LIETUVOS BANKO
FINANSINIŲ PASLAUGŲ IR RINKŲ PRIEŽIŪROS DEPARTAMENTAS

Elektroninių pinigų ir mokėjimo įstaigų vadovams

2023-07-24

Pagal adresatų sąrašą

DĖL PINIGŲ PLOVIMO IR TERORISTŲ FINANSAVIMO RIZIKOS VALDYMO

Lietuvos bankas nuolat siekia nustatyti ir įvertinti elektroninių pinigų ir mokėjimo įstaigoms (EPMĮ) kylančią pinigų plovimo ir teroristų finansavimo (PPTF) riziką, todėl atlikdamas finansų rinkos priežiūrą nustato ir vertina įvairius PPTF rizikos veiksnius bei informuoja EPMĮ apie sektoriui būdingas rizikas.

Lietuvos bankas 2022 m. birželio 13 d. raštu „Dėl pinigų plovimo ir teroristų finansavimo rizikų valdymo“[1] Nr. S 2022/(34.128.E-3900)-12-3132 (toliau – 2022 m. raštas) jau buvo atkreipęs EPMĮ vadovų dėmesį į PPTF rizikas ir tinkamą PPTF rizikų valdymo (mažinimo) poreikį. Pažymime, kad anksčiau nurodytos rizikos (dėl didelės PPTF rizikos klientų, sukčiavimo rizikos, tarptautinių finansinių sankcijų įgyvendinimo, korespondentinių santykių ir korespondentinių santykių požymių turinčių paslaugų, tarpininkų kontrolės ir kt. rizikų) ir raginimai stiprinti kontrolės priemones ir toliau išlieka aktualūs.

2022 m. rašte buvo detaliai aprašytos geografinės rizikos ir galimos neigiamos pasekmės dėl netinkamo šios rizikos valdymo, pvz., bandymas išvengti taikomų tarptautinių finansinių sankcijų, pasitelkiant bendroves iš tikslinių teritorijų, sunkumai nustatant naudos gavėjus ir kita rizika dėl palankių sąlygų nelegaliu būdu įgytoms lėšoms patekti į finansų sistemą dėl šiose valstybėse taikomų silpnesnių PPTF prevencijos kontrolės priemonių. Šios rizikos ir toliau išlieka itin aktualios, atsižvelgiant į tai, kad EPMĮ ir toliau aptarnauja klientus bei vykdo mokėjimo operacijas į tikslines teritorijas[2] ir iš jų. Geografinė rizika lygiai taip pat aktuali ir dėl didelės rizikos valstybių[3] bei trečiųjų valstybių[4] dėl joms būdingų įvairių PPTF rizikos veiksnių, įskaitant silpnesnį reguliavimą PPTF srityje ir atitinkamoms valstybėms būdingas tipologijas. Papildomai pažymėtina, kad ir Europos ekonominės erdvės valstybių keliama PPTF rizika nėra vienoda ir ne visada žema, pvz., neseniai Kroatija buvo įtraukta į Finansinių veiksmų darbo grupės kovai su pinigų plovimu ir teroristų finansavimu (FATF) didelės rizikos valstybių sąrašą, anksčiau į šį sąrašą buvo įtraukta Malta.

Lietuvos bankas, atlikęs EPMĮ Lietuvos bankui pateiktų duomenų analizę (ataskaitinis laikotarpis nuo 2022 m. sausio 1 d. iki 2022 m. gruodžio 31 d.), šiuo raštu papildomai atkreipia EPMĮ vadovų dėmesį į Lietuvos banko priežiūros metu stebimus PPTF rizikos veiksnius, naujai kylančias PPTF rizikas ir būtinybę imtis tinkamų ir proporcingų priemonių PPTF rizikai valdyti.

[1] https://www.lb.lt/uploads/documents/files/Laiskas%20EPiMI%20vadovams(1).pdf.
[2] Valstybės, įvardytos Lietuvos Respublikos finansų ministro 2001 m. gruodžio 22 d. įsakyme Nr. 344 „Dėl tikslinių teritorijų sąrašo patvirtinimo“.
[3] Europos Komisijos ir Finansinių veiksmų darbo grupės kovai su pinigų plovimu ir teroristų finansavimu (FATF) nustatytos didelės rizikos trečiosios valstybės.
[4] Valstybės, kurios nėra Europos Sąjungos narės, nėra Europos Komisijos ir Finansinių veiksmų darbo grupės kovai su pinigų plovimu ir teroristų finansavimu (FATF) nustatytos didelės rizikos trečiosios valstybės ir nėra įvardytos Lietuvos Respublikos finansų ministro įsakyme „Dėl tikslinių teritorijų sąrašo patvirtinimo“.

Dėl atnaujinto Europos Komisijos atlikto pinigų plovimo ir teroristų finansavimo rizikos vertinimo Europos Sąjungos mastu

2022 m. spalio 27 d. Europos Komisija (EK) paskelbė atnaujintą pinigų plovimo ir teroristų finansavimo rizikos vertinimą Europos Sąjungos mastu (toliau – EK vertinimas)[5], kuriame pateikiama informacija apie elektroninių pinigų, mokėjimo operacijų, pinigų perlaidų ir kitų EPMĮ sektoriui aktualių finansinių paslaugų ir produktų PPTF rizikas. Atkreiptinas dėmesys į tai, kad EK vertinime pateikiant PPTF rizikos vertinimą išskiriami šie pagrindiniai EPMĮ sektoriui būdingi PPTF rizikos veiksniai:

- ***su klientais susijusi PPTF rizika***: tapatybės nustatymo vengimas (padirbti dokumentai, fiktyvūs klientų juridinių asmenų direktoriai ir atstovai), prekyba suklastotomis prekėmis pažeidžiant intelektinės nuosavybės teises, sukčiavimas nesuteikiant įsigytų prekių (paslaugų), netinkamas viešųjų lėšų panaudojimas, korupcija ir kyšininkavimas, sutartinės lažybos (lošimai);
- ***su paslaugomis, produktais ir operacijomis susijusi PPTF rizika***: produktai, kuriems būdingas anonimiškumas, išankstinio apmokėjimo kortelės, žemos vertės mokėjimai, kai nėra privaloma nustatyti kliento tapatybę, itin greitai atliekami mokėjimai, kuriuos sunku užkardyti ir atsekti, sudėtingos mokėjimų grandinės, mokėjimo kortelių, kurias klientas gali turėti, skaičiaus neribojimas;
- ***su paslaugų ir produktų teikimo kanalais susijusi PPTF rizika***: nuotolinis kliento tapatybės nustatymas, ilgos tarpininkų grandinės, nesąžininga (neteisėta) tarpininkų veikla.

EK viršnacionaliniame rizikos vertinime[6] išskirtos ir kitų įpareigotųjų subjektų (pvz., azartinių lošimų bendrovių) rizikos bei kitos rizikos (pvz., ne pelno siekiančių organizacijų, patikos bendrovių ir pan.), kurios gali būti aktualios toms EPMĮ, kurios aptarnauja šių sektorių klientus. Papildomai atkreiptinas dėmesys ir į kitas EK vertinime išskiriamas PPTF rizikas, su kuriomis gali susidurti EPMĮ, – patikos ar panašios nuosavybės (kontrolės) struktūros, daugiapakopės nuosavybės (kontrolės) struktūros bendrovės, atstovai, veikiantys kito juridinio ar fizinio asmens vardu, fiktyvios įmonės, ekonominės veiklos, kurioms būdingos didelės vertės grynųjų pinigų apyvartos, klientų vykdoma didesnės rizikos veikla (pvz., susijusi su kriptoturtu, azartiniais lošimais).

Dėl aptarnaujamų klientų, susijusių su kriptoturtu

Kaip jau buvo nurodyta 2022 m. rašte, PPTF rizikos, susijusios su klientais, vykdančiais veiklą, susietą su kriptoturtu, ir toliau išlieka aktualios EPMĮ. Primename, kad kriptoturtas dėl savo decentralizuotumo, anonimiškumo ir reguliavimo stokos yra patraukli priemonė ne tik legalizuoti neteisėtais būdais įgytas lėšas, bet ir išvengti tarptautinių finansinių sankcijų, todėl EPMĮ turėtų itin atidžiai vertinti tokių klientų, kurių veikla susijusi su kriptoturtu, keliamą PPTF riziką bei imtis papildomų sustiprintų priemonių šiai rizikai valdyti, įskaitant klientų lėšų, gaunamų iš kriptoturto, kilmės nustatymą. Jei anksčiau buvo stebima, kad pagrindiniai virtualiųjų valiutų keityklų operatoriai (VVKO) yra Estijoje įsteigtos įmonės, tai remiantis 2022 m. spalio 27 d. Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos (FNTT) atlikta analize,[7] didžiausias virtualiųjų valiutų operatorių steigimosi Lietuvoje šuolis nustatytas 2022 m. Atkreiptinas dėmesys, kad 2022 m. sugriežtinus VVKO keliamus reikalavimus, pvz., įstatinio kapitalo reikalavimus, registruotų VVKO skaičius Lietuvoje sumažėjo, todėl, aptarnaujant tokius klientus, rekomenduojama įvertinti, ar klientas VVKO yra tinkamai registruotas ir turi teisę teikti tokias paslaugas (šią informaciją galima patikrinti VĮ Registrų centro sistemoje[8]).

Papildomai primename apie Lietuvos banko jau anksčiau išleistas rekomendacijas dėl klientų, susijusių su kriptoturtu [9], kuriose akcentuojama, kad užmezgant dalykinius santykius rekomenduojama įvertinti tokių klientų PPTF nustatytus ir taikomus prevencijos kontrolės mechanizmus, įsitikinti, kad klientas tinkamai atlieka savo kliento tapatybės nustatymą, turi įdiegęs reikiamas kontrolės priemones dalykinių santykių ir sandorių stebėsenai atlikti, taip pat

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344&from=EN.

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344&from=EN

[7] https://www.fntt.lt/lt/naujienos/fntt-atliko-virtualiuju-valiutu-sektoriaus-analize-isryskejo-gresmes-vykdomi-patikrinimai/4247.

[8] https://www.registrucentras.lt/jar/sarasai/dvvpo.php.

[9] https://www.lb.lt/lt/naujienos/lietuvos-banko-pozicija-del-virtualiojo-turto-ir-pirminio-virtualiojo-turto-zetonu-platinimo-atspindi-rinkos-aktualijas, https://www.lb.lt/lt/rekomendacijos#ex-13-1, https://www.lb.lt/uploads/documents/files/LB%20Rekomendacijos%20d%C4%97l%20klient%C5%B3%20gaunan%C4%8Di%C5%B3%20l%C4%97%C5%A1as%20i%C5%A1%20kripto%20turto%20kilm%C4%97s%20.pdf.

turi tinkamas priemones lėšų šaltiniui nustatyti (tiek užmezgant dalykinius santykius, tiek atliekant operacijas) ir reikiamus leidimus ar licencijas savo veiklai vykdyti, įvertinti neigiamą viešai prieinamą informaciją apie klientą, naudos gavėjus, atstovus ir pan.

Dėl klientų, vykdančių didesnės PPTF rizikos ekonominę veiklą, aptarnavimo

2022 m. rašte buvo akcentuotos PPTF rizikos dėl aptarnaujamų didesnės rizikos klientų. Pažymėtina, kad sektoriuje ir toliau išlieka didesnė PPTF rizika dėl EPMĮ aptarnaujamų didesnės rizikos klientų, kurių veikla susijusi su kriptoturtu, azartiniais lošimais ir žaidimais, prekyba *Forex* valiutų rinkoje, suaugusiųjų paslaugų teikimu ir pan. Papildomai EPMĮ su didesne kliento PPTF rizika susiduria ir dėl to, kad aptarnauja klientus, teikiančius konsultacines ir panašias paslaugas (verslo konsultacijos, rinkodara, informacinių technologijų (IT) paslaugos, mokymai), kurių suteikimo faktą gali būti sudėtinga patvirtinti. EPMĮ taip pat aptarnauja kontroliuojančias bendroves (angl. *holding company*), bendroves arba klientus, kurie mokėjimus vykdo tik paskolų pagrindu, o jokia kita veikla kliento sąskaitoje nėra vykdoma. Tokių klientų atžvilgiu sudėtingiau vykdyti dalykinių santykių ir operacijų stebėseną, reikia papildomų žinių ir kompetencijų siekiant įvertinti, ar kliento vykdoma veikla yra ekonomiškai ir logiškai pagrįsta, ar mokėjimo operacijų tikslas, pagrindas ir lėšų šaltinis yra aiškūs. Todėl jeigu finansų įstaiga pasirenka aptarnauti tokius klientus, rekomenduojama ne tik stiprinti PPTF prevencijos priemones, bet ir kelti darbuotojų kompetenciją, suteikti specifinių žinių apie tokių klientų keliamą PPTF riziką.

Dėl sukčiavimo prevencijos priemonių

2022 m. Lietuvos banko gaunamų skundų dėl galimo EPMĮ klientų sukčiavimo skaičius buvo didelis. Kaip ir anksčiau, pagrindinė pasitaikanti sukčiavimo tipologija susijusi su investiciniu sukčiavimu, šiuo atveju prarandamos reikšmingos apgaulingai investuotos sumos. Kitos tipologijos susijusios su netikromis elektroninėmis parduotuvėmis, tapatybės vagystėmis, telefoniniu sukčiavimu. Kaip ir anksčiau, pastebima, kad galimų sukčių vykdoma veikla įprastai susijusi su finansinių paslaugų teikimu, kriptoturtu, prekyba *Forex* valiutų rinkoje, IT paslaugomis, rinkodara ir reklama, konsultavimu, IT konsultavimu, įdarbinimo paslaugomis, kontroliuojančiomis bendrovėmis ir pan. Neretai sukčiavimo atvejai ir schemos būna glaudžiai susiję ir su įmonių vykdomu neteisėtu finansinių (investicinių) paslaugų teikimu, t. y. paslaugų teikimu kitose Europos Sąjungos (ES) valstybėse neturint tam finansų rinką reglamentuojančiuose teisės aktuose nustatytos licencijos ar leidimo. Todėl aptarnaujant tokius klientus reikia skirti didelį dėmesį nustatant, kokiose valstybėse klientas turi teisę teikti paslaugas ir ar turi tam išduotas licencijas ar kitokius leidimus.

Pažymėtina, kad ilgą laiką didžioji dalis nukentėjusiųjų nuo sukčiavimo buvo iš užsienio valstybių, tačiau paskutiniais metais pastebima, jog vis dažniau nukenčia ir Lietuvoje licencijuotų kredito įstaigų klientai, kurie perveda lėšas galimiems sukčiams, atsidariusiems sąskaitas Lietuvoje licencijuotose EPMĮ. Dažniausiai tokiais atvejais pasitaikanti tipologija yra SMS atakos, todėl finansų įstaigos, nustačiusios pirmuosius tokių atakų požymius, t. y. atvejus, kai įstaigos klientais naudojamasi lėšų gavimui neteisėtu būdu iš nukentėjusiųjų nuo sukčiavimo, turėtų nedelsiant imtis prevencinių veiksmų, pvz., pagal finansų įstaigos nustatytą tvarką atidžiau ir detaliau peržiūrėti operacijas, gaunamas iš Lietuvos kredito įstaigų, kai įstaigos klientai, t. y. lėšų gavėjai, nėra lietuviai. Papildomai EPMĮ turėtų detaliai analizuoti galimą klientų sukčiavimo veiklą, nustatyti įtartinumo požymius ir juos įdiegti į savo stebėsenos sistemas (pvz., visų pirmų mokėjimų stabdymas iš tam tikros grupės klientų, raktažodžių naudojimas, papildomai kontrolei užtikrinti taikoma intensyvesnė retrospektyvi stebėsena ir pan.).

Pakartotinai primename, kad EPMĮ turėtų taikyti tinkamas klientų tapatybės nustatymo priemones, užmegzdamos dalykinius santykius gerai suprasti kliento veiklą, numatomą dalykinių santykių tikslą ir pobūdį, kad vykdant operacijų ir sandorių stebėseną būtų galima kuo greičiau aptikti neįprastą ar įtartiną veiklą. EPMĮ taip pat turėtų taikyti efektyvias kliento dalykinių santykių ir operacijų stebėsenos priemones, įskaitant retrospektyvias kliento veiklos analizes, nes analizuojant ilgesnio laikotarpio kliento veiklą (vertinant mokėjimo kryptis, mokėtojus ir gavėjus, mokėjimo paskirtyje nurodomą informaciją, atitiktį kliento deklaruotai veiklai) galima geriau pastebėti neįprastas ar įtartinas su sukčiavimu susijusias operacijas[10].

Praktikoje pastebimi atvejai, kai EPMĮ interneto svetainėse nėra aiškiai nurodyti kontaktai, kuriais asmenys, įskaitant tiek policijos pareigūnus, tiek asmenis, kurie nukentėjo dėl EPMĮ klientų galimo sukčiavimo, galėtų kreiptis į EPMĮ. Pakartotinai akcentuojame, kad viena iš pagrindinių sukčiavimo prevencijos priemonių yra tinkamas gaunamų skundų

[10] https://www.lb.lt/lt/leidiniai/sukciavimo-ir-neteisetu-finansiniu-paslaugu-teikimo-rizika-ir-prevencija.

nagrinėjimas, kliento veiklos peržiūra ir analizė. Taip pat svarbu akcentuoti bendradarbiavimą su teisėsaugos ir žvalgybos institucijomis, nes itin svarbu kaip įmanoma greičiau ir efektyviau nustatyti sukčiavimo atvejus ir juos ištirti.

Mokesčių vengimo rizika

Patikrinimų metu nustatoma, kad įstaigos netaiko kontrolės priemonių, siekdamos nustatyti mokesčių vengimo atvejus, neorganizuoja darbuotojams mokymų, kaip atpažinti šią tipologiją. Remiantis įvairių valstybės institucijų, atsakingų už mokesčių surinkimą, informacija, pažymėtina, kad praktikoje dažnai pasitaiko situacijų, kai klientų (tiek juridinių, tiek fizinių asmenų) įplaukos į sąskaitas yra didesnės, nei buvo deklaruota finansinės atskaitomybės ataskaitose arba gyventojų praeitų metų pajamų deklaracijose. Tokia situacija gali rodyti, kad klientai deklaravo ne visas pajamas, todėl įstaigoms rekomenduojama vertinti informaciją, kuri gali indikuoti apie mokesčių vengimą, o ypač tais atvejais, kai klientams taikomas sustiprintas kliento tapatybės nustatymas ir sustiprinta dalykinių santykių stebėsena, ir įstaigos turi surinkusios papildomus dokumentus (pvz., finansinės atskaitomybės arba gyventojų pajamų deklaracijas). Akcentuotina, kad šis neatitikimas taip pat turėtų būti vertinamas kritiškai, nes gali būti atvejų, kad einamaisiais metais, lyginant su praėjusiais metais, plėtėsi kliento veikla. Vis dėlto, jei augimo skirtumas yra ženklus ir klientas per ekonominės veiklos prizmę negali tokio augimo paaiškinti, įstaigos turėtų papildomai vertinti, ar šios operacijos nėra įtartinos. Analogiška rizika kyla ir tais atvejais, kai įplaukos buvo mažesnės nei pajamos (galima rizika, kad vykdomi fiktyvūs sandoriai). Kaip papildoma rizika, gali būti išskiriamos mokesčių vengimo schemos, kai mokesčiai slepiami išsimokant dividendus. Pažymėtina, kad įstaigos turėtų stiprinti žinias šioje tipologijoje, kadangi tai yra aktualu, o priežiūros praktika rodo, jog EPMĮ klientų veikloje neretai atliekamos mokėjimo operacijos, susijusios su dividendų išmokėjimu.

Prekybos finansavimo ir kitų tipologijų rizika

Sektoriuje didelę dalį sudaro klientai juridiniai asmenys, kurie siūlo prekes ir (arba) paslaugas ir kurie veikia plačioje geografinėje teritorijoje. Remiantis 2021 m. *Europol* SOCTA ataskaita[11], apie 80 proc. grupuočių vykdo nusikalstamą veiklą ir pinigų plovimą pasitelkdamos juridinius asmenis. *Wolsfberg* duomenimis[12], apie 80 proc. visų su prekyba susijusių sandorių įvykdoma atliekant tiesioginius mokėjimo pavedimus tarp sandorio šalių vadinamuoju *open account trade* pagrindu, o ne dokumentais paremta prekyba (pvz., pasinaudojant bankų garantijomis). Todėl svarbu akcentuoti, kad su prekybos finansavimu (angl. *trade-based money laundering)* susijusios pinigų plovimo schemos, tokios kaip išrašomos fiktyvios sąskaitos (nurodant per mažą ar per didelę prekių ir (arba) paslaugų vertę), prekių pervežimo imitavimas (angl. *ghost shipping*), fiktyvus paslaugų suteikimas, ir kitos prekybos finansavimo tipologijos yra ypač aktualios šiam sektoriui. Įstaigos, ypač tos, kurios aptarnauja klientus, vykdančius prekių arba paslaugų prekybą, privalo didinti darbuotojų kompetenciją prekybos finansavimo tipologijos srityje.

Kartu akcentuotina, kad įstaigos turi gilinti žinias ir apie kitas tipologijas, pvz., pinigų mulai, azartiniai lošimai, kai įnešamos didelės sumos ir vėliau jos išsiimamos (fiktyvus lošimas), korupciniai nusikaltimai, prekyba žmonėmis (įskaitant priverstinį darbą, vaikų išnaudojimą, vaikų pornografiją), imigrantų gabenimas, prekyba narkotikais, prekyba neteisėtais vaistiniais preparatais, prekyba padirbtomis prekėmis, prekyba tamsiajame internete, siekdamos jas tinkamai atpažinti savo klientų veikloje ir atitinkamai imtis rizikos mažinimo veiksmų. Daugiau apie tipologijas galima rasti FNTT skelbiamose metinėse PPTF ataskaitose[13], *Europol* SOCTA ataskaitose[14] ir kituose šaltiniuose.

Taip pat atkreiptinas EPĮMĮ dėmesys į naujai pasirodžiusią Europolo ataskaitą dėl nusikaltimų internete ataskaitą[15], kurioje nurodomos pagrindinės tipologijos, pvz., sukčiavimai internete, kriptoturto pasinaudojimas PPTF tikslais, vaikų išnaudojimas internete.

Teroristų finansavimo rizika

Atsižvelgiant į tai, kad Lietuvos Respublikos Seimas 2022 m. gegužės 10 d. rezoliucija „Dėl Rusijos Federacijos veiksmų Ukrainoje pripažinimo genocidu ir specialiojo tarptautinio baudžiamojo tribunolo įsteigimo Rusijos agresijos nusikaltimui ištirti“ Nr. XIV-1070 Rusijos Federacijos karą prieš Ukrainą pripažino Ukrainos tautos genocidu, o Rusijos Federacija

[11] https://www.europol.europa.eu/publications-events/main-reports/socta-report.
[12] The Wolfsberg Group, International Chamber of Commerce, and Bankers Association for Finance and Trade, Trade Finance Principles (2019), at 21, available at https://www.wolfsberg-principles.com/sites/default/files/wb/Trade%20Finance%20Principles%202019.pdf.
[13] https://statics.teams.cdn.office.net/evergreen-assets/safelinks/1/atp-safelinks.html.
[14] https://www.europol.europa.eu/publications-events/main-reports/socta-report.
[15] https://www.europol.europa.eu/publications-events/main-reports/iocta-report

pripažinta terorizmą remiančia ir vykdančia valstybe, teroristų finansavimo (TF) rizika EPMĮ sektoriuje didėja. A. Lukašenkos režimui organizuojant neteisėtos migracijos srautus iš Vidurio Rytų ir Afrikos šalių į ES, per Baltarusiją į Lietuvą pateko asmenų iš valstybių, sietinų su didesne teroristų finansavimo rizika (Irakas, Kongas, Sirija, Afganistanas). Irake aktyviai veikia teroristinės ir ekstremistinės organizacijos „Islamo valstybė", „Kurdistano darbininkų partija" ir išpuolius prieš NATO šalių pajėgas Irake vykdančios sukarintos šiitų grupuotės. Nors, remiantis Lietuvos Respublikos valstybės saugumo departamento 2023 m. grėsmių nacionaliniam saugumui vertinimo ataskaita[16], Lietuvoje terorizmo grėsmė yra maža, tačiau išlieka pavienių radikalizuotų asmenų nusikalstamos veiklos rizika. Taip pat šioje ataskaitoje nurodoma, kad Baltarusija ir toliau naudoja migraciją kaip politinio spaudimo priemonę prieš ES. Neatmestina, kad į Lietuvą nelegaliai bandančių patekti migrantų sraute yra grėsmę valstybės saugumui ar viešajai tvarkai keliančių asmenų. Svarbu pažymėti, kad nors terorizmo grėsmė Lietuvoje išlieka žema, tačiau EPMĮ sektorius plačiai aptarnauja klientus iš kitų ES valstybių, kuriose terorizmo grėsmė yra didesnė nei Lietuvoje (pvz., Prancūzija, Vokietija ir kt.), todėl EPMĮ sektoriui būtina turėti proporcingas ir tinkamas priemones TF rizikai valdyti.

Papildomai akcentuotina, kad paskutiniais metais stebima ne tik organizuotų teroristų organizacijų veikla, bet ir ekstremizmo rizika, kai pavieniai asmenys gali įvykdyti teroristinius aktus. Ši rizika itin didėja dėl karo Ukrainoje, nes yra išaugęs ginklų, sprogmenų ir kitų priemonių, galimų panaudoti teroristinėms atakoms, prieinamumas. Papildomai rizika kyla ir dėl žmogiškojo faktoriaus, kadangi žmonės, dalyvaudami kare, įgyja įvairių įgūdžių, kuriuos tam tikroms aplinkybėms susiklosčius (pvz., remiantis kokia nors ekstremizmo ideologija) gali panaudoti ir civiliniame gyvenime.

2023 m. birželio 14 d. išleistas Europolo vertinimas dėl TF grėsmių Europoje[17], kuriame nurodoma, kad TF grėsmė Europoje išlieka aukšta, nes buvo 28 teroristų atakos, iš kurių 16 įvykdyta, didžioji jų dalis susijusi su dešiniosios pakraipos arba anarchistų atakomis (kurios naudoja savadarbius sprogstamuosius užtaisus) ir tik maža dalis – su džihadistų atakomis. Taip pat TF mastą rodo ir tai, kad 2022 m. buvo suimta 380 asmenų, susijusių su TF veikla (daugiausia asmenų suimta Vokietijoje ir Prancūzijoje). Ataskaitoje taip pat rašoma, kad asmenys TF veiklai plačiai verbuojami internete, internete skelbiamos įvairios dešiniųjų pakraipos ideologijos.

Svarbu atkreipti dėmesį ne tik į TF grėsmes šalies viduje, bet ir į galimą EPMĮ paslaugų panaudojimą siekiant finansuoti teroristus, kurie reziduoja ir teroristinius veiksmus planuoja kitose valstybėse. Tai ypač aktualu įstaigoms, kurios turi klientų iš valstybių arba vykdo operacijas su valstybėmis plačioje geografinėje teritorijoje, įskaitant valstybes, kuriose fiksuojama aukštesnė TF rizika (pvz., Afganistanas, Irakas, Somalis, Burkina Fasas, Sirija ir kt.). EPMĮ aptarnauja klientus (pvz., VVKO, ne pelno siekiančios organizacijos), kurių veikloje taip pat stebima didesnė TF rizika, todėl svarbu atkreipti dėmesį į tai, kad EPMĮ, kartu atsižvelgdamos ir į geopolitinę situaciją regione, privalo įvertinti TF riziką ir imtis tinkamų bei proporcingų priemonių šiai rizikai valdyti.

Atsižvelgiant į EPMĮ aptarnaujamų klientų rūšį (tiek finansų įstaigos, tiek NVO ir su kriptoturtu susijusios įmonės) ir į tai, kad didžioji dalis tokių klientų yra nerezidentai, laikytina, jog rizika, susijusi su masinio naikinimo ginklų finansavimu, dėl klientų tipo yra aktuali ir EPMĮ sektoriuje, todėl įstaigos pirmiausia turi suprasti šią riziką ir atitinkamai taikyti rizikos mažinimo priemones.

Dėl tarptautinių finansinių sankcijų, ribojamųjų priemonių įgyvendinimo

Atsižvelgiant į tai, kad Rusija 2022 m. vasario 24 d. pradėjo karą prieš Ukrainą ir jos gyventojus bei į ES ir jos sąjungininkų griežtinamas ir įtvirtinamas sankcijas ir ribojamąsias priemones, skirtas Rusijos Federacijai, Baltarusijos Respublikai ir (arba) susijusiems subjektams, EPMĮ svarbu užtikrinti tinkamą vidaus kontrolės procedūrų, susijusių su tarptautinių finansinių sankcijų, ribojamųjų priemonių įgyvendinimu, nustatymą, kaip tai nustatyta Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymo (PPTFPĮ) 29 straipsnio 1 dalies 4 punkte. Svarbu pabrėžti, kad, atsižvelgiant į Lietuvos geografinę padėtį ir per paskutiniuosius dešimtmečius susiformavusius ekonominius ryšius su Rusijos Federacija ir Baltarusijos Respublika, tinkamas tarptautinių sankcijų įgyvendinimas yra itin reikšmingas. Lietuvos bankui atlikus 2022 m. PPTF rizikų analizę, pastebimas operacijų, susijusių su Nepriklausomų valstybių sandraugos (NVS) valstybėmis, skaičiaus ir vertės išaugimas. Tai gali indikuoti, jog atliekant operacijas per NVS valstybes gali būti siekiama

[16] https://www.vsd.lt/wp-content/uploads/2023/03/Gresmiu-nacionaliniam-saugumui-vertinimas-2023_LT.pdf.
[17] https://www.europol.europa.eu/publications-events/main-reports/tesat-report.

išvengti Rusijos Federacijai taikomų sankcijų, todėl ši rizika toliau išlieka ir įstaigos turėtų užtikrinti tinkamas priemones sankcijų vengimo atvejams identifikuoti.

Patikrinimų metu nustatoma, kad EPMĮ dažnai neturi priemonių sektorinėms (ekonominėms) sankcijoms įgyvendinti ir sankcijų vengimo (apėjimo) atvejams identifikuoti. Priežiūros praktika rodo, kad ne visais atvejais įstaigų vidaus procedūrose nurodomi aiškūs sankcijų įgyvendinimo žingsniai, aiškiai neapibrėžta, kaip priimami sprendimai, kas tikrinama atliekant tarptautinių finansinių sankcijų stebėseną, kaip pranešama FNTT ir pan. Įstaigose įprastai neįtvirtintas sistemų kontrolės ir testavimo procesas (pvz., užtikrinant, kad sankcijų sąrašai atnaujinami, kad sistema veikia efektyviai, ir pan.). Kai kuriais atvejais įstaigose nebūna paskirtas už tarptautinių sankcijų įgyvendinimo organizavimą atsakingas asmuo arba jis būna paskirtas ne visą veiklos vykdymo laikotarpį. Kartais nustatoma, kad įstaigų taikomos tarptautinių sankcijų tikrinimo sistemos yra neefektyvios, tinkamai nesuderintos, nes nenustato dalies į tarptautinių sankcijų sąrašus įtrauktų asmenų, o ypač tais atvejais, kai duomenys yra minimaliai pakeičiami ir tokie pokyčiai nėra nustatomi (angl. *fuzzy match*). Taip pat nustatoma atvejų, kai praktikoje nėra užtikrinamas klientų (ir susijusių asmenų) tikrinimas sankcijų sąrašuose, nes patikros atliktos pavėluotai (pvz., praėjus keliems mėnesiams), o priemonės sektorinėms (ekonominėms) sankcijoms įgyvendinti ne tik nėra tinkamai reglamentuotos vidaus procedūrose, bet ir netaikomos praktikoje.

Papildomai rekomenduojame susipažinti su Lietuvos banko 2022 m. liepos 21 d. parengta tarptautinių sankcijų įgyvendinimo finansų įstaigose apžvalga, kurioje nurodomi gerosios praktikos pavyzdžiai bei atvejai, kada tarptautinių sankcijų įgyvendinimui taikomos priemonės turėtų būti tobulintinos[18]. 2023 m. birželio 6 d. Lietuvos bankas patvirtino nurodymus dėl tarptautinių sankcijų įgyvendinimo, kurie įsigalios 2023 m. rugsėjo 1 d.[19].

Dėl korespondentinių požymių turinčių paslaugų teikimo, kitų finansų įstaigų ir įpareigotųjų subjektų aptarnavimo

Kaip buvo nurodyta 2022 m. rašte, pakartotinai akcentuotina svarba EPMĮ užmezgant dalykinius santykius su subjektais, kurių veikla susijusi su finansinių paslaugų teikimu, taip pat teikiant paslaugas kitiems įpareigotiesiems subjektams, pvz., azartinių lošimų bendrovėms, VVKO, įvertinti PPTF riziką ir tokių klientų taikomas kontrolės priemones šiai rizikai valdyti. Pažymėtina, kad toks vertinimas neturėtų apsiriboti politikų ir procedūrų surinkimu. Vertinimas turėtų būti atliekamas išsamiai, jo išvados dokumentuojamos, pats vertinimas neturėtų būti formalus, pvz., paremtas kliento paties savęs vertinimu ir pan. Siekiant geriau suprasti tokių klientų keliamą PPTF riziką ir įvertinti jų taikomų PPTF prevencijos priemonių veiksmingumą bei efektyvumą, labai svarbu gauti informaciją apie tokių klientų aptarnaujamų klientų portfelį, ekonomines veiklas, jiems teikiamas paslaugas, geografinį klientų pasiskirstymą ir pan.

Sektoriuje toliau išlieka rizika, kai EPMĮ kliento klientams atidaro sąskaitas, tačiau ne visada turi informaciją apie galutinius paslaugos naudotojus, todėl atsiranda anonimiškumas atliekamų mokėjimo operacijų atžvilgiu (pvz., nėra aišku, kas yra tikrasis lėšų mokėtojas ar gavėjas). Pažymėtina, kad tokiu atveju itin sudėtinga užtikrinti tinkamą operacijų stebėseną bei tarptautinių finansinių sankcijų ir ribojamųjų priemonių įgyvendinimą.

Dėl paslaugų teikimo per tarpininkus, elektroninių pinigų platintojus, trečiuosius asmenis ir BaaS (Banking as a Service) modelių taikymas praktikoje

Rinkoje pastebimas paslaugų teikimo per tarpininkus, elektroninių pinigų platintojus, trečiuosius asmenis ir vadinamųjų *BaaS* paslaugų teikimas. Nors dažnai šios paslaugos vadinamos apibendrintu terminu *BaaS*, praktikoje šių paslaugų apimtis skiriasi. Didelę riziką kelia atvejai, kai tokios paslaugos teikiamos naudojantis pagalba partnerių, kuriems finansų įstaiga perduoda pagrindines PPTF prevencijos funkcijas (pvz., klientų tapatybės nustatymas, informacijos atnaujinimas, sustiprintas kliento tapatybės nustatymas, dalykinių santykių ir operacijų stebėsena). Tokie partneriai gali būti tiek įprasti juridiniai asmenys, neturintys jokios licencijos, tiek kitos finansų įstaigos ar kiti įpareigotieji subjektai (pvz., VVKO). Tokiu atveju įstaigos dažnai pernelyg pasitiki savo partnerio taikomomis PPTF prevencijos priemonėmis ir procesais ir tinkamai šių partnerių vykdomų PPTF prevencijos kontrolės priemonių nekontroliuoja. Tai lemia ir aplinkybės, kad su partneriais sudaromose bendradarbiavimo sutartyse nesusitariama dėl PPTF prevencijos funkcijų pasiskirstymo, funkcijos neatskiriamos arba atskiriamos neaiškiai, paliekama vietos šalių įsipareigojimų interpretacijoms, aiškiai nesusitariama dėl informacijos, kurią partneris privalės įstaigai pateikti apie klientus, tai tampa

[18] https://www.lb.lt/lt/apzvalgos-ir-leidiniai/category.85/series.4357.
[19] https://www.lb.lt/lt/naujienos/lietuvos-banko-nurodymai-del-sankciju-pinigu-plovimo-ir-teroristu-finansavimo-prevencijos.

ypač aktualu, kai tarp finansų įstaigos ir partnerio prasideda ginčai ir bendradarbiavimas nebebūna geranoriškas. Pažymėtina, kad būtent finansų įstaiga, kuri pagal *BaaS* modelį yra perdavusi PPTF prevencijos funkcijas savo partneriui, laikoma atsakinga už tinkamą PPTF prevencijos priemonių įgyvendinimą, nes įprastai asmenys, su kuriais dalykiniai santykiai užmegzti per partnerį, laikomi įstaigos klientais.

Praktikoje pastebima, kad partneriai, su kuriais užmezgami dalykiniai santykiai, jau turi savo klientų portfelį, savo veiklos modelį, todėl įstaigos turėtų atidžiau vertinti partnerį ir dėl jo įstaigai kylančias naujas PPTF rizikas.

Ne mažiau svarbu, kad kiekvienu individualiu atveju licencijuotos įstaigos įsivertintų, ar tai, ką finansų rinkos dalyvis vadina *white label* („baltoji etiketė", kai vieno subjekto sukurtam produktui ar paslaugai suteikiamas kito subjekto prekės ženklas), nėra tarpininkavimas, elektroninių pinigų platinimas ar veiklos funkcijų perdavimas kitiems asmenims, kadangi tokį veiklos modelį įvairūs finansų rinkos dalyviai neretai interpretuoja skirtingai. Lietuvos banko vertinimu, *white label* veiklos modelis dažniausiai turi tarpininkavimo požymių. Jei iki šiol elektroninių pinigų ar mokėjimo įstaigos *white label* modelį vertino, kaip veiklos funkcijų perdavimą kitiems asmenims, jos turėtų peržvelgti šio modelio atitiktį teisės aktams. Jeigu jis turi tarpininkavimo požymių, įstaigos turi kreiptis į Lietuvos banką dėl elektroninių pinigų platintojų pasitelkimo ar tarpininkų įrašymo į viešąjį sąrašą. Apie tai plačiau rašoma 2023 m. birželio 22 d. Lietuvos banko išleistame įspėjime dėl prisiimamos atsakomybės, galimų pasekmių ir būtinų kontrolės priemonių, kai savo veikloje jos pasitelkia tarpininkus arba elektroninių pinigų platintojus[20].

Dėl vidaus kontrolės priemonių stiprinimo

Lietuvos bankui atliekant EPMĮ patikrinimus, vizitus ir vykdant kitus sektoriaus priežiūros veiksmus, pastebimi tam tikri EPMĮ sektoriui būdingi PPTF prevencijos priemonių trūkumai: netvari vidaus kontrolės sistema (dėl interesų konflikto, netinkamo funkcijų atskyrimo, netinkamo PPTF prevencijos procesų sudėliojimo ir tarpusavio sąveikos, taip pat darbuotojų atliekamų funkcijų kokybės užtikrinimo (angl. *quality assurance*) pakankamo nebuvimo), netinkamas tarptautinių sankcijų įgyvendinimas, neefektyvi dalykinių santykių ir operacijų stebėsena (nepakankami stebėsenos scenarijai, per mažai naudojamos kitos stebėsenos priemonės, nepakankama apimtimi vykdoma retrospektyvi klientų veiklos analizė), netinkamai atliekamas kliento ir naudos gavėjo tapatybės nustatymas (pvz., daugiapakopėje įmonių struktūroje nesurenkami pagrindžiantys dokumentai tarpinių įmonių atžvilgiu, siekiant įsitikinti, kas yra naudos gavėjas), netinkamai vykdomas sustiprintas kliento tapatybės nustatymas (ne visais atvejais gaunamas vyresniojo vadovo pritarimas, nesiimama papildomų priemonių dėl lėšų ir turto šaltinio nustatymo, netinkamai vykdoma dalykinių santykių ir sandorių stebėsena ir kt.), vykdoma neefektyvi tarpininkų kontrolė, nes nenustatomos pakankamos priemonės tarpininkų veiklai vertinti. Atsižvelgdamos į patikrinimų metu nustatomus trūkumus, sektoriuje veikiančios įstaigos ir toliau turi stiprinti PPTF prevencijos priemones ir investuoti į darbuotojų kompetenciją.

Dėl kokybiško duomenų panaudojimo ir analitinių kompetencijų stiprinimo

Papildomai pažymėtina, kad praktikoje pastebima EPMĮ kylančių iššūkių dėl duomenų saugojimo ir jų panaudojimo vykdant PPTF prevencijos reikalavimus. Nustatoma, kad kai kurios EPMĮ netinkamai saugo klientų duomenis, šių duomenų nesistemina, todėl neužtikrina duomenų, gautų užmezgant dalykinius santykius arba atnaujinant kliento informaciją, integracijos su stebėsenos sistemomis. Kartu pažymėtina, kad tokius duomenis naudoti taip pat svarbu ir nustatant bei vertinant individualią kliento PPTF riziką, vykdant visos veiklos PPTF rizikos vertinimą, tikrinant klientus, jų atstovus, naudos gavėjus dėl tarptautinių finansinių sankcijų atitikties ir pan. Lietuvos bankas pažymi, kad EPMĮ privaloma užtikrinti tinkamą duomenų saugojimą, sisteminimą, strategišką planavimą dėl naujų sistemų įsigijimo ir duomenų tarpusavio integracijos, kad duomenis būtų patogu naudoti tiek vykdant PPTF prevenciją, tiek esant poreikiui nedelsiant pateikti priežiūros, žvalgybos, teisėsaugos ir pan. institucijoms. Praktikoje taip pat pastebimi atvejai, kai įstaigos neturi pakankamai kompetencijų turimiems duomenims gauti iš įstaigų sistemų, juos tinkamai apdoroti, pateikti PPTF prevencijos specialistų analizei, todėl įstaigoms rekomenduojama stiprinti kompetencijas duomenų analitikos srityje.

[20] https://www.lb.lt/lt/naujienos/lietuvos-bankas-atsakomybe-uz-pasirinktu-tarpininku-ir-el-pinigu-platintoju-veikla-tenka-paciai-finansu-istaigai.

Atkreiptinas dėmesys, kad įstaigų naudojamos IT sistemos turėtų atitikti įstaigų veiklos mastą. Jei įstaigoje apdorojamas didelis kiekis mokėjimo operacijų ir sandorių, atitinkamai ir naudojamos IT sistemos ir sprendimai turėtų būti sudėtingesni ir kompleksiniai.

Atsižvelgdami į tai, kas išdėstyta šiame EPMĮ dėmesį atkreipiančiame rašte, raginame įvertinti nurodytas PPTF rizikas ir užtikrinti, kad įstaigos taiko tinkamas ir pakankamas PPTF prevencijos priemones šioms PPTF rizikoms identifikuoti ir jas valdyti.