



ИЗВЕШТАЈ ФАТФ

Индикатори за препознавање сумње

да се ради о прању новца и финансирању
тероризма уз помоћ виртуелне имовине

септембар 2020





Радна група за финансијску акцију (ФАТФ) је независно међувладино тело које развија и промовише политике за заштиту глобалног финансијског система од прања новца, финансирања тероризма и финансирања ширења оружја за масовно уништење. Препоруке ФАТФ признате су као глобални стандард за спречавање прања новца (СПН) и финансирање тероризма (СФТ).

Више информација о ФАТФ можете пронаћи на страници; www.fatf-gafi.org

Овај документ и/или све приказане мапе не доводе у питање статус или суверенитет било које територије, линије разграничења и границе као ни име било које територије, града или области.

Референца за цитирање:

FATF, (2020), Paris, France, *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets*,
www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html

© 2020 FATF/OECD. Сва права задржана.

Умножавање или превод ове публикације нису дозвољени без претходног писменог одобрења. Захтеви за издавање такве сагласности, било за целу публикацију или само један њен део, подносе се на: Секретаријат ФАТФ, на адресу 2 rue André Pascal 75775 Paris Cedex 16, France (факс: +33 1 44 30 61 37 или имејл: contact@fatf-gafi.org)

Права на фотографије задржава ©Gettyimages

Ова публикација је преведена уз финансијску помоћ Европске уније. За садржину ове публикације искључиво је одговоран ФАТФ, и та садржина нипошто не изражава званичне ставове Европске уније. Европска унија не преузима одговорност ни за какве грешке или пропусте у овом преводу.

Публикација [Индикатори за препознавање сумње да се ради о прању новца и финансирању тероризма уз помоћ виртуелне имовине] представља превод на српски језик оригиналне верзије на енглеском језику. Преведена је на српски језик уз одобрење Секретаријата ФАТФ, у оквиру пројекта: Унапређење квалитета и ефикасности извештавања о сумњивим трансакцијама и кључних функција Управе за спречавање прања новца, који финансира Европска унија. Корисник пројекта је Министарство финансија Републике Србије - Управа за спречавање прања новца. Пројекат спроводи конзорцијум који предводи КПМГ.

Званична верзија публикације на енглеском језику доступна је на www.fatf-gafi.org

Ауторско право © ФАТФ/ОЕЦД. Сва права задржана.

Ово је радни превод. У случају сукоба у вези са тумачењем, меродавна је званична верзија текста, објављена на интернет страници ФАТФ.

Садржај

Скраћенице	2
Увод	3
Методологија и извори коришћени приликом састављања списка индикатора ...	4
Питања на која треба обратити пажњу приликом читања овог извештаја	4
Индикатори	5
Индикатори везани за трансакције	5
Индикатори везани за обрасце трансакција.....	7
Индикатори везани за анонимност	9
Индикатори везани за налогодавце или примаоце.....	13
Индикатори везани за извор средстава или богатства.....	16
Индикатори географских ризика	18
Закључак	21
Литература	22

Скраћенице

АЕЦ	Анонимни електронски новац
ЦДД	Познавање и праћење странке
ДНФБП	Одређени нефинансијски сектори и самосталне професије
ДНС	Регистри имена домена
ФАТФ	Радна група за финансијску акцију
ФИ	Финансијске институције
ФИУ	Финансијско-обавештајна служба
ИЦО	Иницијална понуда коина
КУЦ	Упознај свог клијента
ЛЕАс	Органи реда
ПН	Прање новца
ИСТ	Извештаји о сумњивим трансакцијама
ФТ	Финансирање тероризма
ВИ	Виртуелна имовина
ПУВИ	Пружаоци услуга у вези са виртуелном имовином

Увод

1. Виртуелна имовина (ВИ) и услуге повезане са њом имају потенцијал да подстакну финансијске иновације и ефикасност, али њихове посебне карактеристике такође стварају нове могућности за прање новца, за финансијере тероризма и друге криминалце да перу свој приход или финансирају незаконите активности. Могућност брзог обављања прекограничне трансакције не само да омогућава криминалцима да електронски набављају, премештају и складиште имовину често ван регулисаног финансијског система, већ и да замагљују порекло или одредиште средстава и отежавају обвезницима да благовремено открију сумњиве активности. Ови фактори отежавају откривање и истрагу противзаконитих активности од стране националних власти.
2. У октобру 2018. године, Радна група за финансијску акцију (ФАТФ) ажурирала је своје стандарде да боље објасни како се примењују на активности везане за виртуелну имовину и лица која пружају услуге у вези са виртуелном имовином како би, између осталог, помогла државама да ублаже ризике од прања новца (ПН) и финансирања тероризма (ФТ) повезане са активностима у вези са ВИ и да заштите интегритет глобалног финансијског система. У јуну 2019. године, ФАТФ је усвојио напомену са тумачењем уз препоруку 15 да би се боље објаснила примена мера ФАТФ на активности везане за ВИ и лица која пружају услуге у вези са виртуелном имовином, укључујући и извештавање о сумњивим трансакцијама.
3. ФАТФ је припремио овај кратки извештај о индикаторима за препознавање сумње да се ради о ПН/ФТ уз помоћ виртуелне имовине како би помогао обвезницима, укључујући финансијске институције (ФИ), одређене нефинансијске секторе и самосталне професије (ДНФБП) и лица која се баве пружањем услуга у вези са ВИ; у ма којим категоријама да се налазе, да откривају и извештавају о потенцијалним активностима ПН и ФТ уз помоћ виртуелне имовине. Овај извештај такође треба да олакша обвезницима да на основу приступа заснованог на процени ризика примењују меру познавања и праћења странке која захтева да знају ко су њихови клијенти и стварни власници, да разумеју природу и сврху пословног односа и извора прихода.
4. Надлежним органима, финансијско-обавештајним службама (ФОС), органима реда (ЛЕА) и тужиоцима овај извештај може бити корисна литература приликом обављања анализе извештаја о сумњивим трансакцијама (СТР) или за побољшање откривања, истраге и одузимања злоупотребљене виртуелне имовине.
5. С друге стране, регулаторним телима за финансијске институције, ДНФБП и ПУВИ ови индикатори могу бити корисни при припреми извештаја о сумњивим трансакцијама и праћењу усклађености обвезника закона са мерама за спречавање прања новца и финансирања тероризма. Када обвезник има информације које указују на постојање једног или више индикатора без логичног пословног објашњења, али не поднесе ИСТ, упркос недоследном објашњењу клијента или не затражи објашњење о трансакцији, надлежни органи могу размотрити да предузму кораке у вези са обвезником узимајући у обзир пословни профил клијента.

Методологија и извори коришћени приликом састављања списка индикатора

6. Индикатори обухваћени овим извештајем заснивају се на више од сто студија случаја које су различите државе доставиле у периоду 2017-2020. године, на сазнањима приказаним у *Поверљивом извештају ФАТФ о финансијским истрагама у вези са виртуелном имовином* (јун 2019.) и објављеног *извештаја ФАТФ: Виртуелне валуте, кључне дефиниције и потенцијални ризици од ПН/ФТ* (јун 2014.), као и на информацијама о злоупотреби јавно доступне виртуелне имовине.

Трендови које прати употреба ВИ у сврхе ПН/ФТ

Већина кривичних дела повезаних са ВИ тиче се предикатних кривичних дела или кривичних дела ПН. Без обзира на то, криминалци су користили ВИ да избегну финансијске санкције и прикупе средства за подршку тероризму.

Врсте дела које пријављују државе обухватају ПН, продају контролисаних супстанци и других илегалних предмета (укључујући ватрено оружје), злоупотребу, утају пореза, високотехнолошки криминал (нпр. нападе који доводе до крађе), експлоатацију деце, трговину људима, избегавање санкција и ФТ. Међу њима, најчешћи тип злоупотребе је илегална трговина контролисаним супстанцама, било продајом која се обавља директно у ВИ, било употребом ВИ у фази раслојавања. Друга најчешћа категорија злоупотребе односи се на преваре, уцену путем интернета и изнуду. У новије време професионалне мреже перача новца почеле су да користе ВИ као једно од средстава за пренос, прикупљање или раслојавање прихода.

Извор: Студије случајева које су државе достављале у периоду 2017-2020.

Питања на која треба обратити пажњу приликом читања овог извештаја

7. Ови индикатори одсликавају природу виртуелне имовине и са њом повезаних финансијских активности и ни у ком случају нису исцрпни. Сумњива употреба виртуелне имовине може личити са ПН/ФТ које укључују употребу декретног новца или друге врсте имовине. Обвезници закона би зато требало да узму у обзир ризике које представљају њихови купци, производи и рад, као и присуство конвенционалних индикатора ризика. Индикаторе увек треба разматрати у датом контексту.

8. Самостални индикатори попут оних наведених у наставку могу се развити или комбиновати са информацијама надлежних органа, које се заузврат могу даље развијати кроз јавно-приватно партнерство, у цикличном, еволутивном процесу у коме се узима у обзир јединствени ризик и контекст државе, тип клијента или самог обвезника. Само присуство индикатора није нужно основа за сумњу на ПН или ФТ, али би могло подстаћи даље праћење и испитивање. На крају, клијент може

пружити објашњење за уочени индикатор, или објаснити пословне или економске сврхе трансакције.

9. Приликом процене потенцијалне сумњиве активности, надлежни органи, ФИ, ДНФБП и лица за пружање услуга у вези са ВИ морају имати на уму да се неки индикатори могу лакше уочити током општег праћења трансакција, а неки други током специфичних провера трансакција. Посматрање једног или више индикатора зависи од читавих производних линија или производа и услуга које институција или лице које вршу услуге везане за ВИ нуди и од начина на који комуницира са својим клијентима. Када се јавља присуство једног један или више индикатора и са мало или нимало назнака легитимне економске или пословне сврхе, обвезник ће пре развити сумњу о ПН или ФТ.¹ Ови индикатори не треба да буду једини основ за доношење одлуке о подношењу извештаја о сумњивим трансакцијама. Подносиоци извештаја би требало да узму у разматрање подношење извештаја ако знају, сумњају или имају оправдане разлоге да тврде да је извршено ПН/ ФТ.

Индикатори

10. Следећи одељци садрже низ индикатора за препознавање сумњивих активности везаних за ВИ или могуће покушаје избегавања органа реда, који су утврђени у више од стотину студија случаја прикупљаних од 2017. године широм ФАТФ глобалне мреже, као и захваљујући консултовању литературе и истраживању отворених извора. Као што је претходно поменуто, постојање једног индикатора не мора нужно указивати на кривично дело. Присуство више индикатора у трансакцији без логичног пословног објашњења често покреће сумњу на потенцијалну криминалну активност. Присуство индикатора треба да подстакне даље праћење, испитивање и извештавање тамо где је то потребно.

Индикатори везани за трансакције

11. Иако ВИ још увек није толико широко распрострањена у јавности, криминалци је често користе. Виртуелна имовина је први пут употребљена у сврхе ПН пре више од једне деценије, и постаје све заступљенија у криминалним активностима. Овај скуп индикатора показује како су црвене заставице традиционално повезане са трансакцијама које укључују конвенционалнија средства плаћања и даље релевантне за откривање потенцијалних незаконитих активности повезаних са ВИ.

Износ и учесталост трансакција

- Уситњавање трансакција ВИ (нпр. разменом или преносом), разбијање на мале износе или износе испод прага за унос у евиденцију или извештавање, слично структурирању, односно, уситњавању готовинских трансакција.
- Реализација вишеструких трансакција велике вредности –
 - у кратком временском року, на пример у року од 24 сата;

¹ Иако се одређени број индикатора може односити и на ПН и ФТ, примера ради, прикупљање средстава, финансирање страних бораца и куповина оружја (нпр. на мрачном интернету) уз помоћ ВИ, читаоци би требало ово да протумаче у смислу поверљивог извештаја ФАТФ Утврђивање индикатора ризика од значаја за откривање финансирања тероризма (јун 2016.) (приступ одобрен само члановима ФАТФ)

- по обрасцу, без евидентирања даљих трансакција током дужег периода након тога, што је посебно често у случајевима везаним за изнуду путем малициозног софтвера; или
- уплата на новоотворени рачун или на претходно неактиван рачун
- Пренос ВИ без одлагања на више лица која врше услуге везане за виртуелну имовину, посебно на таква лица регистрована или активна у другој држави при чему –
 - Та локација нема везе са местом у коме клијент живи или послује; или
 - Мере за СПН/СФТ у тој држави не постоје или су слабо регулисане
- Уплата ВИ код мењача, а затим често одмах –
 - повлачење ВИ без додатних активности размене у другу ВИ, што је непотребан корак и захтева накнаду за трансакције;
 - претварање ВИ у више типова ВИ, што опет доводи до додатних накнада за трансакције, али без логичног пословног објашњења (нпр. диверзификација портфеља); или
 - повлачење ВИ са рачуна фирме која врши услугу одмах у приватни новчаник. Ово ефикасно претвара мењача/ ПУВИ у миксер који врши услугу мешања за потребе ПН.
- Прихватање средстава за која се сумња да су украдена или потичу из кривичног дела -
 - уплата средстава са адреса ВИ за које је утврђено да се на њима чувају украдена средства, или адреса ВИ повезаних са власницима украдених средстава.

Студија случаја 1. Вишеструки преноси велике количине ВИ на рачуне у страним државама реализовани у кратком временском периоду

Локално лице које врши услугу везану за ВИ поднело је извештај о сумњивим трансакцијама након сумњи у вези са куповином велике количине ВИ од стране различитих појединаца и о њиховим накнадним непосредним трансферима ка лицу у страниој држави. У разним случајевима, особе су имале исту адресу становања; а већини адреса ВИ приступало се са исте ИП адресе - што указује на потенцијалну употребу курира за новац од стране професионалних перача новца за прање незаконите добити.

Поред тога, вишеструко раслојавање декретног новца уређено је пре куповине ВИ од стране курира. Да би се прикрило порекло средстава, готовина је прво депонована на различите рачуне у различитим финансијским институцијама широм државе. Та средства су затим даље пребацивана на различите рачуне отворене у име предузећа регистрованих у датој држави. Електронска плаћања извршена су на рачуне у мањим

износима. Након тога, средства су пребацивана на другу групу рачуна пре него што су стигла на рачуне курира код локалних лица за пружање услуга у вези са ВИ. Виртуелна имовина је одмах купована и пребацивана у страна лица за услуге у вези са ВИ. Више од 150 појединаца било је умешано у овај случај, и они су одговорни за пренос око 108.352.900 УСД (или БТЦ 11.960) на више рачуна ВИ који воде два иностранна лица за вршење услуга у вези са ВИ.

Извор: : Јужна Африка

Студија случаја 2. Велика количина виртуелне имовине и трансфери ка иностранству

Локални мењач ВИ известио је да је приближно 400 милиона КРВ (301 170 ЕУР) украдено од жртава превара на интернету (phishing) и да је тај новац на крају замењен за ВИ током фазе раслојавања. Извештавање су покренуле вишеструке трансакције велике вредности ка једном лицу за ршење услуга у вези са ВИ у једном једином новчанику. Украдена средства у декретном новцу прво су замењена за три различите врсте ВИ, а затим депонована у електронски новчаник осумњиченог код локалног лица за услуге у вези са ВИ. Осумњичени је затим покушао да прикрије извор средстава пребацивањем средстава додатних 55 пута преко 48 одвојених рачуна који се воде у различитим локалним лицима за услуге у вези са ВИ, а затим у други електронски новчаник лоциран у иностранству.

Извор: Јужна Кореја

Индикатори везани за обрасце трансакција

12. Слично као у претходном одељку, индикатори у наставку илуструју како се злоупотреба ВИ у сврхе ПН/ФТ може идентификовати кроз нередовне, необичне или неуобичајене обрасце трансакција.

Трансакције које се тичу нових корисника

- Уплата велике вредности на почетку стварања везе са пружаоцем услуга, а да уплаћени износ није у складу са профилем клијента.
- Уплата велике вредности на почетку стварања везе са пружаоцем услуга када клијент одмах истог, или следећег дана почиње да тргује укупним износом или великим делом износа, или клијент повуче цео износ дан после. Како код већине ВИ постоји ограничење у погледу висине депозита прање у великим количинама такође се може извршити венберзанском трговином (ОТЦ).²
- Нови корисник покушава да размени целокупан износ ВИ или повлачи ВИ и покушава да скине целокупан износ са платформе.

² ОТЦ трговина односи се на хартије од вредности фирми које нису уврштене на формалну берзу као и на трговину преко мреже брокера и дилера.

Студија случаја 3. Почетни депозит није у складу са профилем клијента

Присуство следећих индикатора сумње подстакло је ФИ (банку) да поднесе ИСТ надлежним органима, што је довело до истраге ПН:

- трансакције које нису у складу са профилем власника рачуна - у прва два дана након што је за младог појединца отворен лични рачун, на рачун су стигле велике уплате комерцијалне природе од различитих правних лица у великим износима;
- обрасци трансакција - положена средства су одмах пребачена на рачуне неколико пружалаца услуга (у једном дану) за куповину ВИ (биткоин);
- Профил клијента - један од наручилаца био је познат банци као лице умешано у један случ преваре. Банка је такође доставила властима ИП адресе које се користе за услуге интернет банкарства.

На основу истраге, чинило се да је власник рачуна курир за новац кога су криминалци регрутовали на платформи друштвених мрежа да помаже тако што ће прихватати уплате за робу која се продаје на интернету. Међутим, чини се да су таква средства депоновале друге компаније жртве и нису представљала уплате за робу. Депонована средства су одмах пребацивана са личног банковног рачуна путем неколико подељених уплата на други рачун који је држало акционарско друштво у Чешкој и размењена у ВИ (биткоин) захваљујући неколико локалних пружаоца услуга. Ова средства су одмах повлачена са рачуна. Поред подношења ИСТ, банка је такође суспендовала сумњиве трансфере, што је омогућило накнадно одузимање средстава.

Локални пружалац услуга такође је приметио неправилности у примљеним средствима и пружио корисне информације као помоћ у истрази. Информације су укључивале: околности у којима је ВИ купљена; трансакције и друге информације откривене на основу примене познавања и праћења клијента као што су адреса новчаника, копија злоупотребљеног идентификационог документа за куповину и име наводног купца. То је омогућило властима да од банака затраже додатне информације (нпр. изводе).

Извор: Чешка Република

Трансакције које се тичу свих корисника

- Трансакције које укључују употребу више врста електронског новца или више рачуна, без логичног пословног објашњења.
- Вршење честих трансфера у одређеном временском периоду (нпр. дан, недеља, месец, итд.) На исти рачун ВИ –
 - од више особа;
 - са исте ИП адресе једне или више особа; или
 - у вези са великим износима.
- Уплате са многих неповезаних новчаника у релативно малим износима (акумулација средстава) са накнадним пребацивањем у други новчаник или потпуном разменом за декретни новац. Такве трансакције на више повезаних акумулирајућих рачуна могу у почетку да користе ВИ уместо декретног новца.
- Размена ВИ у декретни новац уз потенцијални губитак (нпр. када вредност ВИ варира или обављање размене упркос необично високој провизији у поређењу са стандардом у датој привредној грани, а посебно када трансакције немају логично пословно објашњење).
- Претварање велике количине декретног новца у ВИ или велике количине једне врсте ВИ у друге врсте ВИ без логичног пословног објашњења.

Студија случаја 4. Трансфери који се обављају у кратком временском размаку

Локална ФИ (фирма за хартије од вредности) поднела је ИСТ у вези са неовлашћеним трансакцијама између рачуна ВИ свог брокера и страног држављанина. Фирма за хартије од вредности пријавила је активност након што је утврдила да страни држављанин намерава да изврши трансфере у укупном износу од 4,8 милиона УСД (две одвојене трансакције које су се десиле у размаку од шест минута истог дана) и поднела брокеру захтев за трговањем следећег радног дана. Електронски новчаник није био држан на Кајманским острвима. Извештавање о сумњивим трансакцијама довело је до успешне размене информација са страним ФОС и успешног враћања већине средстава жртви, јер је платформа у страни држави успела да замрзне рачун осумњиченог пре него што је дело завршено.

Извор: Кајманска острва

Индикатори везани за анонимност

13. Овај скуп индикатора темељи се на карактеристикама и рањивостима које прате основну технологију ВИ. Различите технолошке карактеристике у наставку повећавају анонимност и отежавају откривање криминалних активности од стране власти. Ови фактори чине виртуелну имовину привлачном за криминалце који желе да прикрију или ускладиште своја средства. Ипак, само присуство ових карактеристика у некој активности не значи аутоматски да је реч о недозвољеној

транзакцији. На пример, употреба хардвера или папирног новчаника може бити легитиман начин заштите ВИ од крађе. Поново, присуство ових показатеља треба размотрити у контексту других карактеристика клијента и односа или логичног пословног објашњења.

- Транзакције клијента које укључују више од једне врсте ВИ, упркос додатним накнадама за трансакције, а посебно оне врсте ВИ које пружају већу анонимност, попут анонимног електронског новца (АЕЦ) или електронског новца код кога се гарантује приватност.
- Премештање ВИ која постоји на јавном, транспарентном блокчејну, као што је Bitcoin, на централизовану берзу да би се одмах потом БИ заменила за АЕЦ или електронски новац код кога се гарантује приватност.
- Клијенти који послују као нерегистровани / нелиценцирани пружаоци услуга у вези са ВИ на страницама за размену типа пеер-то-пеер (П2П), посебно када постоји бојазан да обрађују огромну количину трансфера ВИ у име свог клијента и наплаћују високе накнаде у поређењу са накнадом која се плаћа другим сличним лицима која нуде услуге преноса. Коришћење банковних рачуна за олакшавање ових П2П трансакција.
- Ненормалне трансакционе активности (ниво и обим) ВИ након којих следи повлачење готовине из новчаника са П2П платформи без логичног пословног објашњења.
- Виртуелна имовина пренета у или из новчаника активностима које личе на претходно описане обрасце повезане са ангажовањем пружалаца услуга који нуде услуге мешања средстава и П2П платформи.
- Транзакције које користе услуге мешања, што указује на намеру да се замагли проток незаконитих средстава између познатих адреса новчаника и тржишта на мрачном интернету.
- Средства депонована или повучена са адресе ВИ или новчаника са директним и индиректним везама до изложених сумњивих извора, укључујући тржишта на мрачном интернету, услуге мешања, сумњиве коцкарске локације, илегалне активности (нпр. ransomware) и/или извештаји о крађи.
- Коришћење децентрализованих / нехостованих, хардверских или папирних новчаника за транспорт ВИ преко граница.
- Корисници који улазе на платформу пружаоца услуга региструјући име свог интернет домена преко проксија или користећи регистре имена домена (ДНС) који не откривају или чувају поверљивост података о власницима имена домена.
- Корисници који улазе на платформу пружаоца услуга користећи ИП адресу повезану са мрачним интернетом или другим сличним софтвером који омогућава анонимну комуникацију, укључујући шифровану е-пошту и ВПН. Транзакције између партнера који користе различита анонимна шифрована средства комуникације (нпр. форуме, ћаскања, мобилне апликације, мрежне игре итд.) уместо пружаоца услуга.
- Велики број наизглед неповезаних новчаника ВИ контролисаних са исте ИП адресе (или МАЦ адресе), што може подразумевати употребу фантомских новчаника регистрованих на различите кориснике да би се прикрила међусобна веза.

- Коришћење врсте ВИ чији дизајн није адекватно документован или је повезана са могућом преваром или другим алатима за реализацију преварантских шема, као што су пирамидалне преваре.
- Пријем средстава од или слање средстава пружаоцима услуга који примењују очигледно слабе мере познавања и праћења клијента, односно упознавања са клијентом или их уопште не примењују.
- Коришћење банкомата / киоска ВИ –
 - упркос вишим накнадама за трансакције и укључујући оне које обично користе курири или жртве преваре; или
 - на локацијама са високим ризиком и интензивним криминалним активностима.

Употреба банкомата /киоска сама по себи није довољна да представља индикатор сумњиве активности, али то јесте ако се банкомат налази у ризичном подручју или ако се користи за низ малих трансакција (или уз друге додатне факторе).

Студија случаја 5. Употреба ИП адресе повезане са тржиштем на мрачном интернету – Alpha Bay

АлфаБеј, највеће криминално тржиште на мрачном интернету које су власти срушиле 2017. године, стотине хиљада људи користило је за куповину и продају илегалних дрога, украдених и лажних идентификационих докумената и приступ уређајима, фалсификованој роби, малверу и другим алаткама за хаковање рачунара, оружју и токсичним хемикалијама током две године. Интерент страница је функционисала као скривена услуга на ТОР мрежи захваљујући чему су се скривале локације основних сервера, као и идентитети администратора, модератора и корисника. Добављачи са АлфаБеја користили су низ различитих врста ВИ, и имали су приближно 200.000 корисника, 40.000 добављача, 250.000 уноса и омогућили реализацију трансакција вредних више од милијарду УСД у ВИ између 2015. и 2017. године.

У јулу 2017. године, америчка влада, уз помоћ од страних колега, скинула је сервере на којима се чувао АлфаБеј, ухапсила администратора и на основу налога за заплону издатог у Источном округу Калифорније запленила физичку и виртуелну имовину са самог тржишта и ону која је представљала незаконити приход од удруживања ради извршења кривичног дела на АлфаБеју. Федерални агенти су добили налоге након што су пратили трансакције у електронском новцу пореклом са АлфаБеја на друге рачуне ВИ и идентификовали банковне рачуне и другу материјалну имовину под контролом наводног администратора.

Извор: Сједињене Државе

Студија случаја 6. Употреба мешања – Helix

Лице за пружање услуга у вези са ВИ на мрачном интернету - Хеликс је у периоду од три године, у замену за одређену накнаду, пружало услугу мешања средстава уз помоћ које су њихови клијенти прикрили извор или власнике ВИ. Хеликс је наводно пребацио преко 350.000 биткоина, чија је вредност у тренутку преноса била већа од 300 милиона УСД. Оператор је рекламирао услугу као средство скривања трансакција од власти на мрачном интернету. У фебруару 2020. године, против појединца који је управљао компанијом Хеликс поднете су кривичне пријаве, укључујући удруживање ради извршења ПН и неовлашћено вођење посла за пренос новца.

Хеликс је сарађивао са АлфаБејем све док га власти нису срушиле 2017. године

Извор: Сједињене Државе

Студија случаја 7. Употреба децентрализованог новчаника

Овај случај показује како криминалци користе децентрализовани новчаник за прикривање извора нелегалних средстава остварених недозвољеном трговином наркотицима. У овом случају, криминалци су продавали велике количине наркотика на Интернету и тражили су да им се плаћа не само у декретном новцу, већ и у облику ВИ (Bitcoin, EX-codes, EXMO-чекови).

Незаконита средства примљена у декретној валути претварана су у ВИ уз помоћ анонимног рачуна на Интернет платформи за трговину блокчејном. Таква средства, у облику ВИ, претварана су назад у декретни новац код мењача, пре него што су враћана на личне рачуне криминалаца у банци. Што се тиче оних недозвољених средстава примљених у облику ВИ, она су прво пребацивана у децентрализоване биткоин новчанике које држе дотични криминалци, пре него што су даље пребацивана у друге биткоин новчанике на различитим берзама. Ово отежава праћење средстава. Слично томе, опрана средства (у ВИ) претварана су назад у декретни новац пре него што су уплаћивана на рачуне криминалаца у банци. Криминалац је након суђења осуђен на седам година затвора и новчану казну.

Извор: Руска Федерација

Индикатори везани за налогодавце или примаоце

14. Овај скуп показатеља везан је за профил и необично понашање налогодавца или примаоца незаконитих трансакција.

Неправилности уочене током отварања рачуна

- Отварање посебних рачуна под различитим именима како би се заобишла ограничења трговања или повлачења готовине која намећу лица која пружају услуге у вези са ВИ.
- Трансакције покренуте са непроверених ИП адреса, ИП адреса из санкционисаних држава или ИП адреса претходно означених као сумњивих.
- Чести покушаји отварања рачуна у оквиру истог пружаоца услуге са исте ИП адресе.
- Што се тиче трговаца/корпоративних корисника, они региструју своје интернет домене у другим државама, а не у држави седишта или у држави са слабо контролисаним поступком регистрације домена.

Неправилности уочене током примене мере познавања и праћења странке

- Непотпуне или недовољне информације током примене мере или клијент одбија да одговори на захтев за достављање докумената или да одговори на упите у вези са извором средстава.
- Налогодавац/прималац нема сазнања или пружа нетачне информације о трансакцији, извору средстава или односу са другом страном.
- Клијент је доставио фалсификоване документе или измењене фотографије и/или идентификационе документе као део процеса остваривања сарадње са ФИ.

Студија случаја 8. Клијент одбија да пружи информације о извору средстава

ФИ (банка) је доставила ИСТ у вези са рачуном локалне компаније која је држала средства остварена продајом купона којима се тргује производом (у овом случају биопластиком). Средства су депоновала и физичка и правна лица, а нека су првобитно била у ВИ. Упркос даљим истрагама банке, представници власника рачуна нису пружили информације о пореклу средстава. Накнадне анализе власти показале су да су средства која је компанија послала показала везе са субјектима повезаним са организованим криминалом и средствима добијеним од лажног пројекта.

Извор: Италија

Профил

- Купац пружа идентификационе податке или акредитиве налога (нпр. Нестандардну ИП адресу или флеш колачиће) другог налога.
- Појављују се разлике између ИП адреса повезаних са профилем клијента и ИП адреса са којих се покрећу трансакције.
- Адреса ВИ клијента појављује се на јавним форумима повезаним са илегалним активностима.
- Клијент је познат преко јавно доступних информација полицији због претходног удруживања ради вршења кривичних дела.

Студија случаја 9. Профил клијента се не подудара са редовним трговањем са ВИ високе вредности

Лице које пружа услуге у вези са ВИ (мењач) и ФИ (платна институција) поднели су ИСТ финансијско-обавештајној служби у вези са трговањем ВИ велике вредности које је започело када је отворен рачун код мењача. Конкретно, власник рачуна је обављао разне трансакције, куповину и продају ВИ у вредности од изнад ЕУР 180.000 - које се нису подударале са профилем власника рачуна (укључујући занимање и плату).

Анализом је откривено да је ВИ накнадно коришћена за (и) трансакције на тржишту на мрачном интернету; (ии) клађење на интернету; (иии) трансакције са пружаоцима услуга који нису увели одговарајуће мере контроле у циљу спречавања прања новца и финансирања тероризма или су били под претходним истрагама за ПН због више милиона долара; (ив) трансакције ВИ на П2П платформама; и (в) „мешање“. Власник рачуна је такође користио мноштво различитих средстава (нпр. услуге преноса новца, интернет банкарство и припејд картице) да би у истом временском оквиру премештао одговарајућу количину средстава са свог рачуна. Изгледа да су средства која је имао власник рачуна потицала од мреже појединаца који су се налазили у различитим државама у Азији и Европи (укључујући Италију) и куповали ВИ (биткоин) готовином, а затим их слали њему путем услуге преноса новца и путем банкарског система. Такође је примао средства на својим припејд картицама од лица у Африци и на Блиском Истоку, који су заузврат прикупљали средства од суграђана који бораве у Италији и иностранству. Та средства су затим коришћена за прекограничне трансфере и коцкање путем интернета, а подизана су са банкомата у Италији.

Извор: Италија

Профил потенцијалних курира или жртава преваре

- Налогодавац као да није упознат са технологијом ВИ или решењима за кастоди услуге новчаника на интернету. Такве особе могу бити курири ангажовани од стране професионалних перача новца или жртве преваре на основу које су постали курири и на основу које су убеђени да преносе незаконите приходе без знања о њиховом пореклу.
- Клијент који је знатно старији од просечних корисника платформе отвара рачун и укључује се у велики број трансакција, што указује на могућност да има улогу курира или жртве ранијег финансијског искоришћавања.
- Клијент је финансијски рањива особа, а трговци наркотицима их често користе да би им помогли у таквој трговини.
- Клијент купује велику количину ВИ, а не поседује значајно богатство или се то коси са његовим/њеним финансијским профилем што може указивати на прање новца, курирску улогу, жртву преваре.

Студија случај 10. Жртве преваре у улози курира

У овим преварама са инвестицијама страни држављани ступали су у контакт са пензионерима и углавном старијим особама путем телефонских позива, и-мејла или друштвених мрежа и нудили им могућности улагања у биткоин или друге врсте ВИ с обећањем да ће остварити огроман профит због растуће популарности ВИ и пораста вредности. Почетно улагање у малим износима (у многим случајевима не више од 250 ЕУР) вршено је са банковног рачуна жртве, кредитне картице или путем других средстава у разне платне услуге, а затим је тај новац завршавао у рукама криминалаца. Алтернативно, жртве су упућиване да размене декретни новац у биткоин помоћу банкомата и пошаљу средства на адресу коју су одредили криминалци.

Жртве нису биле вичне раду са модерним технологијама и генерално нису разумеле ВИ нити у шта заиста улажу. Криминалци су такође тражили од жртава да инсталирају апликацију за даљинску контролу рачунара како би могли да им помогну да исправно преносе средстава на одређене рачуне. Ово је угрозило уређаје жртава, тако да су криминалци могли да врше неовлашћене новчане трансфере, а да жртва тога није била свесна, све док није приметила да новац недостаје са рачуна. У неким случајевима, криминалци су такође измишљали чланке тврдећи да познате личности или богати пословни људи или новинари промовишу улагања у ВИ, пружајући тако жртвама осећај поверења и легитимитета „инвестиције“.

Извор: Финска

Друге врсте необичног понашања

- Клијент често мења своје идентификационе податке, укључујући адресе е-поште, ИП адресе или финансијске информације, што такође може указивати на преузимање рачуна од клијента.
- Клијент покушава да уђе на платформу једног или више лица која пружају услуге у вези са ВИ са различитих ИП адреса често током дана.
- Употреба израза који указују на трансакције које се спроводе да подрже нелегалне активности или у куповини недозвољене робе, попут лекова или украдених података са кредитних картица.
- Клијент понавља трансакције са одређеном групом појединаца уз значајан добитак или губитак. То би могло указивати на потенцијално преузимање рачуна и покушај извлачења новца жртава путем трговине или на шему ПН за прикривање тока средстава помоћу инфраструктуре лица која пружају услуге у вези са ВИ.

Индикатори везани за извор средстава или богатства

15. Као што показују случајеви које су државе доставиле, злоупотреба ВИ често је повезана са кривичним делима као што су неовлашћена трговина наркотицима и психотропним супстанцама, превара, крађа и изнуда (укључујући високотехнолошка кривична дела). У наставку су описане уобичајене црвене заставице повезане са извором средстава или богатства повезаним са таквим кривичним делима:

- Обављање трансакција са адресама ВИ или банкарским картицама које су повезане са познатим шемама превара, изнуде или крађе података на интернету, санкционисаним адресама, тржиштима на мрачном интернету или другим недозвољеним интернет страницама.
- Трансакције ВИ које потичу или су намењене услугама коцкања на интернету.
- Коришћење једне или више кредитних и/или дебитних картица које су повезане са електронским новчаником за повлачење велике количине декретног новца (крипто-са картице), или куповина ВИ готовинским депозитима на кредитним картицама.
- Средства која се уплаћују на рачун или адресу ВИ знатно су виша од уобичајених и долазе из непознатог извора након чега се претварају у декретни новац, што може указивати на крађу средстава.
- Недостатак транспарентности или недовољне информације о пореклу и власницима средстава, попут оних које укључују употребу фантомских компанија или средстава која се чине иницијалну понуду коина (ИЦО), где лични подаци инвеститора можда неће моћи да се виде или уплате са интернета путем кредитних /дебитних картица након чега одмах следи повлачење средстава са рачуна.
- Средства клијента добијена од треће стране након услуге мешања или мешањем новчаника.
- Већи део богатства клијента проистиче из инвестиција у ВИ, ИЦО или лажне ИЦО и слично.

- Богатство клијента се у непропорционално великој мери добија од лица која врше услуге везане за ВИ које не примењују мере СПН/СФТ.

Студија случаја 11. Употреба фантомских компанија – интернет страница „Deep Dot Web“

У мају 2019. америчке власти заплениле су интернет страницу „DeepDotWeb“ (DDW), на основу налога суда. Наводни власници и оператери ове странице оптужени су за удруживање ради вршења ПН у вези са милионима долара мита које су добили због упућивања појединаца на тржишта на мрачном интернету са странице DDW. Путем линка за упућивање, наводни власници и оператери DDW примали су мито, односно провизију на приход од куповине илегалне робе, попут фентанила и хероина, коју су обавили појединци који су били упућени са DDW странице на тржиште на мрачном интернету.

Мито је уплаћивано у новчаник биткоина DDW. Да би прикрили и замаскирали природу и извор незаконите зараде, која је износила преко 15 милиона УСД, власници и оператери пребацивали су средства уплаћена као мито из свог DDW новчаника за биткоин у друге сличне новчанике, као и на банковне рачуне које су контролисали у име фантомских компанија. Оптужени су користили ове фантомске компаније да би премештали незакониту добит и обављали друге активности повезане са DDW. Током петогодишњег периода, интернет страница примила је мито у вредности од отприлике 8.155 биткоина са тржишта на мрачном интернету што је једнако приближно 8 милиона УСД, кориговано за вредност биткоина на берзи у време трансакције. Биткоин је пребациван у DDW новчаник окривљених, у серији од више од 40.000 уплата, а затим је готовина подизана у преко 2.700 трансакција. Вредност биткоина у време повлачења готовине из DDW новчаника износила је приближно 15 милиона УСД.

Извор: Сједињене Америчке Државе

Студија случаја 12. Употреба више мењача виртуелне имовине, лажна идентификациона документа у поступку ППС и припејд картице

Окривљени у овом предмету наводно су управљали шемом ПН у сарадњи са криминалцима који су хаковали размену ВИ и украли 250 милиона УСД у виртуелној имовини. Двојица окривљених су наводно опрали украдену виртуелну имовину

у вредности од око 91 милион УСД из ове краје, као и 9,5 милиона УСД несталих путем још једне високотехнолошке крађе.

Покрадена ВИ затим је пролазила кроз стотине аутоматизованих трансакција и вишеструких размена за другу валуту. Перачи су у неким случајевима користили модификоване фотографије и фалсификоване идентификационе документе да би заобишли процедуре упознавања са странком на берзама ВИ. Отприлике 35 милиона УСД незаконитих средстава пребачено је на стране банкарске рачуне и коришћено за куповину припејд картица, које су могле да се мењају за ВИ. Оптужени су пословали преко независних као и повезаних рачуна и пружали услуге преноса ВИ, мењали ВИ за декретни новац купцима уз накнаду. Окривљени су такође пословали у САД, али ни у једном тренутку се не пријављују финансијско-обавештајој сужби САД (ФинЦЕН).

Извор: Сједињене Државе

Индикатори географских ризика

16. Овај скуп индикатора показује како криминалци приликом премештања својих недозвољених средстава користе различите фазе примене ревидираних стандарда ФАТФ за ВИ и лица која пружају услуге у вези са ВИ³ у различитим државама. На основу случајева које су пријавиле државе, види се да криминалци користе празнине у режимима спречавања прања новца и финансирања тероризма уз помоћ виртуелне имовине и лица која пружају услуге у вези са ВИ премештањем својих недозвољених средстава код лица која пружају услуге у вези са ВИ са седиштем или активностима у државама које или немају мере за СПН/СФТ уз помоћ ВИ и лица која пружају услуге у вези са ВИ или у државама са минималним таквим прописима. Ове државе можда немају режим регистрације/лицензирања, или нису прошириле мере СПН/СФТ на виртуелну имовину и лица која пружају услуге у вези са ВИ или можда нису на други начин увеле читав спектар превентивних мера у складу са стандардима ФАТФ. Иако овај извештај не настоји да идентификује списак држава са „високим ризиком“, обвезници су позвани да узму у обзир следеће индикаторе приликом разматрања географских ризика. Ови ризици повезани су са извором, одредиштем и транзитном државом трансакције. Такође су релевантни за ризике повезане са првим налогодавцем трансакције и корисником средстава који могу бити повезани са државом високог ризика. Поред тога, могу се применити на држављанство, пребивалиште или место пословања клијента.

- Новчана средства клијента или потичу са берзе или се упућују на берзу која није регистрована у држави у којој се налази клијент или мењач.

³ У јулу 2020. ФАТФ је објавио [12-Month Review of The Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers](#) (Дванаестомесечни преглед ревидираних стандарда ФАТФ о виртуелној имовини и лицима која пружају услуге у вези са виртуелном имовином). Одељак 2 извештаја бави се напретком примене ревидираних стандарда од јуна 2019. године.

- Клијент користи услуге мењача ВИ или лица која врше услуге преноса новца и вредности који се налазе у иностранству у високо ризичној држави која нема или је познато да има неадекватне мере за СПН/СФТ за лица која пружају услуге у вези са ВИ, или неадекватне мере ППС или мере упознај свог клијента.
- Клијент шаље средства лицима која врше услуге у вези са ВИ који послују у државама без прописа о ВИ или не примењују мере СПН/СФТ.
- Клијент успоставља канцеларију или премешта канцеларију у државу која нема прописе или не примењује прописе који регулишу ВИ, или оснива нову канцеларију у држави када за то не постоји јасно пословно оправдање.

Студија случаја 13. Продавац биткоина који послује без дозволе за пренос новца (прекогранични елементи)

У априлу 2019. године окривљени је добио казну од две године затвора за неовлашћени пренос новца након што је продао стотине хиљада долара вредну виртуелну имовину (биткоин) и остварио сарадњу са више од хиљаду купаца у САД. Окривљеном је такође наложено да се преда профит у износу од 823.357 УСД.

Оптужени је оглашавао своје услуге на интернет страницама за кориснике ВИ, лично се састајући са неким купцима којом приликом је узимао готовину у замену за ВИ. Остали купци су га плаћали преко банкомата или лица која врше услугу преноса новца. Окривљени је за своје услуге добијао премију од пет одсто по важећем курсу. Најпре је биткоин набављао на америчкој берзи, али када су његове активности изазвале сумњу и кад му је рачун затворен, окривљени је прешао на берзу у Азији. Користећи ту берзу, окривљени купује 3,29 милиона УСД у биткоину, у стотинама одвојених трансакција, између марта 2015. и априла 2017. Окривљени је такође признао да је своју америчку готовину, коју је држао у другој држави која се граничи са САД дао трговцу драгоценим металима и да су између краја 2016. и почетка 2018. године он и други увезли у САД укупно преко 1 милион америчких долара, у износима нешто нижим од оних који повлаче за собом обавезу извештавања, односно, нижим од 10.000 америчких долара.

Извор: Сједињене Америчке Државе

Лице које пружа услуге у вези са виртуелном имовином премешта своје пословање и државу са неодговарајућим мерама за СПН/СФТ

Уочи примене мера којима ће се забранити рад лица која врше услуге у вези са ВИ у држави А у Азији 2017. године, једно такво лице (мењач) основан у држави А премешта своје пословање у државу Б у истом региону. 2018. године држава Б појачава свој режим за СПН/СФТ у погледу лица која врше услуге у вези са ВИ након озбиљних хакерских напада већих лица која врше услуге у вези са ВИ (мењачи). У марту 2018. једно лице које пружа услуге у вези са ВИ најављује да сели седиште у државу В у Европи (држава која у то време још није увела свеобухватан режим СПН/СФТ који би укључивао ВИ и лица која врше услуге у вези са ВИ). Касније у новембру 2018. држава В уводи одређене прописе за лица која врше услуге у вези са ВИ, и у фебруару 2020. потврђује да поменуто лице није добило дозволу за рад. Новији извештаји из 2020. године наводе да се ово лице већ регистровало и да има адресу у држави Г у Африци.

Извор: : јавни домен

Закључак

17. Овај извештај сачињен је захваљујући опсежном доприносу чланова ФАТФ широм глобалне мреже с циљем да се пружи практично средство и за јавни и за приватни сектор за идентификовање, откривање и на крају спречавање криминалних радњи, прања новца и финансирања тероризма повезаних са виртуелном имовином.

18. Индикатори обухваћени овим извештајем везују се за карактеристике и рањивост који су својствени виртуелној имовини. Списак индикатора није исцрпан нити су сви индикатори примењиви у свакој ситуацији. Индикатори су често само један од многих елемената који помажу да се изгради целокупна слика потенцијалног ризика од ПН или ФТ и важно је да се индикатори (или било који појединачни индикатор) не гледају одвојено од осталих фактора. Треба их ставити у контекст информација добијених од релевантних власти.

19. Приступ заснован на ризику примењен у редовном и динамичном двосмерном дијалогу између јавног и приватног сектора несумњиво би побољшао ефикасност овог извештаја. Стога се подстичу надлежни органи да поделе овај извештај обвезницима и да организују сесије уз њихово активно учешће и сесије изградње свести како би подстакли разумевање овог извештаја.

20. Иако се идентификовани индикатори непрестано развијају, они се најбоље користе када се примењују уз друге контекстуалне информације из домаћих закона и јавних извора. Надлежни органи могу поучити приватни сектор о томе који су индикатори и информације најрелевантнији за дату државу. На пример, они могу да припреме савете обвезницима на основу овог извештаја. Међутим, овај извештај не би требало да буде регулаторно средство код усклађивања и испитивања нити контролна листа приликом надзора институција приватног сектора, јер нису сви индикатори примењиви у свим државама или свим институцијама.

Литература

ФАТФ (јун 2014.), [FATF Report Virtual Currencies Key Definitions and Potential AML/CFT Risks](#)

ФАТФ (јун 2019.), [FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers](#)

ФАТФ (јун 2020.), [12-month Review of Revised FATF Standards – Virtual Assets and VASPs](#)

Извештаји само за чланове ФАТФ

ФАТФ (јун 2016.), [Confidential FATF Report on Detecting Terrorist Financing: Relevant Risk Indicators](#)

ФАТФ (јун 2019.), [Confidential FATF Report on Financial Investigations Involving Virtual Assets](#)

Индикатори за препознавање сумње да се ради о прању новца и финансирању тероризма уз помоћ виртуелне имовине

1. Виртуелна имовина (ВИ) и услуге повезане са њом имају потенцијал да подстакну финансијске иновације и ефикасност, али њихове посебне карактеристике такође стварају нове могућности за прање новца, за финансијере тероризма и друге криминалце да перу свој приход или финансирају незаконите активности

3. ФАТФ је припремио овај кратки извештај о индикаторима за препознавање сумње да се ради о ПН/ФТ уз помоћ виртуелне имовине како би помогао обвезницима, укључујући финансијске институције, одређене нефинансијске секторе и самосталне професије и лица која се баве пружањем услуга у вези са виртуелном имовином да откривају и извештавају о потенцијалним активностима ПН и ФТ уз помоћ виртуелне имовине.

