Рекомендації суб'єктам первинного фінансового моніторингу щодо ризиків дистанційних послуг

Стрімкий розвиток нових технологій у сфері фінансів позитивно впливає на ринкові перетворення в національній економіці та сприяє інтеграції господарських процесів на рівні міждержавних відносин.

В свою чергу, новітні фінансові інструменти дозволяють фінансовій установі з незначними витратами зручно, швидко та якісно надати послуги своїм клієнтам.

Разом з тим, незважаючи на суттєві переваги таких ресурсів використання фінансовими установами технологій, що дозволяють надавати послуги дистанційно, зокрема без безпосереднього контакту з клієнтом можуть нести в собі значні ризики використання для цілей відмивання кошів та фінансування тероризму.

Несанкціоноване списання коштів з банківських рахунків, шахрайство з платіжними картками, втручання в роботу Інтернет-банкінгу, розповсюдження комп'ютерних вірусів, DDoS атаки на Інтернет-ресурси, шахрайство в інформаційних мережах – це не вичерпний перелік кіберзлочинів, тобто злочинів у сфері інформаційних та комп'ютерних технологій.

Підготовка та скоєння кіберзлочину здійснюється практично не відходячи від «робочого місця», тобто такі злочини є доступними, оскільки комп'ютерна техніка постійно дешевшає, злочини можна скоювати з будь- якої точки планети, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця.

Одним з основних критеріїв, що впливають на підвищення ризику є складність ідентифікації осіб, що користуються такими послугами.

Крім того, одним із важливих завдань при наданні дистанційних послуг є забезпечення найвищого рівня безпеки, зокрема систем електронного банкінгу, здатного гарантувати мінімальні ризики відносно несанкціонованого доступу до інформації та рахунків клієнтів.

На сьогодні фінансовими установами, в залежності від специфіки діяльності надають такі дистанційні послуги, зокрема:

- системи «клієнт-банк» (переважно для корпоративних клієнтів);
- інтернет-банкінг;
- банкомати та термінали самообслуговування;
- по телефону через оператора (операторський центр – контакт-центр);
- інтерактивне телебачення;
- мобільні пристрої, що використовують протокол WAP, мобільні телефони стандарту GSM із вбудованим браузером Інтернет.

Дистанційні послуги надаються банками, як правило, у вигляді послуги клієнт-банк для юридичних осіб та інтернет-банкінг для фізичних осіб.

Дистанційні послуги в небанківському фінансовому секторі найбільш поширені серед страховиків:

- інтернет-трейдинг на фондовій біржі;

- поліси обов'язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів замовляються клієнтами через інтернет з подальшим отриманням полісів у страховика;

- надання страхових послуг по страхуванню туризму через інтернет-онлайн тощо.

У зв'язку з цим, відповідно до Міжнародних стандартів Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF), зокрема 15-ої Рекомендації, країни та фінансові установи повинні здійснювати ідентифікацію та оцінку ризиків відмивання коштів або фінансування тероризму, які можуть виникнути у зв'язку з розвитком нових продуктів або новою діловою практикою, включаючи нові механізми постачання та використання нових технологій або таких, що розвиваються, як для нових, так і давно існуючих продуктів.

Фінансові установи повинні бути зобов'язані здійснювати оцінку ризику до запровадження чи використання нових продуктів, ділової практики або технологій та вживати відповідних заходів для управління та зменшення таких ризиків.

Враховуючи зазначене, пунктом 23 частини другої статті 6 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» визначено, що суб'єкт первинного фінансового моніторингу зобов'язаний здійснювати управління ризиками, пов'язаними із запровадженням чи використанням нових та існуючих інформаційних продуктів, ділової практики або технологій, в тому числі таких, що забезпечують проведення фінансових операцій без безпосереднього контакту з клієнтом.

Також, згідно з розділом ІІ Критеріїв ризику легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення, затвердженого наказом Міністерства фінансів України від 08.07.2017 № 584 «Про затвердження Критеріїв ризику легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення» оцінювання ризику клієнта здійснюється, зокрема, за видом товарів та послуг, які клієнт отримує від суб'єкта первинного фінансового моніторингу, в тому числі, якщо це дистанційні послуги.

Крім того, Держфінмоніторингом спільно з іншими заінтересованими державними органами у 2016 році була проведена Національна оцінка ризиків відмивання коштів та фінансування тероризму в Україні.

Вказаним дослідженням було ідентифіковано загрозу використання новітніх технологій для відмивання коштів та фінансування тероризму, при цьому рівень ризику встановлений, як значний.

Враховуючи зазначене суб'єкти первинного фінансового моніторингу мають вживати заходів для обмеження ризику використання дистанційних послуг з метою легалізації (відмивання) доходів, одержаних злочинним шляхом, або фінансування тероризму, зокрема:

- проводити при наданні дистанційних послуг належну ідентифікацію, верифікацію клієнтів (представників клієнтів), вивчення клієнтів, уточнення/додаткове уточнення інформації про клієнтів;

- забезпечувати управління ризиками легалізації кримінальних доходів / фінансування тероризму;

- встановлювати внутрішніми документами особливості здійснення аналізу з метою виявлення фінансових операцій, що підлягають фінансового моніторингу, що здійснюються з використанням нових та існуючих інформаційних продуктів, ділової практики або технологій, у тому числі таких, що забезпечують проведення фінансових операцій без безпосереднього контакту з клієнтом (за наявності);

- встановлювати періодичність , мету та характер проведення операцій;

- здійснювати оцінку розміру та джерел існуючих та очікуваних надходжень, а також встановлювати джерела походження і способи переказу (внесення) грошей, що використовуються в операціях, що здійснюють за допомогою дистанційних послуг;

- враховувати типи продуктів, що використовуються клієнтом для проведення операцій та коло контрагентів клієнта;

- здійснювати виявлення та реєстрацію банками фінансових операцій, що підлягають фінансовому моніторингу або стосовно яких є достатні підстави підозрювати, що вони пов'язані, стосуються або призначені для фінансування тероризму чи фінансування розповсюдження зброї масового знищення.

Крім того, додаткові заходи мають бути спрямовані на виявлення фактів навмисного ухилення клієнта від здійснення операцій, що передбачають необхідність фізичної присутності в банку та або контакту з відповідними працівниками банку.

Також, Держфінмоніторингом під час підготовки рекомендацій пропонується використовувати наступні документи:

- Звіт Національної оцінки ризиків;
- керівництво по застосуванню ризик - орієнтовного підходу «Передплачені картки, мобільні платежі і онлайн платежі», (ФАТФ, червень 2013);

- звіт ФАТФ «Віртуальні валюти – ключові визначення і потенційні ризики в сфері ПВК/ФТ», (ФАТФ, червень 2014);

- керівництво по застосуванню ризик – орієнтовного підходу «Віртуальні валюти», (ФАТФ, червень 2015);

- типологічні дослідження у сфері протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму чи фінансуванню розповсюдження зброї масового знищення, підготовлених та оприлюднених Держфінмоніторингом.