenos sistemą ar kokį nors kitą stebėsenos sprendimą (priemonę) perka iš paslaugų teikėjų, t. y. trečiųjų šalių, tokios stebėsenos priemonės funkcionalumas (įskaitant stebėsenos scenarijus, jeigu naudojama automatinė stebėsenos sistema) turi būti pritaikytos pagal FRD verslo modelį ir klientų bazę, o FRD turėtų kontroliuoti tokių sprendimų veikimą ir gebėti suprasti, kokioms PPTF rizikoms identifikuoti ir valdyti naudojami šie stebėsenos sprendimai ar atitinkamai konkretūs scenarijai, ir gebėti suprasti ir paaiškinti, ar stebėsenos sprendimai veikia korektiškai.

4. STEBĖSENOS SPRENDIMŲ IR STEBĖSENOS SCENARIJŲ INTENSYVUMO BEI APIMTIES PRITAIKYMAS PAGAL FRD VEIKLOS MODELĮ IR KLIENTŲ KELIAMĄ PPTF RIZIKĄ

Nurodymų reikalavimai
58. FRD privalo vykdyti nuolatinę kliento dalykinių santykių ir operacijų (sandorių) stebėseną. Nuolatinė dalykinių santykių ir operacijų (sandorių) stebėsena apima tiek stebėseną realiuoju laiku, t. y. prieš įvykdant kliento operaciją ir (arba) operacijos atlikimo metu (momentinė stebėsena) (angl. *online monitoring*), tiek retrospektyvią stebėseną, t. y. jau įvykdytų operacijų ir (arba) sandorių analizę, siekiant suprasti kliento atliekamų operacijų ir (arba) sudaromų sandorių pobūdį ir (arba) jų atitiktį FRD turimoms žinioms apie klientą, jo rizikos profilį, identifikuoti atliekamas įtartinas operacijas ir (arba) sandorius. 61. Kliento dalykinių santykių ir (arba) operacijų (sandorių) stebėsenos intensyvumą, apimtį, scenarijus ir atitinkamus stebėsenos kriterijus FRD nustato atsižvelgdamas tiek į atlikto visos veiklos PPTF rizikos vertinimo rezultatus, tiek į individualų kliento PPTF rizikos vertinimą. 62. Dalykinių santykių ir operacijų stebėsenos intensyvumas, apimtis, scenarijai ir atitinkami stebėsenos kriterijai parenkami atsižvelgiant bent į šiuos veiksnius: 62.1. atliekamos stebėsenos pobūdį (retrospektyvi, momentinė); 62.2. kliento keliamą riziką; 62.3. geografijos arba teritorijos, kurioje vykdoma veikla, keliamą riziką; 62.4. teikiamų produktų, operacijų (sandorių) riziką.

4.1. STEBĖSENOS SPRENDIMŲ, PRIEMONIŲ, POBŪDŽIO IR JŲ INTENSYVUMO BEI APIMTIES PASIRINKIMAS

Siekiant nustatyti stebėsenos intensyvumą ir apimtį, pirmiausia FRD privalo holistiškai įvertinti ir nuspręsti, kokį stebėsenos modelį planuoja savo veikloje taikyti. Nurodymuose yra įtvirtintas reikalavimas FRD vykdyti tiek momentinę, tiek retrospektyvią stebėseną, tačiau FRD pats privalo nustatyti tokios stebėsenos apimtį atsižvelgęs į FRD kylančias PPTF rizikas ir veiklos modelį.

Kaip jau rašyta ankstesniuose skyriuose, siekiant tinkamai nustatyti ir pritaikyti stebėsenos priemonių visumą, kad ji veiktų veiksmingai, labai svarbu yra tinkamai atliktas FRD visos veiklos PPTF rizikos vertinimas. Paprastai FRD visos veiklos PPTF rizikos vertinimo metu atliekamas klientų grupavimas pagal tam tikras grupes (pvz., fiziniai ir juridiniai klientai, pagal klientui priskirtą PPTF rizikos grupę, kliento veiklos pobūdį ir

pan.), o individualus kliento PPTF rizikos vertinimas ir jo metu renkamos ir vertinamos informacijos apimtis yra svarbi siekiant atlikti klientų grupavimą visos veiklos PPTF rizikos vertinimo metu. Pažymėtina, kad tinkamai atlikus visos veiklos PPTF rizikos vertinimą, FRD turės gerą supratimą apie savo klientų portfelį ir jo keliamą PPTF riziką. Po PPTF rizikos vertinimų (visos veiklos ir individualų kliento), galima pereiti į kitą etapą ir jau imtis priemonių skirtingai klientų keliamai PPTF rizikai suvaldyti – šiuo atveju organizuoti kliento stebėseną, kuri būtų pritaikyta konkrečioms PPTF rizikoms suvaldyti. Vienas iš būdų tinkamai įgyvendinti ši tikslą, kaip įtvirtinta Nurodymų 61 punkte, yra FRD pareiga nustatyti skirtingą stebėsenos sprendimų intensyvumą, apimtį, stebėsenos priemones ir scenarijus atsižvelgus į kylančią PPTF riziką.

Momentinės stebėsenos tikslas yra neleisti įvykti inicijuotai mokėjimo operacijai arba neleisti įskaityti kliento lėšų tol, kol ji nebus išanalizuota atsakingų FRD darbuotojų. Esant didesniam FRD veiklos mastui, suprantama, kad neįmanoma peržiūrėti kiekvienos mokėjimo operacijos, todėl įprastai momentinė stebėsena turėtų būti įdiegta stabdant tokias mokėjimo operacijas, kurios gali kelti didžiausią PPTF riziką, siekiant stabdyti įtartinas operacijas ir užkirsti kelią nusikalstamai veikai.

Vykdant retrospektyvią stebėseną, kliento mokėjimo operacijos prieš jas įvykdant nėra stabdomos, tačiau yra peržiūrimos ir išanalizuojamos kliento jau įvykdytos tam tikro FRD pasirinkto laikotarpio operacijos pagal tam tikrus parametrus. Šio stebėsenos būdo tikslas – geriau suprasti ilgesnio laikotarpio kliento veiklą ir išsamiau išanalizuoti kliento operacijas, įvertinti, ar kliento faktinė veikla atitinka kliento FRD dalykinių santykių užmezgimo metu deklaruotą veiklą, kliento ekonominės veiklos sektoriui būdingą veiklą arba dalykinių santykių metu vykdytą klientui įprastą veiklą. Atsižvelgiant į FRD veiklos modelį ir tokio veiklos modelio keliamą PPTF riziką, retrospektyvi stebėsena gali būti vykdoma su automatinės stebėsenos sistemos pagalba arba rankiniu būdu atsirenkant klientų operacijas pagal tam tikrus kriterijus ir jas analizuojant; arba kompleksiškai taikant abu šiuos stebėsenos būdus kartu. Pažymėtina, kad retrospektyviai peržiūrint automatinės stebėsenos sistemos sugeneruotus įspėjimus, rekomenduojama FRD įsivertinti galimybę peržiūrėti ilgesnio laikotarpio kliento operacijas, o ne vieną konkrečią operaciją, dėl kurios buvo sugeneruotas įspėjimas. Įprastai, tik vertinant ilgesnio laikotarpio kliento vykdomas operacijas, galima geriau suprasti klientą, jo veiklos pobūdį ir atitinkamai identifikuoti neįprastą ar įtartiną kliento veiklą bei operacijas. Be to, ilgesnio laikotarpio kliento mokėjimų peržiūra taip pat padeda patikrinti, ar FRD taikomi stebėsenos sprendimai ir scenarijai veikia tinkamai ir veiksmingai (plačiau žr. 5 skyrių).

Papildomai pažymėtina, kaip nurodyta EBI rizikos veiksnių gairių 4.75 punkte, nors FRD taiko automatinę momentinę ir retrospektyvią stebėsenos sistemą, tačiau, atsižvelgęs į FRD veiklos modelį, mastą ir pobūdį, klientų portfelį, vykdomas operacijas, siūlomus produktus ir paslaugas, jų sudėtingumą ir kitas reikšmingas aplinkybes, FRD gali taikyti ir daugiau papildomų stebėsenos, ypač retrospektyvios, sprendimų ir priemonių, kaip papildomos ilgesnio laikotarpio (pvz., kas 6 mėn., 1 m. ar kitu FRD vidaus kontrolės procedūrose nustatytu periodiškumu) kliento veiklos analizės ar peržiūros (išsamiau žr. toliau), ar papildomų techninių stebėsenos sprendimų (pvz., kliento internetinių puslapių autentiškumo patikra, blokų grandinės technologijos (angl. *blockchain*) analizės priemonės ir pan.). Pažymėtina, kad ir pagrindinėje automatinės stebėsenos sistemoje gali būti nustatyti ilgesnio laikotarpio retrospektyvios stebėsenos scenarijai (pvz., 6 mėn.), tokiu atveju rekomenduojama šiuos skirtingus stebėsenos būdus suderinti ir, pavyzdžiui, atliekant papildomus tyrimus, orientuotus į nuodugnesnių analizių atlikimą, sąsajų ieškojimą (angl. *networks and links analysis*) ir pan.

Papildomos stebėsenos priemonės ir jų pagrindu atliekami išsamesni kliento veiklos ir operacijų tyrimai gali padėti nustatyti FRD taikomos stebėsenos sistemos trūkumus ir kartu padėti tobulinti FRD stebėsenos sistemą (jos būdus, metodus, stebėsenos organizavimą), įskaitant atskirus stebėsenos scenarijus.

Apibendrinant akcentuotina, kad FRD pasirinkti stebėsenos sprendimai, priemonės ir būdai turėtų papildyti vienas kitą, būti pritaikyti PPTF rizikoms, su kuriomis susiduria konkretus FRD, valdyti. Toliau pateikiama keletas praktinių pavyzdžių, į kuriuos FRD gali atsižvelgti kurdami stebėsenos sprendimus ir (arba) stebėsenos scenarijus:

Momentinė stebėsena galėtų būti taikoma ir šiais atvejais:

- stebimos operacijos, neatitinkančios FRD norimos prisiimti rizikos (pvz., tam tikros nepriimtinos valstybės, nepriimtini konkretūs klientai (apie kuriuos yra neigiamos informacijos), specifiniai raktažodžiai (pvz., susiję ir tam tikromis veiklomis (pvz., konsultacinės paslaugos, virtualusis turtas ir t. t.), sankcionuoti bankai ir pan.);
- stebimos didelės vertės operacijos, palyginti su kitais panašaus pobūdžio FRD klientais;
- naudojami scenarijai ir raktažodžiai, skirti teroristų finansavimo atvejams nustatyti;
- siekiama užkardyti atvejus, kai klientas siekia išvengti pateikti informaciją ar dokumentus dėl vykdomų didesnės rizikos operacijų (operacijos didelėmis sumomis, kurios neatitinka vidutinio FRD kliento ekonominio pajėgumo, operacijų skaidymas ir pan.);
- naudojami kiti scenarijai, orientuoti į FRD vertinimu didžiausias PPTF grėsmes;
- naudojami kiti specifiniai scenarijai, kaip tranzitinių sąskaitų, neaktyvių sąskaitų (angl. *dormant accounts*). scenarijai (t. y. kai sąskaitos nenaudojamos ilgą laiką ir jomis pradedama aktyviai naudotis). Pažymėtina, kad šie scenarijai su kitokiais parametrais gali būti naudojami ir retrospektyvios stebėsenos metu;
- mokėjimai inicijuojami iš kito IP adreso, nei kurį įprastai naudoja klientas;
- momentinės stebėsenos metu stebimi tarptautinių finansinių sankcijų ir kitų ribojamųjų priemonių sąrašai.

Retrospektyvi stebėsena galėtų būti taikoma šiais atvejais:

- kai stebėsenos scenarijai yra sudėtingi, turi apimti kelias sudedamąsias dalis, o pagal juos sugeneruotiems įspėjimams išanalizuoti reikia daugiau laiko;
- siekiama nustatyti nukrypimus nuo FRD deklaruoto naudojimosi paslaugomis tikslo ir pobūdžio, pavyzdžiui, kliento anketoje nurodytos apyvartos viršijimas (procentais arba kartais), mokėjimai už nurodytos geografinės teritorijos ribų, mokėjimo operacijos pobūdis (paskirtis) neatitinka kliento veiklos pobūdžio;
- scenarijai, padedantys nustatyti nukrypimą nuo klientui įprastos veiklos;
- neįprastos ir sudėtingos struktūros sandoriai (pvz., ekonomiškai nepagrįsti);
- scenarijai, susiję su geografinėmis rizikomis (geografinės rizikos būdingos tam tikroms valstybėms ar regionams, pavyzdžiui, prekyba žmonėmis, neteisėtas žmonių gabenimas per sieną, narkotikų prekyba, padirbtos prekės, sukčiavimas, teroristų finansavimas ir pan.);
- scenarijai, susiję su didesnės PPTF rizikos klientais, pavyzdžiui, PEP, virtualiojo turto keityklos, išvestinių priemonių *Forex* valiutų rinkoje brokeriai;
- scenarijai, susiję su skirtingais produktais, pavyzdžiui, grynųjų pinigų operacijomis;
- papildomi teroristų finansavimo scenarijai;
- scenarijai, padedantys atpažinti, kai mokėjimo operacijos atliekamos dideliam skaičiui gavėjų arba gaunamos iš didelio skaičiaus mokėtojų (angl. *many to one* ir *one to many*), kurie savo esme labiau tinkami fiziniams asmenims;
- FRD turint pakankamai žmogiškųjų išteklių, didesnės PPTF rizikos klientų atveju dienos, savaitės ar kito FRD nustatyto laikotarpio veiklos peržiūra.

Galimi papildomi tyrimai, retrospektyvios analizės ir kitos priemonės:

- standartiškai atliekant didelės PPTF rizikos klientų sustiprintą dalykinių santykių stebėseną (pvz., atliekant OEDD veiksmus);
- atliekant tam tikrų klientų peržiūrą, kai *ad-hoc* atvejais nustatoma didesnė kliento PPTF rizika ir reikalingos papildomos stebėsenos priemonės;
- atliekant susijusių klientų sąsajų tikrinimą (pvz., bendrus partnerius, per bendrus registracijos adresus, IP adresus, telefono numerius, ir pan.);
- atliekant didelių klientų įmonių grupių bendros veiklos tyrimus;

- darant itin didelį operacijų skaičių ir (ar) apimtį atliekančių klientų veiklos vidaus tyrimus, kai siekiama nustatyti galimas operacijų sąsajas;
- atliekant atskirų klientų vidaus tyrimus dėl gautos svarbios informacijos, pavyzdžiui, kai priežiūros institucija paskelbia, kad galimas klientas teikia finansines paslaugas neturėdamas licencijos ar būtino leidimo, būtina patikrinti, ar per FRD nebuvo vykdomos susijusios operacijos;
- atliekant tyrimus dėl viešai pasirodžiusios informacijos (pvz., *Luanda Leaks, Panama Papers, Pandora Papers, Paradise Papers* ir pan.);
- pasirodžius kitai neigiamai informacijai apie galimus klientus;
- taikant bendrai priemones neigiamai informacijai apie klientą aptikti;
- gavus kompetentingų institucijų užklausų, kitų finansų įstaigų ar paties FRD kitų skyrių pranešimų apie pastebėtą įtartiną kliento elgesį, veiklą ar mokėjimus ir pan.;
- kitais atvejais, kai nėra galimybių pritaikyti momentinės ar retrospektyvios automatinės stebėsenos;
- taikant papildomas specifines techninės stebėsenos priemones (taikant blokų grandinės technologijos analizės priemones, stebint interneto puslapius ir pan.).

4.2. STEBĖSENOS SCENARIJŲ INTENSYVUMAS IR APIMTIS

Vertinant automatinės stebėsenos scenarijų intensyvumo ir apimties pritaikymo būdus, vienas iš jų yra FRD klientų grupavimas į segmentus pagal tam tikrus kriterijus. Toks grupavimas leidžia FRD sukurti ir suprasti, kokius klientus aptarnauja, įskaitant kliento veiklos pobūdį. Turint tokią informaciją, galima geriau pritaikyti stebėsenos scenarijus siekiant nustatyti klientui neįprastą ar įtartiną veiklą. Vis dėlto svarbu pabrėžti, kad toks klientų grupavimas yra veiksmingiausias, kai FRD turi daugiau to paties profilio klientų (pvz., pagal klientui priskirtą PPTF rizikos grupę, kliento vykdomą ekonominę veiklą ir pan.) ir galima atlikti palyginamąją analizę, kurios tikslas – sukurti tikslesnį kliento profilį. Nustačius nukrypimą nuo klientui įprastos veiklos, FRD gali spręsti, ar tokios operacijos yra aiškios, ar reikalinga nuodugnesnė analizė ir galimai papildoma informacija iš kliento.

Klientų ir (arba) FRD siūlomų produktų ir paslaugų grupavimas svarbus ir dėl to, kad, pavyzdžiui, studentas (arba darbuotojas, gaunantis vidutines pajamas) ir labai turtingas fizinis asmuo priklauso tai pačiai fizinių asmenų grupei, tačiau šių klientų vykdomų operacijų skaičius ir (arba) vertė gali reikšmingai skirtis – kas turtingam asmeniui bus įprasta, studento atveju bus neįprasta arba netgi įtartina. Svarbu atkreipti dėmesį, kad net tos pačios PPTF rizikos grupės klientams yra būdinga skirtinga veikla, todėl stebėsenos scenarijaus parametrai turėtų būti orientuoti į tai, kas konkrečiai klientų grupei būtų neįprasta. Pavyzdžiui, lošimų bendrovėms gali būti įprasti dažni mažų sumų mokėjimai ir lošimų bendrovės klientų prisijungimai iš skirtingų valstybių (pagal IP adresus), tačiau kitos veiklos įmonei arba fiziniam asmeniui toks mokėjimo operacijų ir elgesio pobūdis gali būti visiškai neįprastas ir kelti įtarimų dėl padidėjusios pinigų plovimo rizikos. Pritaikant scenarijus svarbu atsižvelgti į visus FRD siūlomus produktus (pvz., mokėjimai, indėliai, prekybos finansavimas, investavimas, valiutos keitimas ir pan.), kliento tapatybės nustatymo būdus, nes tai leidžia sukurti tipinį FRD kliento paveikslą.

FRD pritaikant ir kuriant stebėsenos scenarijus, pažymėtina, kad ne visada reiktų apsiriboti tik vertės (sumos), valstybės (mokėjimų krypties) nustatymu, tačiau būtina atkreipti dėmesį į galimybę nustatyti labiau kompleksinius scenarijus, derinant kelis scenarijų kriterijus, pavyzdžiui, mokėjimo operacijų vertės ir valstybės dėmuo; mokėjimo operacijų vertės ir kliento PEP statuso dėmuo; mokėjimo operacijų vertės, kliento juridinės formos ir klientui priskirtos PPTF rizikos grupės dėmuo.

Remdamasis geriausia patirtimi, FRD, pritaikydamas stebėsenos ir scenarijų intensyvumą, gali atsižvelgti į šiuos kriterijus, tačiau šis sąrašas nėra baigtinis:

- Bendros tipologijos (pvz., sukčiavimas) ir su jomis susiję scenarijai bei PPTF rizikos gali būti būdingos visam klientų portfeliui, o ne vien konkrečiai klientų grupei, ir priešingai, tam tikros tipologijos gali būti labiau būdingos tam tikrai klientų grupei (pvz., prekyba žmonėmis);
- Individuali kliento PPTF rizika: pagal klientui priskirtos PPTF rizikos grupę galima nustatyti scenarijus su skirtingais parametrais;
- Kliento tipai: fiziniai asmenys (studentai, darbuotojai, gaunantys vidutines pajamas, turtingi asmenys (angl. *high net worth individuals*) ir juridiniai asmenys (mikroįmonės, vidutinio dydžio įmonės, didelės įmonės, ne pelno siekiančios organizacijos ir pan.);
- Specifinės klientų veiklos rūšys: mokėjimo paslaugos, virtualusis turtas, azartiniai lošimai, kiti klientai, kurių veiklai reikalinga licencija arba leidimas, ir pan.;
- Klientų ekonominė veikla, kurioje vyrauja grynieji pinigai: stebėsena ir scenarijai grynųjų pinigų operacijoms turėtų būti diferencijuoti pagal kliento veiklą – ar jai įprasti grynieji pinigai (pvz., lauko prekyba, maisto stotelės ir pan.), ar ne (verslo paslaugos, didmeninė prekyba ir pan.);
- Teikiamos paslaugos ir siūlomi produktai: momentiniai ir įprasti mokėjimai, privačios bankininkystės klientai, vietiniai mokėjimai, tarptautiniai mokėjimai, grynųjų pinigų operacijos, perlaidos, prekybos finansavimas, indėliai, investavimo produktai, korespondentiniai santykiai, įvairūs kiti bankų produktai;
- Geografija: pavyzdžiui, į FATF arba EK sąrašus įtrauktos didelės PPTF rizikos valstybės, tikslinės teritorijos, mokesčių tikslais nebendradarbiaujančių jurisdikciją turinčių subjektų ES sąrašas, klientai, siejami su valstybėmis, kuriose didesnė TF rizika. Svarbu atkreipti dėmesį, kad ir EEE valstybės priskiriamos skirtingam PPTF rizikos lygiui, todėl, vertinant geografinę riziką, svarbu atsižvelgti ir į valstybės korupcijos ir nusikalstamumo lygį, jai būdingas tipologijas, atvejus, kai pavyzdžiui, dėl klientų, įsteigtų ar reziduojančių atitinkamoje valstybėje, gaunama daug skundų ar neigiamos informacijos, nors pati valstybė nėra įtraukta į FATF arba EK sudaromus sąrašus, mokesčių tikslais nebendradarbiaujančių valstybių ir panašius sąrašus. Vertinant geografinę riziką, atkreiptinas dėmesys į tokius dėmenis kaip, pavyzdžiui, kliento ar naudos gavėjo pilietybė, rezidavimo valstybė, rezidavimo valstybė mokesčių deklaravimo tikslais, pagrindinės vykdomos ekonominės veiklos vieta ar netgi pagrindinių partnerių veiklos valstybė, IP adreso valstybė, iš kurios jungiamasi nustatant kliento tapatybę arba atliekant mokėjimo operacijas ir pan.).

Labai svarbu akcentuoti, kad, nors pirmiau nurodyti kriterijai yra lengviau pritaikomi FRD nustatant automatinės stebėsenos sistemos scenarijus, tačiau FRD, kurie stebėseną vykdo rankiniu būdu, irgi turėtų vertinti galimybes panašius kriterijus įtraukti į savo stebėsenos modelį (pvz., kaip papildoma stebėsenos priemonė gali būti pasirenkama rankiniu būdu peržiūrėti visas klientų operacijas, atliekamas į tam tikrą didelės PPTF rizikos valstybę ar tikslinę teritoriją ir gaunamas iš jų, ir pan.).

4.3. STEBĖSENOS SCENARIJŲ PARAMETRŲ NUSTATYMAS

Atlikus segmentavimą pagal įvairius pirmiau nurodytus pavyzdinius kriterijus, kitas žingsnis yra konkrečių stebėsenos scenarijų parametrų parinkimas – dažniausiai nustatant laikotarpį, už kurį stebėsenos sistemoje bus generuojamas įspėjimas (pvz., 1 d., 7 d., 1 mėn. ar ilgesni laikotarpiai) ir nustatant operacijų skaičių ir (ar) vertę, kurią pasiekus per atitinkamą laikotarpį, sistemoje bus generuojamas įspėjimas. Kaip jau minėta, atitinkamus parametrus galima pritaikyti ir FRD vykdant operacijų stebėseną rankiniu būdu, jeigu nenaudojama automatinė stebėsenos sistema.

Kuriant arba diegiant papildomus stebėsenos scenarijus, labai svarbu remtis turima statistine informacija apie FRD klientų portfelį bei klientų vykdomas operacijas, siekiant geriau pritaikyti ir nustatyti scenarijų parametrus (operacijų skaičių, vertę) (angl. *thresholds*) ir laikotarpį, per kurį įvyksta operacijos, t. y. laiko matą. Remiantis geriausia patirtimi, rekomenduotina remtis statistine informacija, būdinga būtent atitinkamai klientų grupei (segmentui), nes, pavyzdžiui, fizinių asmenų operacijų dydis ir skaičius gali skirtis nuo juridinių asmenų, ir atvirkščiai.

Scenarijų parametrus galima pasirinkti įvairiais būdais ir metodais: pavyzdžiui, statistiniais ar matematiniais būdais apskaičiuojant tam tikros klientų grupės (pvz., fizinių asmenų, kurie priskirti skirtingai PPTF rizikos grupei, pvz., žema, vidutinė, didelė) vykdomų operacijų skaičiaus ir vertės nuokrypius nuo įprastos veiklos ir ekspertiniu vertinimu adaptuoti (pvz., didelės PPTF rizikos klientų operacijos gali būti didesnės vertės, tačiau FRD, siekdami stebėti didesnę dalį didelės PPTF rizikos grupės klientų veiklos, gali didelės PPTF rizikos grupės klientams taikomiems scenarijams taikyti žemesnius parametrus (pvz., operacijų skaičiaus ar vertės) nei tokių klientų atliekamų operacijų vidurkis). Pažymėtina, kad, nepaisant to, kokį stebėsenos scenarijų parametrų nustatymo būdą FRD pasirenka, svarbiausia, kad FRD gebėtų pagrįsti, kodėl buvo nustatyti būtent tokie stebėsenos scenarijų parametrai ir suprasti, kokioms klientų operacijoms (veiklai) kontroliuoti šie scenarijai skirti.

Ne mažiau svarbu, kad po to, kai FRD sistemose nustatomi scenarijai ir jų parametrai, FRD gebėtų laiku ir bet kuriuo metu pakeisti scenarijų nustatymus, jų parametrus ir dinamiškumą, jeigu pastebi naujas tipologijas ar įtartinas klientų veiklas. Todėl FRD taikomi IT stebėsenos sprendimai turėtų būti lankstūs ir FRD prireikus turėtų gebėti greitai panaudoti ir papildomas stebėsenos priemones.

Siekiant tinkamai nustatyti stebėsenos scenarijų parametrus, FRD svarbu žinoti, kokia veikla klientams ar atitinkamam klientų segmentui yra įprasta ir atvirkščiai – mažiau įprasta. Jeigu bus nustatomi per dideli scenarijų parametrai, operacijos nebus pastebimos, analizuojamos ir atitinkamai nebus pranešama FNTT; jeigu bus nustatomi per žemi – gali susidaryti didelis įspėjimų pavėluotai peržiūrėti sąrašas (angl. *backlog*) ir stebėsenos sistema nebus veiksminga. Vis dėlto FRD turimą statistiką apie savo klientus ir jų vykdomas operacijas reikėtų vertinti racionaliai, o keičiant ir atnaujinant stebėsenos scenarijus, vadovautis ekspertiniu vertinimu. Tokiu atveju bus išvengiama situacijų, kai turimi duomenys teisingai neatvaizduoja įstaigai kylančios PPTF rizikos, pavyzdžiui, jeigu įstaiga turi mažai klientų arba vien didelės PPTF rizikos klientų, kurie atlieka didelės vertės operacijas, operacijų apyvartos vidurkis gali būti netinkamas matas, nes ir žemiau vidurkio esančios operacijos gali būti neįprastos ar įtartinos.

Pažymėtina, kad, kuriant scenarijus ir pasirenkant jų parametrus, nebūtų manipuliuojama statistine informacija, nes scenarijų parametrai turėtų būti nustatomi remiantis kylančia PPTF rizika, o ne turimų išteklių ar darbuotojų, kurie gebės laiku peržiūrėti ir išanalizuoti visus įspėjimus, skaičiumi.

5. STEBĖSENOS SPRENDIMŲ IR SCENARIJŲ VEIKSMINGUMO BEI TINKAMO VEIKIMO TESTAVIMAS

Nurodymų reikalavimai
65. FRD privalo reguliariai peržiūrėti ir vertinti (angl. *backtesting*) taikomus sprendimus, siekdamas užtikrinti, kad jie ir toliau būtų aktualūs ir veiksmingi, atsižvelgiant į įstaigos patiriamą PPTF rizikos lygį, nustatytą FRD visos veiklos PPTF rizikos vertinimo metu.
69. Vidaus kontrolės priemonių, skirtų dalykinių santykių ir operacijų (sandorių) stebėsenai (įskaitant automatinės stebėsenos sprendimus, IT priemones ir pan.), tinkamumas privalo būti reguliariai peržiūrimas siekiant užtikrinti, kad įdiegtos priemonės yra aktualios ir atitinka FRD patiriamas rizikas.

Nurodymuose įtvirtinta, kad FRD turėtų reguliariai peržiūrėti savo stebėsenos modelį (įskaitant tiek stebėsenos rankiniu būdu, tiek automatinės stebėsenos sprendimus). Toks peržiūrėjimas turėtų padėti FRD įsivertinti, ar pasirinkti stebėsenos sprendimai ir konkretūs automatinės stebėsenos ir stebėsenos rankiniu būdu scenarijai apima visas kliento operacijas, atsižvelgta į turimą klientų portfelį bei visus FRD siūlomus produktus ir paslaugas, todėl rekomenduojama:

1) periodiškai peržiūrėti ir vertinti holistiškai visą FRD pasirinktą stebėsenos modelį, atskirus stebėsenos procesus, sprendimus ir taikomas IT priemones. Pažymėtina, kad FRD turėtų vertinti visų taikomų stebėsenos procesų visumą ir jų sąveiką tarpusavyje, siekdamas įvertinti, ar taikomas stebėsenos modelis yra veiksmingas;

2) periodiškai testuoti ir tobulinti taikomus automatinės stebėsenos scenarijus siekiant užtikrinti, kad jie būtų veiksmingi, aktualūs ir būtų orientuoti į rizikingesnes operacijas ir rizikingesnį klientų elgesį. Svarbu atkreipti dėmesį, kad tokio peržiūrėjimo metu neturėtų būti bandoma manipuliuoti testavimo rezultatais ir dirbtinai sumažinti generuojamų įspėjimų skaičių. Pažymėtina, jei FRD klientų portfelį sudaro daug didelės PPTF rizikos klientų, atitinkamai FRD turi skirti pakankamai tiek žmogiškųjų, tiek technologinių išteklių;

3) jeigu FRD naudoja tik stebėsenos rankiniu būdu sprendimus, turėtų būti vertinamas tokios stebėsenos veiksmingumas, pavyzdžiui, ar tikrai operacijų skaičius yra toks, kad galima netaikyti automatinių stebėsenos sprendimų, turėtų būti vertinamas kriterijų, kuriais remiantis rankiniu būdu peržiūrimos klientų operacijos, veiksmingumas ir pan.

Pirma, vertinant holistiškai FRD sistemos modelį ir pasirinktus sprendimus, rekomenduojama FRD įvertinti, kaip tarpusavyje sąveikauja atskiri stebėsenos sprendimai, ar jie leidžia užtikrinti veiksmingą visapusišką klientų veiklos stebėseną. Be to, rekomenduojama FRD įvertinti, ar taikomi stebėsenos sprendimai apima bent tokius toliau nurodytus pagrindinius aspektus (tačiau pažymėtina, kad šis sąrašas nėra baigtinis ir turėtų būti vertinami kiti konkrečiam FRD svarbūs aspektai):

- ar scenarijai ir stebėsenos priemonės pagrįstos SNRA, NRV ir kitomis aktualiomis tipologijomis, įskaitant atvejus, kai nustatomos naujos tipologijos, arba peržiūrima, ar FRD turi stebėsenos priemones tokiems atvejams nustatyti;
- ar stebėsenos sprendimai ir scenarijai pritaikyti pagal FRD verslo modelį ir turimą klientų portfelį (pvz., ar valiutos keityklos operatoriai turi stebėsenos priemones susijusioms valiutos keitimo operacijoms nustatyti, ar finansų įstaigos su sudėtinga klientų struktūra taiko kompleksinius stebėsenos scenarijus bei papildomus stebėsenos sprendimus ir priemones ir t. t.);
- ar taikomos atskiros TF stebėsenos priemonės ir scenarijai, skirti ne tik tarptautinių sankcijų įgyvendinimo kontrolei vykdyti;
- ar visų produktų specifikai (pvz., prekybos finansavimas, kreditavimas, investiciniai produktai ir pan.) yra taikomos stebėsenos priemonės;
- ar visoms mokėjimo priemonėms (pvz., mokėjimo kortelėms) taikomi stebėsenos scenarijai;
- ar stebimos tiek įeinančios, tiek išeinančios mokėjimo operacijos;
- ar naudojami sukčiavimo prevencijai skirti scenarijai arba kitos stebėsenos priemonės;
- ar taikomi stebėsenos sprendimai, padedantys atpažinti atvejus, kai klientas nukrypsta nuo jam įprastos arba panašios pagal ekonominę veiklą klientų grupei būdingos veiklos;
- ar stebima visa kliento veikla, pavyzdžiui, ar visos kliento turimos sąskaitos ir vykdomos operacijos stebimos stebėsenos priemonėmis;
- ar taikomos stebėsenos priemonės FRD vidaus operacijoms, t. y. tais atvejais, kai tiek mokėtojas, tiek gavėjas yra FRD klientas;
- ar nepersidengia tarpusavyje taikomi scenarijai;
- ar taikomos stebėsenos priemonės tranzitinėms sąskaitoms, neaktyvioms sąskaitoms (angl. *dormant accounts*) nustatyti;

- ar techniškai korektiškai veikia momentinės ir retrospektyvios automatinės stebėsenos scenarijai;
- ar stebėseną vykdant rankiniu būdu, įvertinama, kaip peržiūrai atrenkamos operacijos;
- ar laiku peržiūrimi stebėsenos scenarijų sugeneruoti įspėjimai ir ar kontroliuojamas pavėluotai peržiūrėtų įspėjimų procesas;
- ar įdiegtas stebėsenos sprendimų ir scenarijų peržiūros, kokybiško veikimo užtikrinimo procesas.

Atliekant tokią peržiūrą ir testavimą, siekiant patobulinti jau FRD įdiegtus stebėsenos scenarijus ir bendrai taikomą stebėsenos sistemos modelį, irgi rekomenduojama atsižvelgti į toliau nurodytus geriausios patirties būdus:

1) rankiniu būdu peržiūrėti dalį operacijų, kurioms netaikomi jokie scenarijai ar kiti stebėsenos sprendimai, siekiant įsitikinti, ar tarp tokių operacijų nėra klientams neįprastos ar įtartinos veiklos. Pavyzdžiui, atvejai, kai fiziniai asmenys gauna mokėjimus iš didelio skaičiaus asmenų, netaikomas tokiai veiklai atpažinti automatinės stebėsenos sistemos scenarijus, netaikomos papildomos retrospektyvios stebėsenos priemonės, o pagal kitus automatinės stebėsenos scenarijus sugeneruoti įspėjimai analizuojami tik peržiūrint vieną operaciją, dėl kurios buvo sugeneruotas įspėjimas, todėl tikėtina, kad FRD tokios kliento veiklos nepastebės jokiomis turimomis stebėsenos priemonėmis);

2) analizuoti atliktų vidaus tyrimų išvadas ir periodiškai peržiūrėti pateiktus pranešimus FNTT siekiant įvertinti, ar FRD taikomi stebėsenos sprendimai ir konkretūs scenarijai yra veiksmingi nustatant neįprastas ar įtartinas operacijas;

3) įvertinti kitais būdais (pvz., vykdant *ad-hoc* tyrimus kliento informacijos atnaujinimo proceso metu, didelės PPTF rizikos grupės klientų ilgesnio laikotarpio operacijų analizės metu ir pan.) surinktą informaciją ir nustatytas neįprastas arba įtartinas kliento operacijas. Tokio testavimo tikslas – įvertinti, ar veiksmingi FRD pasirinkti stebėsenos sprendimai nustatant tokius įtartinumo požymių turinčius atvejus, o galbūt reikia įdiegti papildomus automatinės stebėsenos scenarijus ar taikyti papildomus stebėsenos būdus.

Antra, kalbant apie automatinės stebėsenos scenarijų peržiūrą ir testavimą, Lietuvos bankas, vykdydamas FRD priežiūrą, pastebi, kad praktikoje FRD naudojamų stebėsenos sprendimų, sistemų veiksmingumo vertinimo, įskaitant stebėsenos scenarijų testavimo, būdai, metodai ir apimtis skiriasi. Galima išskirti kelis geriausios patirties aspektus, kaip testuojamas stebėsenos scenarijų veiksmingumas ir tinkamas stebėsenai naudojamų IT sistemų techninis veikimas:

1) testavimas atliekamas reguliariai (pvz., kartą per metus). Periodinio testavimo metu testuojami patys stebėsenos scenarijai ir juose taikomų parametrų techninis veikimas (pvz., testavimo metu vertinama, ar sistemose sugeneruoti įspėjimai pagal taikomus scenarijus nepersidengia, ar įspėjimų generavimas techniškai veikia be klaidų, ar įspėjimai visada techniškai generuojami pagal IT sistemose nustatytus parametrus, ar atlikus IT sistemos pakeitimus, sistemos ir scenarijų parametrai ir toliau veikia tinkamai bei korektiškai ir visos operacijos patenka į stebėsenos sistemos filtrą;

2) atliekama scenarijų, kurie generuoja daug klaidingai teigiamų įspėjimų (angl. *false positive*), analizė siekiant šiuos scenarijus ir jų parametrus pakoreguoti, kad būtų generuojama daugiau tikslesnių įspėjimų;

3) testuojant scenarijus ir vertinant jų veiksmingumą, remiamasi klaidingai teigiamų įspėjimų santykiu (angl. *false-positive ratio*), t. y. ar pagal stebėsenos scenarijus sugeneruotus įspėjimus atliekami vidaus tyrimai, kokia tokių atliekamų tyrimų dalis;

4) vertinamas stebėsenos scenarijų, kurie visai negeneruoja jokių įspėjimų, reikalingumas;

5) pagal geriausią patirtį, siekiant įsivertinti optimalius scenarijų parametrus, ypač vertės rėžį, atliekami testavimai taikant statistinius *above-the-line* (ATL) – *below-the-line* (BTL) metodus. Šie testavimai itin veiksmingi nustatant scenarijų parametrus siekiant pasitvirtinti nustatytų parametrų aktualumą ir veiksmingumą (efektyvumą). Taikant šiuos statistinius metodus, dažniausiai scenarijų parametrai (operacijų skaičiaus, vertės) yra padidinami arba sumažinami, kad galima būtų pasiekti optimaliausias

parametrų reikšmes, taip FRD gali sumažinti vadinamųjų klaidingai teigiamų įspėjimų rezultatų skaičių. Testuojant ATL metodu peržiūrimi sistemose sugeneruoti įspėjimai, kurie viršija nustatytus FRD parametrus, o BTL metodu testinėje aplinkoje peržiūrimi įspėjimai, sumažinant parametrus, palyginti su galiojančiais parametrais, arba peržiūrimos ir įvertinamos operacijos, kurios nesiekia scenarijuose nustatytų parametrų ribų. Pagal geriausią patirtį verta taikyti abu metodus, itin svarbu atkreipti dėmesį į BTL metodą, kadangi jis leidžia užtikrinti, kad, atsižvelgiant į FRD klientų vykdomas operacijas nustatyti parametrai (pvz., vertė, operacijų skaičius, laikotarpis), nėra per dideli (pvz., jeigu peržiūrint operacijas, kurios nesiekia pagal atitinkamą scenarijų nustatyto parametro, pastebima neįprasta ar įtartina kliento veikla, tai reiškia, kad scenarijų parametrai nustatyti neteisingai ir scenarijų parametrus būtina koreguoti. Atkreiptinas dėmesys, kad šis testavimas veiksmingiausias, kai klientai yra tinkamai sugrupuoti į atitinkamus segmentus (pvz., fiziniai asmenys, juridiniai asmenys, klientai finansų įstaigos ir pan.);

6) atlikti testavimą (angl. *sample testing*) ir retrospektyviai rankiniu būdu peržiūrėti operacijas, kurios nepatenka į dalykinių santykių stebėseną dėl mažesnių už FRD nustatytus scenarijų parametrus (pvz., taikomas toks scenarijus: septyni ir daugiau klientų siunčia mokėjimus vienam fiziniam asmeniui per vieną dieną; rekomenduojama periodiškai peržiūrėti, ar nustatyta riba – septyni ir daugiau klientų atitinka FRD klientų vykdomų operacijų tendencijas, ar nereikia scenarijuose nustatytų ribų mažinti arba didinti).

Prieš įdiegdamas naujus stebėsenos scenarijus, FRD turėtų išbandyti scenarijų pakeitimus testinėje aplinkoje. Pažymėtina, jog testinė aplinka turėtų veikti su realiais duomenimis, kad būtų galima tinkamai sukalibruoti stebėsenos sistemą pagal testavimo rezultatus. Be to, reikėtų įvertinti, ar po naujų scenarijų įdiegimo turėtų būti atliekami testavimai jau realioje aplinkoje, siekiant patikrinti, ar scenarijų atnaujinimas yra veiksmingas (pagal FRD tikslus, dėl kurių buvo atnaujinti scenarijai). Atsižvelgiant į tai, kad scenarijuose nustatyti parametrai (operacijų skaičius, vertė, laikotarpis) gali kisti atitinkamai keičiantis FRD veiklos modeliui ir klientų portfeliui (pvz., pagal klientų ekonominę veiklą, pagal jų keliamą PPTF riziką ir pan.), rekomenduojama scenarijų parametrus periodiškai peržiūrėti ir testuoti. Atkreiptinas dėmesys į tokią geriausią patirtį, kai FRD užtikrina, kad visi naujų (perkalibruotų) scenarijų testavimų rezultatai ir bet kurie vėlesni koregavimai būtų pagrįsti ir patvirtinti atitinkamais dokumentais (dokumentai, patvirtinantys, kad scenarijus buvo testuotas, veikia tinkamai ir yra veiksmingas).

Trečia, kalbant apie FRD vykdomą operacijų stebėseną rankiniu būdu, pažymėtina, kad didžioji dalis pirmiau nurodytų geriausios patirties pavyzdžių tinka ir gali būti pritaikomi ir stebėsenos rankiniu būdu sprendimų veiksmingumui testuoti.

Papildomai pažymėtina, kad labai svarbu supažindinti stebėsenos funkciją vykdančius darbuotojus su FRD taikomu stebėsenos procesu, stebėsenos sprendimais ir atskirais scenarijais, darbuotojams paaiškinti, kodėl parinkti būtent tokie stebėsenos sprendimai arba scenarijai, kokiai rizikingai klientų veiklai identifikuoti tokie stebėsenos sprendimai arba scenarijai yra skirti ir pan. Tokių mokymų tikslas – atkreipti darbuotojų, atliekančių stebėsenos funkcijas, dėmesį, ar FRD pasirinkti stebėsenos sprendimai arba parinkti konkretūs scenarijai teisingai aptinka neįprastą ar įtartiną veiklą. Taip darbuotojai galėtų praktikoje pastebėti, kad tam tikros įtartinos ar neįprastos operacijos neaptinkamos jokiais taikomais scenarijais, galėtų pastebėti naujas tipologijas, tendencijas, todėl jie turėtų būti skatinami siūlyti įdiegti naujus scenarijus arba papildomus stebėsenos sprendimus ir būdus, be to, tokie pasiūlymai turėtų būti tinkamai dokumentuojami. Taikant tokią praktiką stebėsenos scenarijų ir bendrai FRD taikomo stebėsenos modelio peržiūra, testavimas ir tobulinimas būtų nuolatinis ir tęstinis procesas.

FRD darbuotojai turėtų reguliariai informuoti vadovybę apie taikomų stebėsenos sistemų veiksmingumo vertinimo rezultatus, pagrindinius stebėsenos scenarijų pakeitimus ir jų testavimo rezultatus. Tais atvejais, kai, atlikus stebėsenos sprendimų ir scenarijų testavimą, nustatoma, kad taikomi stebėsenos sprendimai arba konkretūs scenarijai nėra veiksmingi arba nepakankamai veiksmingi, už stebėsenos funkcijos įgyvendinimą atsakingi asmenys (skyriaus vadovai, komandų vadovai) turėtų imtis veiksmų šiems trūkumams pašalinti.

Atitinkamai apie pagrindines visos stebėsenos priemonių visumos testavimo rezultatų išvadas ir pakeitimų poreikį turėtų būti informuojami vadovai (pvz., už PPTF atsakingas FRD valdybos narys).

Papildomai atkreiptinas dėmesys, kad tuo atveju, kai FRD savo stebėsenos sprendimus (įskaitant automatinę stebėsenos sistemą) nusiperka iš trečiųjų šalių arba apskritai perduoda stebėsenos funkciją trečiajai šaliai, FRD nėra atleidžiamas nuo įpareigojimo periodiškai peržiūrėti ir vertinti FRD veikloje taikomus stebėsenos sprendimus, kaip nurodyta pirmiau šioje apžvalgoje.

Apibendrinant pabrėžtina, kad FRD stebėsenos sprendimų bei procesų peržiūra ir vertinimas padeda planuoti žmogiškuosius išteklius, apskaičiuoti reikalingą darbuotojų skaičių, įvertinti naudojamų atskirų stebėsenos sistemų veiksmingumą ir reikalingumą (po tokios peržiūros gali būti nusprendžiama diegti naujas sistemas), įvertinti taikomus stebėsenos scenarijus ir bendrai FRD taikomo stebėsenos modelio veiksmingumą bei tobulintinas sritis.

6. SUSTIPRINTA NUOLATINĖ DALYKINIŲ SANTYKIŲ SU KLIENTAIS STEBĖSENA

6.1. SUSTIPRINTOS STEBĖSENOS PRIEMONĖS IR OEDD PROCESO REIKŠMĖ

PPTFPĮ 14 straipsnio 1 dalyje nustatytas reikalavimas FRD atlikti sustiprintą kliento tapatybės nustatymą taikant papildomas kliento ir naudos gavėjo tapatybės nustatymo priemones, jeigu pagal FRD nustatytas rizikos vertinimo ir valdymo procedūras nustatoma didesnė PPTF rizika, bei kitais PPTFPĮ 14 straipsnio 1 dalyje nustatytais atvejais. PPTFPĮ 14 straipsnio 5 dalies 3 punkte viena iš privalomų tokių papildomų priemonių yra vykdyti sustiprintą nuolatinę dalykinių santykių su klientais, kuriems pagal FRD nustatytas rizikos vertinimo ir valdymo procedūras nustatoma didesnė PPTF rizika, stebėseną.

Reikalavimas vykdyti sustiprintą kliento dalykinių santykių stebėseną gali būti įgyvendinamas tiek taikant griežtesnius stebėsenos scenarijus didelės PPTF rizikos grupės klientams, tiek imantis kitų papildomų stebėsenos priemonių. Lietuvos bankui vykdant finansų rinkos priežiūrą, pastebėta, kad geriausia patirtis yra FRD taikomas OEDD procesas, kurio metu ne tik dažnesniais intervalais atnaujinama didelės PPTF rizikos kliento pažinimo informacija, peržiūrima ir papildomai patikrinama, ar iš kliento surinkta visa reikalinga informacija ir dokumentai pagal FRD vidaus tvarkos procedūras, tačiau ir išsamiau analizuojama ilgesnio laikotarpio (pvz., 6 mėn., 1 m.) kliento faktinė veikla. Šiame kontekste pažymėtina, kad šis procesas nėra laikytinas pagrindine stebėsenos priemone, tačiau gali veiksmingai papildyti FRD taikomų stebėsenos sprendimų visumą, kadangi glaudžiai siejasi su retrospektyvia kliento operacijų peržiūra.

Pažymėtina, kad veiksmingas OEDD procesas nėra įmanomas be tinkamai surinktos kliento pažinimo informacijos ir be tinkamai veikiančios stebėsenos modelio sistemos. Remiantis geriausia rinkos patirtimi, rekomenduojama atliekamą OEDD procesą ir jo rezultatus dokumentuoti specialioje formoje, kurioje galėtų būti fiksuojama, pavyzdžiui, tokia informacija, susijusi su kliento veikla ir operacijomis:

- ar faktinė kliento veikla atitinka kliento veiklą, deklaruotą pažinimo anketoje (pvz., vykdoma veiklos rūšis, operacijų apyvarta, mokėjimai, jų kryptis, tikslas ir pagrindas, valstybės atitinka deklaruotą veiklą, operacijos vykdomos nurodytiems partneriams);
- ar kliento operacijos atitinka deklaruotą sąskaitos naudojimosi tikslą (pvz., ar kliento kitos finansų įstaigos sąskaita naudojama klientų lėšoms saugoti, ar ir klientų mokėjimams);
- ar klientas nenukrypsta nuo jam įprastos ir būdingos ankstesnės veiklos;
- ar kliento vykdomos operacijos yra aiškios ir turi aiškų ekonominį pagrindą;
- ar kliento operacijų gavėjai arba siuntėjai (įskaitant verslo partnerius) yra suprantami ir atitinka kliento deklaruotą veiklą;
- ar su operacijomis susijusi lėšų kilmė aiški;
- ar klientas nevykdo neįprastos ar įtartinos veiklos ir (arba) operacijų.

Be operacijų peržiūros taip pat rekomenduojama įvertinti:

- ar aiški kliento juridinio asmens nuosavybės ir kontrolės struktūra ir veiklos pobūdis;
- ar kliento veiklai reikalingi priežiūros institucijų leidimai arba kitoks autorizavimas ir ar tokie leidimai galioja;
- ar bendrai kliento lėšų ir turto šaltinio kilmė yra aiški;
- ar viešuosiuose šaltiniuose nėra neigiamos informacijos apie klientą, kliento atstovus, naudos gavėjus ir partnerius (angl. *counterparties*).

Atliekant šį procesą, taip pat rekomenduojama papildomai peržiūrėti ir įvertinti, ar iš kliento anksčiau buvo surinkta visa reikalinga informacija ir dokumentai, pavyzdžiui:

- ar klientas pateikė visus dokumentus, reikalaujamus pagal FRD tvarkos procedūras (pvz., naudos gavėjų patikros patikimuose ir nepriklausomuose šaltiniuose įrodymai);
- ar įvykdytos visos sąlygos, kurios buvo nustatytos užmezgant dalykinius santykius su klientu (pvz., praėjus atitinkamam laikotarpiui po dalykinių santykių užmezgimo gauti iš kliento atliktą PPTFP audito ataskaitą ir pan.);
- ar klientui tinkamai priskirta PPTF rizikos grupė;
- jei klientui taikomi tam tikri specifiniai ribojimai, ar tie ribojimai tinkamai įgyvendinami ir klientas jų laikosi, ypač, jei nėra galimybės ribojimų taikyti vien techninėmis priemonėmis;
- išvados dokumentuojamos.

FRD apie senus klientus turi daugiau istorinių duomenų, todėl, praėjus atitinkamam laikotarpiui po dalykinių santykių užmezgimo su naujais klientais arba po šių naujų klientų operacijų pradžios, gali būti peržiūrimos visos klientų, kuriems nustatyta didelė PPTF rizikos grupė, operacijos siekiant įsitikinti, ar veikla atitinka kliento deklaruotą ar įprastą veiklą, ar kliento faktinė veikla veiklą, būdingą atitinkamo verslo sektoriaus klientams, kliento operacijos nėra neįprastos arba įtartinos. OEDD procesą galima atlikti ir praėjus tam tikram laikotarpiui po FNTT pateikto pranešimo apie įtartiną kliento veiklą ar operacijas, siekiant įsitikinti, ar klientas toliau nevykdo neįprastos ar įtartinos veiklos.

Labai svarbu, kad kliento pažinimo informacijos surinkimo ir stebėsenos procesas nuolat vienas kitą papildytų, t. y. informacija, gauta stebėsenos metu, turi būti panaudojama atnaujinant kliento pažinimo informaciją, pavyzdžiui, jeigu kliento verslas plėtėsi (atsirado naujų verslo partnerių, plėtėsi mokėjimai geografine prasme) ir dėl to padidėjo mokėjimų srautai, jei klientas deklaravo, kad mokėjimai bus vykdomi tik ES šalyse, o jie vyksta su trečiosiomis didelės PPTF rizikos valstybėmis ir pan. Šiuo atveju rekomenduojama taikyti rizika grindžiamą metodą, t. y. kuo stebėsenos metu pastebėti pokyčiai yra reikšmingesni, tuo svarbiau atnaujinti kliento informaciją FRD sistemose ne vien tik periodinio kliento informacijos atnaujinimo metu. Jeigu pokyčiai nėra reikšmingi, FRD, turėdamas daug klientų, gali neturėti techninių galimybių ir pakankamai žmogiškųjų išteklių atsižvelgti į kiekvieną nuokrypį.

6.2. KITŲ FINANSŲ ĮSTAIGŲ IR ĮPAREIGOTŲJŲ SUBJEKTŲ SUSTIPRINTA NUOLATINĖ DALYKINIŲ SANTYKIŲ STEBĖSENA (KORESPONDENTINIAI SANTYKIAI)

Pastebima, kad FRD dažniausiai pagal savo nustatytas PPTF rizikos vertinimo ir valdymo procedūras priskiria klientus, kurie yra kitos finansų įstaigos (pvz., EPĮ ir MĮ, įvairias rizikingesnes investicines paslaugas teikiančios bendrovės, įvairūs brokeriai, Forex bendrovės ir pan.) ar kiti įpareigotieji subjektai (pvz., azartinius lošimus ir loterijas organizuojančios bendrovės ar virtualiųjų valiutų keityklų operatoriai ir kt.), didelės PPTF rizikos grupei.

Prieš pradedant tokių klientų stebėseną, pirmiausia reikia tinkamai nustatyti tokio kliento tapatybę ir suprasti kliento keliamą PPTF riziką. Šis procesas yra neatsiejamas siekiant vėliau vykdyti veiksmingą stebėseną. Tokie klientai vykdo operacijas savo klientų vardu ir dažnai santykiai su jais yra korespondentiniai ir jie laikomi respondentais, todėl svarbu, kad tokie klientai respondentai savo klientams taikytų tinkamas kliento ir naudos gavėjo tapatybės nustatymo, gautos informacijos patikrinimo ir stebėsenos procedūras.

Remiantis geriausia patirtimi, rekomenduojama skirti pakankamai dėmesio tokių klientų respondentų kontrolės priemonėms, atsižvelgiant į verslo modelį, ir vertinti toliau nurodytus PPTF rizikos veiksnius, jų mastą (pvz., klientų portfelio pasiskirstymą pagal įvairius kriterijus, nes tik suprantant klientų portfelį, galima įvertinti, ar taikomos proporcingos PPTFP priemonės), o vertinimo išvadas tinkamai dokumentuoti. EBI rizikos veiksnių gairių 8.10 punkte bendrai dėl visų korespondentinių santykių, neatsižvelgiant į respondento įsisteigimo valstybę, nurodyta, kad FRD, kurie veikia kaip korespondentai, atsižvelgdami į rizikos lygį, turėtų įvertinti, ar tikslinga rinkti informaciją apie respondento pagrindinę veiklą, tai, kokio pobūdžio klientus jis pritraukia, PPTFP sistemų ir kontrolės priemonių kokybę (įskaitant viešai prieinamą informaciją apie visas neseniai skirtas administracines arba baudžiamąsias sankcijas už PPTFP įpareigojimų nevykdymą). Siekiant tinkamai vykdyti stebėseną ir parinkti veiksmingiausias stebėsenos priemones, pirmiausia svarbu tinkamai įsivertinti kliento respondento PPTF keliamą riziką pagal turimą klientų portfelį, siūlomus produktus ir paslaugas. Todėl didesnės PPTF rizikos atvejais ypač rekomenduojama atkreipti dėmesį į šiuos rizikos veiksnius:

- kliento rizikos (aptarnaujamų klientų tipai, ekonominės veiklos rūšys, PEP ir pan.);
- geografinės rizikos (klientų rezidavimo ir veiklos valstybės, mokėjimų kryptys ir aptarnaujamos jurisdikcijos, didelės rizikos jurisdikcijos ir kt.);
- teikiamos paslaugos (teikiami produktai) ir jų teikimo kanalo rizika.

Po to, kai gaunama informacija apie kliento finansų įstaigos ar kito įpareigoto subjekto PPTF riziką ir ji įvertinama, rekomenduojama nuspręsti dėl tinkamiausių tokio kliento stebėsenos sprendimų. Remiantis geriausia patirtimi ir FRD nustačius didesnę PPTF riziką, FRD rekomenduojama:

- greta momentinės ir retrospektyvios automatinės stebėsenos, peržiūrėti ir analizuoti ilgesnio laikotarpio kliento operacijas retrospektyviai, siekiant geriau suprasti kliento veiklą ir nustatyti galimus nukrypimus nuo deklaruotos veiklos;
- jei klientams atidarytos kelių tipų sąskaitos, pavyzdžiui, einamoji ir kliento klientų mokėjimams vykdyti, galima pritaikyti stebėsenos sprendimus atskirų tipų sąskaitoms, kad būtų lengviau stebėti kliento veiklą;
- kliento tapatybės nustatymo metu FRD turėtų gauti kliento veiklai reikalingų licencijų ar leidimų iš tų valstybių, kuriose klientas įsisteigęs arba kuriose klientas planuoja siūlyti savo paslaugas ir vykdyti leidimų reikalaujančią veiklą, kopijas ir patikrinti, ar klientas tokius leidimus turi, o stebėsenos metu FRD turėtų vertinti, ar kliento faktinė veikla (pvz., mokėjimų kryptis, veiklos pobūdis) atitinka nurodytą tapatybės nustatymo metu, ar klientas nevykdo veiklos tose valstybėse, kuriose neturi teisės atitinkamą veiklą vykdyti;
- pritaikyti techninius sprendimus apriboti arba įvertinti operacijas, ar klientas neatlieka operacijų su valstybėmis, kuriose neturi leidimo arba licencijos teikti paslaugų (šiuo tikslu FRD turėtų būti žinomos ir aiškiai užfiksuotos valstybės, kuriose klientas nevykdo veiklos, kad stebėsenos metu būtų galima sulyginti; taip pat galima vykdyti dažnesnę periodinę kliento operacijų retrospektyvią peržiūrą, ypač tuo atveju, kai klientas yra naujas);
- vertinti, ar, atsižvelgiant į kliento respondento turimo klientų portfelio PPTF riziką, reikia taikyti naujas ar keisti taikomas ribojančias priemones, pavyzdžiui, drausti per FRD sąskaitas atlikti operacijas iš tam tikrų valstybių (į jas), su tam tikrų grupių klientais, apriboti operacijas iki tam tikros vertės ir pan.;

- įvesti ribojimus, kuriuos pasiekus klientas galėtų atlikti operacijas tik pateikęs papildomus dokumentus;
- didelės PPTF rizikos atvejais taikyti sustiprintas stebėsenos priemones konkrečių klientų atžvilgiu ir rankiniu būdu peržiūrėti visas kliento atliekamas operacijas arba, prieš atliekant operacijas, iš kliento gauti pagrindžiančius dokumentus;
- itin didelės PPTF rizikos atvejais FRD gali apsvarstyti paslaugų teikimą baltojo sąrašo (angl. *whitelist*) principu, t. y. kai FRD leidžia tik aiškiai nurodytą kliento veiklą, o nenurodyta veikla yra draudžiama.

7. TERORISTŲ FINANSAVIMO PREVENCIJA

Nurodymų reikalavimai
59. FRD privalo turėti atskiras vidaus kontrolės procedūras (scenarijus), kad pastebėtų:
59.1. teroristų finansavimo atvejus;
59.2. pinigų plovimo atvejus.

Pirmiausia pažymėtina, kad pagal Nurodymus, FRD privalo turėti atskirus stebėsenos sprendimus ir (arba) scenarijus, jog pastebėtų TF atvejus, tačiau praktikoje dažnai pastebima, kad FRD tokių scenarijų neturi arba TF atvejų stebėseną sieja su tarptautinių finansinių sankcijų ir kitų ribojamųjų priemonių kontrolei skirtais scenarijais.

Kalbant apie TF, atkreiptinas dėmesys, kad teroristai naudoja panašias schemas kaip ir pinigų plovėjai siekdami išvengti teisėsaugos institucijų dėmesio ir nuslėpti savo finansuotojų tapatybes, lėšų šaltinį ir galutinių lėšų gavėjų tapatybes. Pažymėtina, kad TF skirtos lėšos gali būti gaunamos iš teisėtos veiklos (pvz., ne pelno siekiančių organizacijų, donorų, darbuotojų atlyginimų ir pan.) arba iš nusikalstamos veikos – išpirkų už pagrobimus, prekybos narkotikais[14], ginklų prekybos. Kalbant apie TF skirtas lėšas iš teisėtos veiklos, ypač didelę riziką kelia vietinio ekstremizmo pavieniai atvejai, kuriems neretai nereikia gauti daug lėšų siekiant įvykdyti teroro aktus. Be to, lėšas, gaunamas iš teisėtos veiklos kaip susijusias su TF, yra sunkiau nustatyti ir dažnai gali būti reikalinga naudoti gerokai daugiau tyrimo priemonių, pavyzdžiui, papildomą neigiamos informacijos apie klientą paiešką, kai klientas viešai reiškia pritarimą teroristų organizacijų veiklai ir pan.

Papildomai pažymėtina, kad kai kurie šaltiniai siūlo teroristų finansavimą vadinti platesne sąvoka kaip „išteklių gavimas" (angl. *resourcing*), kadangi TF šaltiniai gali būti ne tik pervedamos piniginės lėšos, tačiau ir siunčiamos prekės (pvz., elektroninės prekės), kurių pardavimo pajamos gali būti panaudojamos teroro aktams finansuoti. TF gali būti naudojami ir įvairios prekybos finansavimo pinigų plovimo schemos (pvz., angl. *over-invoicing, under-invoicing, ghost-shipping* ir pan.).

Dažnai TF rizika siejama su tam tikromis didesnės rizikos valstybėmis, todėl reikėtų įvertinti ne tik pačias valstybes, tačiau ir atskirus miestus ar regionus, kuriuose yra padidinta TF rizika (pvz., Turkijos ir Sirijos pasienio miestai kaip Gaziantepas, Mardinas, Šanliurfa ir pan.) Vertinant geografinę riziką, svarbu nesusikoncentruoti į vien tik žinomiausias teroristų organizacijas kaip ISIS, tačiau atkreipti dėmesį į TF riziką Afrikos, Šiaurės Kaukazo, Pietryčių Azijos regionuose[15]. Šiuo tikslu rekomenduojama vertinti ir „Transparency International" ir žmogaus teisių organizacijų skelbiamus valstybių rizikos indeksus, nes dažnai teroristų organizacijos yra linkusios veikti tose valstybėse, kuriose aukšta korupcija, neužtikrinamos žmogaus teisės ir pan.

[14] https://www.state.gov/2020-international-narcotics-control-strategy-report

[15] https://cisac.fsi.stanford.edu/mappingmilitants#highlight_text_11651; https://www.state.gov/country-reports-on-terrorism/#crt; https://reliefweb.int/sites/reliefweb.int/files/resources/GTI-2022-web.pdf

Atitinkamai tuo tikslu svarbu atkreipti dėmesį ne tik į jau įprastas teroristų organizacijas kaip „Al-Qaida", ISIS, grupuotė „Boko Haram", tačiau atliekant tyrimus nepamiršti ir radikalėjančių dešiniųjų grupuočių (vietinio terorizmo), kurių rizika nuosekliai auga[16]. Atkreiptinas dėmesys, kad išsamiai terorizmo finansavimui būdingos tipologijos yra nurodomos tiek Grėsmių nacionaliniam saugumui vertinime[17], tiek FATF gairėse[18].

Kalbant apie TF prevenciją ir klientų stebėseną, svarbu turėti ne tik tinkamus stebėsenos sprendimus ir (arba) scenarijus, tačiau ir kokybiškai atlikti vidaus tyrimus, atkreipiant dėmesį į įvairius TF rizikos veiksnius, t. y. FRD, kurdamas TF scenarijus, turėtų įvertinti ne tik geografinius rizikos veiksnius, bet ir tai, iš kokios veiklos gali būti vykdomas finansavimas, pavyzdžiui, iš prekybos narkotikais (pavyzdys Afganistanas ir prekyba opiumu bei heroinu).

Su TF susijusiuose scenarijuose reikėtų atsižvelgti į toliau nurodytus veiksnius, tačiau pabrėžtina, kad šis sąrašas tik pavyzdinis ir jis negali būti laikomas nei minimaliai reikalingu taikyti, nei baigtiniu:

- grynųjų pinigų įnešimas, po kurio atliekamos operacijos į konfliktų zonas (fiziniai asmenys, ne pelno siekiančios organizacijos);
- kliento gaunamų pajamų ir mokėjimų vertė neatitinka kliento deklaruotos darbinės veiklos;
- mokėjimai trečiųjų asmenų vardu, siekiant nuslėpti tikrąjį mokėtoją arba gavėją;
- sąskaita naudojama lėšoms surinkti ir vėliau joms persiųsti į didesnės PPTF rizikos valstybes;
- mokėjimai vykdomi į valstybes, kurios nėra susijusios su kliento įprasta arba ekonomiškai paaiškinama veikla;
- prisijungimai iš IP adresų, esančių konflikto zonose arba valstybėse, kuriose padidinta TF rizika;
- mokėjimai į konflikto zonas arba iš jų bei grynųjų pinigų išgryninimas konflikto zonose;
- mokėjimai į labdaros organizacijas, esančias Sirijoje ir kitose konflikto zonose arba valstybėse greta jų;
- finansinė kliento veikla susijusi su keliavimu į konfliktų zonas, pavyzdžiui, perkant lėktuvo bilietus į Siriją per Turkiją ir kitus atvykimo taškus, įskaitant Jordaniją, Libaną ar Izraelį;
- virtualiojo turto naudojimas siekiant įgyti tam tikrą anonimiškumą;
- kompleksiniai scenarijai, pagal kuriuos būtų stebimas ir bendras kliento vaizdas, t. y. ne vien valstybės, į kurias klientas siunčia ar iš kurių gauna mokėjimus atskirai, bet ir būtų vertinamos kartu mokėjimų kryptys.

Papildoma informacija apie praktinę TF veiklą ir naujausias tipologijas neretai atspindima ir įvairiose viešose ataskaitose ir tyrimuose, pavyzdžiui, Europolo, RUSI instituto[19].

[16] https://www.theguardian.com/us-news/2021/sep/08/post-911-domestic-terror

[17] Grėsmių nacionaliniam saugumui vertinimas, 2019 (https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-LT.pdf).

[18] Terrorist Financing Risk Assessment Quidance, 2019 (https://rm.coe.int/terrorist-financing-risk-assessment-guidance-fatf/16809676a3, https://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf; https://www.fatf-gafi.org/publications/methodsandtrends/documents/tf-west-africa.html).

[19] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/659446/EPRS_BRI(2021)659446_EN.pdf; https://rusi.org/explore-our-research/topics/terrorist-financing

8. VIDAUS TYRIMAI

Nurodymų reikalavimai
66. FRD, vykdydamas kliento dalykinių santykių ir operacijų (sandorių) stebėseną, privalo užtikrinti, kad kiekvienas automatinės stebėsenos sprendimo (jeigu FRD turi įdiegtų automatinės stebėsenos sprendimų) sugeneruotas įspėjimas (angl. *alert*) arba kiekviena kliento operacija (jeigu FRD neturi įdiegtų automatinės stebėsenos sprendimų), atitinkanti įtartinumo kriterijus, būtų FRD darbuotojų laiku peržiūrima ir tinkamai išanalizuojama, o šie veiksmai dokumentuojami ir saugomi tokiu formatu, kad prireikus galėtų būti pateikti priežiūros institucijai.
67. Kai FRD taikomo dalykinių santykių ir operacijų (sandorių) stebėsenos proceso metu nustatoma, kad dėl kliento (-ų) veiklos turi būti atliekamas vidaus tyrimas, atlikto vidaus tyrimo rezultatai ir išvados privalo būti dokumentuojami, aiškiai nurodoma atlikto vidaus tyrimo eiga ir rezultatai, įskaitant ir informaciją, kokiu pagrindu buvo priimtas atitinkamas sprendimas (sprendimas nutraukti vidaus tyrimą, jį išplėsti arba pranešti FNTT apie nustatytas įtartinas operacijas ir pan.), ir tai turi būti saugoma PPTFPĮ nustatytais terminais.

Pirmiausia pažymėtina, kad, nors teisės aktuose nėra apibrėžta vidaus tyrimo sąvoka, tačiau praktikoje pastebima, jog įprastai tyrimu laikoma išsamesnė analizė, kurią atlikti reikia papildomų FRD darbuotojų veiksmų, o ne vien įprastai peržiūrėti stebėsenos sistemos sugeneruotą įspėjimą ir jį uždaryti. Taigi, FRD gali patys apsibrėžti tyrimo sąvoką ir tyrimo metu privalomus atlikti veiksmus, tačiau akcentuotinas galutinis rezultatas, kad tiek stebėsenos sistemos sugeneruotų įspėjimų analizė, tiek išsamesni tyrimai neturėtų būti atliekami formaliai. Peržiūrint stebėsenos sistemos sugeneruotus įspėjimus ar vykdant išsamesnius tyrimus, turėtų būti kritiškai vertinama tiek anksčiau kliento pateikta, tiek iš kliento gauta nauja informacija ir šie aspektai (tačiau pažymėtina, kad šis sąrašas nėra baigtinis):

- mokėjimo operacijų paaiškinamumas, loginis ir ekonominis pagrįstumas;
- vertinama bendrai, ar kliento faktinė veikla atitinka kliento deklaruotą veiklą arba veiklą, būdingą atitinkamo verslo sektoriaus klientams;
- vertinama, ar kliento veiklos pokyčiai (pvz., pasikeičia mokėjimų kryptys, valstybės, atsiranda naujų partnerių) gali būti pagrįstai paaiškinami;
- vertinama su operacijomis susijusi lėšų kilmė, mokėjimo kryptys ir mokėjimų pagrindas (pvz., mažai tikėtina, kad Saudo Arabija, daugiausia pasaulyje išgaunanti naftos, importuos naftos produktus arba Brazilija apelsinus, nes ji yra didžiausia apelsinų augintoja pasaulyje);
- vertinama, ar kliento vykdomi mokėjimai, susiję su prekėmis arba paslaugomis, atitinka kliento deklaruotą vykdomo verslo pobūdį;
- vertinama operacijų vertė (pvz., vertė neatitinka kliento nurodytos ekonominės veiklos arba panašiam verslo sektoriui įprastų sandorių vertės);
- vertinami atvejai, kai vykdomos operacijos yra pernelyg sudėtingos ir klientas nepateikia pagrįsto paaiškinimo dėl tokių operacijų sudėtingumo arba operacijos vykdomos su partneriais tikslinėse teritorijose ir klientas negali pagrįstai paaiškinti, kodėl lėšos pervedamos per tikslinėse teritorijose įsisteigusias bendroves;
- atidžiai vertinama viešų šaltinių informacija tiek apie klientą, tiek apie jo partnerius, su kuriais vykdomos operacijos.

Pastebima geriausia patirtis, kai, nustačius įtartinus vieno kliento partnerius dėl galimo PP ar TF, FRD atliekamas platesnis vidaus tyrimas ir visų klientų operacijų duomenų bazėje paieškoma, ar daugiau klientų nevykdė operacijų, susijusių su tokiais partneriais, o nustačius tokių operacijų, imamasi PPTF rizikos valdymo

veiksmų. Pažymėtina, kad vidaus tyrimų rezultatas (pvz., darbuotojo išvados dėl kliento operacijų ar veiklos, sprendimo (pvz., sprendimas nutraukti vidaus tyrimą, jį išplėsti arba pranešti FNTT apie nustatytas įtartinas operacijas ir pan.) priėmimo pagrindas ir t. t.) turėtų būti aiškiai dokumentuojamas. Be to, turėtų būti dokumentuojami ne tik atliekamų išsamesnių tyrimų rezultatai, bet ir stebėsenos sistemos sugeneruoto įspėjimo peržiūros ir analizės rezultatai.

8.1. ĮSPĖJIMŲ PERŽIŪRĖJIMO SVARBOS NUSTATYMAS

FRD, kurių veiklos mastas yra platesnis, naudoja daugiau skirtingų stebėsenos scenarijų ir turi daugiau darbuotojų, vykdančių stebėsenos funkciją, gali pasirinkti teikti pirmenybę įspėjimams pagal skirtingą riziką ir „rizikingiausius" įspėjimus pavesti analizuoti daugiau patirties turintiems darbuotojams.

Įspėjimų svarbos nustatymas turėtų atitikti rizika grindžiamo metodo taikymą ir tai reiškia, kad didžiausią PPTF riziką kelianti kliento veikla turėtų būti peržiūrėta pirmiausia. Atitinkamai diegiant automatinės stebėsenos scenarijus, galima nustatyti scenarijų peržiūros eiliškumo prioritetą (pvz., žemas, vidutinis, aukštas). FRD turėtų organizuoti stebėseną taip, kad įspėjimai būtų peržiūrimi laikantis FRD vidaus terminų ir nesusidarytų pavėluotai peržiūrėtų sugeneruotų įspėjimų sąrašas, o tokiam sąrašui susidarius, pirmenybė būtų teikiama anksčiau sugeneruotų įspėjimų peržiūrai. Be to, rekomenduojama, kad FRD stebėsenos sistemos sugeneruoti įspėjimai būtų peržiūrimi pagal nustatytą kliento PPTF rizikos grupę (pvz., jei klientas yra PEP, dėl jo operacijos stebėsenos sistemoje sugeneruotam įspėjimui bus suteikiamas prioritetas) ir scenarijaus rizikos lygį (pvz., TF scenarijai bus svarbesni už PP scenarijus ir pan.).

8.2. VIDAUS TYRIMO TERMINAI

Teises aktuose nėra nustatytas konkretus terminas, per kurį turi būti atlikta stebėsenos sistemoje sugeneruotų įspėjimų peržiūra arba vykdomas nuodugnesnis vidaus tyrimas. Akcentuotina, kad pačios PPTF prevencijos tikslas – užkirsti kelią nusikalstamai veikai, dėl to įspėjimų peržiūra arba tyrimai dėl įtartinos kliento veiklos turi būti atliekami kaip įmanoma operatyviau. Tuo atveju, kai tyrimai yra pradedami, tačiau nebūtinai užbaigiami per pagrįstą laikotarpį nuo įspėjimo sugeneravimo dienos, kyla rizika, kad nebus užtikrinta veiksminga PPTF prevencija, susijusi su įtartinų piniginių operacijų identifikavimu ir pranešimu FNTT laiku.

8.3. VIDAUS TYRIMŲ DOKUMENTAVIMAS

Kaip nurodyta ir Nurodymuose, įspėjimų peržiūros ir vidaus tyrimų metu atliktų veiksmų seka (angl. *audit trail*) turėtų būti matoma ir aiškiai dokumentuojama nuo pat įspėjimo sugeneravimo stebėsenos sistemoje momento arba vidaus tyrimo pradžios kitu pagrindu. Tinkamai įgyvendinus šį procesą, turėtų būti aišku, koks darbuotojas, kada ir kokius veiksmus atliko pradėjęs tyrimą, kokios ir kuo remiantis buvo padarytos tyrimo išvados.

Toks veiksmų sekos dokumentavimas turėtų būti vykdomas automatiškai su IT sistemos pagalba, jog būtų kuo mažiau darbuotojo įsikišimo į patį procesą, taip būtų išvengiama, kad jis sąmoningai praleidžia tam tikrus žingsnius.

Pats tyrimo dokumentavimas turi būti aiškus, grįstas faktais (informacija), pagrindžiančia, kas, kada, kur, kokiu būdu ir kodėl vykdė operacijas (ar vieną operaciją). Turi būti aiškiai nurodytas tiek laikotarpis, kurio buvo peržiūrėtos mokėjimo operacijos, tiek pateiktos išvados, kodėl kliento veikla yra arba nėra neįprasta ar įtartina, priimtų sprendimų (pvz., nutraukti vidaus tyrimą) pagrįstumas. Siekiant pasisemti idėjų dėl tyrimų

dokumentavimo turinio, rekomenduojama atkreipti dėmesį ir į FNTT parengtą pranešimų apie įtartinas pinigines operacijas ar sandorius atmintinę[20].

Siekiant nuoseklumo, rekomenduotina, kad finansų įstaigoje būtų vienas šablonas arba pagrindinės gairės, pagal kurias būtų dokumentuojamas tyrimas, nepaisant to, kuris specialistas atlieka tyrimą. Pažymėtina tai, kad, norint užtikrinti patį tyrimo dokumentavimo nuoseklumą, remiantis geriausia patirtimi, rekomenduotina, kad svarbiausi „laukeliai" dokumentuojant tyrimą būtų privalomi, be kurių užpildymo tyrimas negalėtų būti baigtas.

Tinkamai dokumentuotas tyrimas svarbus ne tik konkrečiu metu vertinant kliento veiklą, tačiau aktualus ir ateityje, kai kitas ar tas pats darbuotojas iš naujo vykdys kliento veiklos tyrimą, todėl svarbu, kad tyrimo išvada būtų aiški ir būtų galima palyginti dabartinę kliento veiklą su ankstesne.

8.4. DARBUOTOJŲ VYKDOMOS STEBĖSENOS KOKYBĖS UŽTIKRINIMAS

Siekiant nuolat tobulinti stebėsenos veiksmus, stebėti, ar praktikoje darbuotojai vadovaujasi nustatytomis procedūromis, ir užtikrinti tinkamą stebėsenos procesą, rekomenduojama vykdyti atskirų stebėsenos procesų darbuotojų atliekamo darbo kokybės patikrą.

Atliekant kokybės patikrą (angl. *quality assurance*), rekomenduojama naudoti standartizuotą formą, kurioje būtų fiksuojami patikros rezultatai. Be to, FRD gali įtvirtinti atskira procedūra kokybės patikros rezultatų apskaičiavimo metodiką ir nustatyti rėžius, kuriuos darbuotojams pasiekus būtų laikoma, kad kokybės rezultatai yra priimtini arba neatitinka kokybės reikalavimų.

Kokybės užtikrinimo patikras rekomenduojama atlikti periodiškai (pvz., kas mėnesį ar kelis mėnesius) ir su patikros rezultatais supažindinti darbuotojus, o pastebėjus dažnai pasikartojančių klaidų, rekomenduojama atlikti mokymus atitinkamą funkciją vykdantiems darbuotojams.

Kartu rekomenduojama FRD taikyti rizika grindžiamą metodą dėl atliekamų kokybės patikrų apimties, pavyzdžiui, taikyti dažnesnę ir didesnės apimties kokybės patikrą (pvz., peržiūrėti didesnę imti klientų bylų) naujų darbuotojų atžvilgiu, pakeitus ar įdiegus naują procesą, pradėjus naudoti naują IT sistemą, vidaus PPTF audito ar išorės patikrinimo metu nustačius tam tikrų trūkumų srityje, kurią reikią tobulinti, siekiant įsitikinti, kad trūkumai nesikartoja ir pan.

8.5. VEIKSMAI PATEIKUS PRANEŠIMĄ FNTT

Kai FRD praneša FNTT apie įtartiną kliento veiklą ar operaciją ir nusprendžia toliau tęsti dalykinius santykius su klientu, pažymėtina, kad ankstesnis pranešimas FNTT neatleidžia FRD nuo pareigos toliau vykdyti tokio kliento stebėseną, ypač tuo atveju, jeigu kliento veikloje buvo nustatyta įtarimų ar neįprastos veiklos požymių, o tai reiškia, kad tokie klientai kelia didesnę PPTF riziką. Tokių klientų atvejais vykdoma stebėsena gali būti ir sustiprinta, pavyzdžiui, tam tikrais nustatytais intervalais išsamiau peržiūrima kliento veikla, kiekviena operacija peržiūrima rankiniu būdu, dėl operacijų gaunami vyresniojo vadovo pritarimai, vertinama, ar klientas toliau nevykdo operacijų, apie kurias buvo pranešta FNTT. Tačiau pažymėtina, kad FRD, vykdydamas tokią sustiprintą stebėseną, turi užtikrinti, kaip ir įpareigoja teisės aktai, kad klientas nesuprastų, jog apie jo veiklą jau buvo pranešta FNTT.

[20] https://www.fntt.lt/lt/naujienos/parengta-pranesimu-apie-itartinas-pinigines-operacijas-ar-sandorius-atmintine/4137

8.6. NETINKAMAI VYKDOMOS STEBĖSENOS PAVYZDŽIAI

Toliau pateikiama pavyzdžių, kai stebėsena ir vykdomi tyrimai turėjo trūkumų. Dažniausiai pasitaikančios klaidos yra tos, kai, nors FRD stebėsenos priemonėmis vykdomas operacijas pastebi, tačiau vykdomi tyrimai yra formalūs, visapusiškai nevertinamas visas kliento veiklos vaizdas, nepakankamai aiškinamasi dėl kliento vykdomos veiklos ir lėšų kilmės, nepakankamai vertinama įtartinumo požymių turinti veikla ir atitinkamai nesurenkama kliento veiklai pagrįsti reikalinga pakankama informacija ir dokumentai.

1 pavyzdys

Klientas A – fizinis asmuo, kurio mokėjimo operacijų apyvarta sudarė apie 1 mln. Eur per kelerius metus. Per septynias kalendorines dienas klientas gavo keturis mokėjimo pavedimus, kurių bendra suma 205 000 Eur, iš savo asmeninės sąskaitos Katare į savo sąskaitą, kuri atidaryta FRD. KYC anketoje nurodyta, kad klientas yra Ukrainos pilietis, dirbantis teisininku Lietuvoje ir gaunantis 800 Eur bruto darbo užmokestį. Iš praėjusių metų kliento sąskaitos išrašo matyti, kad klientui tokios didelės mokėjimo operacijos nėra būdingos ir FRD neturėjo žinių apie kitus kliento lėšų šaltinius. FRD sustabdė minėtas operacijas ir išsiaiškino, kad šių gautų lėšų tikslas – nekilnojamojo turto pirkimas. FRD nurodė, kad lėšos gautos už klientui priklausančio automobilio pardavimą (pridėta sutartis). Papildomų dokumentų dėl lėšų kilmės, ypač atsižvelgiant į darbo užmokesčio ir parduoto automobilio vertės neatitiktį, FRD neatliko, neatliko ir papildomo tyrimo.

2 pavyzdys

Kliento B mokėjimo operacijų apyvarta – apie 4 mln. Eur per metus. Užmezgant dalykinius santykius, klientas KYC anketoje nurodė, kad sąskaita FRD bus skirta gauti pajamoms iš įmonės veiklos ir vykdyti su pagrindine veikla susijusius mokėjimus; pagrindiniai įmonės partneriai buvo nurodytos įmonės, užsiimančios farmacijos veikla, o planuojama vidutinė mėnesio apyvarta iki 150 000 Eur. Kliento pirmosios operacijos sąskaitoje buvo tokios: gegužės 25 d. gauta 700 000 Eur suma iš Įmonės X ir per valandą išsiųsta Įmonei Y, gauta 500 000 Eur suma iš Įmonės Z ir per valandą išsiųsta Įmonei Y, tų pačių metų gegužės 26 d. gauta 200 000 Eur suma iš Įmonės Z, 200 000 Eur suma iš Įmonės X ir 400 000 Eur per valandą išsiųsta Įmonei Y. Minėtos operacijos neatitiko kliento deklaruotos veiklos KYC anketoje, o prieš tai jokių mokėjimų sąskaitoje nebuvo vykdoma, tačiau FRD šių operacijų nevertino kaip neįprasto dydžio ir neįprastos struktūros sandorių, ypač atsižvelgiant į tai, kad gaunamos lėšos iš karto persiunčiamos, o tai atitinka tranzitinės sąskaitos požymius.

3 pavyzdys

Klientas C priskirtas didelės PPTF rizikos grupei. Kliento registracijos vieta – Šiaurės Kipro laisva ekonominė zona, kliento teisinis statusas – juridinis asmuo. Per metus klientas atliko 520 operacijų, kurių vertė apie 120 mln. Eur, didžioji jų dalis buvo analizuojama po įspėjimų sugeneravimo stebėsenos sistemoje. Kliento nurodyta veikla – IT įrangos tiekimas ir paslaugų teikimas verslo klientams, nurodyti keli verslo partneriai. Sutartyje su Partneriu X nurodyta, kad Klientas C teiks mokėjimų aptarnavimo paslaugas (angl. *acquiring*), tačiau praktikoje atliekamų mokėjimų pobūdis bei suma neatitinka sutartyje numatytų sąlygų. Vienintelės Kliento C įplaukos į sąskaitą (60 mln. Eur į kliento sąskaitą gautų mokėjimų) yra gaunamos iš virtualiojo turto keitimo platformos. Gaunamų mokėjimų paskirtis – virtualiojo turto keitimas į eurus. Tokia mokėjimų paskirtis nesusijusi su FRD turima kliento informacija bei jo veiklos pobūdžiu. Pastebėtina, jog FRD darbuotojai atliko didelės dalies mokėjimų analizę, tačiau visais atvejais konstatuota tik tai, kad virtualiojo turto keitimo platforma yra žinoma virtualiojo turto keitykla ir dėl to papildomų klausimų nekyla, papildomų veiksmų nesiimta, nors mokėjimų pobūdis neatitiko FRD turimos informacijos apie klientą.

4 pavyzdys

Kliento D apyvarta nuo dalykinių santykių pradžios, t. y. per dvejus metus, sudaro apie 1,80 mln. Eur. Klientas yra fizinis asmuo, kuris turi sąsajų su to FRD darbuotoju, kuris atliko šio kliento mokėjimų analizę. Analizės išvados sutampa su mokėjimo paskirtyje nurodyta informacija – „dovana“, „tas pats gavėjas“ ir pan. Klientas atliko 95 mokėjimus, kurių vertė daugiau nei 150 tūkst. Eur ir kurių paskirtyje nurodyta „labdara, auka“ įvairiems fiziniams ir juridiniams asmenims, tačiau jokios informacijos byloje apie šiuos mokėjimus nepateikta. Klientas dar atliko vienkartinį 250 000 Eur

pavedimą gavėjui, tačiau darbuotojo, atlikusio operacijų stebėseną, išvadoje, atlikus šio mokėjimo analizę, nurodyta „tas pats gavėjas", o papildomi dokumentai nesurinkti.

5 pavyzdys

Kliento E apyvarta nuo dalykinių santykių pradžios, t. y. per dvejus metus, sudaro apie 140 mln. Eur. Klientas yra finansų įstaiga, kuri FRD paslaugomis naudojasi savo klientų mokėjimams vykdyti. Pagal FRD pateiktą informaciją, beveik visas į kliento sąskaitą įeinančias lėšas sudarė Įmonės A pervestos lėšos, kurių vertė apie 60 mln. Eur. Nors pagal FRD pateiktą informaciją beveik visos operacijos buvo automatiškai sustabdytos, prie visų šių operacijų yra nurodytas tas pats neišsamus bendro pobūdžio komentaras: „tas pats gavėjas". Jokių kitų komentarų dėl šių lėšų kilmės, operacijų pobūdžio, pagrįstumo ir pan. nenurodyta. Remiantis įmonių registro duomenimis, Įmonė A nevykdo veiklos nuo 2012 m., o Kliento E ir Įmonės A naudos gavėjai yra tie patys asmenys. FRD nurodė, kad tai sandoriai tarp dviejų finansų įstaigų, tačiau papildomų dokumentų ar išsamesnių paaiškinimų nepateikė.

6 pavyzdys

Kliento F ir Kliento G teisinis statusas – juridinis asmuo. Dalykiniai santykiai su klientais užmegzti panašiu metu, jų apyvarta nuo dalykinių santykių pradžios, t. y. per pusę metų, sudarė atitinkamai apie 25 mln. ir 18 mln. Eur. Nors abiejų klientų atstovas yra tas pats asmuo, tačiau naudos gavėjai yra skirtingi, klientų veiklos modelis yra panašus. Abu klientai užsiima internetine prekyba ir, nors įmonės parduoda skirtingus produktus, tiek viena, tiek kita įmonė turi po keletą interneto puslapių, kurių dizainas labai panašus, o parduodamos prekės ir net jų išdėstymas visuose interneto puslapiuose yra identiškas. Abiejų klientų operacijos ir sąskaitose vykdoma veikla yra labai panaši – beveik visos įeinančios lėšos yra atsiskaitymai už parduotas prekes ir beveik visos išeinančios lėšos yra atsiskaitymai už IT, rinkodaros ar konsultacijų paslaugas. Abi įmonės tiek gauna lėšas iš tų pačių siuntėjų, tiek siunčia jas tiems patiems gavėjams. Atkreiptinas dėmesys, kad pagal abiejų klientų sutartis su Įmone B, kurios yra identiškos, abu klientai iš Įmonės B įsigyja interneto puslapių ir mobiliųjų programėlių kūrimo bei diegimo paslaugas, tačiau, pagal informaciją Įmonės B interneto svetainėje, Įmonė B veikia mokėjimo paslaugų srityje ir nesiūlo paslaugų, kurios yra įvardytos sutartyse su klientais F ir G. Akcentuotina, kad, nors klientas F ir klientas G yra įmonės, kurios įsteigtos anksčiau nei prieš metus, tačiau per pusę veiklos metų už parduodamas prekes gavo itin dideles sumas. Atsižvelgiant į abiejų įmonių steigimo datą, veiklos pobūdį ir dydį (remiantis viešai prieinama informacija abiejose įmonėse yra įdarbinta tik po vieną asmenį), tiek sumos už parduotas prekes, tiek sumos už įsigytas paslaugas yra nepagrįstai didelės.

7 pavyzdys

Kliento H nurodyta veikla – virtualiojo turto keitykla ir išvestinių investavimo priemonių teikėjas, teisinis statusas – juridinis asmuo. Kliento registracijos vieta – Kipras, licencija veiklai išduota taip pat Kipre. Kliento anketoje teigiama, kad jis teikia paslaugas visose ES valstybėse, išskyrus Vengriją, Lenkiją, Latviją, Ispaniją, Belgiją, Vokietiją ir Prancūziją (pažymėtina, kad būtent šiose valstybės klientas neturi licencijos teikti paslaugas). Kliento atliktų mokėjimų vertė apie 30 mln. Eur, dauguma šių mokėjimų buvo analizuojami FRD stebėseną vykdančių darbuotojų. Pavyzdžiui, klientas gavo 10 mokėjimų iš kliento fizinio asmens Prancūzijoje, jų bendra vertė 70 tūkst. Eur, ir prie tokių mokėjimų FRD nurodo, kad kliento veikla atitinka deklaruotą. Tačiau FRD, analizuodamas kliento mokėjimus, neatsižvelgia į kliento anketoje nurodytą informaciją dėl valstybių, kuriose klientas neturi teisės teikti paslaugų. Vertinant bendrai kliento veiklą, beveik 20 proc. operacijų buvo atlikta iš valstybių, kuriose klientas veiklos neplanuoja arba negali atlikti. Pažymėtina, kad apie 80 proc. gautų skundų dėl kliento veiklos yra iš klientų iš valstybių, kuriose klientas yra nurodęs, kad neteikia paslaugų. Be kita ko, klientų skunduose yra nurodoma papildoma informacija, kad klientas naudoja daugiau internetinių puslapių, nei buvo nurodęs dalykinių santykių užmezgimo metu, tačiau FRD šios pasikartojančios informacijos apie kitus kliento naudojamus puslapius ir jose siūlomas paslaugas papildomai netikrino ir nevertino.

8 pavyzdys

Klientas I – fizinis asmuo, jo deklaruota veikla prekyba internetu, susijusi su elektroniniais prietaisais. Klientas per keturis mėnesius atliko 900 operacijų, kurių vertė apie 110 tūkst. Eur, su daugiau nei 700 mokėtojų ir gavėjų. Kliento nurodyta gimimo valstybė – Sirija, o pagal kliento IP duomenis matyti, kad klientas prie sąskaitos jungiasi iš Turkijos pasienio su Sirija miestų (Gaziantepo, Mardino, Hatay ir pan.), kurie siejami su didesne tiek pabėgėlių, tiek TF rizika. FRD, nors ir rinko informaciją

apie kliento IP adresus, tačiau išsamiau šios informacijos neanalizavo ir nevertino, kliento neprašė paaiškinti jo atliekamų operacijų tikslo ir pagrindo.

9 pavyzdys

Klientas J – fizinis asmuo, jo deklaruota veikla (dalykinių santykių užmezgimo metu) – studentas, vėliau – individuali veikla. Per pirmus du mėnesius nuo dalykinių santykių pradžios klientas atliko 700 operacijų, kurių vertė apie 400 tūkst. Eur, su daugiau nei 550 mokėtojų ir gavėjų. Apie 20 proc. kliento mokėjimų buvo vykdomi išskaidant operacijas per kelias minutes, nors toks operacijų išskaidymo tikslas nėra aiškus. Pažymėtina, kad, nors FRD vykdydamas stebėseną pastebėjo daugumą kliento atliktų mokėjimo operacijų ir nustatė, jog kliento veikla neatitinka jo deklaruotos veiklos ir FRD turimos informacijos, tačiau nebuvo imtasi jokių papildomų veiksmų siekiant išsiaiškinti neatitikimus ir vykdomų kliento operacijų pagrindą bei tikslą. Taip pat nebuvo tinkamai identifikuotas kliento veiklos pobūdis ir pajamų šaltinis.

10 pavyzdys

Klientas L priskirtas didelės PPTF rizikos grupei, jo registracijos valstybė – Turkija, teisinis statusas – juridinis asmuo. Klientas iš savo sąskaitos Turkijos finansų įstaigoje persivedė 3 mln. Eur į FRD atidarytą sąskaitą. Šis mokėjimas buvo sustabdytas, tačiau FRD nurodė, kad operacija įvyko tarp pačios įmonės sąskaitų, todėl sugeneruotas įspėjimas buvo uždarytas nenustačius įtartinumo. FRD nevertino kliento lėšų kilmės, nenustatė, ar pradinė lėšų kilmė nėra iš trečiųjų asmenų, ypač atsižvelgiant į tai, kad mokėjimas atliktas iš finansų įstaigos, kuri yra trečiojoje valstybėje, sąskaitos.

11 pavyzdys

Kliento M registracijos valstybė – tikslinė teritorija, teisinis statusas – juridinis asmuo. Deklaruota kliento veikla – rinkodaros paslaugos. Per du mėnesius į kliento sąskaitą gauti 85 mokėjimai iš Vokietijoje ir Austrijoje esančių finansų įstaigų sąskaitų, kurios priklauso 60 skirtingų fizinių asmenų. Atskirų operacijų vertė buvo nuo 500 iki 20 tūkst. Eur. Beveik visų operacijų paskirtis yra nurodyta vienoda, t. y. identiškas raidžių ir skaičių derinys, pavyzdžiui, „ABCM55669984“. FRD analizavo tik dvi kliento vykdytas operacijas, dėl kurių FRD kreipėsi į klientą su prašymu pateikti tik mokėtojo asmens dokumento kopiją ir gyvenamosios vietos adresą pagrindžiantį dokumentą. Klientui pateikus minėtus dokumentus, lėšos įskaitytos į sąskaitą. Pažymėtina, kad FRD nesiaiškino, kokiu tikslu lėšos yra pervedamos į kliento sąskaitą, kokia yra šių lėšų kilmė, kokios sąsajos yra tarp lėšų mokėtojo ir kliento, ar siuntėjai iš tiesų įsigijo prekes ar paslaugas iš kliento ir pan., o tokia informacija nebuvo savaime aiški, remiantis FRD apie klientą surinkta informacija ar operacijų paskirties informacija.

12 pavyzdys

Kliento N registracijos valstybė – Jungtinė Karalystė, teisinis statusas – juridinis asmuo. Deklaruota kliento veikla prieglobos paslaugos (angl. *hosting services*). Per tris mėnesius į kliento sąskaitą įeinančios lėšos buvo pervestos iš atskirų fizinių asmenų. Atskirų operacijų vertė buvo nuo 100 iki 50 tūkst. Eur, o bendra operacijų vertė sudarė 2 mln. Eur. Lėšas į kliento sąskaitą pervedė apie 250 skirtingų fizinių asmenų iš įvairių Europos valstybių: Belgijos, Austrijos, Vokietijos, Nyderlandų, Prancūzijos, Ispanijos, Italijos, Portugalijos, Jungtinės Karalystės ir kt. Vykdydamas operacijų stebėseną, FRD analizavo tik operacijas, o sustabdęs kliento operacijas, kreipėsi į klientą su prašymu pateikti mokėtojo asmens dokumento kopiją ir siuntėjo adresą pagrindžiantį dokumentą. Klientui pateikus dokumentus, operacijos buvo įvykdytos. Minėtais atvejais kliento pateiktos siuntėjų asmens dokumentų kopijos ir adresą pagrindžiantys dokumentai nepaaiškina operacijų tikslo, pobūdžio, ekonominio pagrindo ar lėšų kilmės, o FRD įskaitė operacijas į kliento sąskaitą nesiėmęs priemonių tam išsiaiškinti. Pavyzdžiui, neprašė pateikti dokumentų, įrodančių kad siuntėjai iš tiesų įsigijo paslaugas (pvz., sutartis), už kurias apmoka, neprašė pateikti sąskaitų faktūrų, kurių pagrindu vykdomas mokėjimas, ir pan. Be to, FRD gavo 43 prašymus atšaukti inicijuotas operacijas. Kliento gautos lėšos buvo pervestos Įmonei R, susijusiai su virtualiuoju turtu ir investavimu, tačiau FRD nesiaiškino, kokias prekes ar paslaugas klientas įsigijo iš Įmonės R, neprašė pateikti dokumentų, pagrindžiančių, kad prekės ar paslaugos tikrai buvo įsigytos, suteiktos ir kad mokėjimas atliekamas būtent už pristatytas prekes ar suteiktas paslaugas. Pažymėtina, kad tokia kliento veikla gali atitikti tipologiją, kai, surinkus lėšas iš daugelio skirtingų mokėtojų (angl. *many-to-one*), jos pervedamos į kitą sąskaitą, siekiant užmaskuoti lėšų kilmę.