FATF

КЕРІВНИЦТВО З РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ

ВІРТУАЛЬНІ АКТИВИ ТА ПОСТАЧАЛЬНИКИ ПОСЛУГ З ПЕРЕКАЗУ ВІРТУАЛЬНИХ АКТИВІВ

ЧЕРВЕНЬ 2019

Група з розробки фінансових заходів боротьби з відмиванням грошей (FATF) – це незалежна міжурядова організація, що розробляє та популяризує свої принципи для захисту світової фінансової системи від загроз відмивання коштів, фінансування тероризму та фінансування розповсюдження зброї масового знищення. Рекомендації FATF є загальновизнаними міжнародними стандартами з протидії відмиванню коштів (ПВК) та фінансуванню тероризму (ФТ).

Для більшої інформації щодо FATF, відвідайте сайт http://www.fatf-gafi.org

Неофіційний переклад здійснено Державною службою фінансового моніторингу України.

Цей документ та/або будь-яка мапа, що розміщена у цьому документі, не завдають шкоди статусу або суверенітету будь-якої території, розмежуванню міжнародних кордонів, а також назвам будь-яких територій, міст чи зон.

Посилання для цитування:

FATF (2019), *Керівництво щодо Ризик-Орієнтованого Підходу до Віртуальних Активів та Постачальників Послуг з Переказу Віртуальних Активів*, FATF, Париж, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

Зміст

АБРЕВІАТУРИ

AEC	Криптовалюта з Посиленою Анонімністю (Anonymity-Enhanced Cryptocurrency)
CDD	Належна Перевірка Клієнта (Customer Due Dilligance)
ICO	Первинна Пропозиція/Розміщення Монет (Initial Coin Offering)
MSB	Установа, що Надає Фінансові Послуги (Money Services Business)
MVTS	Послуги з Переказу Грошових Цінностей (Money or Value Transfer Service)
OTC	Позабіржова Торгівля (Over-the-Counter)
P2P	Переказ Вартості без Використання Посередника (Peer-to-Peer)
VASP	Постачальник Послуг з Віртуальних Активів (Virtual Asset Service Provider)
ВА	Віртуальний Актив
ВК	Відмивання Коштів
ВНУП	Визначені Нефінансові Установи та Професії
ПВК	Протидія Відмиванню Коштів
ПВК/ФТ	Протидія Відмиванню Коштів та Фінансуванню Тероризму
РОП	Ризик-Орієнтований Підхід
ФТ	Фінансування Тероризму

СТИСЛИЙ ВИСНОВОК

У жовтні 2018 року FATF запровадила зміни до своїх Рекомендацій для того, аби чітко заявити, що вони застосовуються й до фінансової діяльності, що включає віртуальні активи, а також для додавання двох нових визначень до Словника: «віртуальний актив» (ВА) та «постачальники послуг з віртуальних активів» (VASP). Змінена Рекомендація 15 вимагає, щоб VASP були регульовані в цілях здійснення діяльності з ПВК/ФТ, отримували ліцензію чи реєструвались та були об'єктом ефективної системи моніторингу та нагляду.

У червні 2019 року FATF прийняла Пояснювальну Записку до Рекомендації 15 для подальшого уточнення того, як вимоги FATF мають застосовуватись до ВА та VASP, особливо щодо застосування ризик-орієнтованого підходу (РОП) до діяльності та операцій із ВА та до VASP; нагляду та моніторингу за VASP в цілях ПВК/ФТ; ліцензування та реєстрації; превентивних заходів таких як належна перевірка клієнта, ведення обліку та звітування про підозрілі операції; санкцій та інших правозастосовних методів; а також міжнародної співпраці.

Також FATF прийняла це Керівництво[1] щодо застосування РОП до ВА та VASP у червні 2019 року. Воно покликане допомогти як національним органам влади у розумінні, а також розвитку регуляторних та наглядових відповідей на діяльність з ВА та VASP, так і підприємствам приватного сектору, які хочуть бути залучені у діяльність з ВА, для розуміння їх зобов'язань з ПВК/ФТ і того, як вони можуть ефективно дотримуватись цих вимог.

Це Керівництво підкреслює необхідність для країн, VASP та інших підприємств, залучених до діяльності з ВА, розуміти ризики ВК/ФТ, що пов'язані з їх діяльністю, та вживати відповідних пом'якшувальних заходів для їх вирішення. Зокрема, Керівництво надає приклади індикаторів ризику, які мають бути окремо розглянуті в контексті ВА з акцентом на факторах, що будуть більше заплутувати операції чи перешкоджати здатності VASP ідентифікувати клієнтів.

Керівництво досліджує, яким чином діяльність з ВА та VASP підпадає під сферу дії Рекомендацій FATF. Воно розглядає п'ять типів діяльності, що охоплюються визначенням VASP, та надає приклади видів діяльності, що пов'язані з ВА, які підпадають під визначення VASP і які будуть виведені з-під охоплення FATF. У цьому відношенні, воно висвітлює ключові

[1] Це Керівництво оновлює Керівництво FATF щодо Ризик-Орієнтованого Підходу до Віртуальних Валют 2015 року.

елементи, які мають кваліфікуватись як VASP, а саме виступати як бізнес від імені клієнтів та активно сприяти діяльності, що пов'язана із ВА.

Керівництво описує застосування Рекомендацій FATF для країн та компетентних органів влади; а також для VASP та інших підзвітних суб'єктів, що залучені до діяльності із ВА, в тому числі фінансових установ таких як банки та дилери з цінних паперів. Практично усі Рекомендації FATF мають безпосереднє відношення до вирішення ризиків ВК/ФТ, що пов'язані із ВА та VASP, в той час як інші Рекомендації не настільки сильно пов'язані із ВА або VASP, хоча все ще залишаються актуальними та такими, що застосовуються. Тому VASP мають такий самий повний набір зобов'язань, як і фінансові установи чи ВНУП.

Керівництво детально описує весь спектр зобов'язань, що застосовуються до VASP та до ВА у відповідності до Рекомендацій FATF. Це включає уточнення того, що усі кошти чи вартісні вираження у Рекомендаціях FATF (*напр.,* «майно», «доходи», «кошти», «гроші та інші активи», а також інша «еквівалентна вартість») включають ВА. Таким чином, країни повинні застосовувати усі відповідні заходи до ВА, діяльності з ВА, та до VASP згідно з Рекомендаціями FATF.

Керівництво пояснює вимоги до реєстрації та ліцензування VASP, зокрема як визначити у якій країні VASP має бути зареєстровано чи надано ліцензію – як мінімум там, де вони були створені; або в юрисдикції, де вони проводять свою ділову діяльність, якщо мова йде про фізичну особу, втім юрисдикції також мають право обирати, чи вимагати від VASP отримати ліцензію або ж пройти реєстрацію перед здійснення діяльності в своїй юрисдикції. Керівництво й надалі підкреслює, що від національних органів влади вимагається вживати заходів для виявлення фізичних чи юридичних осіб, які проводять діяльність з ВА без необхідної ліцензії чи реєстрації. Це в рівній мірі стосується країн, які вирішили заборонити ВА та діяльність з ВА на національному рівні.

Що стосується нагляду за VASP, Керівництво чітко вказує на те, що тільки компетентні органи влади можуть діяти як органи, що здійснюють нагляд чи моніторинг за VASP. Вони мають проводити ризик-орієнтований нагляд чи моніторинг, з належними повноваженнями, в тому числі повноваженнями з проведення перевірок, примушення до надання інформації та введення санкцій. Встановлюється спеціальний наголос на важливості міжнародної співпраці між наглядовими органами, враховуючи транскордонну природу діяльності VASP та надання послуг.

Керівництвом чітко встановлюється, що VASP та інші підприємства, що залучені у діяльність з ВА, повинні впроваджувати усі превентивні

заходи, що описані у Рекомендаціях FATF з 10 по 21. Керівництвом пояснюється, яким чином ці зобов'язання мають виконуватись у контексті ВА та надається класифікація особливих вимог, що застосовуються до порогового значення у 1000 USD/EUR для окремих операцій з ВА, при перевищенні якого VASP повинні проводити належну перевірку клієнта (Рекомендація 10); та зобов'язань отримувати, зберігати та передавати необхідну інформацію про відправника та отримувача у невідкладний та надійний спосіб, при проведенні операцій з ВА (Рекомендація 16). Як зазначається керівництвом, відповідні органи влади мають координувати свою діяльність для забезпечення того, що це робиться у спосіб, який відповідає національним правилам з захисту даних та конфіденційності.

Врешті, Керівництво надає приклади юрисдикційних підходів до регулювання, нагляду та правозастосування до діяльності з ВА, VASP та інших підзвітних суб'єктів у сфері ПВК/ФТ.

РОЗДІЛ I – ВСТУП

Загальні відомості

1. Нові технології, продукти та пов'язані послуги мають потенціал до стимулювання фінансових інновацій та ефективності й покращення фінансових послуг, але вони також створюють нові можливості для злочинців та терористів у відмиванні їх доходів або фінансування їх незаконної діяльності. Ризик-орієнтований підхід є ключовим в ефективній імплементації переглянутих Міжнародних Стандартів з Протидії Відмиванню Коштів та Фінансуванню Тероризму й Розповсюдження Зброї Масового Знищення Групи з Розробки фінансових заходів боротьби з відмиванням грошей (FATF), які члени FATF запровадили у 2012 році і тому FATF активно здійснює моніторинг ризиків, що пов'язані з новітніми технологіями.

2. У червні 2014 року, FATF випустив Віртуальні Валюти: Ключові Визначення та Потенційні Ризики ПВК/ФТ у відповідь на розвиток віртуальних валют та пов'язаних з ними платіжних механізмів, що надають нові методи переказу грошової вартості через інтернет. У червні 2015 року FATF випустила Керівництво з Ризик-Орієнтованого Підходу до Віртуальних Валют (Керівництво щодо ВВ 2015 року) як частину поетапного підходу до вирішення ризиків Відмивання Коштів та Фінансування Тероризму (ВК/ФТ), що пов'язані з платіжними продуктами та послугами віртуальних валют.

3. Керівництво щодо ВВ 2015 року фокусується на моментах, коли діяльність з віртуальними валютами перетинається з традиційними регульованими фінансовими системами, зокрема пункти обміну віртуальних валют. Тим не менш, в останні роки простір віртуальних активів розширився і включив у себе ряд нових продуктів та послуг, бізнес моделей, видів діяльності та взаємодії, в тому числі операції між різними видами віртуальних активів.

4. Зокрема, в екосистемі віртуальних активів спостерігалося зростання криптовалют з посиленою анонімністю (AEC), міксерів та тумблерів (послуги, що пропонуються для змішування потенційно «брудної» криптовалюти з іншими, для приховування сліду до походження коштів), децентралізованих платформ та обмінників, а також інших видів продуктів та послуг, що дозволяють знижувати прозорість та посилювати прихованість фінансових потоків, а також розширювати інші бізнес-моделі віртуальних активів чи діяльність, таку як первинне розміщення

монет (ICO), що представляє ризики ВК/ФТ, включно з шахрайством та ризиком маніпулювання ринком. Більш того, продовжують з'являтись нові типології незаконного фінансування, в тому числі використання схем нашарування, які додатково заплутають операції у порівняно легкий, дешевий та безпечний спосіб.

5. Враховуючи розвиток додаткових продуктів та послуг, а також появу нових типів постачальників у цій сфері, FATF визнає необхідність подальшого уточнення застосування Стандартів до нових технологій та постачальників. Зокрема у жовтні 2018 року FATF впровадило два нових визначення – «віртуальний актив» (ВА) та «постачальник послуг з віртуальних активів» (VASP) – та оновила Рекомендацію 15 (див. Додаток А). Метою цих змін було подальше уточнення щодо застосування Стандартів FATF до діяльності із ВА та VASP для того, аби забезпечити міжнародний рівень регуляторного поля для VASP та допомогти юрисдикціям пом'якшити ризики ВК/ФТ, що пов'язані із діяльністю з ВА та захистити цілісність світової фінансової системи. FATF також пояснила, що Стандарти застосовуються як до операцій між різними видами віртуальних активів, так і до операцій між віртуальними активами та фіатними коштами.

6. У червні 2019 року FATF прийняла Пояснювальну Записку до Рекомендації 15 (ПЗР. 15) для більшого уточнення того, яким чином вимоги FATF мають застосовуватись по відношенню до ВА та VASP, зокрема у зв'язку із застосуванням ризик-орієнтованого підходу до діяльності чи операцій із ВА або до VASP; нагляду чи моніторингу за VASP в цілях ПВК/ФТ; ліцензування чи реєстрації; превентивних заходів, таких як належна перевірка клієнта, ведення обліку та звітування про підозрілі операції; санкцій та інших правозастосовних методів; та міжнародної співпраці (див. Додаток А).

7. FATF прийняло це Керівництво на своєму Пленарному Засіданні у червні 2019 року.

Мета Керівництва

8. Це оновлене Керівництво розширює Керівництво щодо ВВ 2015 року та роз'яснює застосування ризик-орієнтованого підходу до заходів ПВК/ФТ для ВА; вказує на підприємства, які проводять діяльність чи операції пов'язані з ВА – *тобто* VASP; та більш чітко пояснює застосування Рекомендацій FATF по відношенню до ВА та VASP. Керівництво має допомогти національним органам влади у розумінні та розробці нормативно-правових заходів для охоплення діяльності із ВА та VASP, в

тому числі вносячи зміни у чинне законодавство для того, аби відповісти на ризики ВК/ФТ, що пов'язані із ВА та VASP.

9. Керівництво також має допомогти підприємствам із приватного сектору, які мають намір долучитися до діяльності чи операцій із ВА, краще розуміти свої зобов'язання з ПВК/ФТ і те, яким чином вони можуть ефективно дотримуватись вимог FATF. Воно надає керівні настанови країнам, компетентним органам влади, а також галузі в цілому з розробки та імплементації ризик-орієнтованої нормативної та наглядової структури з ПВК/ФТ для діяльності із ВА та VASP, включаючи застосування превентивних заходів, таких як належна перевірка клієнта, ведення обліку та звітування про підозрілі операції.

10. Керівництво включає терміни, запроваджені FATF у жовтні 2018 року та для ознайомлення з ними йде посилання на визначення Словника FATF «віртуальний актив» та «постачальники послуг з віртуальних активів» (Додаток А).

11. Керівництво намагається пояснити, яким чином Рекомендації FATF мають застосовуватись до діяльності із ВА та до VASP; надає найбільш відповідні чи корисні приклади; та виявляє перешкоди до запровадження пом'якшувальних заходів разом із потенційними рішеннями. Воно має слугувати додатком до Рекомендації 15 щодо Нових Технологій (Р.15) та Пояснювальної Записки до неї, який описує повний перелік зобов'язань, що застосовуються до VASP та до ВА у відповідності до Рекомендацій FATF, в тому числі Рекомендацій, що стосуються «майна», «доходів», «коштів», «грошей та інших активів» та іншої «еквівалентної вартості». Таким чином, Керівництво сприяє ефективній імплементації національних заходів з ПВК/ФТ для регулювання та нагляду за VASP (та іншими підзвітними суб'єктами) та за діяльністю із ВА до якої вони залучені, а також розвитку загального розуміння того, що саме ризик-орієнтований підхід до ПВК/ФТ несе за собою.

12. Хоча FATF відзначає, що деякі уряди розглядають цілий ряд регуляторних відповідей на діяльність із ВА та регулювання VASP, багато юрисдикцій все ще не мають ефективної діючої системи з ПВК/ФТ для пом'якшення ризиків ВК/ФТ, що пов'язані із діяльністю з ВА, не дивлячись на те, що діяльність із ВА розвивається по всьому світу та VASP проводять все більше операцій. Швидкий розвиток, зростаюча функціональність, все більше визнання та глобальна, транскордонна природа ВА робить негайні дії з пом'якшення ризиків ВК/ФТ, що представляє діяльність із ВА, ключовим пріоритетом FATF. Хоча це Керівництво й повинне допомогти в імплементації ризик-орієнтованого підходу до діяльності із ВА та до VASP в цілях ПВК/ФТ, FATF визнає,

що інші типи міркувань щодо політики можуть мати місце й впливати на нормативне регулювання сектору VASP в окремих юрисдикціях.

Сфера дії Керівництва

13. Рекомендації FATF вимагають від усіх юрисдикцій встановлювати спеціальні вимоги з ПВК/ФТ до фінансових установ (ФУ) та визначених нефінансових установ та професій (ВНУП), що базуються на конкретному виді діяльності, а також забезпечувати їх відповідність цим зобов'язанням. FATF погодило, що всі терміни, пов'язані із коштами чи вартістю, у Рекомендаціях FATF (*напр.,* «майно», «доходи», «кошти», «гроші та інші активи», а також інша «еквівалентна вартість») включають ВА, а також те, що країни мають застосовувати усі відповідні заходи згідно з Рекомендаціями FATF до ВА, діяльності із ВА та до VASP. Основна увага Керівництва приділяється описанню того, як Рекомендації застосовуються до ВА, діяльності з ВА та до VASP, для того аби допомогти країнам краще розуміти те, яким чином їм варто ефективно імплементувати Стандарти FATF.

14. Також Керівництво зосереджується на ВА, які можна конвертувати в інший вид коштів чи цінностей, в їх числі на ВА, які можна конвертувати в інші ВА, ВА, які можна конвертувати у фіатну валюту чи які перетинаються із фіатною фінансовою системою, враховуючи визначення ВА та VASP. Воно не вирішує інші нормативні питання, які можуть бути потенційно пов'язані із ВА чи VASP (*напр.,* захист прав споживачів, пруденційна безпека та надійність, оподаткування, боротьба з шахрайством чи антиринковими маніпуляціями, стандарти безпеки мережі ІТ, питання фінансової стабільності).

15. Керівництво відмічає, що ефективний ризик-орієнтовний підхід відображатиме природу, різноманітність та «зрілість» сектору VASP у країні, профілю ризику сектору, профілю ризику окремих VASP, що діють у секторі, а також правового та регуляторного підходів у країні, враховуючи транскордонну он-лайн природу та світову доступність до більшості видів діяльності із ВА. Керівництво визначає різні елементи, які країни та VASP мають розглянути при розробці та імплементації ризик-орієнтованого підходу. При розгляді загальних принципів, окреслених у Керівництві, національні органи влади повинні взяти до уваги національний контекст, в тому числі наглядовий підхід та законодавчу базу, а також ризики, що представлені в їх юрисдикції, знову ж таки у світлі потенційного доступу до діяльності із ВА з усього світу.

16. Керівництвом враховується, що як незаконні гравці на ринку можуть використовувати будь-яку установу, що залучена до фінансової діяльності, так само вони можуть використовувати VASP, залученого до діяльності з ВА, для ВК, ФТ, ухилення від санкцій, шахрайства та інших підступних діянь. Керівництво щодо ВВ 2015 року, документи FATF щодо Ризику, Трендів та Методів 2018 року та звіти й заяви FATF, що пов'язані із ризиками ВК/ФТ від діяльності із ВА та VASP,[2] висвітлюють та надають більше контексту щодо ризиків ВК/ФТ, які пов'язані із діяльністю з ВА. Хоча ВА може надавати іншу форму вартості для здійснення ВК та ФТ, а діяльність із ВА може слугувати ще одним механізмом для незаконних переказів коштів, країни не повинні в обов'язковому порядку надавати VASP чи діяльності з ВА притаманно високий ризик ВК/ФТ. Натомість, транскордонна природа, підвищена анонімність та відсутність безпосередніх (face-to-face) ділових відносин при діяльності із ВА мають ставати об'єктом проведення країною оцінки ризиків. Наповненість та якість регуляторної та наглядової системи країни, а також імплементація усіма VASP ризик-орієнтованого контролю та пом'якшувальних заходів впливають на загальний ризик та загрози, пов'язані із діяльністю з ВА. Керівництво також вказує, що не дивлячись на ці заходи, все одно може бути певний залишковий ризик, який компетентні органи та VASP мають брати до уваги при розробці відповідних рішень.

17. Керівництво визнає, що «нові» або інноваційні технології чи механізми із залучення до фінансової діяльності чи її сприянню, не завжди автоматично мають кращі підходи і тому юрисдикції мають також оцінювати та належним чином пом'якшувати ризики, що постають від подібних нових методів здійснення традиційної чи вже регульованої фінансової діяльності, таких як використання ВА в контексті платіжних послуг чи діяльності із цінними паперами.

18. Інші зацікавлені сторони, в тому числі ФУ та інші підзвітні суб'єкти, що надають банківські послуги для VASP чи для клієнтів, що залучені до діяльності із ВА або самі є VASP, мають також враховувати вищезгадані фактори. ФУ має застосовувати ризик-орієнтований підхід при вирішенні питання встановлення чи продовження ділових відносин із VASP чи клієнтом залученим до діяльності із ВА, оцінювати ризики ВК/ФТ таких ділових відносин та надавати оцінку тому, чи ці ризики можуть бути пом'якшені належним чином (див. Розділ IV). Важливо, щоб ФУ застосовували ризик-орієнтований підхід належним чином та не

[2] Для прикладу див: Звіт FATF до Міністрів Фінансів та Керівників Центральних Банків G-20 від липня 2018 року; Публічна заява FATF щодо пом'якшення ризиків від віртуальних активів від лютого 2019 року; та Звіт FATF до Міністрів Фінансів та Керівників Центральних Банків G-20 від квітня 2019 року.

вдавались до загального відтермінування чи надання винятків для відносин із клієнтами у секторі VASP без відповідної оцінки ризиків.

19. При вивченні Керівництва, країни, VASP та інші підзвітні суб'єкти, які залучені до чи надають послуги з діяльності із ВА, повинні пригадувати ключові принципи, які лежать в основі розробки та застосування Рекомендацій FATF і які є актуальними у контексті ВА:

    a) *Функціональна еквівалентність та підхід заснований на цілях*. Вимоги FATF, в тому числі те, як вони викладені у контексті ВА, сумісні з різними правовими та адміністративними системами. Вони широко пояснюють те, що має бути зроблено, але не у надмірно деталізований спосіб, для здійснення імплементації. Будь-які уточнення до вимог не повинні вимагати від юрисдикцій, які вже мають впроваджені адекватні заходи, що дозволяють досягати цілей Рекомендацій FATF, змінювати зміст своїх законів та нормативно-правових актів. Керівництво намагається підтримувати імплементацію відповідних Рекомендацій FATF, а не накладати жорсткий припис, один для всіх регуляторних режимів у всіх юрисдикціях.

    b) *Технологічний нейтралітет та напрацювання на майбутнє*. Вимоги застосовуються до ВА, як до вартості чи коштів, та до VASP, в незалежності від технологічної платформи, що використовується. Так само не має наміру вимагати надання пріоритету якимось специфічним продуктам, послугам чи рішенням, які пропонуються комерційними постачальниками, в тому числі рішення з технологічної реалізації, які націлені допомагати постачальникам дотримуватись своїх зобов'язань у сфері ПВК/ФТ. До певної міри вимоги мають достатню гнучкість, яку країни та відповідні установи можуть використовувати до існуючих технологій, а також до тих технологій що розвиваються, не вдаючись до додаткових змін.

    c) *Рівні умови*. Країни та їх компетентні органи повинні відноситись до всіх VASP на рівних умовах з регуляторної та наглядової точок зору для того аби уникнути юрисдикційного арбітражу. Як і з ФУ та ВНУП, країни повинні зробити VASP об'єктом вимог з ПВК/ФТ, які функціонально будуть еквівалентні для інших установ, коли вони пропонуватимуть схожі продукти та послуги, та

базуватимуться на тому виді діяльності до якого залучена установа.

20. Керівництво не є обов'язковим до виконання та не превалює над компетенцією національних органів влади, в тому числі над їх оцінкою та класифікацією VASP, ВА та діяльності із ВА, у відповідності до національних чи регіональних обставин, превалюючого ризику ВК/ФТ та інших контекстуальних факторів. Воно спирається на досвід країн та приватного сектору, і створено для допомоги компетентним органам влади, VASP й відповідним ФУ (*напр.,* банкам залученим до діяльності із ВА) в ефективній імплементації Рекомендацій FATF із використанням ризик-орієнтованого підходу.

Структура

21. Це Керівництво побудовано наступним чином: Розділ II вивчає, яким чином діяльність із ВА та VASP підпадають під сферу дії Рекомендацій FATF; Розділ III описує застосування Рекомендацій FATF для країн та компетентних органів влади; Розділ IV пояснює застосування Рекомендацій FATF для VASP та інших підзвітних суб'єктів, які залучені до чи забезпечують діяльність, що охоплює ВА, в тому числі для ФУ, таких як банки та брокери з цінних паперів; Розділ V наводить приклади підходів юрисдикцій до регулювання, здійснення нагляду та правозастосування по відношенню до діяльності із ВА та VASP (та інших підзвітних суб'єктів) у сфері ПВК/ФТ.

22. Додатки A,B та C включають відповідні ресурси, які підживлювали це Керівництво, в тому числі документ *FATF щодо Віртуальних Валют: Ключові Визначення та Потенційні Ризики ВК/ФТ* від червня 2014 року, Керівництво щодо ВВ від червня 2015 року, оновлений текст Рекомендації 15 та Пояснювальної Записки до неї, а також визначення «віртуальний актив» та «постачальник послуг з віртуальних активів» зі словника FATF.

РОЗДІЛ II – СФЕРА ДІЇ СТАНДАРТІВ FATF

23. У Розділі II обговорюється застосування ризик-орієнтованого підходу до діяльності із ВА та до VASP, і пояснюється в який спосіб ця діяльність та постачальники мають ставати об'єктами вимог з ПВК/ФТ у відповідності до міжнародних стандартів. Як описано у параграфі 2 ПЗР. 15, згідно із Рекомендаціями FATF VASP є об'єктом відповідних заходів, що базуються на виді діяльності, до якої вони залучені. Аналогічно, ВА охоплюється відповідними заходами згідно з Рекомендаціями FATF, які відносяться до коштів та вартості у широкому розумінні, чи які окремо посилаються на умови щодо коштів чи іншого вираження вартості.

24. Необхідно підкреслити, що коли VASP залучено тільки до традиційної діяльності з фіатними коштами (що знаходиться поза межами визначення діяльності з переказу між різними видами віртуальних активів чи між віртуальними та фіатними), вони, безумовно, є об'єктом заходів аналогічних до тих, що застосовуються до інших традиційних установ або підприємств у відповідності до стандартів FATF.

Первісна Оцінка Ризику

25. Рекомендації FATF не визначають наперед будь-який сектор як високоризикований. Стандартами визначаються сектори, які можуть бути вразливі до ВК та ФТ; разом з тим, загальний ризик має бути визначено через оцінку сектору – в даному випадку, сектору VASP – на національному рівні. Різні установи в середині сектору можуть становити вищий чи нижчий ризик в залежності від різних факторів, в тому числі продуктів, послуг, клієнтів, географічного розташування та того, наскільки сильною є програма комплаєнсу в установі. Рекомендацією 1 визначається сфера застосування ризик-орієнтованого підходу таким чином: хто має бути об'єктом режиму країни; як за цими об'єктами режиму ПВК/ФТ має здійснюватися нагляд та моніторинг відповідності режиму; як від цих об'єктів режиму ПВК/ФТ має вимагатись відповідність; розгляд участі у взаємовідносинах з клієнтами з боку VASP та інших підзвітних суб'єктів, що залучені до діяльності з ВА. Більш того, FATF не підтримує повне припинення чи обмеження ділових відносин з конкретним сектором (*напр.,* відносини ФУ з VASP) для уникнення, а не управління ризиком у відповідності з ризик-орієнтованим підходом FATF.

26. FATF оцінила ризики ВК/ФТ, що існують у зв'язку із ВА, фінансовою діяльністю чи операціями з ВА, а також із VASP. Таким чином, у відповідності до ризик-орієнтованого підходу та згідно з параграфом 2 ПЗР. 15, країни повинні виявляти, оцінювати та розуміти ризики ВК/ФТ, що виникають у цій сфері, та зосереджувати свої потуги з ПВК/ФТ на потенційно високоризикованих ВА, видах діяльності з ВА та VASP. Аналогічним чином, країни мають вимагати від VASP (так само як і від інших підзвітних суб'єктів, які залучені до фінансової діяльності чи операцій із ВА, або надають продукти та послуги, що пов'язані із ВА) виявляти, оцінювати та вживати ефективних заходів для пом'якшення своїх ризиків ВК/ФТ.

27. Оцінка ризику VASP має брати до уваги усі фактори ризику, які вважаються VASP та його компетентними органами влади відповідними, поміж іншими факторами, включно із видом послуги, продукту чи операції, що розглядається; ризиком клієнта; географічними факторами; а також видами обміну ВА.

28. Як і багато інших методів фінансових платежів, ВА може дозволити ведення ділових відносин на відстані (non-F2F). Більш того, ВА може бути використано для швидкого переміщення коштів по всьому світу та для полегшення певного переліку фінансових видів діяльності – від послуг з переказу коштів до діяльності пов'язаної із цінними паперами, біржовими товарами чи деривативами. Таким чином, відсутність безпосереднього контакту при здійсненні фінансової діяльності чи операцій із ВА, може бути індикатором високого ризику ВК/ФТ. Аналогічно, продукти та послуги ВА, що сприяють анонімним операціям чи операціям, що проводяться під псевдонімом, також становлять високий ризик ВК/ФТ, особливо якщо вони заважають можливості VASP встановлювати бенефіціара. Останнє викликає особливе занепокоєння у контексті ВА, чия природа є транскордонною. Якщо заходи із ідентифікації та верифікації клієнта неналежним чином вирішують ризик, пов'язаний із non-F2F чи прихованими операціями, ризик ВК/ФТ збільшується, як і складність у відслідковуванні коштів та виявленні сторін операції.

29. Ще одним важливим фактором, який країни мають враховувати при визначенні рівня ризику є міра в якій користувачі можуть використовувати ВА чи VASP у світовому масштабі для проведення платежів чи переказу коштів. Користувачі, що використовують ВА для незаконних цілей, можуть отримувати перевагу від світового охоплення та швидкості операцій, які надають ВА, а також від неналежного регулювання чи нагляду за фінансовими операціями з ВА та за постачальниками, що створює мінливе правове та регуляторне поле в екосистемі ВА. Як це відбувається і з іншими мобільними, чи тими що

відбуваються в інтернеті, платіжними послугами та механізмами, які можуть бути використані для переказу коштів по всьому світу або у широкій географічній зоні з великою кількістю залучених сторін, ВА можуть бути більш привабливими для використання злочинцями в цілях ВК/ФТ, а не для суто національних бізнес-моделей.

30. На додаток, VASP, що розташовується в одній юрисдикції, може пропонувати свої продукти та послуги для клієнтів, що знаходяться в іншій юрисдикції, де вони можуть бути об'єктом інших зобов'язань та нагляду з ПВК/ФТ. Це необхідно брати до уваги, коли VASP знаходиться у юрисдикції зі слабким або навіть неіснуючим контролем з ПВК/ФТ. Аналогічно, широкий спектр постачальників у сфері ВА та їх присутність у декількох, якщо не в усіх, юрисдикціях може збільшити ризик ВК/ФТ, пов'язаний із ВА через потенційні пробіли в інформації про клієнта та операцію. Це викликає особливу занепокоєність у контексті транскордонних операцій та тоді, коли існує брак ясності того, які саме підприємства чи особи (фізичні або юридичні), що залучені до операції, є об'єктами заходів з ПВК/ФТ та які країни відповідальні за регулювання (в тому числі ліцензування та/або реєстрація) та нагляд чи моніторинг за цими підприємствами щодо відповідності їх вимогам з ПВК/ФТ.

31. На додаток для доповнення попередніх робіт FATF щодо цього предмету,[3] країни та VASP повинні розглянути наступні елементи, наприклад, при ідентифікації, оцінці та визначенні того, яким чином найкраще пом'якшувати ризики пов'язані із діяльністю ВА та наданням VASP продуктів чи послуг:

    a) Потенційно високий ризик, пов'язаний як із ВА, що переміщує вартість з та до фіатної валюти, так і з традиційною фінансовою системою та операціями поміж різними видами віртуальних активів.

    b) Ризик пов'язаний із централізованими та децентралізованими бізнес-моделями VASP;

    c) Особливі види ВА, які пропонують чи планують пропонувати VASP та будь-які унікальні особливості кожного ВА, такі як AEC, вбудовані міксери та тумблери чи інші продукти та послуги, що можуть представляти підвищений ризик потенційно заплутуючи операції чи підриваючи спроможність VASP дізнатись свого клієнта та

3 Наприклад, Керівництво щодо ВВ 2015 року, документи групи FATF щодо Ризиків, Трендів та Методів щодо цієї тематики, а також заяви та звіти FATF щодо ризиків ВК/ФТ пов'язаних із ВА, діяльністю ВА та/або VASP.

запровадити ефективну належну перевірку клієнта (CDD) та інші заходи з ПВК/ФТ;

d) Особливі бізнес-моделі VASP та те, чи така бізнес-модель представляє чи загострює якісь специфічні ризики;

e) Чи проводить VASP свою діяльність виключно он-лайн (*напр.,* платформа для он-лайн обміну) чи особисто (*напр.,* торгові майданчики, які сприяють безпосередньому взаємному обміну або обміну у кіосках);

f) Вразливість до анонімайзерів, таких як TOR чи I2P, які можуть ще сильніше заплутати операцію чи діяльність та завадити VASP дізнатись своїх клієнтів і запровадити ефективні заходи з ПВК/ФТ;

g) Потенційні ризики ВК/ФТ, що пов'язані зі зв'язками VASP із декількома юрисдикціями;

h) Природа та сфера дії рахунку, продукту чи послуги (*напр.,* рахунки для збереження та розміщення маленьких сум, які дають змогу клієнтам, які не мають доступу до фінансових послуг, розміщувати обмежену суму);

i) Природу та сферу дії платіжних каналів та систем (*напр.,* відкриті та закриті системи або системи, які сприяють мікроплатежам чи платежу від держави до особи / від особи до держави); а також

j) Будь-які чинні параметри чи заходи, які потенційно знижують схильність провайдера (VASP чи іншої підзвітної установи, що залучена до діяльності із ВА чи надає продукти та послуги, пов'язані із ВА) до ризику (*напр.,* обмеження щодо суми операцій чи балансу рахунку).

32. Деякі країни можуть вирішити заборонити діяльність із ВА чи VASP, базуючись на своїй оцінці ризиків та національному нормативному контексті або для того аби підтримати інші цілі політики, які не вказані у цьому Керівництві (*напр.,* захист прав споживачів, безпека та надійність, монетарна політика). В таких випадках, деякі з особливих вимог Р.15 не будуть застосовуватись, але юрисдикції все одно повинні оцінювати ризик, пов'язаний із діяльністю з ВА чи постачальниками, та мати інструменти і повноваження для здійснення відповідних дій за недотримання заборони (див. підрозділ 3.1.1.).

Визначення FATF та Особливості Сектору VASP, що Стосуються ПВК/ФТ

33. Рекомендації FATF вимагають від усіх юрисдикцій запроваджувати певні вимоги з ПВК/ФТ для ФУ та ВНУП, а також впевнюватись у дотриманні ними цих зобов'язань. У Словнику FATF визначено:

a) «Фінансову установу» як фізичну або юридичну особу, яка здійснює в якості ділової активності один або декілька видів діяльності чи операцій на користь чи від імені клієнта;

b) «Віртуальний актив» як цифрове представлення вартості, яким можна торгувати в цифровому форматі або переказувати, і яке може використовуватись для платіжних або інвестиційних цілей. Віртуальні активи не включають в себе цифрове представлення фіатних валют, цінних паперів та інших фінансових активів, які вже охоплені в інших Рекомендаціях FATF.

c) «Постачальника послуг з віртуальних активів» як будь-яку фізичну чи юридичну особу, яка не охоплена в інших місцях відповідно до рекомендацій, і як суб'єкт господарювання провадить один або декілька наступних видів діяльності або операцій для або від імені іншої фізичної або юридичної особи:

i. Обмін між віртуальними активами та фіатними валютами;

ii. Обмін між однією або декількома формами віртуальних активів;

iii. Переказ[4] віртуальних активів:

iv. Зберігання та/або управління віртуальними активами або інструментами, що забезпечують контроль над віртуальними активами; та

v. Участь і надання фінансових послуг, що пов'язані із пропозицією емітента та/або продажом віртуального активу.

[4] У контексті віртуальних валют, під переказом мається на увазі проведення операції від імені іншої фізичної чи юридичної особи, яка переміщує віртуальний актив з однієї адреси чи рахунку на інший.

34. Зокрема, визначення FATF включає як операції чи фінансову діяльність між різними видами віртуальних активів, так і операції між віртуальними та фіатними активами.

35. В залежності від конкретної фінансової діяльності, до VASP входять ті, хто надають послуги з обміну та переказу; деякі постачальники послуг гаманця для ВА, як ті що ведуть гаманці чи підтримують зберігання або контроль над ВА, гаманцем та/або приватними ключами іншої юридичної чи фізичної особи; постачальники фінансових послуг, пов'язаних із емісією, пропозицією чи продажом ВА (таких як ICO); та інші можливі бізнес-моделі.

36. При визначенні того, чи підпадає певний вид діяльності або підприємство під визначення, а отже чи є об'єктом регулювання, країни мають брати до уваги широкий перелік різних послуг чи бізнес-моделей із ВА, які існують в цій екосистемі, а також досліджувати їх функціональні можливості чи види фінансової діяльності, яким вони сприяють у контексті діяльності із ВА (*тобто*, пункти (i) – (v) з визначення VASP, що описані вище). Більш того, країни повинні розглядати чи залучено до діяльності фізичну або юридичну особу, яка проводить в якості ділової активності п'ять описаних видів функціональної діяльності для чи від імені іншої фізичної / юридичної особи, обидва з яких є суттєвими елементами визначення, а останній передбачає наявність певного рівня «зберігання» чи «контролю» віртуального активу, або «спроможності активно сприяти фінансовій діяльності» на користь фізичної чи юридичної особи, яка проводить ділову діяльність для клієнта.

37. Наприклад, обмін між віртуальними активами та фіатними валютами (пункт (i)), обмін між різними видами віртуальних активів (пункт (ii)) та переказ віртуальних активів (пункт (iii)), в тому числі з одного гаманця на інший, якими володіє одна й та сама особа, потенційно відноситься до різних видів діяльності з обміну та переказу ВА. Обмінні біржі чи обмінники можуть існувати у різних формах та бізнес-моделях та надавати послуги третім сторонам, які дозволять їх клієнтам купляти та продавати ВА в обмін на традиційні фіатні, валюти, інші ВА чи інші активи або товари.[5] Бізнес-моделі з обміну та/або переказу можуть включати «традиційні» обмінні біржі ВА чи послуги з переказу ВА, які активно сприяють обміну ВА на реальну валюту чи інші форми ВА та/або на дорогоцінні метали за певну винагороду (*напр.,* за окрему плату,

[5] У багатьох юрисдикціях термін «обмін» є досить широким і може відноситись як до обмінних бірж з переказу грошових коштів , так і до будь-якої організації, асоціації чи групи осіб, в незалежності від того чи зареєстровані вони, які утворюють, підтримують чи забезпечують ринок або обладнання для залучення покупців та продавців або для виконання інших (*напр.,* по відношенню до цінних паперів) функцій, які зазвичай виконують фондові біржі, як це розуміється визначення загалом, а також включає ринок та утримання ринкового обладнання біржою.

комісійні, через спред чи іншу вигоду). Ці моделі, зазвичай, приймають широкий перелік платіжних методів, в тому числі готівку, електронні перекази, кредитні картки та ВА. Традиційні послуги з обміну чи переказу ВА можуть бути пов'язані або не пов'язані з адміністратором і надаватись третіми сторонами. Постачальники «кіосків» - які часто називаються «АТМ», «біткоїн-банкомати», «біткоїн АТМ» або «торгові автомати» - можуть також підпадати під зазначені вище визначення, оскільки вони надають або активно сприяють діяльності із ВА через фізичні електронні термінали (кіоски), які дозволяють власнику/оператору активно сприяти обміну ВА на фіатні валюти чи інші види ВА.

38. Інші послуги чи бізнес-моделі можуть також створювати діяльність з обміну чи переказу, базуючись на пунктах (i) – (iii) визначення, а тому фізичні чи юридичні особи, що стоять за такою діяльністю, будуть вважатись VASP, якщо вони будуть проводити чи сприяти діловій діяльності від імені інших осіб. Це може включати: послуги з депонування ВА, в тому числі послуги до яких залучено технології розумного договору, який покупці ВА використовують для відправки чи переказу фіатної валюти в обмін на ВА, коли підприємство, що надає послуги, має право зберігання коштів; брокерські послуги, що сприяють емісії та торгівлі ВА від імені клієнтів фізичних чи юридичних осіб; послуги з обміну портфелю замовлень, в яких збираються замовлення для покупців та продавців,[6] надаючи їм можливість знаходити контрагентів, виявляти ціни та торгувати, потенційно через використання відповідного механізму, який відповідає на замовлення користувачів з купівлі та продажу;[7] а також передові торговельні послуги, які дозволяють користувачам придбавати портфоліо ВА та мати доступ до більш складних методів торгівлі, таких як маржинальна торгівля або алгоритмічна торгівля.

---

6 Країни повинні оцінювати сукупність заходів та технологій, що були використані для збору замовлень від декількох покупців та продавців на цінні папери із використанням встановлених недискреційних методів у відповідності до яких такі замовлення взаємодіють.. Система збирає до купи замовлення покупців та продавців якщо, наприклад, вона відображає для користувачів торговельний інтерес, введений у систему, або якщо система централізовано отримує замовлення користувачів для подальшої обробки та виконання.

7 Приклад наведеної тут послуги з обміну портфелю замовлень є звичайною «книгою замовлень», яка зазвичай виступає у вигляді інтерфейсу веб-сайту, який збирає та відображає замовлення для покупців та продавців, та дозволяє користувачам знаходити контрагентів, дізнаватись ціни та торгувати через відповідний механізм. EtherDelta (справа Комісії з Цінних Паперів і Бірж США, листопад 2018) є прикладом он-лайн платформи, яка дозволяє покупцям та продавцям торгувати Ефіром та токенами ERC20 на вторинному ринку із залученням послуги з обміну портфелю замовлень, яка надавала користувачам інтерфейс із книгою замовлень, щоб відповідати торговим операціям і відправляти їх на запис до розподіленого реєстру. (На противагу, однорангова платформа обмінну більш схожа на дошку оголошень, де один продавець та один покупець можуть знайти один одного, а потім перейти в інше місце для здійснення торгівлі між собою.)

39. Однорангові торговельні платформи є веб-сайтами, які дозволяють покупцям та продавцям ВА знаходити один одного. Деякі торговельні платформи сприяють угодам в якості посередників. В залежності від законодавства юрисдикції, якщо торговельна платформа тільки надає місце, де покупці та продавці ВА можуть виставляти свої пропозиції та ціни (із наявністю або відсутністю автоматичної взаємодії замовлень), а самі сторони здійснюють угоди вже поза межами платформи (або через використання індивідуальних гаманців або інших гаманців, які не відносяться до цієї торговельної платформи), тоді платформа не являє собою VASP як його визначено вище. Проте, коли платформа сприяє здійсненню обміну, переказу чи іншій фінансовій діяльності із залученням ВА (як це описано у пунктах (i) – (v)), в тому числі придбання ВА, коли транзакції, ставки та пропозиції узгоджуються на торговельній платформі, тоді платформа є VASP, що проводить діяльність з обміну та/або переказу від імені своїх клієнтів.

40. Послуги з обміну та переказу можуть також виникати на децентралізованих обмінних пунктах чи платформах. «Децентралізований (розподілений) додаток (DApp)» - термін, який відноситься до програм, які діють в одноранговій мережі комп'ютерів, що працюють із блокчейн платформами – тип розподіленого публічного реєстру, який дозволяє розробляти вторинні блокчейни – які розроблені таким чином, що вони не контролюються жодною особою і таким чином не мають адміністратора, якого можна ідентифікувати. Власник/оператор DApp може використовувати його для здійснення різних функцій, в тому числі для діяльності як неінкорпорована організація, така як агентство з програмного забезпечення, для надання доступу до діяльності із віртуальним активом.[8] Загалом, користувач DApp повинен сплачувати внесок до DApp, який зазвичай сплачується у ВА, на користь власника/оператора для того аби запустити програмне забезпечення. Коли DApp сприяє чи проводить обмін або переказ вартості (чи то у ВА, чи у традиційній фіатній валюті), то DApp, його власник/оператор(и), або обидва можуть підпасти під визначення VASP. Так само, особа яка розробила децентралізовану платіжну систему може бути VASP, коли залучається до проведення ділової активності зі сприяння чи проведення видів діяльності, що описані раніше, від імені іншої фізичної чи юридичної особи.

41. В контексті визначення VASP у пункті (iv), *зберігання та/або управління віртуальними активами або інструментами, що дозволяють здійснювати контроль над віртуальними активами*, країни повинні

8 Для прикладу DApp, див. Реліз № 81207 / 25 липня, 2017 Комісії з цінних паперів і бірж США (SEC), «Звіт щодо розслідування у відповідності до Розділу 21(a) Закону про Торгівлю Цінними паперами від 1934 року», доступний за посиланням: https://www.sec.gov/litigation/investreport/34-81207.pdf

враховувати послуги чи бізнес моделі, які комбінують функції збереження вартості ВА клієнта із повноваженнями управляти або переказувати ВА незалежно від власника, із припущенням, що таке управління чи переказ будуть здійснюватися лише відповідно до інструкцій власника/клієнта. Послуги зі збереження та адміністрування включають осіб, які мають ексклюзивний чи незалежний контроль над приватним ключем, який пов'язаний із ВА, що належать іншій особі, чи ексклюзивний та незалежний контроль над розумними договорами, в яких вони не виступають учасником, який включає ВА, що належать іншій особі.

42. Фізичні чи юридичні особи, які активно сприяють пропозиції чи випуску та торгівлі ВА, в тому числі акцептуючи замовлення та кошти на купівлю, а також купляючи ВА від інших емітентів для подальшого перепродажу та розподілення коштів чи активів, також можуть підпадати під сферу дії пунктів (i), (ii) та (iii), а також пункту (v), участь у постачанні фінансових послуг, пов'язаних із пропозицією та/або продажом віртуального активу емітентом.[9] Наприклад, ICO зазвичай виступає засобом збору коштів для нового проекту від перших спонсорів, а фізичні чи юридичні особи, які активно сприяють емісії, можуть надавати послуги, які включають діяльність з обміну чи переказу, а також діяльність з випуску пропозицій та/або продажу.

43. Зобов'язання з ПВК/ФТ, що застосовуються юрисдикціями і регулюють постачальників послуг, які беруть участь у або надають фінансові послуги, пов'язані із пропозицією емітента та/або продажом, можуть включати як нормативну базу юрисдикції з переказу коштів, так і регулювання діяльності з управління цінними паперами, біржовими товарами чи деривативами.

44. VASP може підпасти під одну з п'яти категорій (або більше) діяльності чи операцій, що описані у визначенні VASP (тобто, «обмін» віртуальний/фіатний актив, «обмін» віртуальний/віртуальний, «переказ», «зберігання та/або адміністрування», та «участь й надання фінансових послуг, пов'язаних з пропозицією та/або продажом від емітента»).

45. Наприклад, кількість он-лайн платформ, що надають механізм для торгівлі активами, в тому числі ВА, що пропонуються та продаються при первинному розміщенні, можуть відповідати визначенню підприємства, що пов'язано із цінними паперами та/або обмінного пункту, працюючи із

[9] Діяльність (v) націлена на охоплення таких самих видів діяльності, що проводяться у контексті ВА, як ті, що описані у Діяльності 8 визначення Фінансових Установ зі Словника FATF *«Участь в емісії цінних паперів та наданні фінансових послуг, що пов'язані із такою емісією»*.

ВА, які є «цінними паперами» у багатьох законодавчих системах різних юрисдикцій. Інші юрисдикції можуть мати інший підхід, який може включати платіжні токени. Тому компетентні органи влади у юрисдикціях повинні прагнути застосовувати функціональний підхід, який враховує відповідні факти та умови платформи, активів та діяльності, при визначенні чи задовольняє підприємство визначенню «обмінного пункту» чи іншого підзвітного суб'єкту (як підприємства, пов'язаного із цінними паперами) у відповідності до національного законодавства та чи підпадає це підприємство під конкретне визначення. При досягненні рішення, країни та компетентні органи влади мають розглянути ті види діяльності та функції, які виконує підприємство, щодо якого є питання, в незалежності від технологій, які пов'язані зі здійсненням цієї діяльності.

46. Чи є фізична або юридична особа, що залучена до діяльності із ВА, VASP залежить від того, як і в яких цілях вона використовує ВА. Як наголошувалось вище, якщо особа (фізична або юридична) займається будь-якою діяльністю, описаною у визначенні FATF (*тобто* пункти (i) – (v)), на користь або від імені іншої особи, як бізнесом, тоді вона є VASP, в незалежності від того яку технологію вона використовує для проведення діяльності із ВА. Більш того, вона є VASP також і в незалежності від того чи використовує вона централізовану або децентралізовану платформу, розумні договори або інші механізми. Разом з тим, особа, яка не займається вищезазначеною діяльністю як бізнесом на користь чи від імені іншої особи, не є VASP.

47. Те як FATF не прагне регулювати окремих користувачів (які не діють як бізнес) ВА як VASP – хоча визнає, що такі користувачі можуть підлягати зобов'язанням з комплаєнсу у відповідності до санкційної чи правозастосовної системи[10] - так само FATF не намагається охопити елементи замкнутого типу, які не можна переказати, обміняти та які не є взаємозамінними. До таких елементів можуть відноситись милі авіаліній, бонусні програми кредитних карток (наприклад, кешбек) або аналогічні програми лояльності, які особа не може продати на вторинному ринку. Визначення ВА та VASP призначені для охоплення певних видів фінансової діяльності, функцій (*тобто*, переказ, обмін, зберігання та адміністрування, емісія і т.д.) та активів, які є взаємозамінними – віртуальний актив на віртуальний чи віртуальний на фіатний.

10 У Сполучених Штатах Америки, наприклад, подібні «користувачі» повинні, як й всі громадяни США чи особи, які так чи інакше підпадають під юрисдикцію США, дотримуватись усіх санкцій та регламентів США, які накладені Управлінням по контролю за іноземними активами Міністерства фінансів США. Більш того, зобов'язання з дотримування санкцій США є однаковими, в незалежності від того чи здійснюється операція у цифровій валюті чи традиційній фіатній, або в іншій формі активу чи власності.

48. Схожим чином FATF прагне регулювати не технології, що лежать в основі ВА та діяльності VASP, а фізичних чи юридичних осіб, які стоять за такими технологіями та програмами і можуть їх використовувати для сприяння фінансовій діяльності чи проводити ділову активність з вищезгаданими видами діяльності із ВА, від імені іншої фізичної чи юридичної особи. Таким чином, особа, яка розробила чи продала програмний додаток нової платформи ВА (*тобто* розробник) може не бути VASP, якщо обмежилась тільки розробкою та продажом, але вона може стати VASP, якщо використовувала новий додаток чи платформу для проведення ділової діяльності з обміну чи переказу коштів або будь-якої іншої фінансової діяльності, описаної вище від імені іншої фізичної чи юридичної особи. Більш того, FATF не прагне регулювати фізичних або юридичних осіб VASP, які надають допоміжні послуги або продукти для мереж віртуальних активів, в тому числі виробників апаратних гаманців та гаманців, де ключ не зберігається третіми особами, до тих пір, доки вони не долучаються до чи не сприяють будь-якій з вище перелічених видів ділової активності з ВА від імені своїх клієнтів.

49. Важливо відзначити, що у ПЗР. 15 FATF не виключає окремі активи, базуючись на умовах, щодо яких може не вистачати загального розуміння поміж юрисдикціями або навіть поміж галузями, таким чином Рекомендація 15 та Пояснювальна Записка до неї частково можуть залишатись технологічно-нейтральними. Навпаки, формулювання Рекомендацій, в тому числі Рекомендації 15, активно базується та зосереджується на функціях, для того аби надати юрисдикціям достатню гнучкість.

50. Гнучкість є особливо актуальною в контексті діяльності з ВА та VASP, де залучено широкий спектр продуктів та послуг до простору який швидко розвивається. Деякі елементи – або токени – які, як видається, не є ВА, насправді можуть бути ВА, який робить можливим переказ чи обмін вартості або ж сприяє ВК/ФТ. Деякі ICO, які пов’язані або включають у себе «ігрові токени», можуть бути використані для заплутування операційних потоків між ігровими токенами та їх обміном на або переказом в ВА. Вторинні ринки для взаємозамінних товарів та послуг, що також можуть бути передані, існують як у секторі цінних паперів так і біржових товарів. Наприклад, користувачі можуть розробити та придбати певний віртуальний елемент, який діє як засіб розміщення вартості і по факту накопичують вартість і можуть бути продані за цю вартість у секторі ВА.

51. Як обговорено вище, країни повинні зосередитись на фінансовій поведінці чи діяльності, що оточує ВА або її базові технології і на тому, як це створює ризики ВК/ФТ (*напр.,* потенційне розширення анонімності,

сплутування, відсутність посередників та зменшення прозорості чи наявність технологій, платформ або ВА, які підривають спроможність VASP проводити ПВК чи CDD), а також на заходах, що вживаються.

52. Країни повинні вирішувати ризики ВК/ФТ, пов'язані із діяльністю з ВА, як тоді, коли така діяльність перетинається з регульованою фінансовою системою фіатних валют (у відповідності до національної законодавчої системи, яка пропонує різні варіанти для регулювання такої діяльності), так і тоді, коли така діяльність не пов'язана із фінансовою системою фіатних валют та складається виключно зі взаємодії між різними видами віртуальних активів.

53. Аналогічно, регулювання з ПВК/ФТ буде застосовуватись до діяльності з ВА та до VASP, в незалежності від типу ВА, який використовується при здійсненні фінансової діяльності (*напр.,* VASP, який використовує чи пропонує AEC для своїх клієнтів для різних фінансових операцій), базових технологій чи додаткових послуг, які платформа може потенційно пропонувати (такі як міксери чи тумблери або інші потенційні функції для заплутування).

54. VASP є об'єктами відповідних заходів FATF, які аналогічним чином застосовуються до інших підприємств, які є об'єктом регулювання з ПВК/ФТ у відповідності до Рекомендацій FATF, в незалежності від того, як юрисдикція може визначати таких провайдерів, базуючись на виді діяльності до якого залучено VASP. Більш того, як описано у ПЗР. 15, заходи які застосовуються до «власності», «доходів», «коштів», «грошей та активів» та іншої «еквівалентної вартості» згідно з Рекомендаціями FATF, також застосовуються й до ВА (*напр.,* Рекомендації 3-8, 30, 33, 35 та 38).

РОЗДІЛ III – ЗАСТОСУВАННЯ СТАНДАРТІВ FATF ДЛЯ КРАЇН ТА КОМПЕТЕНТНИХ ОРГАНІВ ВЛАДИ

55. Розділ III пояснює як Рекомендації FATF, що пов'язані із ВА та VASP, застосовуються до країн та компетентних органів влади та зосереджуються на виявленні та пом'якшенні ризиків, пов'язаних із діяльністю з ВА, застосуванні превентивних заходів, реалізації вимог з ліцензування чи реєстрації, імплементації ефективного нагляду нарівні з наглядом за фінансовою діяльністю ФУ, створенні ряду ефективних та переконливих санкцій, а також на сприянні національній та міжнародній співпраці. Майже усі Рекомендації FATF безпосередньо стосуються розуміння того, як країни мають використовувати державні органи та міжнародну співпрацю для протидії ризикам ВК/ФТ, пов'язаних із ВА та VASP, в той час як інші Рекомендації менш явно пов'язані із ВА та VASP, хоча залишаються актуальними та можливі до застосування.

56. ВА та VASP є об'єктами повного спектру зобов'язань у відповідності до Рекомендацій FATF, як описано у ПЗР. 15, в тому числі й тих зобов'язань, які застосовуються до інших установ, які є об'єктами регулювання у сфері ПВК/ФТ, базуючись на фінансовій діяльності, до якої залучено VASP, та беручи до уваги ризики ВК/ФТ, що пов'язані із охопленою діяльністю чи операціями із ВА.

57. У цьому розділі також розглядається застосування ризик-орієнтованого підходу з боку наглядових органів VASP.

Застосування Рекомендацій у Контексті ВА та VASP

Ризик-Орієнтований Підхід та Національна Координація

58. **Рекомендація 1.** Рекомендації FATF дають зрозуміти, що країни повинні застосовувати ризик-орієнтований підхід для забезпечення того, що заходи для запобігання чи пом'якшення ризиків ВК/ФТ є сумірними з виявленими ризиками у відповідних юрисдикціях. У відповідності до ризик-орієнтованого підходу, країни повинні посилювати вимоги для ситуацій та видів діяльності із ВА, де має місце високий рівень ризику. При оцінці ризиків ВК/ФТ, пов'язаних з ВА, конкретним видом фінансової діяльності із ВА та з діяльністю чи операціями VASP, різниця між централізованими та децентралізованими ВА, як обговорено у Керівництві щодо ВВ 2015 року, скоріш за все залишатиметься для країн ключовим аспектом до розгляду. У зв'язку із підвищеною анонімністю або заплутуванням фінансових потоків ВА та із викликами, що пов'язані

з проведенням ефективної ідентифікації та верифікації клієнта, ВА та VASP можуть розглядатись як такі, що мають підвищений ризик ВК/ФТ, що потенційно, за необхідності, може вимагати застосування заходів розширеної належної перевірки.

59. Рекомендація 1 вимагає від країн ідентифікувати, розуміти та оцінювати свої ризики ВК/ФТ та вживати дії, що будуть націлені на ефективне пом'якшення цих ризиків. Вимога застосовується по відношенню до ризиків пов'язаних із новими технологіями згідно з Рекомендацією 15, в тому числі з ВА та ризиками, пов'язаними з VASP, які беруть участь у або надають види діяльності, операції, продукти чи послуги, що пов'язані із ВА. Співпраця державного та приватного секторів може допомогти компетентним органам влади у розробці політики з ПВК/ФТ у сфері діяльності із ВА, а також для інновацій, пов'язаних із технологіями ВА та, коли це доречно, нових продуктів та послуг. Співпраця має також допомогти країнам у вірному визначенні пріоритетів та розміщенні ресурсів з ПВК/ФТ компетентними органами влади.

60. Національні органи мають проводити координовану оцінку ризиків діяльності, продуктів та послуг, пов'язаних із ВА, а також ризиків, що пов'язані із VASP та сектором у своїй країні в цілому. Оцінка ризиків повинна: (i) забезпечити розуміння усіх відповідних органів щодо специфічних функцій продуктів та послуг ВА, та їх вплив на усі відповідні регуляторні юрисдикції в цілях ПВК/ФТ (*напр.,* механізми переказу коштів та платежів, кіоски ВА, товари ВА, цінні папери ВА або діяльність з їх емісії, і т.д., як це висвітлено у визначенні VASP) та (ii) сприяти здійсненню однакових заходів з ПВК/ФТ для однакових продуктів та послуг зі схожими профілями ризику.

61. Оскільки сектор VASP розвивається, країни повинні дослідити взаємозв'язки між заходами з ПВК/ФТ для діяльності із ВА та іншими регуляторними та наглядовими заходами (*напр.,* захист прав споживачів, пруденційна безпека та надійність, оподаткування, стандарти безпеки мережі ІТ та інші), оскільки заходи, які вживаються в інших сферах, можуть вплинути на ризики ВК/ФТ. В цьому відношенні, країни повинні розглянути коротко- та довгострокову політику для розвитку всеосяжних нормативних та наглядових баз для охоплення діяльності з ВА та VASP (та інші підзвітні суб'єкти, що діють у сфері ВА), оскільки продовжується широкомасштабне поширення ВА.

62. Країни також повинні вимагати від VASP (та інших підзвітних суб'єктів) ідентифікувати, оцінювати та вживати ефективних заходів для пом'якшення ризиків ВК/ФТ, що пов'язані із наданням або залученням до діяльності із ВА чи з пропонуванням конкретного продукту або послуги ВА. Коли діяльність VASP дозволена у відповідності до національного

законодавства, то VASP так само як ФУ та ВНУП – в тому числі ФУ та ВНУП, що залучені до діяльності із ВА або надають продукти та послуги віртуальних активів – повинні оцінювати пов'язані ризики ВК/ФТ та застосовувати ризик-орієнтований підхід для забезпечення того, щоб відповідні заходи з попередження чи пом'якшення цих ризиків імплементувались в належний спосіб.

63. Юрисдикція має право заборонити діяльність з ВА чи VASP, базуючись на власній оцінці ризиків та національному регуляторному контексті, для підтримки власних політичних цілей, які не зазначені у цьому Керівництві (*напр.,* захист прав споживачів, безпека та надійність, монетарна політика). Коли країни вирішують заборонити діяльність з ВА або VASP, вони повинні враховувати ефект, який матиме ця заборона на їх ризики ВК/ФТ. В незалежності від того, чи вибере країна заборону або регулювання сектору, проведення додаткових заходів все одно можуть бути корисними у зменшенні загального рівня ризику ВК/ФТ. Наприклад, якщо країна забороняє діяльність із ВА та VASP, заходи з пом'якшення мають включати виявлення VASP (чи інших підзвітних суб'єктів, що можуть долучатись до діяльності із ВА), які незаконно діють у юрисдикції, та застосовувати пропорційні й переконливі санкції до таких підприємств. Базуючись на профілі ризику країни, заборони все ще можуть вимагати від країни проведення просвітницьких та правозастосовних дій, а також розробки стратегій з пом'якшення ризику, враховуючи транскордонний елемент в діяльності з ВА (*напр.,* транскордонні платежі чи перекази ВА) та операцій VASP.

64. **Рекомендація 2** вимагає національної співпраці та координації у сфері ПВК/ФТ, в тому числі сектору VASP, і тому непрямо застосовується до країн в контексті регулювання та нагляду за діяльністю із ВА. Країни повинні вирішити питання створення механізмів, таких як міжвідомчі робочі групи чи цільові групи, щоб дозволити регуляторам, наглядовим органам, підрозділам фінансової розвідки (ПФР) та правоохоронним органам співпрацювати один з одним та будь-яким іншим відповідним компетентним органом влади для того, аби розробити та впровадити ефективну політику, нормативно-правові акти та інші заходи, що сприятимуть вирішенню ризиків ВК/ФТ, пов'язаних з діяльністю із ВА та VASP. Сюди має входити співпраця та координація між відповідними органами влади для забезпечення сумісності вимог з ПВК/ФТ із правилами Захисту Даних та Конфіденційності, а також іншими схожими положеннями. Національна співпраця та координація є особливо важливими у контексті ВА, частково через їх високу мобільність та транскордонну природу, а також через те, в який спосіб регулювання діяльності з ВА може охоплювати декілька регуляторних органів (*напр.,* компетентні органи, що регулюють діяльність із переказу коштів,

цінними паперами та біржовими товарами або деривативами). Більш того, національна співпраця, що стосується емісії ВА, є життєво необхідною у контексті подальших розслідувань та використання різних міжвідомчих інструментів для вирішення проблем у кібер-екосистемі та/або екосистемі ВА.

Підхід до Віртуальних Активів: Трактування Термінів, що Стосуються Коштів чи Вартості

65. В цілях застосування Рекомендацій FATF, країни повинні розглянути усі терміни щодо коштів чи вартості у Рекомендаціях, такі як «майно», «доходи», «кошти», «гроші та інші активи», а також іншу «еквівалентну вартість», які включають ВА. Зокрема, країни повинні застосовувати відповідні заходи згідно з Рекомендаціями 3-8, 30, 33, 35 та 38, які несуть в собі посилання на раніше згадані терміни, пов'язані з коштами та вартістю чи інші аналогічні визначення у контексті ВА, для того аби запобігти зловживанню ВА у ВК, ФТ та фінансуванні розповсюдження зброї масового знищення (ФР), та проводити відповідні дії проти усіх злочинних доходів, які включають ВА. Вищезгадані Рекомендації – деякі з яких на перший погляд не мають прямого зв'язку з VASP та аналогічними підзвітними суб'єктами, але насправді застосовуються у цій сфері – відносяться до злочинів ВК, конфіскацій та тимчасових заходів, злочинів ФТ, цільових фінансових санкцій, неприбуткових організацій, повноважень правоохоронних органів, санкцій та міжнародної співпраці.

66. **Рекомендація 3.** В цілях імплементації Рекомендації 3, злочин ВК необхідно поширити на будь-який тип власності, в незалежності від її вартості, який прямо представляє злочинні доходи, в тому числі в контексті ВА. При доведенні того, що власність є злочинним доходом, не обов'язково щоб особа була звинувачена за предикатним злочином, в тому числі якщо мова йде про доходи від діяльності із ВА. Тому країни повинні розширити свої заходи щодо злочинів ВК й на злочинні доходи, що включають ВА.

67. **Рекомендація 4.** Аналогічно, конфіскація та тимчасові заходи, що відносяться до «(a) відмитого майна, (b) доходів від, або інструментарій що використовувався чи мав місце намір використання у, відмивання коштів чи предикатних злочинів, (c) майна, що використовувалось, чи мав місце намір його використання, у фінансуванні тероризму, терористичних актах чи терористичними організаціями, (d) чи власності відповідним вираженням вартості» також застосовуються до ВА.

68. Що стосується конфіскації та тимчасових заходів, які застосовуються до фіатних валют та товарів, правоохоронні органи (ПО) повинні мати можливість робити запит на тимчасове замороження активів, коли є

підстави вважати або коли встановлено, що вони походять від злочинної діяльності. Для того аби подовжити термін заморозки або зробити запит на конфіскацію активів, ПО повинні отримати відповідну постанову суду.

69. **Рекомендація 5.** Схожим чином, описані у Рекомендації 5 злочини ФТ мають бути розширені до «будь-яких коштів чи інших активів», в тому числі ВА, чи то від законного або незаконного джерела (див. ПЗР. 5).

70. **Рекомендація 6.** Також країни повинні одразу заморожувати кошти та інші активи – в тому числі ВА – визначених осіб чи установ та забезпечити, щоб жодні кошти чи інші активи – в тому числі ВА – не були доступні визначеним особам чи установам в контексті цільових фінансових санкцій, пов'язаних із тероризмом та фінансуванням тероризму.

71. **Рекомендація 7.** В контексті цільових фінансових санкцій, пов'язаних із розповсюдженням, країни повинні невідкладно заморожувати кошти та інші активи – в тому числі ВА – визначених осіб чи установ та забезпечити, щоб ці кошти чи інші активи – в тому числі ВА – не стали доступні визначеним особам та установам.

72. **Рекомендація 8.** Країни також повинні застосовувати заходи, у відповідності до ризик-орієнтованого підходу, для захисту неприбуткових організацій від їх використання в цілях фінансування тероризму, як це викладено у Рекомендації 8, в тому числі, коли таємне нецільове переведення коштів до терористичних організацій включає й ВА (див. Рекомендація 8(c)).

73. **Рекомендація 30** застосовується до діяльності із ВА та до VASP у контексті застосовності усіх термінів, що стосуються коштів чи вартості, зазначених у підрозділі 3.1.2 цього Керівництва. Як і з іншими типами злочинної власності чи доходів, країни повинні забезпечити, щоб компетентні органи влади несли відповідальність за оперативне виявлення, відслідковування та ініціювання дій для заморожування та вилучення власності, пов'язаної із ВА, що є або може стати предметом конфіскації чи підозрюється у тому що є злочинним доходом. Країни повинні імплементувати Рекомендацію 30, в незалежності від того, як юрисдикція класифікує ВА у своєму національному законодавстві (*тобто* в незалежності від того, як ВА юридично класифікуються у відповідності до законів про власність).

74. **Рекомендація 33.** Статистика, яку ведуть країни, має включати дані щодо звітів про підозрілі операції (STR), які компетентні органи отримують, а також щодо власності, яка була заморожена, вилучена та конфіскована компетентними органами. Тому країни також повинні імплементувати

Рекомендацію 33 у контексті VASP та діяльності з ВА, та ведення статистики щодо STR, які компетентні органи влади отримують від VASP та від інших підзвітних суб'єктів, таких як банки, що подають звіти пов'язані із VASP, ВА та діяльністю з ВА. Як і в інших рекомендаціях, які містять умови щодо коштів чи вартості (*напр.,* Рекомендація 3-8, 30, 35 та 38), країни також повинні вести статистику щодо будь-яких ВА, які компетентні органи заморозили, вилучили чи конфіскували, в не залежності від того як юрисдикція класифікує ВА у своєму національному законодавстві. Додатково, країни повинні розглянути питання оновлення STR та пов'язаної статистики для включення індикаторів, пов'язаних з ВА, які сприяють розслідуванням та фінансовому аналізу.

75. **Рекомендація 35** зобов'язує країни мати ряд ефективних, пропорційних та переконливих санкцій (кримінальних, цивільних чи адміністративних) для того аби розбиратись із фізичними чи юридичними особами, які охоплені Рекомендаціями 6 та 8-23, та які не можуть виконати необхідні вимоги з ПВК/ФТ. Як вимагається параграфом 6 у ПЗР. 15, країни аналогічним чином повинні мати чинні санкції для боротьби з VASP (та іншими підзвітними суб'єктами, які залучені до діяльності з ВА), які не виконують свої зобов'язання з ПВК/ФТ. Як і у випадку з ФУ та ВНУП, а також іншими фізичними та юридичними особами, подібні санкції, коли доцільно, повинні застосовуватись не тільки до VASP, але й до їх директорів та високопосадових осіб.

76. **Рекомендація 38** також містить умови щодо коштів та вартості й застосовується у контексті ВА, але більш детально розглядається у підрозділі 3.1.8 щодо *Міжнародного Співробітництва* та імплементації Рекомендацій 37-40, як це описано у параграфі 8 ПЗР. 15.

Ліцензування чи Реєстрація

77. Країни повинні визначити один чи декілька органів влади, які будуть відповідальні за ліцензування та/або реєстрацію VASP.

78. У відповідності до параграфу 3 ПЗР.15, від VASP вимагається зареєструватись у юрисдикції, де вони були створені. Посилання на створення юридичної особи[11] включає реєстрацію компаній чи будь-якого іншого механізму, який використовується для формалізації існування юридичної особи, такі як реєстрація у державному реєстрі, комерційному реєстрі або іншому аналогічному реєстрі компаній чи юридичних осіб; визнання нотаріусом чи будь-яким іншим державним

11 Див. виноску 40 у ПЗР. 24.

представником; подання статуту чи інших установчих документів компанії; виділення податкового номеру для компанії, і т.д.

79. У випадках, коли VASP є фізична особа, вона має зареєструватись чи отримати ліцензію у юрисдикції, де розміщено бізнес – визначення якого може включати декілька факторів. Місце ведення бізнесу фізичною особою може характеризуватись основним місцем ведення бізнесу або місцем, де ведуться та зберігаються записи і бухгалтерський облік підприємства, а також місцем де фізична особа проживає (*тобто* де фізична особа знаходиться фізично, або де вона є резидентом). Коли фізична особа здійснює ділову діяльність поза межами юрисдикції проживання, або місце ведення бізнесу неможливо визначити, основним місцем ведення бізнесу можна вважати місце реєстрації особи. Місце ведення ділової діяльності може також, потенційно, включати місцерозташування серверів бізнесу фізичної особи.

80. Зареєстровані VASP або ті, що отримали ліцензію, повинні дотримуватись відповідних критеріїв, що встановлені відповідними органами влади. Органи влади мусять накладати подібні умови на зареєстровані VASP для того, аби ефективно здійснювати нагляд за ними. Такі умови повинні дозволяти здійснення відповідного нагляду та можуть потенційно включати, в залежності від розміру та природи ділової діяльності VASP, вимогу мати виконавчого директора резидента, наявність профільних керівників або якісь особливі фінансові вимоги.

81. Юрисдикції також можуть вимагати від VASP, що пропонують свої продукти та/або послуги клієнтам у цій юрисдикції, чи здійснюють операції з цієї юрисдикції, мати ліцензію чи бути зареєстрованими у них. Тому юрисдикція може вимагати реєстрацію чи отримання ліцензії від VASP, до чиїх послуг можуть мати доступ люди, що знаходяться чи проживають у цій юрисдикції.

82. Компетентні органи влади повинні вживати необхідних заходів для запобігання випадкам, коли злочинці чи їх партнери тримають чи є бенефіціарними власниками істотної чи контролюючої частки у VASP, або займають там пости із керівними функціями. Подібні заходи повинні включати вимогу до VASP попередньо погоджувати істотні зміни у структурі акціонерів та господарській діяльності.

83. Країни повинні вживати заходи для виявлення фізичних чи юридичних осіб, які проводять діяльність чи операції з ВА без ліцензії чи реєстрації та застосовувати до них відповідні санкції, в тому числі в контексті традиційних підзвітних суб'єктів, які можуть долучатись до діяльності чи операцій із ВА (*напр.,* банк, який надає ВА своїм клієнтам). Національні

органи влади повинні мати механізми для здійснення моніторингу за сектором VASP, а також іншими підзвітними суб'єктами, які можуть долучатись до діяльності чи операцій із ВА або надавати продукти чи послуги, пов'язані із ВА; забезпечення існування належних каналів інформування VASP та інших підзвітних суб'єктів щодо їх зобов'язань зареєструватись чи подати заявку на отримання ліцензії у відповідного органу влади. Країни також повинні визначити орган, який буде відповідальний за виявлення та накладання санкцій на незареєстровані чи неліцензовані VASP (та інші підзвітні суб'єкти, які здійснюють діяльність із ВА). Як обговорено вище у Керівництві, навіть країни, які вирішили заборонити діяльність з ВА чи VASP, повинні мати механізми та органи влади для виявлення та вжиття заходів проти фізичних чи юридичних осіб, які не виконують свої зобов'язання, як це вимагається Рекомендацією 15.

84. Для виявлення осіб, які діють без ліцензії та/або реєстрації, країни повинні розглянути перелік інструментів та ресурсів, які вони можуть мати для здійснення розслідування щодо наявності неліцензованих чи незареєстрованих VASP. Наприклад, країни повинні взяти до уваги веб-скрапінг та інформацію з відкритих джерел для знаходження он-лайн реклами або можливих пропозицій для бізнесу незареєстрованими чи неліцензованими підприємствами; інформацію з галузевих кіл (включаючи створення каналів для отримання публічного фідбеку) щодо наявності певних ділків, які можуть бути неліцензовані чи незареєстровані; інформацію від ПФР чи інших установ, що звітують, таку як STR чи слідчі висновки, надані банками, які можуть викрити наявність неліцензованої чи незареєстрованої фізичної або юридичної особи; інформацію, що недоступна у публічному просторі, чи подавало підприємство до цього заявку на реєстрацію чи отримання ліцензії, чи була відкликана реєстрація або ліцензія, та звіти правоохоронних органів і розвіддані; а також інші слідчі інструменти та можливості.

85. Координація між різними національними органами влади, залученими до регулювання та ліцензування чи реєстрації VASP, є важливою, як попередньо описано в контексті Рекомендації 2, оскільки різні органи влади можуть мати інформацію, пов'язану із неавторизованими постачальниками та видами діяльності. Країни повинні мати діючи відповідні канали обміну інформацією, аби в належний спосіб підтримувати ідентифікацію та накладення санкцій неліцензованих чи незареєстрованих VASP.

Нагляд або моніторинг

86. **Рекомендації 26 та 27.** Як описано нижче, Рекомендація 15 вимагає від країн робити VASP об'єктами ефективної системи з нагляду або

моніторингу у сфері ПВК/ФТ. Як встановлено Рекомендаціями 26 та 27, параграфом 5 ПЗР. 15 аналогічним чином вимагається від країн забезпечити, щоб VASP підлягали належному регулюванню та нагляду або моніторингу з ПВК/ФТ, а також ефективно імплементували Рекомендації FATF у відповідності до їх ризиків ВК/ФТ. VASP мають бути об'єктами ефективної системи моніторингу та забезпечувати комплаєнс національним вимогам з ПВК/ФТ. Нагляд чи моніторинг за VASP має здійснюватися компетентним органом влади, не органом саморегулювання (ОСР), який має проводити ризик-орієнтований нагляд чи моніторинг. Наглядові органи повинні мати належні повноваження для здійснення нагляду чи моніторингу та забезпечення комплаєнсу з боку VASP (а також інших підзвітних суб'єктів, які залучені до діяльності з ВА) вимогам боротьби з відмиванням коштів та фінансуванням тероризму, включно з правом здійснювати перевірки, змушувати до надання інформації, накладати дисциплінарні та фінансові санкції, в тому числі повноваження відкликати, обмежувати чи призупиняти ліцензію або реєстрацію VASP, коли це необхідно.

87. Враховуючи транскордонну природу діяльності та надання послуг VASP, а також потенційні виклики, що пов'язані з конкретним VASP та юрисдикцією, міжнародна співпраця між відповідними наглядовими органами отримує особливу важливість, як це підкреслено у параграфі 8 ПЗР. 15 (див також підрозділ 3.1.8). Юрисдикції також можуть посилатись на відповідну роботу інших органів, що встановлюють міжнародні стандарти, таких як Міжнародна Організація Комісій з Цінних Паперів та Базельський Комітет з Питань Банківського Нагляду.[12]

88. Як більш детально описано у підрозділі 3.1.9 цього Керівництва, коли ВНУП долучається до діяльності VASP, країни повинні піддати установу усім відповідним заходам, що встановлені для VASP у Рекомендаціях FATF, в тому числі тих, що стосуються нагляду та моніторингу.[13]

Превентивні Заходи

89. Параграф 7 ПЗР. 15 роз'яснює, що усі превентивні заходи, що містяться у Рекомендаціях 10-21, у контексті ВА та фінансової діяльності з ВА, застосовуються як до країн, так і до підзвітних суб'єктів. Проте, Рекомендації 9, 22 та 23 мають непряме застосування у цій сфері і також

12 Для прикладу також див. Принципи 3 (щодо співпраці та взаємодії) та 13 (щодо відносин між приймаючими країнами та країнами походження) з *Ключових Принципів Ефективного Банківського Нагляду* Базельського Комітету: https://www.bis.org/publ/bcbs230.pdf

13 Як зазначено у підрозділі 2.2, юрисдикції можуть визначати VASPяк «ФУ» чи як «ВНУП». Проте, в незалежності від того, як країни вирішать називати VASP, вони все одно будуть об'єктами того ж рівня регулювання та нагляду, як і ФУ, у відповідності до видів фінансової діяльності, до яких буде залучено VASP, а також видів фінансових послуг, які вони надаватимуть.

розглядаються нижче. Відповідно, наступний підрозділ надає пояснення по зазначеним Рекомендаціям для того, аби допомогти країнам у подальшому вирішенні питання імплементації превентивних заходів у контексті ВА. Окрім того, підрозділ 4.1 надає особливе керівництво для VASP та інших підзвітних суб'єктів, що залучені до діяльності з ВА, щодо того, як вони мають імплементувати превентивні заходи описані нижче, а також інші заходи з ПВК/ФТ, що вказані у Рекомендаціях FATF.

90. **Рекомендація 9** призначена для забезпечення того, що закони про нерозголошення не заважатимуть імплементації Рекомендацій FATF. Як і з ФУ, країни повинні забезпечити, щоб закони про нерозголошення не перешкоджали імплементації Рекомендацій FATF відносно VASP, хоча Рекомендація 9 не містить чіткого посилання на VASP.

91. **Рекомендація 10.** Країни та підзвітні суб'єкти повинні розробити процес здійснення CDD для того, аби відповідати Стандартам FATF та національним законодавчим вимогам. Процес CDD має допомогти VASP (а також іншим підзвітним суб'єктам, які залучені до діяльності з ВА) в оцінці ризиків ВК/ФТ, що пов'язані з діяльністю із ВА чи діловими відносинами або окремими переказами, що перевищують порогову суму. Початкова CDD містить виявлення клієнта та, коли необхідно, бенефіціарного власника клієнта, верифікацію особистості клієнта на основі ризику та на основі надійних та незалежних інформаційних даних чи документах, як мінімум в тій мірі, яка передбачена законодавчою системою. Процес CDD також включає розуміння цілей та передбачуваного характеру ділових відносин, а також отримання більшої інформації у ситуаціях з високим ризиком.

92. На практиці, зазвичай VASP відкривають та ведуть рахунки (*тобто* встановлюють відносини з клієнтами) та збирають відповідну інформацію під час CDD, коли надають послуги або долучаються до діяльності із ВА від імені своїх клієнтів. У випадках, коли VASP проводять окремі операції, існує визначена порогова сума, при перевищені якої VASP зобов'язані провести CDD, у відповідності до ПЗР. 15 параграфу 7(а) ця сума складає 1000 USD/EUR.[14]

93. В незалежності від природи взаємовідносин чи операції, країни повинні забезпечити, щоб VASP мали ефективні процедури з ідентифікації та верифікації, на основі ризику, особистості клієнта, в тому числі при встановленні ділових відносин з цим клієнтом; коли у VASP є підозра щодо ВК/ФТ, в незалежності від перевищення порогової суми; а також

14 FATF погодив зниження порогової суми операції до 1000 USD/EUR, враховуючи ризики ВК/ФТ, пов'язані із транскордонною природою діяльності з ВА.

коли існують сумніви щодо достовірності та належності ідентифікаційних даних, отриманих раніше.

94. Деякі юрисдикції можуть розглядати використання кіосків ВА (які деякі можуть називати «АТМ», як це описано у розділі вище щодо послуг та бізнес-моделей ВА) як одноразові операції, за умови, що постачальник чи власник/оператор кіоску та клієнт, який використовує кіоск, здійснюють одноразові операції. Інші юрисдикції можуть вимагати від власників/операторів таких кіосків зареєструватись в якості VASP чи іншої фінансової установи (*напр.,* як установа, що здійснює грошові перекази), і не розглядатимуть такі операції як одноразові.

95. Як було обговорено раніше, у ВА присутні певні характеристики, які роблять їх більш схильними до використання злочинцями в цілях відмивання коштів, фінансування тероризму та інших незаконних дій. Серед таких характеристик, зокрема, можна виділити глобальне охоплення, можливість здійснювати швидкі операції, спроможність забезпечити операції «окремий користувач – окремий користувач» (інколи називаються одноранговими), а також потенціал до підвищеної анонімності та заплутаності у фінансових потоках та контрагентах. В світлі зазначених характеристик, країни можуть піти далі тих вимог, що зазначені у Рекомендації 10 щодо необхідності проведення повної CDD для усіх операцій, що включають ВА або здійснюються VASP (а також іншими підзвітними суб'єктами, такими як банки, що залучені до діяльності з ВА), в тому числі по відношенню до «одноразових операцій», що не перевищують поріг у 1000 USD/EUR, у відповідності до національної законодавчої бази. Такий підхід узгоджується із ризик-орієнтованим підходом, який встановлено Рекомендацією 1, за умови, що це обґрунтовано на основі оцінки ризиків країни (*напр.,* через виявлення підвищеного ризику). Додатково, юрисдикції, при встановленні своїх регуляторних та наглядових режимів, повинні розглянути питання того, як VASP може визначити та забезпечити, що операції проводяться разово чи епізодично, а не на більш послідовній основі.

96. Як описано у Пояснювальній Записці до Рекомендації 10, існують умови, коли ризик ВК/ФТ є підвищеним і коли вимагається проведення посилених заходів з CDD. У контексті діяльності, пов'язаної з ВА та VASP, країни повинні розглядати особливі фактори ризику географічного характеру. Наприклад, чи розташовано VASP в, або операція з ВА відбувається за участі, країні, яка представляє потенційно підвищений ризик відмивання коштів чи фінансування тероризму (див. ПЗР. 10, параграф 15(b)).

97. Хоча на даний момент не існує узгодженості у визначенні або методології для визначення, чи представляє юрисдикція, в якій проводить свою діяльність VASP або з якої можуть виходити операції з ВА, підвищений ризик ВК/ФТ, розгляд специфічних для країни ризиків, у поєднанні з іншими факторами ризику, надають корисну інформацію для подальшого виявлення ризиків ВК/ФТ. До індикаторів підвищеного ризику входять:

    a) Країни або географічні зони, які за даними надійних джерел[15], надають фінансування чи підтримку терористичній діяльності або мають діючі терористичні організації на своїй території;

    b) Країни, які визначені надійними джерелами, як такі, що мають високий рівень організованої злочинності, корупції чи іншої злочинної діяльності, в тому числі країни, які постачають (чи через які проходить транзит) наркотики, де здійснюється торгівля людьми, високий рівень контрабанди та незаконних азартних ігор;

    c) Країни, які є об'єктами санкцій, ембарго чи схожих заходів, які накладені міжнародними організаціями, такими як Організація Об'єднаних Націй; та

    d) Країни, які визначені надійними джерелами, як такі, що мають слабкі уряд, правоохоронні органи та регуляторні режими, в тому числі, країни, які визначені документами FATF, як такі, що мають слабкий режим з ПВК/ФТ, і до яких фінансові установи повинні приділяти особливу увагу при ділових відносинах та проведенні операцій.

98. Країни також повинні розглядати фактори ризику, пов'язані з продуктами, послугами, операціями чи каналами доставки ВА, в тому числі, коли діяльність здійснюється під псевдонімами чи це «анонімна операція» «non-F2F ділові відносини чи операції» та/або «платежі отримані від невідомих чи не пов'язаних третіх сторін» (див. ПЗР. 10, параграф 15(c), а також приклади індикаторів підвищеного та низького ризику, що перелічені у параграфі 31 цього Керівництва). Той факт, що майже усі ВА включають одну з цих особливостей чи характеристик, може вплинути на рішення країни щодо притаманного високого ризику у

15 Під «надійними джерелами» розуміється інформація, яка надана всесвітньо визнаними міжнародними організаціями чи іншими органами із високою репутацією, які роблять таку інформацію публічною та широко доступною. Окрім FATF та органів типу FATF, до таких джерел можуть відноситись, але не обмежуватись ними, наднаціональні чи міжнародні органи, такі як Міжнародний Валютний Фонд, Світовий Банк та Егмонтська Група.

цій сфері діяльності, базуючись на самій природі продуктів, послуг, операцій чи механізмів постачання ВА.

99. В цих та інших випадках, до заходів з посиленої належної перевірки (EDD), які можуть пом'якшити потенційно високі ризики, що пов'язані з вищезазначеними факторами, входять:

    a) підтвердження інформації про особу, що надійшла від клієнта, такі як індивідуальний податковий номер, з інформацією, що зазначена у базах даних третіх сторін чи інших надійних джерелах;

    b) потенційне відслідковування IP-адреси клієнта; та

    c) здійснення пошуку в мережі Інтернет для підтвердження того, що інформація про діяльність відповідає профілю операцій клієнта, за умови, що такий збір інформації проводиться в рамках національного законодавства про конфіденційність. [16]

100. Країни також повинні розглядати заходи з посиленої CDD, що розписані у ПЗР. 10, параграфі 20, в тому числі збір додаткової інформації щодо клієнта та цільового характеру ділових відносин, щодо джерела коштів клієнта, щодо мети здійснюваної операції, а також проведення посиленого моніторингу щодо ділових відносин. Більш того, країни повинні розглянути заходи, що вимагаються від ФУ, які залучаються до діяльності з деномінації фіатних активів, які є non-F2F (такі як мобільні послуги) або які можна порівняти із операціями з ВА, при оцінці їх ризиків та відповідній розробці пом'якшувальних засобів контролю.

101. Додатково, країни повинні вимагати від VASP та інших підзвітних установ, які залучені до надання продуктів та послуг ВА, зберігати документи, дані чи інформацію, що були зібрані під час проведення CDD, оновленими та актуальними, проводячи перегляд існуючих записів, особливо щодо високоризикованих клієнтів чи категорій продуктів або послуг ВА, та проводячи поточну належну перевірку (див. Розділ IV для подальшого ознайомлення з поточною належною перевіркою та зобов'язань з моніторингу для VASP та інших підзвітних суб'єктів). Такі перегляди операцій та записів є важливими у здійсненні ефективного нагляду.

16 Див. Керівництво щодо ВВ від 2015 року, параграф 44, а також Керівництво щодо Застосування Ризик-Орієнтованого Підходу до Нових Платіжних Продуктів та Послуг, параграф 66.

102. **Рекомендація 11** вимагає від країн забезпечити, щоб VASP вели записи усіх операцій та заходів з CDD, щонайменше за останні п'ять років, у такий спосіб, аби можна було реконструювати окремі операції, а необхідні елементи швидко направити до компетентного органу влади. Країни повинні вимагати від VASP та інших підзвітних суб'єктів, що долучаються до діяльності з ВА, зберігати записи щодо операцій та інформації, отриманої внаслідок проведення CDD, в тому числі: інформацію, пов'язану з ідентифікацією відповідних сторін; відкритими ключами (або схожими ідентифікаторами); залученими адресами та рахунками; датами проведення та природи операції; а також сумою операції. Публічна інформація на блокчейні чи іншому відповідному розподіленому реєстрі відповідного ВА, може забезпечити початковий фундамент для ведення діловодства, за умови, що установи можуть належним чином ідентифікувати своїх клієнтів. Проте, спирання виключно на блокчейн чи інший тип розподіленого реєстру, що лежить в основі облікової інформації ВА, не є достатнім для того, аби відповідати вимогам Рекомендації 11.

103. Наприклад, інформація, що знаходиться на блокчейні чи іншому розподіленому реєстрі може дозволити відповідним органам прослідити операцію до адреси гаманця, хоча може й не вказати на зв'язок між адресою гаманця та іменем особи. Адреса гаманця містить код користувача, який слугує цифровим підписом у розподіленому реєстрі (*тобто,* закритий ключ) в формі унікального рядка чисел та літер. Проте, для того аби зв'язати адресу та реальну особу, знадобиться додаткова інформація.

104. **Рекомендація 12** вимагає від країн імплементувати заходи, що вимагають від підзвітних суб'єктів, таких як VASP, мати належні системи управління ризиками для визначення того, чи є клієнт або бенефіціарний власник публічною особою (PEP), або ж пов'язаний із іноземним PEP[17] і, якщо так, вживати додаткових заходів, окрім звичного CDD (як це визначено у Рекомендації 10), для визначення того, чи мають вони з ними ділові відносини, в тому числі, за необхідності, виявляючи джерело коштів.

105. **Рекомендація 13** передбачає, що країни повинні вимагати від ФУ застосовувати певні інші зобов'язання, окрім здійснення звичайних заходів з CDD, коли вони долучаються до транскордонних кореспондентських відносин. Окремо від традиційних ФУ, які можуть долучатись до діяльності з ВА і щодо яких вже застосовано усі заходи у

17 «Іноземними PEP» є особи, які наділені або були наділені важливими державними функціями в іноземній країні. Наприклад, Голова уряду, вищі політичні діячі, урядовці, судові чи військові посадові особи, виконавчі директори державних корпорацій, а також вищі представники політичних партій (Словник FATF).

відповідності до Рекомендації 13, деякі інші ділові відносини або види діяльності із ВА у секторі VASP можуть мати характеристики подібні до транскордонних кореспондентських банківських відносин. ПЗР. 13 передбачає, що для кореспондентських банківських відносин чи інших подібних транскордонних відносин, ФУ мають застосовувати критерії (a) – (e) Рекомендації 13, що доповнюватимуть звичайні заходи з CDD. До «інших подібних відносин» відносяться послуги з переказу коштів чи грошової вартості (MVTS), коли постачальники MVTS діють як посередники для інших постачальників MVTS, або коли постачальник MVTS отримує доступ до банківських чи подібних послуг через рахунок іншого MVTS-клієнта банку (див. *Керівництво FATF щодо Кореспондентських Банківських Відносин* від 2016 року).

106. У тій самій мірі, в якій відносини у секторі VASP мають, або матимуть у майбутньому[18], характеристики подібні до транскордонних кореспондентських банківських відносин, країни повинні імплементувати превентивні заходи, встановлені Рекомендацією 13, по відношенню до VASP (та інших підзвітних суб'єктів, що діють у сфері ВА), що допоможе розвитку таких відносин.

107. **Рекомендація 14** скеровує країни до реєстрації чи ліцензування фізичних чи юридичних осіб, які надають MVTS, та до забезпечення ними комплаєнсу відповідним заходам з ПВК/ФТ. Як описано у Керівництві щодо ВВ 2015 року, сюди входить встановлення контролю за MVTS, що діють у країні, у комплаєнсі заходам з реєстрації чи ліцензування, або інші заходи, що застосовуються з ціллю ПВК/ФТ. Разом з тим, вимоги Рекомендації 15 з реєстрації та ліцензування, застосовуються до усіх VASP, навіть тих, що залучені до діяльності MVTS (*напр.,* національне підприємство, яке надає послуги з обміну ВА на фіатні валюти і навпаки).

108. **Рекомендація 15.** У жовтні 2018 року, FATF запровадило оновлення до Рекомендації 15, що посилюють фундаментальний ризик-орієнтований підхід та пов'язані зобов'язання для країн та підзвітних суб'єктів у контексті нових технологій, для того аби прояснити застосування Рекомендації у контексті ВА, фінансової діяльності з ВА та VASP. Рекомендація 15 вимагає від країн ідентифікувати та оцінювати ризики ВК/ФТ, що пов'язані із розвитком нових продуктів та ділових практик, в тому числі нових механізмів доставки та використання нових технологій чи тих, що розвиваються, як для існуючих так і для нових продуктів. Показово, що вона також вимагає від країн забезпечити вжиття

18 Наприклад, певна кількість дослідників та аналітиків зазначили, що вони бачать великий потенціал для VASP та протоколів ВА у поєднанні з існуючими клієнтами кореспондентського банкінгу та дозволі їм надсилати та отримувати кошти з-за кордону без посередництва традиційних ФУ, що, потенційно, призведе до швидшого здійснення операцій та зниження їх вартості.

відповідних заходів для управління та пом'якшення ризиків ВК/ФТ ліцензованими фінансовими установами у своїй юрисдикції, до запуску нових продуктів чи ділових практик, або використання нових технологій (див. Додаток А).

109. У відповідності до духу Рекомендації 15, оновлення від жовтня 2018 року уточнюють, що країни повинні управляти та пом'якшувати ризики, які виникають від ВА та забезпечувати регулювання VASP в цілях ПВК/ФТ, їх реєстрацію чи ліцензування, та забезпечити, щоб вони були об'єктом ефективних систем моніторингу та дотримувались комплаєнсу відповідним заходам, що передбачені Рекомендаціями FATF. ПЗР. 15, яка була запроваджена FATF у червні 2019 року, уточнює Рекомендацію 15 та більш детально описує, яким чином вимоги FATF застосовуються по відношенню до ВА, діяльності з ВА та до VASP, в тому числі в контексті: оцінки пов'язаних ризиків ВК/ФТ; ліцензування чи реєстрації; нагляду чи моніторингу; превентивних заходів, таких як CDD, ведення обліку та звітування про підозрілі операції; санкцій та інших правозастосовних заходів; а також міжнародної співпраці (див. Додаток А).

110. У контексті ВА та VASP, країни повинні забезпечити, щоб ліцензовані, або які здійснюють діяльність, у їх юрисдикції VASP розглядали питання, чи можуть VASP управляти та пом'якшувати ризики від залучення до діяльності, яка включає використання технологій чи механізмів з посиленою анонімністю, серед яких AEC, міксери, тумблери та інші технології, які приховують особистість відправника, отримувача, утримувача або бенефіціарного власника ВА. Якщо VASP не може управляти та пом'якшувати ризики, пов'язані із залученням до такої діяльності, тоді VASP не має отримувати дозвіл на здійснення такої діяльності.

111. **Рекомендація 16** була розроблена з метою попередження необмеженого доступу для терористів та інших злочинців до переказу коштів в електронній формі для переміщення їх коштів, а також для виявлення подібного використання, коли воно виникає. Вона встановлює вимоги для країн, що пов'язані із електронними переказами та відповідними повідомленнями, та застосовується як до національних так і транскордонних електронних платежів. Рекомендація 16 визначає «електронні платежі» як будь-яку транзакцію, яка проводиться від імені відправника через фінансову установу за допомогою електронних засобів з метою зробити певну суму коштів доступною для отримувача у фінансовій установі отримувача, в незалежності від того, чи є відправник та отримувач однією особою.

112. У відповідності з функціональним підходом Рекомендацій FATF, вимоги пов'язані з електронними переказами та відповідними повідомленнями,

згідно з Рекомендацією 16 застосовуються до усіх постачальників подібних послуг, в тому числі VASP, які надають послуги або долучаються до діяльності, такої як переказ ВА, які функціонально подібні до електронних переказів. Країни повинні застосовувати Рекомендацію 16 в незалежності від того, чи деномінується вартість традиційного електронного переказу або переказу ВА у фіатній валюті чи у ВА. Разом з тим, країни повинні встановлювати мінімальний поріг для переказу ВА у сумі 1000 USD/EUR, враховуючи ризики, пов'язані із різними ВА та видами діяльності із ВА.

113. Отже, вимоги Рекомендації 16 повинні застосовуватись до VASP щоразу, коли їх операції, у фіатній валюті чи ВА, включають: (a) традиційний електронний переказ; (b) переказ ВА чи іншу відповідну операцію між VASP та іншим підзвітним суб'єктом (*напр.,* між двома VASP, чи між VASP та іншою підзвітною особою, як банк чи ФУ). В останніх сценаріях (*тобто* при операціях з ВА), країни повинні відноситись до усіх переказів ВА, як до транскордонних електронних переказів, у відповідності з Пояснювальною Запискою до Рекомендації 16 (ПЗР. 16), а не як до національних електронних переказів, враховуючи транскордонну природу діяльності з ВА та операцій VASP.

114. Як описано у ПЗР. 15, параграфі 7(b), усі вимоги, що встановлені Рекомендацією 16 застосовуються до VASP чи інших підзвітних суб'єктів, які залучені до операцій з ВА, включно з зобов'язаннями щодо отримання, зберігання та надання необхідної інформації про відправника та отримувача, для того аби виявляти та звітувати про підозрілі операції, перевіряти доступність інформації, вживати заходів із заморожування, а також забороняти проведення операцій з визначеними особами та підприємствами. Тому країни повинні забезпечувати, щоб установи відправники (VASP чи інший підзвітний суб'єкт, такий як ФУ), які залучені до переказу ВА збирали та зберігали необхідну та точну[19] інформацію щодо відправника та отримувача, а також передавали інформацію до установи отримувача (VASP чи інший підзвітний суб'єкт, такий як ФУ). Додатково, країни повинні забезпечити, щоб установи отримувачі (VASP чи інший підзвітний суб'єкт) збирали та зберігали необхідну (не обов'язково точну) інформацію про відправника та необхідну й точну інформацію щодо отримувача, як це вказано у ПЗР. 16. До необхідної інформації включено: (i) ім'я/назва відправника; (ii) рахунок відправника, коли рахунок використовується для здійснення переказу (*напр.,* гаманець ВА); (iii) фізична (географічна) адреса відправника або ідентифікаційний код, або ідентифікаційний номер

19 Див. Словник FATF конкретних визначень, що використовувались у Рекомендації 16, де «точна» використовується для опису інформації, яка була перевірена на достовірність.

клієнта (не номер операції), який є унікальним для відправника в установі відправника, або дата та місце народження; (iv) ім'я/назву отримувача; та (v) номер рахунку отримувача, коли рахунок використовується для здійснення операції (*напр.,* гаманець ВА). Інформація не обов'язково повинна бути прикріплена до самого переказу ВА. Інформація може надаватись безпосередньо чи опосередковано, як це встановлено у ПЗР. 15.

115. Дуже важливо, щоб країни забезпечували *негайну* та *безпечну* передачу необхідної інформації щодо відправника та отримувача провайдерами переказів ВА - чи то VASP, чи іншим підзвітним суб'єктом – особливо враховуючи швидку і транскордонну природу переказів ВА та у відповідності до цілей Рекомендації 16 (так само, як і традиційної вимоги у Рекомендації 16 щодо інформації про відправника та отримувача «супроводжувального […] електронного переказу», що включає фіатну валюту). *«Безпечну»* у контексті ПЗР. 15, параграфу 7(b), має на меті донести, що провайдери повинні захищати цілісність та доступність необхідної інформації для сприяння ведення обліку (поміж інших вимог) та використання такої інформації шляхом отримання її від VASP чи інших підзвітних суб'єктів, а також для її захисту від несанкціонованого розкриття. Використання терміну не означає перешкоджання цілям Рекомендації 16 чи Рекомендації 9. *«Негайну»*, - також у контексті ПЗР. 15, параграфу 7(b) та враховуючи транскордонну природу, глобальне охоплення та швидкість операції – означає, що провайдери повинні надавати необхідну інформацію одночасно зі здійсненням операції. (Див. Розділ IV для додаткової інформації щодо цих питань, характерних для VASP та інших підзвітних суб'єктів).

116. У відповідності до свого національного законодавства, країни повинні вимагати від установ відправника та отримувача робити необхідну інформацію, що зазначена вище, доступною для відповідних органів влади. Більш того, вони повинні вимагати від цих установ вживати заходів із замороження та заборони операцій із визначеними особами та установами (*тобто*, перевірку клієнтів, з метою виконання своїх зобов'язань з цільових фінансових санкцій). Відповідно, установа-відправник повинна мати відповідну інформацію щодо свого клієнта відправника, а установа-отримувач повинна мати необхідну інформацію щодо свого клієнта отримувача, у відповідності до вимог належної перевірки клієнта, що встановлені Рекомендацією 10.

117. FATF визнає, що на відміну від традиційних фіатних електронних переказів, не до кожного переказу ВА може бути залучено два підзвітні суб'єкта, VASP чи інші підзвітні суб'єкти, такі як ФУ. У випадках, коли до переказу ВА залучено один підзвітний суб'єкт (*напр.,* коли VASP-відправник чи інший підзвітний суб'єкт відправляє ВА від імені свого

клієнта відправника, до отримувача, який не є клієнтом установи-отримувача, а є окремим користувачем ВА, із використанням власної технології розподіленого реєстру (DLT), оф-лайн гаманець), країни все ще повинні забезпечувати, щоб підзвітний суб'єкт дотримувався зобов'язань Рекомендації 16 відносно свого клієнта (відправника чи отримувача). FATF не очікує, що VASP та фінансові установи будуть відправляти необхідну інформацію окремому користувачу, який не є підзвітним суб'єктом, при відправленні переказу. VASP, який отримує переказ ВА від установи, яка не є VASP чи іншим підзвітним суб'єктом (*напр.,* від окремого користувача ВА, який використовує власне DLT, оф-лайн гаманець), повинен збирати необхідну інформацію щодо відправника від свого клієнта.

118. Аналогічним чином, можуть бути сценарії переказу ВА, коли до операції залучено «посередника VASP» чи іншого посередника з підзвітних суб'єктів або ФУ, який сприяє проведенню операції з ВА, як елемент посередництва у ланцюжку переказу ВА. Країни повинні забезпечити, щоб подібні посередницькі установи (чи то VASP, чи то інший підзвітний суб'єкт) також дотримувались вимог Рекомендації 16, як це встановлено у ПЗР. 15, в тому числі кваліфікуючи усі перекази ВА, як транскордонні перекази. Як і традиційні посередницькі ФУ, що обробляють традиційні фіатні транскордонні електронні перекази, повинні забезпечити, щоб уся необхідна інформація щодо відправника та отримувача, яка доповнює електронний переказ, зберігалась, так і VASP-посередник чи інша відповідна посередницька установа, яка сприяє переказу ВА, повинні забезпечити, щоб необхідна інформація переказувалась протягом усього ланцюжка переказу ВА, а також аби зберегти необхідні записи та зробити інформацію доступною для відповідних органів влади, за їх запитом. Посередницькі установи, які залучені до переказів ВА, також мають зобов'язання у відповідності до Рекомендації 16 щодо виявлення підозрілих операцій, впровадження заходів із замороження, а також заборони проведення операцій із визначеними особами та установами – аналогічно до VASP відправників та отримувачів (або інших підзвітних установ відправників чи отримувачів, що сприяють проведенню операції з ВА).

119. Відповідно до технологічно-нейтрального підходу FATF, необхідна інформація не повинна передаватись як частина (або бути вбудованою до) переказу на блокчейні чи іншій платформі розподіленого реєстру. Надання інформації VASP отримувачу може бути повністю відокремленим процесом від того, що відбувається на блокчейні чи іншому розподіленому реєстрі, де відбувається переказ ВА. Будь-яка технологія чи програмне рішення може бути допустимим, за умови, що рішення дозволяє установі відправнику чи отримувачу відповідати

вимогам Рекомендації 16 (і, звичайно, якщо не перешкоджає їх можливості дотримуватись своїх зобов'язань з ПВК/ФТ у відповідності до Рекомендацій FATF). Країни повинні співпрацювати зі своїм приватним сектором щодо потенційного застосування доступних технологій або можливих рішень щодо комплаєнсу Рекомендації 16 (див. Розділ IV для отримання додаткової інформації щодо постачальників та інших підзвітних суб'єктів в контексті Рекомендації 16).

120. **Рекомендація 17** дає можливість країнам дозволяти підзвітним суб'єктам покладатись на третіх сторін для впровадження бізнесу та/або здійснювати частину CDD процесу, в тому числі ідентифікацію та верифікацію особистості клієнтів. Разом з тим, третя сторона має бути регульованим підприємством, над яким компетентні органи влади здійснюють нагляд та моніторинг в цілях ПВК/ФТ, із чинними заходами щодо дотримання вимог з CDD та ведення обліку.

121. Країни можуть дозволяти VASP діяти як треті сторони, у відповідності до їх статусу згідно з Рекомендацією 15. Крім перевірки регламентованого статусу третьої сторони, підзвітні суб'єкти повинні проводити їх відбір на основі ризику. У контексті VASP, які виступають третьою стороною, країни та підзвітні суб'єкти повинні розглянути питання ризиків, які потенційно можуть становити треті сторони, природу ділової діяльності та операцій, групи клієнтів чи цільові ринки VASP, що виступає третьою стороною, а також, за необхідності, їх ділових партнерів. Коли VASP покладається на інший VASP для провадження бізнесу або проведення CDD, така довіра, особливо в контексті переказів ВА, повинна проявлятись у спосіб, який відповідає усім вимогам Рекомендації 16.

122. **Рекомендація 18** зобов'язує країни вимагати від підзвітних суб'єктів, таких як VASP, мати механізми внутрішнього контролю для ефективності політик та процесів з ПВК/ФТ та високої якості управління ризиками під час здійснення операцій, у своїх департаментах, відділеннях та дочірніх підприємствах, як всередині країни так і закордоном. Цей внутрішній контроль має включати відповідні механізми управління, коли відповідальність за ПВК/ФТ чітко розподілена, а відповідальна особа призначається на рівні правління; контроль за доброчесністю персоналу, який імплементується у відповідності до чинного національного законодавства; поточне навчання персоналу; та (зовнішній чи внутрішній) незалежний аудит для тестування системи.

123. **Рекомендація 19** зобов'язує країни вимагати від підзвітних суб'єктів, таких як VASP, застосовувати заходи з посиленої належної перевірки для ділових відносин та операцій, які проводяться з фізичними чи юридичними особами з високоризикованих країн. Це має особливе

значення для діяльності із ВА та VASP, враховуючи транскордонну природу їх діяльності.

124. **Рекомендація 20** вимагає від усіх ФУ, які підозрюють або мають ґрунтовні підстави вважати, що кошти є злочинними доходами або пов'язані з фінансуванням тероризму, одразу повідомляти про свої підозри відповідному ПФР. Відповідно, країни повинні забезпечити, щоб VASP та інші підзвітні суб'єкти, які залучені до діяльності із ВА, надсилали STR (див. Розділ IV для додаткової інформації, що стосується VASP та інших підзвітних суб'єктів).

125. Згідно з параграфом 7 ПЗР. 15, який відноситься до застосування превентивних заходів, та у контексті Рекомендації 16, країни також повинні вимагати від усіх VASP відповідати усім вимогам Рекомендації 16 в тих країнах, де вони проводять свою діяльність (для додаткової інформації, див. Розділ IV).

126. В деяких юрисдикціях, де вже імплементували комплексні зобов'язання з ПВК/ФТ для VASP та інших підзвітних суб'єктів, які беруть участь у діяльності з ВА, STR, які відносяться до ВА, були визнані дуже важливими у подальших розслідуваннях правоохоронних органів, а також у покращенні спроможності ПФР ліпше розуміти та аналізувати, як постачальників, так і види діяльності в екосистемі ВА.[20]

127. **Рекомендація 21** відноситься до заходів з інформування та конфіденційності, що застосовуються до ФУ, у відповідності до Рекомендацій FATF. Країни також повинні застосовувати такі заходи до VASP, як це вказано у параграфі 7 ПЗР. 15, що відноситься до застосування превентивних заходів. VASP, їх директори, відповідальні особи та працівники повинні бути захищені законом від кримінальної та цивільної відповідальності за порушення будь-яких положень щодо розкриття інформації та забороненого законодавством розкриття STR, як це детально описано у Рекомендації 21.

[20] Наприклад, STR, що надавались як депозитарною установою, так і VASP (особливо це стосується обмінників) дозволили правоохоронним органам США вжити необхідних заходів у 2017 році проти BTC-e – установа, що діяла в інтернеті і обмінювала фіатні валюти та ВА, й сприяла операціям, де мали місце вимога викупу, злам комп'ютеру, крадіжка ідентифікаційних даних, схеми з ухилення від оподаткування, корупція та торгівля наркотиками – надавши їм допомогу у виявленні адреси гаманця ВА, який використовувала BTC-e, та незаконних видів діяльності, що проходили через цей обмінний пункт.

Прозорість та Бенефіціарне Володіння Юридичними Особами та Утвореннями

128. **Рекомендації 24 та 25.** Словник FATF визначає VASP як *будь-яку фізичну чи юридичну* особу, яка, в якості своєї ділової активності, проводить види діяльності чи операції, що зазначені у визначенні VASP. Рекомендації 24 та 25 чітко вказують на те, що країни повинні вживати заходів для попередження використання юридичних осіб та утворень для відмивання коштів та фінансування тероризму. Як і з ФУ та ВНУП, країни повинні вживати заходів для попередження злочинного використання VASP та розглянути можливість застосування заходів, що сприятимуть доступу до інформації про бенефіціарну власність та здійснення контролю над VASP, втілюючи вимоги, що встановлені Рекомендаціями 10 та 22.

Оперативна та Правоохоронна Діяльність

129. **Рекомендація 29.** STR, які надсилаються VASP (чи іншими підзвітними суб'єктами, такими як традиційні ФУ, які можуть діяти у сфері ВА або долучатись до діяльності із ВА) у відповідності до рекомендації 20, мають бути подані до ПФР. Більш того, у ПФР має бути змога отримати додаткову інформацію від звітуючої організації у своїй юрисдикції, куди входять й VASP, а також у них має бути своєчасний доступ до фінансової, адміністративної та правоохоронної інформації, яку ПФР може запитати для належного виконання своїх функцій.

130. Читачі цього Керівництва повинні відмітити, що Рекомендація 30 була розглянута вище у розділі термінів, що стосуються коштів чи вартості.

131. **Рекомендація 31.** Як і у випадку з ФУ та ВНУП, країни та компетентні органи влади повинні мати можливість отримувати доступ до усіх необхідних документів та інформації, включно з повноваженнями використовувати примусові заходи щодо складання звітів, які ведуться VASP. Вони повинні мати ефективні механізми для виявлення того, чи фізична або юридична особа, така як VASP, веде чи контролює рахунки або гаманці ВА, а також механізми для забезпечення того, щоб компетентні органи мали діючі процеси для виявлення активів, в тому числі ВА, без попереднього повідомлення власнику. Застосування Рекомендації 31 є особливо важливим для країн та їх компетентних органів влади у питаннях вирішення та пом'якшення ризиків ВК/ФТ, пов'язаних із діяльністю з ВА та VASP.

132. **Рекомендація 32.** Юрисдикції повинні застосовувати ризик-орієнтований підхід при розгляді застосування Рекомендації 32 по відношенню до діяльності із ВА та до VASP. Окремо юрисдикції повинні

розглянути в своїх ризик-орієнтованих підходах (a) чи підпадає діяльність VASP та діяльність із ВА під параметри перевезення фізичних грошових інструментів та (b) як на практиці працюватимуть вимоги щодо декларування та системи для виявлення транскордонних переміщень таких активів, а також, яким чином вони пом'якшуватимуть ризики ВК/ФТ у своїх юрисдикціях.

133. Як і з Рекомендацією 30, читачі цього Керівництва мають відмітити, що **Рекомендація 33** розглянута вище у розділі термінів, що стосуються коштів чи вартості.

134. **Рекомендація 34** є важливим компонентом у підходах країн до виявлення та вирішення ризиків ВК/ФТ, пов'язаних із діяльністю ВА та із VASP, а також із самими ВА. Відповідні компетентні органи влади повинні створювати керівництва та надавати фідбек, який допоможе VASP (а також іншим підзвітним суб'єктам, в тому числі й традиційним ФУ) у застосуванні національних заходів з протидії відмиванню коштів та фінансуванню тероризму та, зокрема, у виявленні та звітуванні підозрілих операцій – будь то операція віртуальний/фіатний актив чи віртуальний/віртуальний.

Міжнародна Співпраця

135. **Рекомендації 36-40.** Враховуючи транскордонну та мобільну природу діяльності з ВА та сектору VASP, міжнародна співпраця та імплементація Рекомендацій 36-40 країнами та компетентними органами влади є життєве необхідною, особливо заходи, які застосовуються до країн та компетентних органів влади у Рекомендаціях 37-40. Більш того, ефективна імплементація вимог, що мають відношення до міжнародної співпраці, є важливою для обмеження спроможності провайдерів діяльності з ВА в одній юрисдикції отримувати нечесну конкурентну перевагу над провайдерами в інших юрисдикціях, які, потенційно, можуть бути краще регульованими, та обмежити торговий, регуляторний арбітраж та арбітраж з використанням криптохоперів (торгових віртуальних платформ, які дозволяють торгувати різними криптоактивами).

136. Визнаючи, що ефективне регулювання, нагляд та правозастосування, що пов'язані із сектором VASP, вимагають глобального підходу та рівня регуляторної системи у юрисдикції, параграфом 8 ПЗР. 15 підкреслюється важливість застосування Рекомендацій 37-40 з метою пом'якшення ризиків, пов'язаних із ВА, діяльністю з ВА та із VASP. Країни, окрім іншого, повинні мати діючі інструменти необхідні для співпраці один з одним, надання взаємної правової допомоги

(Рекомендація 37); допомоги у виявленні, заморожуванні, вилученні та конфіскації доходів та засобів злочину, які можуть приймати вигляд ВА, так само як і інших традиційних активів, пов'язаних із діяльністю VASP (Рекомендація 38); та надання ефективної допомоги в екстрадиції в контексті злочинів, пов'язаних із ВА, або суб'єктів, що знаходяться поза законом та долучаються до незаконної діяльності (Рекомендація 39).

137. Як і з іншими Рекомендаціями, які включають в себе умови, що стосуються коштів чи вартості, країни повинні застосовувати конфіскацію та попередні заходи по відношенню до «власності, що походить від; доходів від; засобів, що використовувались у; чи засобів призначених для використання у відмиванні коштів, вчиненні предикатних злочинів, фінансуванні тероризму» у контексті ВА.

138. Параграф 8 ПЗР. 15 також окремо вимагає від наглядових органів за VASP обмінюватись інформацією зі своїми іноземними контрагентами в оперативний та конструктивний спосіб, в незалежності від природи чи статусу наглядового органу, а також в незалежності від відмінностей в номенклатурі чи статусі VASP (див. підрозділи 3.1.4 та 3.18 вище).

139. Міжнародне співробітництво також є актуальним у контексті VASP, які бажають зареєструватись чи отримати ліцензію в одній юрисдикції, але надавати продукти та послуги для клієнтів, що розташовані в інших юрисдикціях. Це важливо, щоб ПФР співпрацювали та обмінювались інформацією щодо відповідних STR зі своїми контрагентами у своєчасний спосіб, особливо це стосується транскордонної діяльності з ВА чи операцій VASP. Належний нагляд та регуляторний контроль за VASP, що діють в їх юрисдикції дозволяє країнам краще надавати допомогу в розслідуваннях та інших видах міжнародної співпраці у сфері ВА. На даний момент, брак можливостей у регулюванні та розслідуванні в більшості країн може представляти собою перепону для спроможності країн надавати значущу міжнародну допомогу. Більш того, велика кількість країн не має законодавчої системи, яка б дозволила їм криміналізувати певні види діяльності з ВК/ФТ, які пов'язані із ВА, що у подальшому може обмежити їх спроможність надавати ефективну взаємну правову допомогу в ситуаціях, коли необхідне обопільне визнання скоєного діяння злочинним.

ВНУП, що Залучені до або є Провайдерами Діяльності з ВА

140. Коли ВНУП долучається до діяльності VASP (*напр.,* коли казино пропонує гру, що базується на ВА, або залучено до іншої діяльності, продуктів або послуг з ВА), країни повинні піддати установи усім заходам, що передбачені для VASP Рекомендаціями FATF. Країни повинні звернути увагу на те, що Рекомендації 22 та 23 вимагають

проведення CDD, ведення обліку та інші вимоги для таких типів ВНУП у наступних ситуаціях: (a) казино; (b) агентства з нерухомості; (c) торговці дорогоцінним металом та камінням; (d) адвокати, нотаріуси, інші незалежні правники та бухгалтери; та (e) постачальники послуг зі створення юридичних осіб. Рекомендацією 22 особливо відмічається, що вимоги встановлені у Рекомендаціях 10, 11, 12, 15 та 17 застосовуються до ВНУП. Таким чином, при вирішенні питання, як здійснювати регулювання та нагляд і застосовувати превентивні заходи до ВНУП, що залучені до діяльності VASP, країни, окрім інших Рекомендацій, що стосуються VASP, повинні звернутись до питання застосування Рекомендацій 10, 11, 12, 15 та 17 та застосувати належні CDD, ведення обліку та інші відповідні заходи.

141. Аналогічно, Рекомендація 28 вимагає від країн та компетентних органів влади піддавати ВНУП регуляторним та наглядовим заходам, як це встановлено Рекомендаціями FATF. Як було зазначено раніше, країни повинні піддавати VASP, в тому числі й ВНУП, що залучені до діяльності VASP, регулюванню та нагляду на тому ж рівні, що й ФУ, а не на рівні звичайних ВНУП. Коли ВНУП долучається до діяльності VASP (*напр.,* казино надає продукти та послуги ВА чи долучається до діяльності з ВА), країни повинні піддавати такий ВНУП вищому рівню нагляду (*напр.,* нагляд «ВНУП плюс»), що відповідав би більш високому рівню нагляду за VASP, який є еквівалентним рівню нагляду та регулювання для ФУ, як це викладено у Рекомендаціях 26 та 27. У таких випадках, підприємство, по суті, є VASP, що займається особливою фінансовою діяльністю, а не ВНУП, в незалежності від того, яке визначення буде використовувати країна і як буде називати таке підприємство, установу, постачальника продуктів чи послуг. Такий підхід допоможе забезпечити однаковий рівень регулювання VASP в усьому світі, а також той рівень нагляду, що відповідатиме тим видам діяльності, якими вони займатимуться.

Ризик-Орієнтований Підхід до Нагляду чи Моніторингу VASP

Розуміння Ризиків ВК/ФТ

142. Ризик-орієнтований підхід у сфері ПВК/ФТ націлений на розвиток превентивних та пом'якшувальних заходів, які співвідносяться із ризиками ВК/ФТ, які виявляються країнами та відповідними підзвітними суб'єктами. В плані нагляду, ризик-орієнтований підхід застосовується до способу, в якій наглядові органи розподіляють ресурси. Він також застосовується до наглядових органів, що виконують свої функції в такий спосіб, який сприяє застосуванню ризик-орієнтованого підходу VASP.

143. Ефективний ризик-орієнтовний режим повинен відображати політичний, законодавчий та регуляторний підходи країни. Національні політична, правова та регуляторна системи також повинні відображати ширший контекст політичних цілей фінансового сектору, які переслідує країна, включно з фінансовими послугами, фінансовою стабільністю, фінансовою надійністю, цілями фінансового захисту споживачів та розглядати ці фактори як ринкову конкуренцію. Міра, до якої національне законодавство дозволяє VASP застосовувати ризик-орієнтований підхід, повинна відображати природу, різноманітність та рівень розвитку сектору VASP і його профіль ризику, в тому числі ризиків ВК/ФТ, що пов'язані із окремими VASP та особливими продуктами, послугами ВА чи видами діяльності з ВА.

144. Наглядові органи повинні також розвивати глибоке розуміння ринку VASP, його структури та роль у фінансовій системі й економіці країни, для кращого підкріплення своїх оцінок ризику у секторі. Це може вимагати інвестування у навчання, персонал чи інші джерела, які дозволяють наглядовим органам здобути практичних навичок та досвіду, які необхідні для регулювання та здійснення нагляду за постачальниками ВА та видами діяльності, що описані серед послуг чи бізнес моделей ВА на початку цього Керівництва.

145. Наглядові органи повинні використовувати різні джерела для виявлення та оцінки ризиків ВК/ФТ, що пов'язані з продуктами, послугами та діяльністю з ВА, а також із VASP. До подібних джерел мають включатись, але не обмежуватись ними, національні та секторальні оцінки ризиків юрисдикцій, національні та міжнародні типології та наглядовий досвід, керівництва ПФР та зворотній зв'язок від них. Коли компетентні органи не належним чином розуміють сектор VASP чи екосистему ВА, для компетентних органів влади може бути доцільним провести більш цільові секторальні оцінки ризиків щодо сектору VASP та/або середовища ВА, для того аби розвити розуміння відповідних ризиків ВК/ФТ на національному рівні для наявності уявлення про інституційні оцінки, які мають бути проведені VASP.

146. Доступ до інформації щодо ризиків ВК/ФТ є основним для ефективного ризик-орієнтованого підходу. Рекомендація 1 (див ПЗР. 1.3) вимагає від країн, включно з наглядовими органами, вживати відповідних кроків для виявлення та оцінки ризиків ВК/ФТ у країні на постійній основі для того, аби робити таку інформацію доступною в цілях проведення оцінки ризиків у сфері ПВК/ФТ, що проводяться ФУ та ВНУП, в тому числі VASP. Країни, включно з наглядовими органами, повинні тримати свої оцінки ризиків актуальними та повинні мати механізми для надання відповідної інформації щодо результатів до усіх відповідних компетентних органів влади, ФУ та ВНУП, включно з VASP. У ситуаціях,

коли деякі частини сектору VASP мають обмежену можливість для виявлення ризиків ВК/ФТ, пов'язаних із продуктами, послугами та видами діяльності з ВА, країни, включно з наглядовими органами, повинні працювати із сектором для розуміння його ризиків та надання допомоги приватному сектору у створенні його власного розуміння ризиків. В залежності від можливостей сектору VASP, може знадобитись загальна чи більш деталізована інформація.

147. При розгляді окремих VASP чи конкретних продуктів, послуг чи видів діяльності із ВА, наглядові органи повинні брати до уваги рівень ризику, пов'язаного з продуктами та послугами, бізнес моделями, механізмами корпоративного управління, фінансовою та бухгалтерською звітністю, каналами постачання, профілями клієнтів, географічним розташуванням, рівнем комплаєнсу заходам з ПВК/ФТ VASP, а також ризиками, що відносяться до окремих токенів та продуктів ВА, які потенційно можуть заплутати операції та перешкодити спроможності VASP та наглядових органів імплементувати ефективні заходи з ПВК/ФТ. Наглядові органи влади повинні також звернути увагу на заходи з контролю, які є у VASP, в тому числі на якість політики VASP з управління ризиками чи на функціонування механізмів внутрішнього нагляду. Інша інформація, яка може бути важливою у контексті ПВК/ФТ, включає придатність та сумлінність функцій управління та комплаєнсу у VASP.

148. Деяка вищезгадана інформація може бути зібрана через пруденційні наглядові органи у країнах, де VASP чи інший підзвітний суб'єкт, що долучився до діяльності з ВА, є об'єктом пруденційного регулювання (*тобто* коли VASP є традиційною ФУ, що підпорядковуються Основним Принципам[21], такою як банк, страхова компанія, постачальник послуг з цінними паперами або інвестиційна компанія), який, в такому разі, включає відповідний обмін інформацією та співпрацю між пруденційними наглядовими органами з ПВК/ФТ, особливо, коли відповідальність покладається на окремі агентства. В інших моделях регулювання, як в тих, що зосереджуються на ліцензуванні та реєстрації VASP на національному рівні, але мають спільний нагляд та правозастосування на державному рівні, до обміну інформацією необхідно включати обмін результатами досліджень.

149. Коли це необхідно, інформація від інших зацікавлених сторін, таких як наглядові органи (в тому числі закордонні наглядові органи та наглядові

21 У відповідності до Рекомендацій FATF, під «основні принципи» розуміються Основні Принципи Ефективного Банківського Нагляду, що випущені Базельським Комітетом з Банківського нагляду; Цілі та Принципи Регулювання Ринку Цінних паперів, що випущені Міжнародною Організацією Комісій з Цінних Паперів; а також Принципи Нагляду за Страховою діяльністю, що випущені Міжнародною Асоціацією Органів Нагляду за Страхуванням.

органи за платіжними системами й інструментами, а також за цінними паперами, сировиною та деривативами), ПФР та правоохоронні органи також може бути корисною для наглядових органів у визначенні ступеню ефективності управління ризиками ВК/ФТ, до яких існує схильність, що здійснює VASP. Деякі режими, як ті, що вимагають тільки реєстрацію (без серйозної перевірки бекграунду), все ще можуть дозволити правоохоронним органам та регулятором - залишатись обізнаними про існування VASP, його ділової діяльності, конкретні продукти чи послуги ВА та/або його контрольні пакети акцій.

150. Наглядові органи повинні періодично переглядати свою оцінку профілів ризику як сектору VASP в цілому, так і самих VASP окремо, а також тоді, коли існує суттєва зміна обставин чи з'являються нові відповідні загрози. Приклади існуючих наглядових практик за VASP чи сектором VASP в цілому, а також приклади країн, що стосуються ризиків ВК/ФТ, пов'язаних з конкретним продуктом, послугою чи моделлю бізнесу ВА, можна знайти у Розділі V цього Керівництва.

Пом'якшення Ризиків ВК/ФТ

151. Рекомендації FATF вимагають від наглядових органів направляти більше наглядових ресурсів та надавати більшого пріоритету сферам підвищеного ризику ВК/ФТ. Це означає, що наглядові органи повинні визначити частоту та інтенсивність періодичних оцінок, базуючись на рівні ризику ВК/ФТ, до якого є схильним сектор чи окремий VASP. Наглядові органи повинні надавати пріоритет потенційним сферам підвищеного ризику або в межах окремого VASP (*напр.,* до конкретного продукту, послуги чи напрямку ділової діяльності, які пропонує VASP, такі як конкретні ВА чи послуги ВА, на кшталт AEC чи міксерів та тумблерів, які можуть сильніше заплутати операції чи підірвати спроможність VASP імплементувати заходи з CDD), або по відношенню до VAS, що діє в якомусь конкретному секторі (*напр.,* по відношенню до VASP, який тільки чи переважно сприяє фінансовій діяльності з обміну віртуальних активів на віртуальні, або який пропонує конкретні продукти чи послуги з ВА, що заплутують операції, або по відношенню до VASP, який сприяє переказам ВА від імені свого клієнта до окремого користувача, який не є клієнтом іншої регульованої установи). Якщо юрисдикція вирішить класифікувати увесь сектор, як такий, що має підвищений ризик, країни все ще повинні будуть розуміти та бути готовими надати певні пояснення та деталі щодо категоризації окремих VASP у секторі, базуючись на їх клієнтській базі, країнах з якими укладаються угоди та їх контролі з ПВК/ФТ.

152. Також важливо, щоб компетентні органи влади визнавали, що у ризик-орієнтованому режимі не усі VASP запровадять ідентичний контроль з

ПВК/ФТ і те, що поодинокі, мимовільні та ізольовані інциденти з переказу чи обміну незаконних доходів не обов'язково будуть говорити про відсутність цілісності у контролі VASP з ПВК/ФТ. З іншого боку, VASP мають розуміти, що гнучкий ризик-орієнтовний підхід не звільняє їх від застосування ефективних засобів контролю з ПВК/ФТ.

153. До прикладів шляхів, якими наглядові органи можуть коригувати свій підхід, включають:

a) *Регулювання типу нагляду чи моніторингу з ПВК/ФТ:* наглядові органи повинні використовувати, як зовнішній, так і внутрішній доступ до усієї інформації щодо відповідних ризиків та комплаєнсу. Разом з тим, в межах, дозволених їх режимом, наглядові органи можуть визначати правильне поєднання виїзного та невиїзного нагляду чи моніторингу за VASP. Невиїзного нагляду, самого по собі, може бути недостатньо у ситуаціях з підвищеним ризиком. Проте, коли результати попередньої перевірки (виїзної чи невиїзної) говорять про низький ризик ВК/ФТ, ресурси можуть бути розподілені для зосередження на VASP, що мають вищий ризик. У такому випадку, VASP, що мають низький ризик, можуть бути перевірені без виїзду на місце, наприклад через перевірку операцій та заповнення запитальника.

b) *Регулювання частоти та природи здійснення поточного нагляду чи моніторингу з ПВК/ФТ:* наглядові органи повинні коригувати частоту перевірок з ПВК/ФТ у відповідності до виявлених ризиків та комбінувати періодичні огляди зі спеціальними перевірками у сфері ПВК/ФТ, коли виникають проблеми. (*напр.,* як результат доносу, надходження інформації від правоохоронних органів, аналізу фінансових звітів чи інших результатів здійснення нагляду). Інші ризик-орієнтовні підходи до нагляду можуть включати розгляд географічного розташування, статусу реєстрації чи ліцензії, клієнтську базу, тип операцій (*напр.,* віртуальні/фіатні чи віртуальні/віртуальні операції), тип ВА, кількість рахунків чи гаманців, дохід, пропоновані продукти чи послуги (*напр.,* більш прозорі послуги проти тих продуктів та послуг, що заплутують операції, такі як AEC), попередню історію з комплаєнсу та/або суттєві зміни в керівництві.

c) *Регулювання інтенсивності здійснення нагляду чи моніторингу з ПВК/ФТ:* наглядові органи повинні

визначитись з відповідним обсягом чи рівнем перевірки, у відповідності до виявлених ризиків, з метою оцінити належність політик та процедур VASP, які розроблені для попередження використання VASP в злочинних цілях. Приклади більш інтенсивного нагляду можуть включати деталізовану перевірку системи та файлів для перевірки впровадження та адекватності оцінки ризиків VASP, політик та процесів зі звітування та ведення обліку, проведення зовнішнього аудиту, розмови з операційним персоналом, старшими керівниками та Радою Директорів, коли це необхідно.

154. Наглядові органи повинні використовувати свої висновки для перегляду та оновлення своїх оцінок ризику ВК/ФТ та, коли необхідно, для вирішення питання, чи залишились їх підхід до нагляду з ПВК/ФТ, правила та керівництва актуальними. Наглядові органи повинні повідомляти про свої висновки VASP, тоді коли це доречно, у відповідності до будь-яких стандартів чи вимог стосовно конфіденційності такої інформації, для того, аби надати їм можливість посилити якість свого ризик-орієнтованого підходу.

Загальний Підхід

155. Наглядові органи повинні розуміти ризики ВК/ФТ, з якими стикаються VASP, або які пов'язані із сектором VASP. Наглядові органи повинні мати комплексне розуміння ліній підвищеного та низького ризиків у проведенні діяльності із конкретним продуктом, послугою ВА, з особливо глибоким розумінням продуктів, послуг та видів діяльності із підвищеним ризиком.

156. Наглядові органи повинні переконатись, що їх персонал оснащений для оцінки політик, процедур та контролю VASP в належний спосіб та пропорційно, з точки зору оцінки ризиків та процедур з управління ризиками VASP. Для підтримки розуміння наглядових органів щодо загальної сили заходів у секторі VASP, країни повинні розглянути можливість проведення порівняльного аналізу програм VASP з ПВК/ФТ, для того аби їх судження щодо якості контролю з боку окремого VASP, були краще інформаційно обґрунтовані.

157. У контексті ризик-орієнтованого підходу, наглядові органи повинні визначитись, чи комплаєнс з ПВК/ФТ та програма з управління ризиками у VASP є достатніми для (i) відповідності регуляторним вимогам; та (ii) належного та ефективного пом'якшення й управління відповідними ризиками. При цих діях, наглядові органи повинні взяти до уваги оцінку ризиків самого VASP. Якщо мова йде про VASP, який діє у декількох

юрисдикціях через наявність декількох ліцензій чи реєстрацій, наглядовий орган, який надав ліцензію чи зареєстрував VASP, враховуючи транскордонну природу діяльності з ВА, повинен розглянути ризики, до яких цей VASP схильний, а також те, в якій мірі ці ризики пом'якшуються в належний спосіб.

158. В рамках своїх процедур перевірки, наглядові органи повинні повідомляти про свої результати та висновки щодо контролю з ПВК/ФТ, що здійснюється окремими VASP, а також чітко повідомляти про свої очікування щодо заходів, які мають бути вжиті VASP для того, аби відповідати діючій законодавчій та нормативній базі. У юрисдикціях, де фінансова діяльність із ВА може стосуватись декількох компетентних органів, наглядові органи у юрисдикції також повинні комунікувати поміж собою, для ефективного та чіткого донесення своїх очікувань до VASP та інших підзвітних суб'єктів, що можуть бути залучені до діяльності із ВА або до надання продуктів та послуг ВА. Це особливо важливо у контексті VASP, що долучаються до різних типів діяльності із ВА (*напр.,* послуги з переказу грошей чи вартості, або діяльність із цінними паперами, товарами чи деривативами, що виражені у ВА) або до фінансової діяльності із ВА, яка може стосуватись регуляторів банків, ринку цінних паперів чи інших.

Керівні принципи

159. Наглядові органи повинні повідомляти про свої очікування щодо відповідності VASP своїм правовим та регуляторним зобов'язанням та можливості залучення до консультативного процесу із відповідними зацікавленими сторонами. Подібні керівні принципи можуть бути у формі загальних вимог, що базуються на бажаних результатах, ризик-орієнтованих зобов'язаннях та інформації щодо того, як наглядові органи інтерпретують відповідне законодавство чи норми про те, як VASP краще застосовувати відповідний контроль з ПВК/ФТ.

160. Наглядові органи та інші компетентні органи влади можуть розглядати керівні принципи та внесок технічних експертів ВА з метою більш глибокого розуміння відповідних бізнес-моделей та операцій VASP, їх потенційної схильності до ризиків ВК/ФТ, а також до ризиків ВК/ФТ, що пов'язані з конкретними типами ВА або видами діяльності з ВА, та для того, аби зробити усвідомлене судження щодо існуючих або необхідних до впровадження заходів з пом'якшення.

161. Як було обговорено раніше, надання керівних принципів та фідбеку сектору VASP є дуже важливим і обов'язковим у відповідності до Рекомендації 34. Керівні принципи можуть включати кращі практики, які

дозволять VASP проводити оцінку та розвивати системи з пом'якшення ризику та управління комплаєнсом, аби відповідати своїм правовим та регуляторним зобов'язанням. Підтримка постійної та ефективної комунікації між наглядовими органами та VASP є важливим компонентом успішної імплементації ризик-орієнтованого підходу.

162. Наглядові органи за VASP повинні також розглянути можливість взаємодії з іншими відповідними національними регуляторними та наглядовими органами, для того аби забезпечити узгоджене тлумачення правових зобов'язань VASP та сприяти рівним умовам гри, в тому числі між різними VASP та між VASP і іншими підзвітними суб'єктами, такими як ФУ та ВНУП. Подібна координація особливо важлива, коли за нагляд відповідає декілька наглядових органів (*напр.,* коли пруденційний наглядовий орган та наглядовий орган з ПВК/ФТ це різні агентства або різні управління в одному агентстві). Це особливо актуально у контексті VASP, які надають різні продукти чи послуги, або долучаються до різних видів фінансової діяльності, які можуть входити у сферу компетенції різних регуляторних чи наглядових органів в межах однієї юрисдикції. Кілька джерел керівних принципів не повинні створювати можливостей для регуляторного арбітражу, лазівок чи зайвої плутанини серед VASP. Також, коли це можливо, регуляторні та наглядові органи у юрисдикції повинні підготувати спільні керівні принципи.

Навчання

163. Навчання є важливим для персоналу наглядових органів для розуміння сектору VASP та різних існуючих бізнес моделей. Зокрема, наглядові органи повинні забезпечити, щоб персонал проходив навчання з оцінки якості оцінки ризиків ВК/ФТ у VASP, а також для прийняття рішень щодо належності, пропорційності, ефективності та продуктивності політик, процедур та внутрішнього контролю VASP.

164. Навчання повинно дозволити працівникам наглядових органів формувати ґрунтовні судження щодо якості оцінки ризиків VASP та належності й пропорційності контролю з ПВК/ФТ у VASP. Воно також повинно бути націлено на досягнення послідовності у наглядовому підході на національному рівні, у випадках, коли існує декілька компетентних наглядових органів чи коли наглядова модель децентралізована чи має фрагментарний характер.

165. Аналогічно, країни повинні розглянути можливість надання навчання державному та приватному секторам, а також ширшої співпраці для подальшого підняття обізнаності як серед операційних, так і серед інших компетентних органів влади та у галузі в цілому, щодо різних проблемних питань, які пов'язані із ВА та діяльністю VASP.

Обмін Інформацією

166. Обмін інформацією між державним та приватним сектором є важливим і повинен формувати цілісну стратегію країни з протидії ВК/ФТ у контексті ВА та діяльності VASP. Державні органи влади повинні ділитись інформацією про ризик, для кращого підґрунтя оцінки ризиків VASP. До типу інформації, що стосується ризиків у сфері ВА, якими державний та приватний сектор можуть обмінюватись, повинні бути включені:

    a) Оцінка ризиків ВК/ФТ;

    b) Типології та методології того, як використовуються VASP в цілях відмивання коштів та фінансування тероризму, пріоритету одних конкретних механізмів ВА над іншими (*напр.,* переказ ВА чи діяльність з обміну на противагу діяльності з емісії ВА у контексті відмивання коштів чи фінансування тероризму) чи ВА у більш загальному вигляді;

    c) Загальний фідбек щодо якості та корисності STR та інших відповідних звітів;

    d) Інформація щодо підозрілих індикаторів, пов’язаних із діяльністю з ВА чи операціями VASP.

    e) Коли це доречно, цільові незасекречені розвіддані, у відповідності до відповідних гарантій, таких як угоди про конфіденційність; та

    f) Країни, особи чи організації, чиї активи або операції мають бути заморожені у відповідності до цільових фінансових санкцій, як це вимагається Рекомендацією 6.

167. Більш того, країни повинні розглянути питання того, яким чином вони розповсюджуватимуть інформацію серед приватного сектору із метою допомогти йому, в тому числі й VASP, краще розуміти природу інформаційних запитів від правоохоронних органів чи інших запитів від органів влади щодо отримання більшої інформації, чи з метою допомогти окреслити природу запиту, щоб VASP, коли це буде необхідно, міг надати більш точну та конкретну інформацію компетентним органам влади.

168. Національна співпраця та обмін інформацією між наглядовими органами банківського сектору, ринку цінних паперів, ринку біржових товарів, деривативів та наглядовими органами за сектором VASP; між правоохоронними органами, розвідкою, ПФР на наглядовими органами за

сектором VASP; а також між ПФР та наглядовими органами за сектором VASP також є дуже важливими для здійснення ефективного моніторингу та нагляду за VASP.

169. Аналогічно, згідно з Рекомендацією 40, транскордонний обмін інформацією між органами влади та приватним сектором з їх іноземними контрагентами є критично важливим у секторі VASP, враховуючи транскордонну природу та можливе одночасне охоплення VASP декількох юрисдикцій.

РОЗДІЛ IV – ЗАСТОСУВАННЯ СТАНДАРТІВ FATF ДО VASP ТА ІНШИХ ПІДЗВІТНИХ СУБ'ЄКТІВ, ЩО ЗАЛУЧЕНІ ДО ДІЯЛЬНОСТІ З ВА

170. Рекомендації FATF застосовуються як до країн, так і до VASP та інших підзвітних суб'єктів, що надають послуги чи проводять фінансові операції, пов'язані із ВА, в тому числі до банків, брокерів за операціями з цінними паперами та інших ФУ. Відповідно, Розділ IV надає додаткові керівні принципи спеціально для VASP та інших підзвітних суб'єктів, що можуть бути залучені до діяльності із ВА.

171. Окрім виявлення й оцінки своїх ризиків ВК/ФТ та вжиття необхідних заходів задля їх пом'якшення, як це описано у **Рекомендації 1**, VASP та інші підзвітні суб'єкти повинні застосовувати усі попереджувальні заходи з Рекомендацій 9-21, як це зазначено вище у Розділі III, в тому числі й в контексті здійснення CDD при залученні до будь-якої діяльності з ВА. Аналогічно, ВНУП повинні бути обізнані про свої зобов'язання з ПВК/ФТ, коли долучаються до діяльності з ВА, як це викладено у ПЗР. 15 та описано у підрозділі 3.1.9.

172. Читачі цього Керівництва повинні відмітити, що параграфи нижче, які відносяться до окремих попереджувальних заходів та Рекомендацій FATF, призначені для надання додаткових конкретних вказівок для VASP та інших підзвітних суб'єктів щодо певних питань. Відсутність спеціального пункту для кожної Рекомендації FATF в рамках превентивних заходів, що наведені у Розділі III, не означає, що відповідні Рекомендації чи попереджувальні заходи, що описані у них, можуть не застосовуватись VASP чи іншими підзвітними суб'єктами, які надають послуги чи беруть участь у діяльності з ВА.

173. **Рекомендацією 10** викладено необхідні заходи з CDD, що ФУ мають імплементувати для усіх клієнтів, в тому числі ідентифікацію та верифікацію клієнта із використанням надійних, незалежних джерел даних чи інформації; ідентифікацію бенефіціарного власника; розуміння та отримання інформації про мету та природу ділових відносин; проведення постійної належної перевірки відносин та вивчення операцій.

174. Рекомендація 10 також описує сценарії, у відповідності до яких ФУ зобов'язані вживати заходів з CDD, в тому числі в контексті започаткування ділових відносин, проведення окремих операцій на суму понад визначений поріг (1 000 USD/EUR для операцій з ВА), проведення окремих операцій, що, згідно з Рекомендацією 16 та її Пояснювальною Запискою, є електронними переказами, коли є підозра щодо ВК/ФТ, або коли у ФУ є сумніви щодо достовірності та відповідності попередньо отриманої інформації відносно даних клієнта. Хоча країни можуть ввести

до законодавства мінімальний поріг у 1 000 USD/EUR для операцій із ВА, які здаються окремими (як описано у Розділі III), або для переказів ВА, усі з яких розглядаються як транскордонні кваліфіковані електронні перекази в цілях імплементації Рекомендації 16, необхідно підкреслити, що банки, брокери та інші ФУ повинні дотримуватись своїх відповідних порогових значень CDD, при участі у діяльності з ВА. ВНУП, такі як казино, що долучаються до діяльності з ВА, повинні застосовувати мінімальних поріг у 1 000 USD/EUR для окремих операцій та операцій, що є електронними переказами, як описано у Розділі III і як це обговорено нижче. Як відзначено у Розділі III в контексті країн, VASP, при встановленні своїх оперативних процедур та процесів, слід розглянути, як вони можуть визначити та впевнитись у тому, що операції насправді проводяться лише разово чи періодично, а не на постійній основі.

175. Хоча мінімальне порогове значення, при перевищенні якого казино та торговці дорогоцінними металами та камінням мають проводити CDD для окремих операцій та операцій, що є окремими електронними переказами, складає 3 000 USD/EUR та 15 000 USD/EUR відповідно, коли ВНУП долучаються до будь-якої діяльності VASP чи операцій з ВА, вони стають об'єктом застосування стандартів CDD, що визначені у ПЗР. 15 (*тобто*, мінімальний поріг для таких операцій складає 1 000 USD/EUR).

176. В незалежності від природи відносин чи операцій з ВА, VASP та інші підзвітні суб'єкти повинні мати діючи процедури з CDD, які ефективно імплементуються та використовуються для виявлення та верифікації особистості клієнта на основі ризику, в тому числі при започаткуванні ділових відносин з цим клієнтом; коли існує підозра ВК/ФТ, в незалежності від будь-якого звільнення від порогових значень; а також коли існують сумніви щодо достовірності та достатності попередньо отриманих ідентифікаційних даних.

177. Як і інші підзвітні суб'єкти, при проведенні CDD для виконання своїх зобов'язань у відповідності до Рекомендації 10, VASP повинні збирати та перевіряти ідентифікаційну інформацію про клієнта у відповідності до національного законодавства. Зазвичай, до необхідної ідентифікаційної інформації про клієнта включається ім'я клієнта та інші ідентифікатори, такі як фізична адреса, дата народження та унікальний ідентифікаційний код (*напр.,* ІПН чи номер паспорту). В залежності від вимог національного законодавства, VASP також заохочуються до збирання додаткової інформації, що допомагає їм у підтвердженні особистості клієнта при започаткуванні ділових відносин; у засвідченні особи клієнта для доступу до рахунку; у визначенні ділового профілю ризиків клієнта та проведенні постійної належної перевірки відносно ділових відносин; у пом'якшенні ризиків ВК/ФТ, пов'язаних з клієнтом та його фінансовою діяльністю. Така додаткова та неосновна інформація про особу, яку деякі

VASP вже збирають, може включати, наприклад, IP-адресу із пов'язаною позначкою часу; дані геолокації, ідентифікатори пристроїв; адреси гаманців ВА та хеши операцій.

178. Для операцій із ВА, верифікація інформації про клієнта та бенефіціарного власника має бути завершена до, або під час, встановлення відносин.[22]

179. На основі цілісного уявлення про інформацію, отриману в контексті застосування заходів з CDD – що може включати традиційну та додаткову інформацію, як описано вище – VASP та інші підзвітні суб'єкти повинні мати можливість підготувати профіль ризику клієнта у відповідних справах. Профіль клієнта визначить рівень та тип необхідного поточного моніторингу та підтримає рішення VASP щодо того, чи варто започатковувати/продовжувати ділові відносини чи краще їх припинити. Профілі ризику можуть застосовуватись на рівні клієнтів (*напр.,* природа та обсяг торгової діяльності, походження розміщених віртуальних коштів) або на рівні групи, коли група клієнтів показує однорідні характеристики (*напр.,* клієнти проводять операції з ВА однакового типу або в одному виді ВА). VASP повинні періодично проводити оновлення профілів ризику клієнтів у ділових відносинах для того, аби застосовувати належний рівень CDD.

180. Якщо VASP, дізнавшись адреси ВА, які є у клієнтів, вирішив не встановлювати чи не продовжувати ділові відносини або не взаємодіяти через підозру у ВК/ФТ, VASP повинен розглянути можливість відкриття доступу до свого «чорного списку адрес гаманців», з дотриманням законів тієї юрисдикції де VASP діє. VASP повинен зберегти адресу гаманця свого клієнта чи контрагента у подібних доступних чорних списках адрес гаманців, виконуючи свій постійний моніторинг. VASP повинен проводити власну оцінку ризиків та визначати чи необхідно застосовувати додаткові пом'якшувальні чи превентивні заходи, якщо є позитивний результат.

181. VASP та інші підзвітні суб'єкти, що долучені до діяльності із ВА, можуть скорегувати міру застосування CDD, в межах, що дозволені або вимагаються їх національними регуляторними вимогами, у відповідності до ризиків ВК/ФТ, пов'язаних з окремими діловими відносинами, продуктами чи послугами, а також видами діяльності з ВА, як це обговорено вище в рамках застосування Рекомендації 1. VASP та інші підзвітні суб'єкти повинні збільшувати кількість чи тип інформації, що збирається або ступінь перевірки такої інформації, коли ризик, пов'язаний із діловими відносинами чи діяльністю із ВА є підвищеним, як це описано у Розділі III. Аналогічно, VASP та інші підзвітні суб'єкти

22 *Див. також* Керівництво щодо ВВ від 2015 року, параграф 45.

можуть також спрощувати ступінь застосування заходів з CDD, коли ризик, пов'язаний із діловими відносинами є низьким. Разом з тим, VASP та інші підзвітні суб'єкти не мають права застосовувати спрощену CDD або виключення до інших превентивних заходів виключно на основі того, що фізична чи юридична особа надає послуги чи проводить діяльність з ВА на поодинокій або дуже обмеженій основі (ПЗР. 1.6(b)). Більш того, спрощені заходи CDD неприпустимі, коли є підозра відмивання коштів чи фінансування тероризму або коли застосовуються конкретні сценарії з підвищеним ризиком (див. Розділ III для роз'яснення щодо потенційних ситуацій з підвищеним ризиком).

182. Постійний моніторинг на основі ризику означає перевірку операцій для визначення, чи відповідають ці операції інформації VASP (або іншого підзвітного суб'єкта) щодо клієнта та природи й мети здійснення ділових відносин. До моніторингу операцій також входить виявлення змін у профілі клієнта (*напр.,* поведінка клієнта, використання продуктів та залучені суми) та зберігання його актуальним, що може вимагати застосування розширених заходів з CDD. Моніторинг операцій є важливим компонентом в ідентифікації операцій, що потенційно є підозрілими, в тому числі в контексті операцій з ВА. Операції, що не відповідають поведінці, яка очікується від клієнта у відповідності до його профілю, або яка має відхилення від звичайного шаблону, можуть бути потенційно підозрілими.

183. Моніторинг має проводитись на постійній основі і може бути спровокований певними операціями. Якщо регулярно проводяться операції із великими сумами, автоматичні системи можуть бути єдиним реальним методом моніторингу операцій, а позначені системою операції вже проходять через експертний людський аналіз для визначення того, чи є ця операція підозрілою. VASP та інші підзвітні суб'єкти повинні розуміти свої правила роботи, регулярно перевіряти їх цілісність та переконуватись, що вони враховують продукти чи послуги або фінансові активи ВА для виявлених ризиків ВК/ФТ, пов'язаних із ВА.

184. VASP та інші підзвітні суб'єкти повинні коригувати ступінь та глибину свого моніторингу у відповідності з їх інституційною оцінкою ризиків та профілями ризику окремих клієнтів. Посилений моніторинг може вимагатись для ситуацій із підвищеним ризиком (що описано у Розділах II та III) та у межах, що виходять за рамки миттєвих переказів між VASP та клієнтом, контрагентом. Адекватність систем моніторингу та фактори, що привели VASP та інших підзвітних суб'єктів для зміни рівня моніторингу мають регулярно переглядатись для збереження актуальності до програм ризику з ПВК/ФТ.

185. При ризик-орієнтованому підході, моніторинг дозволяє VASP чи іншим підзвітним суб'єктам створювати монетарний чи інший поріг для визначення того, які види діяльності будуть переглянуті. Визначені ситуації чи порогові значення, що використовуються для цих цілей, мають постійно переглядатись для визначення їх відповідності встановленому рівню ризику. VASP та інші підзвітні суб'єкти повинні чітко встановити та задокументувати критерії та параметри, що використовуються для сегментації клієнтів та для розподілу рівня ризику для кожної групи клієнтів. Критерії, що застосовуються для вирішення частоти та інтенсивності перевірок різних груп клієнтів (або навіть продуктів ВА), також мають бути прозорими. З цією метою, VASP та інші підзвітні суб'єкти повинні належним чином записувати, зберігати та ділитись інформацією щодо результатів своїх перевірок, а також щодо піднятих та вирішених питань, із національними компетентними органами влади та іншими зацікавленими сторонами.

186. **Рекомендація 12.** Для національних PEP[23] та PEP міжнародних організацій[24], підзвітні суб'єкти, такі як VASP, повинні вживати достатніх заходів аби визначити чи є клієнт або бенефіціар національним PEP чи PEP міжнародної організації, а потім оцінити ризик ділових відносин. Для ділових відносин із підвищеним ризиком, VASP та підзвітні суб'єкти повинні вжити додаткових заходів, відповідних до тих, що застосовуються до іноземних PEP, включаючи виявлення джерела статків та коштів.[25]

187. **Рекомендація 16.** Як зазначено у Розділі III, постачальники у цій сфері повинні відповідати вимогам Рекомендації 16, включаючи зобов'язання збирати, утримувати та передавати необхідну інформацію про відправника та отримувача, що пов'язана із переказом ВА, для того аби виявити та прозвітувати про підозрілу операцію, вжити заходів із замороження та заборони операції для визначених осіб і установ. Вимоги застосовуються як до VASP, так і до інших підзвітних суб'єктів, таких як ФУ, коли вони відправляють чи отримують перекази ВА від імені клієнта.

188. FATF є технологічно-нейтральною і не наказує використовувати конкретний технологічний чи програмний підхід, який постачальники мають запровадити для дотримання Рекомендації 16. Як зазначено

---

23 «Національні PEP» - особи, яких у країні наділили повноваженнями виконувати відповідними державні функції, наприклад Голови держави чи уряду, високопоставленого політика, міністра, судового чи військового високопосадовця, виконавчих директорів державних корпорацій, важливих партійних діячів (Словник FATF).

24 «Особи, яких наділили важливими функціями у міжнародній організації», відноситься до найвищого керівництва, *тобто* директори, заступники директорів та члени правління або еквівалентні посади (Словник FATF).

25 Більше інформації щодо PEP зазначено у *Керівництві FATF щодо Публічних Діячів (Рекомендації 12 та 22)* від 2013 року.

раніше, будь-яке технологічне чи програмне рішення є допустимим якщо воно дозволяє установі відправнику чи отримувачу відповідати своїм вимогам з ПВК/ФТ. Наприклад, рішенням щодо збору, утримування та передачі необхідної інформації (на додаток до дотримання різних інших вимог Рекомендації 16) може бути код, що вбудований до переказу ВА і лежить в основі DLT у протоколі операції, або який працює поверх платформи DLT (*напр.,* використовуючи розумний договір, мультипідпис або будь-яку іншу технологію); незалежна (*тобто* не DLT) платформа обміну повідомленнями або інтерфейс прикладного програмування (API); або інший ефективний засіб для дотримання заходів Рекомендації 16.

189. VASP та інші підзвітні суб'єкти при проведенні переказів ВА, чи як установа відправник чи як установа отримувач, повинні розглянути питання того, як вони можуть використовувати існуючи комерційно доступні технології для дотримання вимог Рекомендації 16, а особливо вимогам, що зазначені у ПЗР. 15, параграфі 7(b). До прикладів існуючих технологій, які постачальники можуть розглянути в якості фундаменту для ідентифікації отримувачів переказів ВА, а також для надсилання необхідної інформації щодо відправника та отримувача на платформу DLT у режимі реального часу, відносяться:

a) *Відкриті та приватні ключі*, які створюються у парі для кожної установи, що бере участь у переказі та шифрує й дешифрує інформацію під час початкової стадії переказу, таким чином, щоб тільки відправник та отримувач могли дешифрувати та прочитати інформацію, при цьому відкритий ключ є доступним для кожного, в той час як приватний ключ відомий тільки тому, хто створив ключі;

b) *Підключення до Захисту на Транспортному Рівні / Рівня Захищених Сокетів (TLS/SSL),* які використовують відкриті та приватні ключі серед сторін при встановленні зв'язку та захищають майже всі перекази в інтернеті, в тому числі e-mail, перегляд веб-сторінок, логіни та фінансові операції, забезпечуючи, що будь-яка інформація, яка пройде між веб-сервером та браузером залишиться приватною та захищеною;

c) *Сертифікати X.509,* які є цифровими сертифікатами, що управляються органами сертифікації, які використовують стандарт X.509 PKI для підтвердження того, що відкритий ключ належить користувачу, комп'ютеру чи послузі вказаної у сертифікаті, та які використовуються у всьому світу в державному та приватному секторах;

d) *Атрибутів сертифікатів X.509*, які можуть кодувати атрибути (такі як ім'я, дата народження, адреса та унікальний ідентифікаційний номер), криптографічно приєднуються до сертифікату X.509 та управляються відповідними органами влади;

e) *Технології API,* які забезпечують процедури, протоколи та інструменти для побудови програмних додатків та визначають, як програмні компоненти повинні взаємодіяти; а також

f) Інші комерційно доступні технології чи потенційні програмні рішення, чи рішення з обміну даними.

190. Як зазначено у ПЗР. 15, параграфі 7(b), дуже важливо, щоб VASP та інші підзвітні суб'єкти, які залучені до переказів ВА, передавали необхідну інформацію у захищений спосіб, так аби захистити інформацію про клієнта, пов'язану із переказом ВА, від неавторизованого розкриття та для того, аби дозволити установі отримувача ефективно відповідати своїм зобов'язанням з ПВК/ФТ, в тому числі виявляти підозрілі перекази ВА, вживати заходи із замороження та забороняти проведення операцій із визначеними особами та установами. Більш того, як висвітлено у Розділі III, важливо, щоб провайдери подавали необхідну інформацію невідкладно – тобто одночасно із самим переказом – особливо, враховуючи транскордонну природу, глобальне охоплення та швидкість проведення операції при діяльності із ВА.

191. **Рекомендація 18.** Успішна імплементація та ефективне використання ризик-орієнтованого підходу до ПВК/ФТ, залежить від сильного управлінського менеджменту, яке включає нагляд за розвитком та впровадженням ризик-орієнтованого підходу у секторі VASP. Рекомендація 18 також вимагає, коли це необхідно, обмінюватись всередині групи інформацією стосовно незвичних операцій чи нетипової діяльності.

192. VASP та інші підзвітні суб'єкти повинні мати програми та системи з ПВК/ФТ, завдяки яким можуть управляти та пом'якшувати свої ризики. Природа та ступінь контролю з ПВК/ФТ буде залежати від ряду факторів, в тому числі природи, масштабу та складності ділової активності VASP, різноманітності його операцій, в тому числі географічної різноманітності, клієнтської бази, профілю продуктів та видів діяльності, а також рівень ризику у кожній зі сфер його діяльності.

193. **Рекомендація 20**. VASP та інші підзвітні суб'єкти, які залучені до діяльності із ВА або надають продукти та послуги з ВА, повинні мати

можливість позначати для подальшого аналізу будь-які незвичні або підозрілі операції – в тому числі ті, де залучені або що стосуються ВА - чи рухи коштів, або ж діяльність, що вказує на потенційне залучення до незаконної діяльності, в незалежності від того, яка природа операції: фатна-фатна, віртуальна-віртуальна, фіатна-віртуальна, віртуальна-фіатна. VASP та інші підзвітні суб'єкти повинні мати належні системи, щоб такі кошти чи операції своєчасно перевірялись та аби можна було визначити чи є ці кошти та операції підозрілими.

194. VASP та інші підзвітні суб'єкти повинні негайно звітувати про кошти чи операції, в тому числі про ті, що пов'язані із ВА та/або постачальниками, які є підозрілими для ПФР, у спосіб, визначений компетентним органом влади. Процеси, які здійснюють VASP та інші підзвітні суб'єкти для опрацювання своїх підозр та, зрештою, надання звіту до ПФР, також повинні відображати це. Хоча VASP та інші підзвітні суб'єкти можуть застосовувати політики та процеси, які ведуть їх до формування підозри на основі чуттєвості до ризику, вони все одно повинні звітувати про свої підозри з ВК/ФТ як тільки вони сформовані та в незалежності від суми операції чи факту завершення операції. Саме тому зобов'язання VASP та інших підзвітних суб'єктів звітувати про підозрілі операції не базуються на ризику, а сам факт звітування не звільняє їх від інших зобов'язань з ПВК/ФТ. Більш того, VASP та інші підзвітні суб'єкти повинні відповідати вимогам щодо подання STR навіть тоді, коли діють у різних юрисдикціях.

195. Відповідно до ПЗР. 15 та стосовно Рекомендації 16, у випадку, коли VASP (чи інший підзвітний суб'єкт) контролює як отримувача так і відправника ВА чи електронного переказу, VASP чи інший підзвітний суб'єкт повинен врахувати усю інформацію з обох боків, для того аби визначити, чи ця інформація надає підстави для підозри, та, за необхідності, відправити STR відповідному ПФР й зробити інформацію щодо операції доступною для ПФР. Брак інформації з боку відправника чи отримувача повинен розглядатись, під час оцінки переказу ВА чи переказу до якого залучено VASP, як фактор, що може бути підозрілим та як такий, що має бути повідомлений до ПФР. Те ж саме відноситься до інших підзвітних суб'єктів, таких як традиційні ФУ, що залучені до переказу ВА.

РОЗДІЛ V – ПРИКЛАДИ КРАЇН З РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ ДО ВІРТУАЛЬНИХ АКТИВІВ ТА ПОСТАЧАЛЬНИКІВ ПОСЛУГ З ПЕРЕКАЗУ ВІРТУАЛЬНИХ АКТИВІВ

Ризик-Орієнтований Підхід до Нагляду чи Моніторингу VASP

196. Розділ V надає огляд підходів різних юрисдикцій до регулювання та нагляду за фінансовою діяльністю із ВА та відповідних постачальників послуг, включаючи підхід до створення інструментів та інших заходів для накладання санкцій чи вжиття правозастосовних дій проти осіб, що не відповідають своїм зобов'язанням з ПВК/ФТ, які країни повинні розглядати при розробці чи розширені своєї національної законодавчої бази. Ці країни ще не були оцінені щодо відповідності вимогам, які прописані у ПЗР. 15.

Італія

197. Декрет № 231 від 2007 року, доповнений Законодавчим Декретом №90 від 2017 року, включає провайдерів, залучених до послуг з обміну між ВА та фатними валютами (*тобто* обмінники віртуальних валют), до категорії суб'єктів, які зобов'язані відповідати вимогам з ПВК/ФТ.

198. Від постачальників послуг, що пов'язані з ВА, вимагають зареєструватися у спеціальному розділі реєстру, який веде *«Organismo degli Agenti e dei Mediatori»* (OAM), орган, що реєструє агентів та посередників. Реєстрація є необхідною умовою для постачальників послуг, пов'язаних із ВА, для здійснення своєї діяльності в Італії. На даний момент ведуться роботи по впровадженню реєстру.

199. VASP вважаються підзвітними суб'єктами та підпадають під повний комплекс заходів з ПВК/ФТ.

200. Були запровадженні оновлення до Національної Оцінки Ризиків (НОР) 21 березня 2019 року. Вони включають оцінку ризиків ВК/ФТ, які походять від ВА. Результати оновленої НОР будуть використовуватись для посилення національної стратегії. Підзвітні установи та суб'єкти (фінансові та нефінансові) зобов'язані взяти до уваги результати оновленої НОР для того аби провести/оновити свої оцінки ризиків.

201. STR та подальший аналіз, що проводиться італійським ПФР, дозволяють йому збирати інформацію про: i) VASP, що діють в Італії, в тому числі дані ділової діяльності (типологія послуг, що надаються); розташування; дані щодо бенефіціарного власника, адміністратора та інших пов'язаних суб'єктів; ii) детальну інформацію по окремим операціям (*напр.,* дата,

сума, виконавець, сторони операції та рахунки гаманців); дані щодо залучених банківських рахунків (*напр.,* власник, довірені особи, походження коштів та загальні особливості фінансових потоків); iii) дані економічного профілю клієнта або власника гаманця; інформацію, що корисна для узгодження адрес ВА з особистістю власника ВА; однозначні ідентифікаційні дані (*напр.,* фіскальний код та ІПН); iv) інформація про гаманець чи рахунок (*напр.,* загальна сума ВА, якими володіє один чи більше суб'єктів); деталізована інформація щодо основних рухів ВА, які відслідковуються до одного суб'єкта чи пов'язаних суб'єктів у певний часовий проміжок; виписка по рахунку/гаманцю у форматі, який можна редагувати; та v) вид та основні особливості ВА.

202. З 2015 року Банк Італії попереджає споживачів щодо високого ризику купівлі та/або утримання ВА, а також проводить нагляд над фінансовими посередниками щодо можливих ризиків, пов'язаних з ВА. Зокрема, було випущено застереження для споживачів та проведено обмін інформацією з фінансовими посередниками, за якими здійснюється нагляд (січень 2015 року), а також нове застереження для споживачів, яке нагадало про те, що було випущено трьома Європейськими фінансовими органами влади – Європейською Організацією з Цінних Паперів та Ринків (ESMA), Європейською Банківською Організацією (EBA) та Європейською Організацією зі Страхування та Пенсійного Забезпечення (EIOPA) – у березні 2018 року. Для покращення співпраці із приватним сектором, італійський ПФР випустив Повідомлення від 30 січня 2015 року щодо аномального використання крипто-активів, звертаючись, насамперед, до фінансових установ (*тобто* банків та платіжних установ), а також до операторів азартних ігор, підкреслюючи важливість зосередження їх уваги на можливих аномальних транзакціях, пов'язаних із придбанням чи інвестуванням у крипто-активи, таких як електронні платежі, вкладення та зняття готівкових коштів, використання передплачених карток.

203. ПФР здійснює свій аналіз, зосереджуючись на нових ризиках та виникаючих трендах. Оновлене Повідомлення було випущено у 2019 році для допомоги підзвітним суб'єктам у виконанні їх завдань. Зокрема, ПФР оновила своє Повідомлення від 2015 року щодо аномального використання крипто-активів, надавши більше деталізованої інформації щодо повторюваних елементів, операційних методів та поведінкового профілю ризику, які були виявлені у STR, пов'язаних із ВА. Повідомленням встановлюються особливі інструкції щодо заповнення даних у форматі STR, зокрема по відношенню до інформації про VASP, операції, користувачів/клієнтів та гаманців/рахунків.

204. У грудні 2016 року та липні 2018 року, ПФР публікувало збірки кейсів відмивання коштів та фінансування тероризму, які були виявлені в ході

фінансового аналізу, в тому числі типології пов'язані з аномальним використанням ВА.

Норвегія

205. VASP є об'єктами Закону з ПВК у Норвегії та його вимог із жовтня 2018 року. Відповідне положення постанови з ПВК виглядає наступним чином:

> *Застосування Розділів 1-3 Закону з Протидії Відмиванню Коштів до Віртуальних Валют*
>
> (1) Постачальники послуг з обміну віртуальної валюти та офіційної валюти є підзвітними установами у відповідності до змісту Закону з Протидії Відмиванню Коштів. Відповідно, це застосовується й до послуг зі зберігання віртуальних валют.
>
> (2) Під віртуальною валютою розуміється цифрове вираження вартості, яке випущено не центральним банком чи урядовим органом влади, яке не обов'язково має зв'язок із законно встановленою валютою та не має легального статусу валюти чи грошової одиниці, але приймається як засіб обміну, який можна переказати, розмістити або продати в електронному вигляді.
>
> (3) Під послугами зі зберігання віртуальних валют розуміється зберігання приватного криптографічного ключа від імені клієнта, для переказу, розміщення та торгівлі віртуальною валютою.
>
> (4) Фінансові Наглядові Органи можуть проводити перевірки комплаєнсу Закону з Протидії Відмиванню Коштів у постачальників, зазначених у параграфі 1. Ці постачальники мають бути зареєстровані Фінансовим Наглядовим Органом. При реєстрації має бути надана наступна інформація:
>
> a) ім'я/назва
>
> b) тип установи та номер організації
>
> c) юридична адреса
>
> d) послуги, що пропонуються

е) ім'я, дійсна адреса та ідентифікаційний номер

i) генерального менеджера чи осіб, що займають аналогічні позиції

ii) членів ради директорів чи осіб, що займають аналогічні позиції

iii) будь-якої іншої контактної особи

206. Станом на червень 2019 року вже було зареєстровано шість VASP і більше 20 VASP подали заявки на реєстрацію, але їх заявки очікують на розгляд через недоліки в їх політиках та процедурах з ПВК. Три АТМ з ВА були закриті у листопаді 2018 року після того, як ФНО видав указ щодо припинення подальших протиправних дій, і після того жодні нові АТМ не починали працювати. ФНО тільки розпочне перевірку сектору, але базуючись на заявках на реєстрацію у другій половині 2019 року, стає зрозумілим, що сектор VASP включає широкий перелік дійових осіб, які є різними за своїми розмірами, компетенцією, знанням правил з ПВК та за своїм професіоналізмом.

Швеція

207. Фінансові Наглядові Органи у Швеції визнали біткоїн та ефір як засоби платежу ще 2013 року, що означає, що професійні послуги з обміну є об'єктом режиму з ліцензування[26], а після успішної заявки на отримання ліцензії, нагляду з ПВК/ФТ. Положення не є чітким регулюванням послуг з обміну ВА у сфері ПВК/ФТ (*тобто*, вони не визначені особливим чином у законі), а радше неявним визнанням того, що вони повинні регулюватись. Як тільки обмінник отримає ліцензію, усі види діяльності (*тобто*, не важливо, чи знаходиться під питанням операція з ВА) стають об'єктами регулювання та нагляду з ПВК/ФТ. Було проведено тематичні перевірки. В результаті, частина сектору припинила свою діяльність. VASP надсилали STR до ПФР, і фідбек від оперативних органів влади свідчить про те, що злочинці вирішують перенести свою діяльність до нерегульованих обмінників в інших місцях.

Фінляндія

208. Закон про Постачальників Віртуальних Валют (572/2019) вступив в силу 1 травня 2019 року. Від VASP вимагається проходити реєстрацію

26 Це не зовсім повний режим ліцензування у пруденційному сенсі цього слова, та в цілях ПВК/ФТ він є таким, включаючи належне тестування власників та керівників, а також оцінку того, чи ділова діяльність ведеться у відповідності до нормативно-правових актів з ПВК/ФТ.

(авторизацію) у фінському Фінансовому Наглядовому Органі (ФІН-ФНО).[27] Ті, хто надавав послуги до того, як закон вступив в силу, повинні зареєструватись до 1 листопада 2019 року. Нові гравці у секторі повинні зареєструватись до початку здійснення своєї діяльності. До визначення VASP входять обмінні пункти (як ті, що здійснюють обмін фіатних валют на ВА, так і поміж ВА, а також ті, що здійснюють обмін ВА на інші товари, такі як золото), постачальники гаманців зберігання та ICO. Вимоги до реєстрації включають основні перевірки, вимоги щодо використання коштів клієнтів та прості правила щодо маркетингу (*тобто*, зобов'язання щодо надання усієї відповідної інформації та зобов'язання щодо правдивості інформації). Як визначено у Законі про ПВК (444/2017), VASP є підзвітними суб'єктами і повинні відповідати зобов'язанням з ПВК/ФТ від 1 грудня 2019 року. Оцінка ризиків VASP з ПВК/ФТ та їх процедури й керівні принципи, що стосуються ПВК/ФТ, переглядаються як частина процесу реєстрації.

209. ФІН-ФНО була наділена повноваженнями випускати нормативно-правові акти та керівництва щодо певних видів діяльності VASP. Проект положення ФІН-ФНО було опубліковано для проведення консультацій 21 травня. Проект містить положення щодо використання та захисту грошей клієнта та сегрегації грошей клієнта із власними коштами. Надаються рекомендації щодо дотримання комплаєнсу вимогам з ПВК/ФТ. Положення планується опублікувати вже впродовж літа.

210. До прийняття Закону, ФІН-ФНО працював з організаторами ICO у сфері законодавства з ринку цінних паперів та фінансових інструментів. Ціллю було ідентифікувати, коли ВА є фінансовим інструментом (*тобто*, переказними цінними паперами). З цією ціллю ФІН-ФНО склав контрольний список, який використовувався у всіх операціях пов'язаних з ICO. Контрольний список, як і часті запитання, що стосуються ВА, доступні на вебсайті ФІН-ФНО.[28]

211. Наглядовий досвід ФІН-ФНО показав, що VASP зараз бажають бути регульованими і намагаються отримати схвалення від органів нагляду за їх діяльність. Задача полягає у тому, щоб донести до громадськості думку, що авторизація ще не означає схвалення. ФІН-ФНО побачило суттєву зміну у поведінці VASP по відношенню до регулювання. Деякий час тому назад вони не хотіли, щоб їх регулювали, але зараз вони шукають бізнес моделі через які їх можна було б регулювати. У VASP є певні складнощі

27 https://www.finanssivalvonta.fi/en/banks/fintech--financial-sector-innovations/virtuaalivaluutan-tarjoajat/

28 https://www.finanssivalvonta.fi/en/banks/fintech--financial-sector-innovations/virtuaalivaluutan-tarjoajat/frequently-asked-questions-on-virtual-currencies-and-their-issuance-initial-coin-offering/

у відкритті банківських рахунків, що частково може пояснити зміни у їх поведінці, стосовно регулювання.

Мексика

212. У Мексиці Федеральний Закон про *Протидію та Виявлення Операцій з Ресурсами від Нелегальних Доходів* було реформовано у березні 2018 року для того, аби встановити обмін ВА, що проводиться установами відмінними від Установ Фінансових Технологій та Кредитних Установ, як *Вразливу Діяльність*.

213. Так само, у березні 2018 року, Мексикою було опубліковано *Закон про Регулювання Установ Фінансових Технологій*, яким зазначається, що Установи Фінансових Технологій можуть діяти з ВА, що вони мають дозвіл Банку Мексики та працюють із ВА, який ним визначається.

214. Згодом, стандарти, що встановлюють заходи та процедури стосовно ПВК/ФТ пов'язаної із ВА, були опубліковані у вересні 2018 року.

215. У березні 2019 року Центральним Банком було опубліковано стандарти для визначення внутрішніх операцій, які Кредитні Установи та Установи Фінансових Технологій, прямо чи опосередковано претендують здійснювати при операціях із ВА.

216. Центральним банком зазначається, що ВА несуть істотний ризик ВК/ФТ, через легкість здійснення переказу ВА до різних країн, а також через відсутність однорідного контролю та превентивних заходів на глобальному рівні. Разом з тим, він прагне сприяти використанню технологій, які можуть принести користь, якщо ці технології будуть використовуватись всередині поміж Установами Фінансових Технологій та Кредитними Установами.

217. Врешті, у березні 2019 року, *Загальні положення, зазначені у статті 115 Закону про Кредитні Установи* було змінено, започатковано заходи та процедури, яким кредитні установи мають слідувати для того, аби відповідати зобов'язанням з ПВК/ФТ, що стосуються ВА.

Японія

218. Японія змінила *Закон про Платіжні Послуги* та *Закон про Попередження Переказів Злочинних Доходів* (ППЗД) у 2016, як відповідь на банкротство великого VASP у 2014 році та Керівництво FATF відносно ВВ від 2015 року. Слідом за прийняттям законів, у квітні 2017 року, ЯФНО створив

команду з моніторингу за VASP у серпні 2017 року, яка складалась зі спеціалістів у сфері ПВК/ФТ та технологій.

219. Як частина реєстраційної процедури, ЯФНО оцінює програми з ПВК/ФТ тих, хто подав заявки, концентруючись на відповідності бізнес плану кандидатів їх оцінці ризику, через оцінку, що базується на документах, а також виїзних й невиїзних перевірках (станом на березень 2019 року, було зареєстровано 19 VASP).

220. ЯФНО накладає на VASP періодичні накази про подання звіту, для пошуку якісної та кількісної інформації щодо притаманних ризиків та заходів з контролю. ЯФНО використовує зібрану інформацію для власної оцінки ризиків та моніторингу за VASP. До березня 2019 року ЯФНО провів виїзні перевірки у 22 VASP (в тому числі у 13 організаціях, які тоді вважались VASP, *тобто* установи, які вже діяли до вступу в силу законів і яким було дозволено діяти на попередніх засадах) та наклав адміністративні стягнення (21 постанова щодо покращення ділової діяльності та шість постанов щодо припинення ділової діяльності, а також одна відмова у реєстрації).

221. ЯФНО близько співпрацює із Японською Асоціацією з Обміну Віртуальних Валют (ЯАОВВ), органом саморегулювання, що було сертифіковано у жовтні 2018 року, для належної та гнучкої відповіді на виклики, пов'язані із VASP. ЯАОВВ діє як навчальний орган, а також орган зі здійснення моніторингу для членів VASP. Відповідність правилам та рекомендаціям з питань ПВК/ФТ підготовлюється ЯАОВВ. ЯФНО, за сприяння ЯАОВВ, провів інформаційно-просвітницьку діяльність, деякі тренінги були зроблені у співпраці з іншими органами влади, обмінюючись інформацією та ідеями з VASP, що сприяло покращенню їх комплаєнса у сфері з ПВК/ФТ.

222. Додатково, ЯФНО:

- Створив *«Дослідницьку Групу з Ділової Діяльності по Обміну Віртуальних Валют»* у березні 2018 року для перевірки інституційних відповідей на різні проблемні питання, пов'язані з діловою діяльністю VASP. У світлі пропозицій щодо доповіді Групи, ЯФНО, у березні 2019 року вніс до Парламенту законопроект про зміну законодавчих актів. Поправки включають: застосування Закону про Платіжні Послуги та ППЗД до постачальників послуг, які надають послуги зі зберігання ВА; та впровадження системи попереднього сповіщення щодо кожної зміни типу ВА, з якими проводять операції VASP, враховуючи анонімну природу ВА.

- У квітні 2019 року підготував та опублікував індикатори червоних прапорів підозрілих операцій, які є особливими для VASP. Індикатори охоплюють декілька видів операцій, де використовуються технології анонімності.

Сполучені Штати Америки

Всеосяжна та Технологічно-Нейтральна Система

223. Сполучені Штати мають всеосяжну та технологічно-нейтральну регуляторну та наглядову систему для здійснення регулювання та нагляду за «цифровими фінансовими активами»[29] у сфері ПВК/ФТ, у відповідності до якої охоплені постачальники та види діяльності в цій сфері підпорядковувались майже тому самому регулюванню, що й постачальники нецифрових активів, які підпадають під дію нормативної бази з ПВК/ФТ для фінансових установ США. Підхід США спирається на інструменти та органи різних відомств, в тому числі Служби по Боротьбі з Фінансовими Злочинами Міністерства Фінансів США (FinCEN), ПРФ США та адміністратору первинного Закону з ПВК, Закону про Банківську Таємницю (BSA); Управління з Контролю за Іноземними Активами (OFAC); Служби Внутрішніх Доходів (IRS); Комісії з Цінних Паперів і Бірж США (SEC); Комісії США з Торгівлі Товарними Ф'ючерсами (CFTC); та інших відомств й агентств. FinCEN, IRS, SEC та CFTC мають регуляторні, наглядові та правозастосовні повноваження для здійснення контролю за певними видами діяльності із цифровими активами, які включають переказ коштів; цінних паперів, біржових товарів чи деривативів; або, які мають податкові наслідки, а також у них є повноваження пом'якшувати використання цифрових активів для незаконних фінансових операцій чи ухилення від сплати податків.

224. Коли особа (термін, визначений в американському регулюванні, що виходить за рамки фізичних та юридичних осіб) долучається до певної фінансової діяльності, де використовуються цифрові активи, до неї застосовуються зобов'язання з ПВК/ФТ. В залежності від виду діяльності, особа або установа є об'єктом регулювання для наглядових органів FinCEN, SEC та/або CFTC таким як передавач грошей, національна біржа цінних паперів, брокер-дилер, інвестиційний консультант, інвестиційна компанія, агент з переказу, визначений ринок контрактів, установа з виконання свопів, організація з клірингу деривативів, посередник у

[29] З точки зору США, термін «цифрові фінансові активи» (або «цифрові активи») є комплексним терміном, який стосується певного переліку видів діяльності в екосистемі цифрових фінансових послуг, в тому числі фінансову активність із цифровими валютами – як національними цифровими валютами, так і тими цифровими валютами, що випущені не національним урядом та не гарантуються ним, такі як цифрові форми конвертованих віртуальних валют, на кшталт біткоїну – а також цифрові цінні папери, цифрові біржові товари чи цифрові деривативи.

ф'ючерсних операціях, оператор товарного пулу, радник з торгівлі біржовими товарами, своп-дилер, основний учасник свопу, роздрібний іноземний дилер з обміну валют або представляючий брокер.

225. Якщо особа підпадає під регуляторне визначення «банк», FinCEN та федеральні банківські агентства США – Рада Керівників Федеральної Резервної Системи, Федеральна Корпорація зі Страхування Вкладів, Управління Контролера Грошового Обігу та Національна Адміністрація Кредитного Союзу – мають повноваження, іноді збіжні із тими, що мають державні банківські регулятори, здійснювати регулювання та нагляд за особами, коли вони долучаються до фінансової діяльності із залученням цифрових активів. Більш того, існуючі загальні податкові принципи застосовуються до операцій, де використовуються цифрові активи, у США, оскільки IRS класифікує їх як власність.

Кейс: Регулювання та Нагляд (В Тому Числі Ліцензування та Реєстрація) за Постачальниками, Що Пов'язані із Цифровими Активами

Переказ Грошей. На федеральному рівні FinCEN регулює будь-яку особу, що залучена до діяльності з приймання та переказу грошової вартості, в незалежності від того у фізичному чи цифровому вираженні, яка переказує валюту (в тому числі конвертовані віртуальні валюти) від однієї особи до іншої або до іншого місця за допомогою будь-яких засобів. У відповідності до BSA, ті, хто переказує кошти, повинні реєструватись у FinCEN як бізнес, пов'язаний із грошовими послугами та вводити програми з ПВК, ведення обліку та заходів зі звітування, в тому числі звітів про підозрілу діяльність. Вимоги з ПВК застосовуються однаково до національних та іноземних передавачів, навіть якщо іноземна особа фізично не присутня у США і в незалежності від того, де вона створена чи розташована, у тому випадку якщо ділова активність повністю або частково здійснюється у Сполучених Штатах. З 2014 року, IRS та FinCEN проводять перевірки різних постачальників, пов'язаних із цифровими активами, включаючи адміністраторів, деякі найбільші обмінні пункти за обсягом, окремі F2F обмінники, обмінні пункти, що знаходяться за кордоном, торгівців цифровими активами / криптовалютою, а також різні торгові платформи та фінансові установи, як зареєстровані так і не зареєстровані. Закони штатів, що застосовуються, також вимагають від відповідних охоплених установ отримувати державні ліцензії на переказ коштів у більшості штатів, в яких

вони працюють, в незалежності від їх юрисдикції чи місця створення або розташування їх головного офісу. Передавачі коштів також можуть бути об'єктом інших регуляторних вимог, в тому числі з безпеки, надійності та вимог щодо резервного капіталу, в залежності від штату США, в якому вони розташовуються чи провадять ділову діяльність та в залежності від того, чи роблять їх операції, що вони проводять, об'єктами з дотримання правил інших регуляторних органів США.

Діяльність з Цінними Паперами. В тих межах, в яких цифрові активи є цінними паперами у Сполучених Штатах, SEC має регуляторні та правозастосовні повноваження, які поширюються на пропозицію, продаж та торгівлю, а також здійснення інших фінансових послуг по відношенню до цих цифрових активів. Платформи, на яких цифрові активи, які є цінними паперами, торгуються на вторинному ринку, мають бути зареєстровані в якості національної біржі цінних паперів, або ж діяти у відповідності до виключень по відношенню до реєстрації, наприклад виключення у відповідності до вимог SEC щодо альтернативної торгової системи, та подавати інформацію про свої операції та торгівлю до SEC. Навіть якщо біржа цінних паперів, брокер-дилер чи інша подібна установа, пов'язані із цінними паперами, знаходиться закордоном й немає фізичної присутності у Сполучених Штатах, така особа може бути об'єктом регулювання з боку SEC, якщо вона пропонує, продає чи емітує цінні папери (в тому числі, потенційно, певні токени ICO) особам чи інвесторам з США, чи впливає на ринок цінних паперів США іншим чином. Додаткове зобов'язання штатів з ліцензування може застосовуватись в залежності від виду діяльності, до якого залучена установа, і штату, де це відбувається. Деякі види торгівлі цифровими активами, в тому числі торгівля на платформах, можуть все ще кваліфікуватись як переказ коштів у відповідності до BSA та законів чи актів штату. Якщо цифровий актив є цінним папером, він знаходиться під юрисдикцією SEC, будь-який деривати від цінного паперу також знаходиться в сфері впливу SEC.

Діяльність із Біржовими Товарами та Деривативами. У Сполучених Штатах цифрові активи можуть також кваліфікуватись як біржові товари чи деривативи, навіть якщо вони не є цінним папером, і у подібних ситуаціях особи, що проводять операції із такими цифровими активами, підпадають під сферу впливу CFTC. CFTC має повні регуляторні повноваження щодо деривативів від цифрових активів, які не є

цінними паперами (*напр.,* ф'ючерсні угоди). CFTC здійснює регуляторні анти-шахрайські та анти-маніпулятивні повноваження щодо продажу таких активів, та вимагає проведення реєстрації для здійснення торгівлі ф'ючерсами чи іншими деривативами подібних біржових товарів. У відповідності до Закону про Обмін Біржовими Товарами та пов'язаними із ним Положеннями, CFTC має широкі повноваження для вжиття заходів проти будь-якої особи чи установи, що знаходиться в межах або поза межами Сполучених Штатів, і яка пов'язана або залучена до шахрайської чи маніпулятивної діяльності (*напр.,* CFTC США проти Blue Bit Banc).

Загалом, фізична або юридична особа, яка здійснює операції із цінними паперами, біржовими товарами чи деривативами, є об'єктом здійснення додаткового нагляду органами саморегулювання. Діяльність із цінними паперами вимагає додаткової реєстрації Регуляторного Органу Фінансової Галузі (FINRA), а діяльність із біржовими товарами та деривативами вимагає реєстрації у Національній Асоціації Ф'ючерсів (NFA). В залежності від їх діяльності, від фізичної чи юридичної особи може вимагатись реєстрація обома органами, FINRA та NFA, які, у відповідності до федеральних законів США щодо цінних паперів та біржових товарів, мають визначені цими законами зобов'язання. Більш того, аналогічно до ліцензування передавачів коштів, фізична чи юридична особа має отримати ліцензію у кожного регуляторного органу тих штатів, де вони проводять свою діяльність.

Деякі реєстратори SEC та CFTC також мають зобов'язання у відповідності до BSA, включно зі створенням програм з ПВК, звітуванням про підозрілу діяльність до FinCEN, проведенням ідентифікації та верифікації клієнтів, застосуванням посиленої належної перевірки по відношенню до певних рахунків, які пов'язані з іноземцями. Відповідні регуляторні та наглядові органи також здійснюють перевірку діяльності із цифровими активами та перевіряють реєстраторів на комплаєнс їх регуляторним зобов'язанням, в тому числі зобов'язанням з ПВК/ФТ.

Правоохоронні Органи США, Санкції та Інші Правозастосовні Можливості

226. Правоохоронні органи США використовують фінансові розвіддані від FinCEN для проведення розслідувань щодо цифрових активів. Подібна інформація – яка походить від звітів та аналізів, які збираються у FinCEN, та надсилається компетентним правоохоронним органам США – є корисною при розробці доказів злочинної діяльності та виявленні осіб, які могли бути залучені до діяльності з ВК чи ФТ. FinCEN має доступ до широкого переліку фінансової, адміністративної та правоохоронної інформації. Інформація, що знаходиться у розпорядженні FinCEN включає дві ключові частки інформації, які можуть бути інструментарієм у виявленні підозрілих цифрових активів, що можуть бути пов'язані із ВК чи ФТ: (i) звіти про підозрілу діяльність (STR) надсилаються традиційними фінансовими установами, такими як банки чи брокери-дилери на ринку цінних паперів, які переказали фіатну валюту для її подальшої конвертації чи обміну на цифровий актив в обміннику цифрових активів або в пов'язаному з цим бізнесі, або які отримали фіатну валюту від обмінника цифрових активів або пов'язаного з ним бізнесу після конвертації чи обміну з цифрового активу; та (ii) звіти про підозрілу діяльність надсилаються постачальниками цифрових активів, які отримують кошти та конвертують їх у цифрові активи або дозволяють розміщення та/або торгівлю й обмін цифрових активів. FinCEN також збирає звіти щодо рахунків іноземних банків, валютних та монетарних інструментів й валютних операцій – кожен з яких може містити докази необхідні для стримування й переслідування злочинної діяльності, що пов'язана з цифровими активами.

227. Відомства та агентства США вжили рішучих цивільних та кримінальних правозастосовних дій й в адміністративних справах, й у федеральних судах для боротьби з незаконною діяльністю, пов'язаною з цифровими активами, наприклад, шляхом пошуку різних форм допомоги, включаючи постанови про заборону протиправного діяння, судові заборони, повернення незаконно привласнених доходів, цивільні грошові стягнення за умисні порушення та прийняття кримінальних вироків, пов'язаних з конфіскацією та позбавленням волі.[30] Регулятори та наглядові органи США активно взаємодіють один з одним, з регуляторами штатів, Міністерством Юстиції США (DOJ), та іншими правоохоронними

[30] *До обраних правозастосовних, слідчих та/або санкційних заходів США входять:* цивільне грошове стягнення з Ripple Labs.Inc 2015 року; Операція Dark Gold 2016 року; цивільне грошове стягнення з BTC-e та супутній обвинувальний акт Олександру Віннику у 2017 році; кейс ФТ 2017 року, США проти Зубі Шахназ; винесення вироку неліцензованому торгівцю біткоїном у 2018 році; та виявлення адрес цифрових валют, пов'язаних із визначенням OFAC з приводу вірусу SamSam.

органами, з метою сприяння слідчим діям та судовому переслідуванню у сфері цифрових активів.

228. Різноманітність кримінальних та цивільних органів влади, політичних інструментів та існуючих легальних процесів допомагають урядовим агентствам США у виявленні незаконної діяльності, пов'язаної із цифровими активами, присвоєнні операцій конкретній особі чи організації, пом'якшувальних заходах та проведенні аналізу, що пов'язаний з їх відповідними регуляторними чи слідчими функціями. Для подібних розслідувань та судових переслідувань, DOJ покладається на коло, встановлених законом, кримінальних та цивільних органів влади, включаючи федеральні закони відносно відмивання коштів, реєстрації ділової діяльності з грошових послуг, вимог щодо ведення обліку та звітування фінансовими установами, шахрайства, ухилення від сплати податків, продажу регульованих речовин та інших нелегальних предметів та послуг, комп'ютерних злочинів та фінансування тероризму. Сполучені Штати звинувачують та притягують до відповідальності осіб, що діють як безпосередні обмінні пункти для порушення BSA чи для відмивання коштів, а також осіб та організації, що знаходяться закордоном та порушують закони США, в тому числі й у сфері цифрових активів.

229. Аналогічно до FinCEN, SEC та CFTC, DOJ має широкі повноваження для переслідування постачальників цифрових активів, які порушують закон США, навіть якщо вони фізично знаходяться поза межами Сполучених Штатів. Коли операція з цифровим активом дотикається фінансової, комп'ютерної чи іншої системи у Сполучених Штатах, DOJ має повноваження переслідувати осіб, які проводять або управляють такою операцією. Сполучені Штати також мають повноваження переслідувати осіб, що знаходяться закордоном, і які використовують цифрові активи для імпорту нелегальних продуктів чи контрабанди до Сполучених Штатів, або які використовують цифрові активи, що знаходяться у бізнесу з США, або постачальників чи фінансові установи, в цілях відмивання коштів. На додаток, особи, що знаходяться закордоном, і які надають незаконні послуги для обману чи пограбування резидентів США, можуть також переслідуватись за порушення законів США.

230. OFAC, зазвичай у співпраці з іншими агентствами, управляє фінансовими санкціями США та пов'язаними із цим ліцензіями, правилами та штрафами, усі з яких пов'язані із цифровими та іншими видами активів. OFAC чітко роз'яснює, що зобов'язання відносно комплаєнсу санкціям США є однаковими, в незалежності від того чи проводилась операція у цифровій валюті (національній цифровій валюті чи ненаціональній цифровій валюті, такій як конвертована віртуальна валюта біткоїн), чи у традиційній фіатній валюті, а громадяни США та інші особи, що так чи

інакше підпадають під повноваження OFAC, є відповідальними за забезпечення того, що вони не будуть долучатись до операцій, що заборонені санкціями OFAC.

Міжнародне Співробітництво є Ключовим

231. Притаманна глобальна природа екосистеми цифрових активів робить діяльність із цифровими активами особливо зручною для проведення та сприяння злочинам, які за своєю природою є транснаціональними. Послуги можуть надаватись, а клієнти взаємодіяти, особливо не звертаючи увагу на національні кордони, створюючи юрисдикційні складнощі. Ефективна протидія злочинній діяльності, до якої залучено цифрові активи, вимагає тісного міжнародного партнерства.

232. Відомства та агентства США, особливо правоохоронні органи США, тісно співпрацюють з іноземними партнерами у проведенні розслідувань, затримань та вилучення злочинних активів. Сполучені Штати заохочували ці партнерства для підтримки мульти-юрисдикційних розслідувань та переслідувань, особливо в тих випадках, де були залучені іноземні громадяни, постачальники цифрових активів та транснаціональні злочинні організації. Запити взаємної правової допомоги залишаються ключовим механізмом посилення співпраці. Оскільки незаконні гравці можуть швидко знищувати, розповсюджувати чи приховувати цифрові активи та пов’язані з цим докази, Сполучені Штати розробили політику зі збору свідчень та обмеження активів, що знаходяться закордоном, визнаючи, що цифрові активи та пов’язані операційні дані й свідчення можуть бути розміщені через технологічні засоби та процеси, що не передбачені чинними правовими методами та договорами.

Додаток А. Рекомендація 15, Пояснювальна Записка до неї та Визначення FATF

Рекомендація 15 – Нові Технології

Країни та фінансові установи повинні здійснювати ідентифікацію та оцінку ризиків відмивання коштів або фінансування тероризму, які можуть виникнути у зв'язку з (a) розвитком нових продуктів або новою діловою практикою, включаючи нові механізми постачання; та (b) використанням нових або таких, що розвиваються, технологій як для нових, так і давно існуючих продуктів. У випадку фінансових установ, така оцінка ризику повинна мати місце до запровадження нових продуктів, ділової практики або застосовування нових чи таких, що розвиваються, технологій. Вони повинні вживати відповідних заходів для управління та зменшення таких ризиків.

З метою управління та зменшення ризиків, що виникають у зв'язку з використання віртуальних активів, країни повинні забезпечити, що надавачі послуг з віртуальних активів регулюються для цілей ПВК/ФТ, ліцензуються чи реєструються та є предметом ефективних систем для здійснення моніторингу та забезпечення відповідності заходам, передбаченим Рекомендаціями FATF.

Пояснювальна Записка до Рекомендації 15

1. З метою застосування Рекомендацій FATF, країни повинні розглядати віртуальні активи як «власність», «доходи», «кошти», «грошові кошти та інші активи» чи іншу «еквівалентну вартість». Країни мають застосовувати відповідні заходи згідно з Рекомендаціями FATF відносно віртуальних активів та постачальників послуг з віртуальними активами (VASP).

2. У відповідності до Рекомендації 1, країни повинні виявляти, оцінювати та розуміти ризики відмивання коштів та фінансування тероризму, що виникають через діяльність із віртуальними активами та через діяльність або операції, що проводять VASP. Базуючись на цій оцінці, країни повинні застосовувати ризик-орієнтований підхід для забезпечення того, що заходи для попередження чи пом'якшення відмивання коштів та фінансування тероризму відповідають виявленим ризикам. Країни повинні вимагати від VASP виявляти, оцінювати та вживати ефективних заходів для пом'якшення своїх ризиків відмивання коштів та фінансування тероризму.

3. VASP мають бути зареєстровані або повинні отримувати ліцензію. Як мінімум, це має бути проведено у тій юрисдикції, де вони були створені.[31] В тих випадках, коли в якості VASP виступає фізична особа, вона має бути зареєстрована чи ліцензована у юрисдикції за місцем здійснення ділової діяльності. Юрисдикції можуть також вимагати від VASP, які пропонують товари та/або послуги клієнтам, чи здійснюють операції на території їх юрисдикції, були зареєстровані чи ліцензовані у цій юрисдикції. Компетентні органи влади повинні вживати необхідних правових та регуляторних заходів для запобігання можливості злочинцям чи їх пов'язаним особам здійснювати контроль, ставати бенефіціарними власниками чи власниками значної або контрольної частки акцій, чи брати участь в управлінні VASP. Країни мають вживати заходів для виявлення фізичних або юридичних осіб, що здійснюють діяльність як VASP без необхідної ліцензії чи реєстрації, та вживати до них відповідних санкцій.

4. Країни не повинні застосовувати окремі процедури ліцензування чи реєстрації по відношенню до фізичних або юридичних осіб, що вже зареєстровані як фінансові установи (як визначено Рекомендаціями FATF) в межах країни, яким відповідно до такого ліцензування чи реєстрації дозволяється проводити діяльність VASP, та які вже виконують повний спектр зобов'язань, встановлених Рекомендаціями FATF.

5. Країни повинні забезпечувати, щоб VASP підлягали адекватному регулюванню і нагляду чи моніторингу з ПВК/ФТ та ефективно впроваджували відповідні Рекомендації FATF, для пом'якшення ризиків відмивання коштів та фінансування тероризму, що виникають від віртуальних активів. VASP мають бути об'єктом ефективної системи моніторингу та забезпечувати дотримання національних вимог з ПВК/ФТ. VASP повинні підлягати нагляду чи моніторингу з боку компетентних органів влади (не органів саморегулювання), які мають здійснювати ризик-орієнтований нагляд чи моніторинг. Наглядові органи повинні мати адекватні повноваження для здійснення нагляду або моніторингу, та забезпечити виконання вимог щодо боротьби з відмиванням грошей та фінансуванням тероризму з боку VASP, в тому числі повноваження на проведення перевірок, з примушення до надання інформації та накладання санкцій. Наглядові органи повинні мати повноваження накладати ряд дисциплінарних та фінансових санкцій, в тому числі повноваження відкликати, обмежувати чи призупиняти ліцензію або реєстрацію VASP, коли це є необхідним.

---

31 Посилання на створення юридичної особи включає реєстрацію компанії чи будь-який інший механізм, який може використовуватись.

6. Країни повинні забезпечити наявність ряду ефективних, пропорційних та переконливих санкцій, кримінальних, цивільних або адміністративних, що застосовуються до VASP, які не виконують вимоги з ПВК/ФТ, у відповідності до Рекомендації 35. Санкції повинні застосовуватись не тільки до VASP, але й до їх директорів та вищого керівництва.

7. Що стосується превентивних заходів, вимоги, викладені в Рекомендаціях 10-21, застосовуються до VASP, з урахуванням наступних вимог:

   (a) R.10 – Встановлений поріг для разових операцій, при перевищенні якого VASP зобов'язані проводити CDD, становить USD/EUR 1 000.

   (b) R.16 – Країни повинні забезпечити, щоб VASP відправник збирав та зберігав необхідну та точну інформацію про відправника та необхідну інформацію про отримувача[32] віртуального активу, негайно відправляв[33] цю інформацію до VASP отримувача чи фінансової установи у безпечний спосіб, та надавав її за запитом відповідного органу влади. Країни повинні забезпечити, щоб VASP отримувач збирав та зберігав необхідну інформацію про відправника та необхідну й точну інформацію про отримувача переказу віртуального активу, та робив цю інформацію доступною за запитом відповідного органу влади. Інші вимоги R.16 (в тому числі моніторинг доступності інформації, здійснення заходів з замороження та заборони здійснення операцій із визначеними особами та установами) застосовуються на аналогічній основі, що встановлена у R.16. Аналогічні зобов'язання застосовуються й до фінансових установ, коли вони відправляють чи отримують переказ віртуального активу від імені клієнта.

8. Країни повинні швидко, конструктивно та ефективно надавати в найширшому можливому обсязі міжнародну співпрацю щодо відмивання коштів, предикатних злочинів та фінансування тероризму, пов'язаних із віртуальними активами, на правових підставах, викладених у Рекомендаціях 37-40. Зокрема, наглядові органи сектору VASP повинні оперативно та конструктивно обмінюватись інформацією з іноземними компетентними органами, в незалежності від типу чи статусу компетентних органів та розбіжностей у класифікації чи статусі VASP.

---

32 Що встановлена у R.16, параграф 6, або іншу еквівалентну інформацію у контексті віртуальних активів.

33 Інформація може бути надіслана прямо чи опосередковано. Ця інформація не має бути в обов'язковому порядку прикріплена до операції з переказу віртуального активу.

Словник FATF

Віртуальний актив є цифровим вираженням вартості, яким можна торгувати в цифровому форматі або переказувати, і яке може використовуватися для платіжних або інвестиційних цілей. Віртуальні активи не включають в себе цифрове представлення фіатних валют, цінних паперів та інших фінансових активів, які вже охоплені в інших Рекомендаціях FATF.

Постачальник послуг з віртуальних активів означає будь-яку фізичну чи юридичну особу, яка не охоплена в інших місцях відповідно до Рекомендацій, і як суб'єкт господарювання провадить один або декілька наступних видів діяльності або операцій для або від імені іншої фізичної або юридичної особи:

i) обмін між віртуальними активами та фіатними валютами;
ii) обмін між однією або більше формами віртуальних активів;
iii) переказ[34] віртуальних активів;
iv) зберігання та/або адміністрування віртуальних активів або інструментів, що дозволяють контролювати віртуальні активи;
v) участь і надання фінансових послуг, пов'язаних із пропозицією емітента та/або продажем віртуальних активів.

[34] Мається на увазі проведення операції від імені іншої фізичної або юридичної особи, що переміщає віртуальний актив з однієї віртуальної адреси до іншої віртуальної адреси