Серійний номер: ДСФМУ-ДК-2024-006
Травень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Консультації FinCEN для фінансових установ щодо протидії фінансуванню терористичних організацій, яких підтримує Іран

🚨 Мережа боротьби з фінансовими злочинами Міністерства фінансів США (FinCEN) видала рекомендації, щоб допомогти фінансовим установам виявляти незаконні транзакції, пов'язані з терористичними групами, підтримуваними Іраном, на тлі підвищеної активності на Близькому Сході.

У рекомендаціях описано, як ці організації використовують різні методи для доступу до коштів і ухилення від фінансових систем 🔍💰

зокрема:

☑ У рекомендаціях висвітлюється, як терористичні організації отримують підтримку з боку Ірану, і описується кілька типологій, які ці терористичні організації використовують для незаконного доступу до міжнародної фінансової системи або її обходу для збору, переміщення та витрачання коштів (підказка: партнери та довірені особи)

💰 ЗБИРАННЯ КОШТІВ: Іран використовує доходи від продажу товарів, зокрема нафти

💰 ПЕРЕМІЩЕННЯ КОШТІВ: Урядові установи Ірану, такі як Центральний банк Ірану (CBI) і IRGC-QF, а також спонсоровані державою організації, такі як Хезболла, відіграють ключову роль у спрямуванні коштів терористичним осередкам за допомогою закордонних підставних компаній і фінансових установ

▶ Зверніть увагу на важливий розділ під назвою (стр. 12-13): «Індикатори червоних прапорців, пов'язаних зі збором і відмиванням коштів терористичними організаціями, які підтримує Іран».

https://bit.ly/3yk7vLW

Знання, обізнаність та навчання у сфері ПВК/ФТ у секторі дистанційних азартних ігор – тематичний огляд 2023

У першому кварталі 2023 року FIAU, спільно з MGA, провели тематичний огляд сектору віддаленого ігрового бізнесу. Метою було оцінити знання нормативних вимог та практичні знання з протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ), а також обізнаність з політиками і процедурами компаній у цій сфері серед відповідальних працівників віддалених операторів ігор.

Загалом респонденти продемонстрували ґрунтовні знання ключових концепцій ПВК/ФТ. Однак існують сфери для покращення, зокрема щодо адміністративних заходів, процедур для ігрового сектору, обізнаності з притаманними та залишковими ризиками операторів ігор. Також потребують вдосконалення знання джерел для оцінки юрисдикцій, термінів оцінки ризику клієнтів, вимог до належної перевірки різних рівнів ризику, випадків посиленої перевірки, скринінгу публічних діячів та періодів зберігання записів.

https://bit.ly/3UT1MWg

Керівні настанови з фінансових санкцій та грошових штрафів

2 травня 2024 року OFSI Великобританії повторно опублікував свої керівні настанови щодо фінансових санкцій і грошових штрафів, дотримуючись змін, оголошених у своєму блозі від 13 лютого 2024 року. OFSI прагне надати «високоякісні та прості для розуміння» вказівки щодо ефективного впровадження фінансових санкцій.

https://bit.ly/3UVl1ib

РЕГУЛЮВАННЯ

Торгівля людьми: депутати Європарламенту приймають більш широкий закон для захисту жертв

Європейський парламент схвалив оновлені законодавчі норми, спрямовані на посилення заходів щодо запобігання торгівлі людьми та кращого захисту жертв. Закон, який отримав сильну підтримку від депутатів (563 "за", 7 "проти" та 17 "утримались"), розширює існуючі заходи, також криміналізуючи примусові шлюби, незаконне усиновлення та експлуатацію сурогатного материнства по всьому ЄС. Основні особливості нового закону включають покращення координації між органами боротьби з торгівлею людьми та органами з надання притулку, криміналізацію використання послуг жертв експлуатації, введення покарань для компаній, які беруть участь у торгівлі людьми, та надання більш комплексної підтримки жертвам. Директива також наголошує на захисті найбільш уразливих груп, включаючи положення для осіб з інвалідністю та неповнолітніх дітей без супроводу. Наступні кроки включають формальне схвалення Радою, після чого директива набуде чинності через 20 днів після її публікації в офіційному журналі ЄС, а державам-членам буде надано два роки для впровадження змін.

https://bit.ly/3Kb5YLb

Поправка до Положення про звітність, процедури та штрафи (RPPR)

Міністерство фінансів США опублікувало оголошення про внесення змін до Положення про звітність, процедури та штрафи (RPPR). RPPR встановлює стандартні вимоги до звітності та ведення записів, заявки на отримання ліцензії та інші процедури, пов’язані з програмами економічних санкцій, які адмініструються OFAC.

Оголошення складається з 26 сторінок і впорядковане тематично. Коментарі громадськості збиратимуться протягом наступних 30 днів. Після схвалення остаточних правил воно набуває чинності через 90 днів.

Ось список змін

🔑 Більше немає варіантів надсилання пошти чи факсу

🔑Звітність подається в електронному вигляді

🔑Блокування та відхилення потрібно здійснювати через ORS

🔑Звітування для txns з певними критеріями

🔑Про розблоковану власність потрібно повідомляти

🔑Про передане майно необхідно повідомляти

🔑Розблокування помилкових блокувань (опечатки/схожі назви)

🔑Запити FOIA можуть бути відхилені

🔑Люди можуть подати запит на виключення зі списку

🔑Багато підтверджуючих і технічних правок

https://ofac.treasury.gov/recent-actions/20240508

Широкомасштабна реформа ПВК в Австралії

У червні 2023 року Департамент генерального прокурора (AGD) опублікував свою першу консультацію щодо модернізації австралійського режиму з ПВК у багатьох секторах. Що стосується цифрових активів, AGD запропонував розширити сферу застосування регулювання, щоб узгодити його з Рекомендацією 15 FATF і запровадити зобов'язання щодо Travel Rule.

Минулого тижня AGD оприлюднив свою подальшу консультацію, яка значною мірою просувається вперед із пропозиціями та детально описує, як вони будуть реалізовані. Ось основні моменти.

1️⃣ Цифрові валюти ➡ Цифрові активи

AGD запропонувала замінити поточний термін «цифрова валюта» в Законі про ПВК на «цифрові активи», щоб усунути «регуляторні прогалини» через «концепцію цифрових валют, що розвивається», як-от трактування NFT та CBDC (які пропонується підв'язати під визначення «гроші»). «Цифрові активи» також узгоджується з пропозицією Міністерства фінансів щодо комплексної нормативної бази для цифрових активів. Однак такі альтернативи, як «криптоактиви» або «віртуальні активи», також підлягають обговоренню.

2️⃣ Розширення послуг з цифрових активів, які підпадають під регулювання

Пропозиція передбачає розширення сфери регульованих послуг цифрових активів, щоб повністю відповідати Рекомендації FATF 15, зокрема:

- Обмін між цифровими активами та фіатними валютами (наразі регулюється)
- Обмін між двома цифровими активами
- Зберігання цифрових активів
- Фінансові послуги, пов'язані з ICO або подібними угодами

Визначення послуг передачі вартості також буде оновлено та спрощено для охоплення транзакцій цифрових активів.

3️⃣ Зобов'язання ***Travel Rule***

Відповідно до стандартів FATF, ця пропозиція підпорядковує всі передачі цифрових активів від однієї фінансової установи або постачальника послуг цифрових активів до іншого під повні зобов'язання щодо Travel Rule.

Для операцій із ***self-hosted wallets*** застосовуються обмежені зобов'язання щодо збору інформації від власних клієнтів.

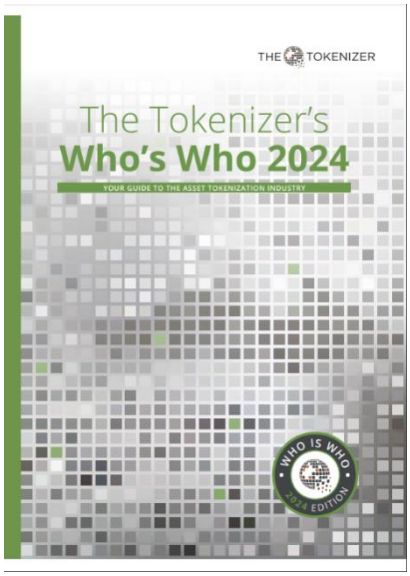
Відповідно до існуючих вимог до фінансових установ, AGD планує застосовувати Travel Rule до усіх транзакцій. Це буде більш суворою вимогою, ніж рекомендований FATF поріг у 1000 доларів США/євро.

4️⃣ Розширення повноважень ***AUSTRAC***

Пропозиція також надає AUSTRAC розширені повноваження забороняти особам надавати, контролювати або виконувати функції в цих регульованих послугах, а також оцінювати придатність, належність і здібності ключового персоналу, подібно до повноважень ASIC щодо установ, які мають ліцензію австралійських фінансових послуг (AFSL).

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Хто є хто в галузі токенізації активів



Документ під назвою "The Tokenizer's Who's Who 2024" являє собою всеосяжний довідник по індустрії токенізації активів. Це щорічний довідник, який надає глибокі знання та інформацію про різні аспекти галузі, розрахований як на досвідчених фахівців, так і на новачків.

Путівник починається з передмови, яка обговорює ширші імплікації та актуальні тенденції в токенізації активів, пропонуючи макроперспективу її еволюції та впливу як на децентралізовані фінанси (DeFi), так і на традиційні фінанси (TradFi). Окремі розділи в довіднику включають детальні інтерв'ю з піонерами галузі, аналізи різних платформ токенізації активів і огляди постачальників послуг та правових аспектів, що стосуються цифрових активів.

Крім того, документ висвітлює технічні та регулятивні нововведення в галузі, підкреслюючи важливість дотримання регулівних норм і інтеграцію технології блокчейну в різні фінансові послуги. Також він звертає увагу на прогнози щодо майбутнього індустрії, відзначаючи значний потенціал для росту та інновацій.

Загалом, "The Tokenizer's Who's Who 2024" є авторитетним ресурсом, який має на меті освітити своїх читачів щодо динамічного ландшафту токенізації активів, надаючи багатство знань та думок експертів для полегшення розуміння та залучення у цю сферу, що швидко розвивається.

https://bit.ly/4b1OYmf

Кейс: відстеження ончейн діяльності підозрюваних імітаторів FTC

Шахрайство з видаванням себе за іншу особу стрімко зростає, у 2023 році збитки склали понад 1 мільярд доларів США. Федеральна торгова комісія (FTC) випустила попередження про шахраїв, які видають себе за посадових осіб FTC, щоб обдурити жертв, часто терміново спрямовуючи їх до біткоїн-банкоматів з фінансовими погрозами. В одному випадку зловмисники виманили у жінки приблизно 2 мільйони доларів США, заявивши, що її номер соціального страхування скомпрометовано. Незважаючи на те, що більшість шахраїв працюють за допомогою фіатних операцій, спостерігається помітний зсув у бік криптовалюти через зростання прийняття у споживачів.

Аналіз мережі показує, що імітатори FTC можуть бути частиною більшої групи.

https://bit.ly/3ULEKRd

Використання фінансової системи для посилення експортного контролю

🔀Санкції проти Росії - назустріч 14-му пакету санкцій ЄС🔀

Офіційне прийняття наступного пакету санкцій ЄС може зайняти більше часу, ніж очікувалося, таким чином даючи певний простір галузі для поглинання цього шуму та запланованих рішень.

З цією метою, і оскільки Європейська комісія, схоже, прагне розширити контроль над неєвропейськими суб'єктами, було б доцільно переглянути один із останніх звітів Брейгеля – Поліпшення економічної політики щодо товарів, що надходять у Росію.

Кілька висновків із їхнього висновку:

Проблеми багатогранні та зосереджені навколо складних ланцюгів поставок, відсутності прозорості в документації та непрозорих фінансових структур. Таким чином, посилення експортного контролю стикається з проблемами, подібними до тих відомих, та детально розглянутих, проблемних питань з протидії відмиванню коштів та фінансуванню тероризму.

Необхідно посилити критичну роль фінансової системи в міжнародній торгівлі. У торговельному фінансуванні фінансовим установам було б просто контролювати мету фінансової операції. Проте, поза цим, потрібні зміни нормативної бази для усунення лазівок, покращення доступу до критично важливої інформації, пов'язаної з торгівлею товарами щодо яких здійснюється експортний контроль, і надати чіткі вказівки фінансовій індустрії щодо переходу до ризик-орієнтованого підходу. Це пріоритети для того, щоб експортний контроль працював ефективніше. Нарешті, можна винести уроки зі значного досвіду банків у проведенні належної перевірки та застосувати їх до нефінансових компаній. Компанії повинні мати чіткі стимули для відстеження транзакцій, пов'язаних з товарами під експортним контролем, та ефективного контролю своїх ланцюгів постачання. Знання своїх клієнтів

це важливий перший крок, який має стати обов'язковим для всіх компаній, що займаються військовими товарами. Але для проведення цього дорогого моніторингу також необхідно встановити стимули. У сфері фінансів фінансовим установам знадобилися значні штрафи, щоб створити суттєві відділи комплаєнсу. Збільшення штрафів і ймовірність виявлення, а також надання підтримки компаніям для проведення належної перевірки є вирішальними. Включення пунктів до угод про державні субсидії із західними компаніями, пов'язаних із дотриманням експортного контролю, могло б ще більше стимулювати фірми активізувати зусилля.

https://www.bruegel.org/working-paper/using-financial-system-enforce-export-controls

Як IRS-CI використовувала Blockchain Intelligence, щоб закрити xDedic Marketplace

Управління кримінальних розслідувань IRS (IRS-CI) відповідає за розслідування кримінальних порушень Кодексу внутрішніх доходів США та пов'язаних фінансових злочинів. Тож коли ринок даркнет xDedic продав понад 700 000 ідентифікаційних даних на своєму сайті, що дозволило зловмисникам генерувати мільйони доларів у вигляді шахрайських відшкодувань податків, IRS-CI почала діяти.

Дізнайтеся, як IRS-CI використала TRM blockchainintelligence, щоб розгадати мережу пов'язаних адрес, і подивіться, як вони співпрацювали з міжнародними правоохоронними органами, щоб закрити xDedic Marketplace — і осіб, які стоять за ним.

https://bit.ly/4bab9Xw

Синтетичний набір даних для порівняння методів боротьби з відмиванням коштів

Стаття в журналі Scientific Data описує розробку SynthAML, синтетичного набору даних для тестування методів протидії відмиванню коштів. Набір даних базується

на реальних даних від банку Spar Nord та включає підозрілі транзакції та інші банківські операції, з метою надання дослідникам інструменту для оцінки методів виявлення фінансового шахрайства у безпечному форматі, що не розкриває особисті дані клієнтів. Використання SynthAML дозволяє порівнювати різні підходи у контексті відмивання грошей. Цей набір даних створений з метою забезпечити анонімність, але зберегти реалістичність паттернів транзакцій, що допомагає у розробці більш ефективних систем протидії.

https://www.nature.com/articles/s41597-023-02569-2

Унеможливлення засобів для обходу санкцій

Політична довідка від RUSI і OCCRP розглядає механізми обходу санкцій і рекомендації для подолання цієї проблеми. Після воєнного вторгнення Росії в Україну в 2022 році запроваджені санкції на заборону фінансування російської армії та замороження активів членів внутрішнього кола Путіна. Особи, які вже були або могли бути під санкціями, наймають професіоналів для приховання активів та обходу санкцій. Звіт аналізує понад 100 інформаційних звітів про такі практики та рекомендує заходи, які можуть вжити політики для обмеження цих дій. Він закликає до збільшення відповідальності за обхід санкцій, поліпшення співпраці між країнами та регулювання професіоналів, які допомагають у таких діях.

https://bit.ly/3wu7fJN

Рекомендації щодо запобігання шахрайству

Банк Литви випустив Керівні настанови щодо запобігання шахрайству для фінансових установ, які надають платіжні послуги. Основні пункти Керівні настанов:

1. Роль FPO (Fraud Prevention Officer) є критичною для оцінки та застосування заходів з запобігання шахрайству.

2. Регулярні оцінки ризиків шахрайства обов'язкові для адаптації до нових тенденцій у шахрайстві та нормативних змін.

3. Управління ризиками шахрайства включає моніторингові інструменти, які адаптуються до змін у схемах шахрайства.

4. Комплексне навчання для персоналу, який займається запобіганням шахрайству, є важливим для забезпечення ефективності.

5. Звіти з оцінки ризиків шахрайства повинні деталізувати рівень шахрайства, ефективність контролів та необхідні поліпшення.

6. Моніторинг операцій з платежів повинен включати нові технологічні рішення для виявлення та запобігання шахрайству.

Керівні настанови набули чинності з 1 травня 2024 року. Фінансові установи повинні виконати такі дії для відповідності Керівним настановам:

1. Призначити FPO відповідальним за оцінку ефективності процесу моніторингу операцій з платежів та заходів управління ризиками шахрайства, а також за застосування запобіжних заходів.

2. Проводити щорічні незалежні перевірки заходів безпеки та інструментів запобігання шахрайству.

3. Інтегрувати запобігання шахрайству в регулярні оцінки ризиків та внутрішні перевірки.

4. Забезпечувати відкриті канали для скарг та запитів користувачів платіжних послуг для допомоги у виявленні шахрайства.

5. Оновлювати навчання та інструменти запобігання шахрайству регулярно, щоб відповідати поточним тенденціям у шахрайстві.

6. Проводити щорічну оцінку компетентності персоналу для визначення необхідної кількості та компетентності співробітників для застосування контролів шахрайства.

https://www.lb.lt/uploads/documents/docs/44241_70beec1fbe93d7db41ad427d63a1b63d.pdf

Чому кредитування DeFi? Свідчення з Aave V2

● Робочі документи BIS щодо кредитування DeFi >> Децентралізоване фінансування (DeFi) відноситься до практики пропонування та отримання позик, що здійснюється безпосередньо через технологію блокчейн і смарт-контракти, в обхід традиційних централізованих фінансових посередників, таких як банки. У цій системі учасники можуть позичати активи в безпечному середовищі, покладаючись на незмінний і прозорий характер транзакцій блокчейну. Процентні ставки встановлюються попитом і пропозицією капіталу відповідно до заздалегідь визначеної функції.

https://www.bis.org/publ/work1183.htm

ІНШІ НОВИНИ

Створення Управління ЄС з протидії відмиванню коштів (AMLA)

Нове Управління ЄС з протидії відмиванню коштів (AMLA) планує розпочати більшу частину своєї діяльності до середини 2025 року. Орган об'єднає зусилля для нагляду за фінансовими установами з високим ризиком і підтримки підрозділів фінансової розвідки (ПФР) у всьому Європейському Союзі.

Основні функції AMLA:

1. AMLA здійснюватиме нагляд за суб'єктами фінансового сектору, які здійснюють транскордонну діяльність принаймні в шести державах-членах і піддаються значним ризикам ВК/ФТ.
2. Це допоможе ПФР у ЄС зміцнити співпрацю та підвищувати ефективність обміну інформацією.
3. AMLA має на меті сприяти конвергенції нагляду та розвивати спільну культуру нагляду між національними органами.

Персонал і менеджмент:

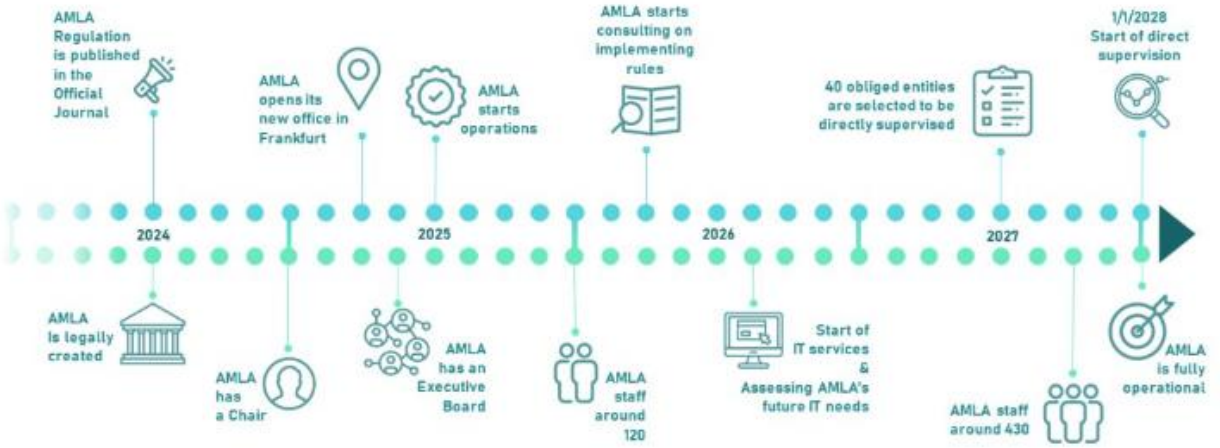
- AMLA буде поступово розширювати свій штат, досягнувши понад 430 членів до 2027 року.
- Ним керуватимуть Виконавча рада та Генеральна рада, до складу яких входитимуть представники національних наглядових органів та ПФР.

Місцезнаходження:

- Штаб-квартира AMLA буде розташована у Франкфурті-на-Майні, Німеччина.

Початок роботи та обсяг:

- Управління має розпочати роботу до 2025 року, а безпосередній нагляд за вибраними організаціями розпочнеться у 2028 році.
- AMLA не замінить національні наглядові органи, але тісно співпрацюватиме з ними, щоб покращити систему правозастосування ПВК/ФТ у ЄС.



Підбірка новин від за тиждень від AML Intelligence

Туреччина може бути виключена з так званого "сірого списку" FATF, що спонукало до спекуляцій покращення її системи фінансового моніторингу. З іншого боку, Австралія вкладає значні витрати в боротьбу з фінансовими злочинами, щоб уникнути втрати до цього списку. У США FinCEN планує розширити заходи проти відмивання коштів у секторі нерухомості, тоді як у Швеції регулятор фінансових послуг шукає нових повноважень перевірки

кримінального права колишніх працівників фінансових компаній. У Сінгапурі компанія Swiss-Asia Financial Services отримала штраф за порушення правил AML, а в Італії мафія змінює свої методи, відходячи від кровопролиття до більш низькопрофільних злочинів, таких як злочини білих комірців. Також криптовалютна біржа Binance зіткнулася з юридичними викликами в Нігерії, яка виступає проти компанії через погашення у податкових ухиленнях та відмиванні грошей.

https://bit.ly/4bs0kQc

Криптовалютний міксер було закрито органами влади

Нещодавнє звинувачення Кеонне Родрігезу та Вільяму Лонергану Хіллу, засновникам криптовалютного гаманця Samourai, привернуло увагу до світу міксерів криптовалют.

Чим був **Samourai**?

🔹 Samourai був мобільним криптовалютним гаманцем із функціями, призначеними для підвищення конфіденційності користувачів. Це дозволило користувачам зберігати свої приватні ключі для біткойнів і проводити транзакції.

🔹 Samourai пропонував такі функції, як «Whirlpool» і «Ricochet», які допомагали користувачам приховувати джерело своїх коштів, змішуючи транзакції з іншими користувачами.

🔹 Гаманець діяв як «змішувач» криптовалют, який часто називають «тумблером», що покращує анонімність цифрових транзакцій.

У результаті влада звинуватила засновників Samourai у:

☞ Змові з ціллю відмивання коштів

▶ Самурай обробив понад 100 мільйонів доларів злочинних доходів з різних джерел, включаючи ринки даркнету, схеми шахрайства та іншу незаконну діяльність.

▶ Засновники нібито знали про це та розробили функції (Whirlpool та Ricochet) спеціально, щоб допомогти користувачам приховати джерело своїх коштів.

▶ Публічні заяви та маркетингові матеріали засновників рекламували послуги Samourai користувачам, які прагнуть відмити гроші.

☞ Змові з метою ведення послуг з переказу коштів без ліцензії

Самурай сприяв послугам переказу грошей на суму понад 2 мільярди доларів США без отримання необхідної ліцензії, як того вимагає національне законодавство.

Ясно одне: битва між правоохоронними органами та міксерами криптовалют далека від завершення.

Оскільки технологія розвивається та боротьба з фінансовими злочинами посилюється, ми можемо очікувати, що обидві сторони адаптують свої стратегії в цьому постійному перетягуванні каната між конфіденційністю та безпекою.

Тижневий огляд від TRM Labs

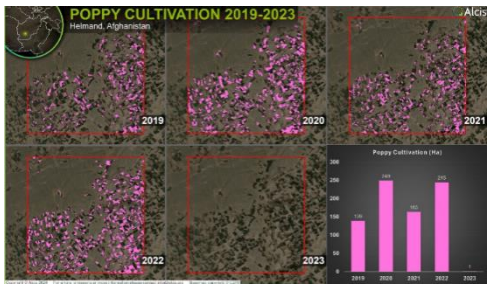
TRM Labs — це компанія, що займається питаннями пошуку інформації у блокчейнах, яка допомагає фінансовим установам, криптобізнесу та державним установам виявляти та розслідувати пов’язані з криптовалютою фінансові злочини та шахрайство. Щодня вони вирішують завдання в галузі обробки даних, data science та аналізу загроз.

Цього тижня вони більш детально розглянули наступні питання:

- Реформа регулювання ПВК в Австралії
- Санкції США та Великої Британії проти групи LockBit
- Збройне пограбування криптовалюти на мільйони доларів у Сінгапурі та Малайзії
- Подкаст TRM з німецьким прокурором Яною Рінгвальд
- Як IRS-CI закрила xDedic Marketplace
- «Маленькі кроки» та «гігантські стрибки» на BIS Innovation Summit

https://bit.ly/3QDloLE

«Золото ніколи не старіє»: магазини опіуму мають вирішальне значення для розуміння наслідків поточної заборони наркотиків Талібаном



Стаття аналізує наслідки заборони Талібаном вирощування маку в Афганістані. Попри оголошення про зниження обсягів культивації маку, значна частина населення все ще вирощує цю культуру через економічні потреби та неможливість знайти альтернативні джерела доходу. Заборона Талібаном вплинула на мільйони людей, спричинивши економічні труднощі та збільшення міграції. Також зазначено, що ціни на опіум зросли, що може вказувати на низьку ефективність заборони та продовження торгівлі наркотиками.

https://www.alcis.org/post/understanding-taliban-drug-ban

Забудьте про джанкет відмивачів у Макао, брудна китайська готівка має новий дім: шахрайські казино Південно-Східної Азії

В останні роки після жорстких заходів проти азартних ігор у Макао, кримінальні організації почали шукати нові шляхи для відмивання грошей, звертаючи свою увагу на казино в Південно-Східній Азії. Регіон став особливо привабливим через слабке регулювання та високу доступність ліцензій для казино. Відомо, що китайські кримінальні організації використовують цей регіон як новий центр для своїх фінансових операцій, оскільки регулювання та нагляд тут менш строгі, ніж, наприклад, у Макао. Основними країнами, де виявлено ці діяльності, є Камбоджа, Філіппіни та В'єтнам. Влада цих країн вже почала вживати заходів для боротьби з цією проблемою, але поки що результати обмежені. Одним із методів відмивання грошей є використання так званих "junket operators", які виступають посередниками для великих гравців, дозволяючи їм вносити великі суми готівки, які потім відмиваються через азартні ігри. Ці оператори часто мають зв'язки з організованою злочинністю і є частиною ширших мереж відмивання грошей.

https://bit.ly/3QzDM7Z

Нова мережа для боротьби з контрабандистами мігрантів у цифровій сфері

Europol запустив нову мережу, що має на меті боротьбу з незаконним переміщенням мігрантів використовуючи інструменти цифрового простору. Ця ініціатива спрямована на підвищення співпраці та обмін інформацією між правоохоронними органами по всій Європі для кращого виявлення та перешкоджання діяльності контрабандистів. Мережа використовуватиме передові технології та стратегії для боротьби з усе більш складними методами, якими злочинці експлуатують мігрантів.

https://bit.ly/4akalho

Інформаційний бюлетень ЄБА щодо ПВК/ФТ

Останній випуск новин від Європейського банківського органу (EBA) містить оновлення щодо керівництва для постачальників послуг з криптоактивами, нові керівні принципи нагляду, доступні всіма мовами ЄС, та завершення розробки керівництва щодо "Travel Rule". Також розглядаються питання ризик-орієнтованого нагляду та боротьби з фінансовими злочинами в криптосекторі, а також оновлення бази даних EuReCA, яка відстежує слабкі місця та коригувальні заходи в сфері AML/CFT.

https://ec.europa.eu/newsroom/eba/newsletter-archives/52914

Наднаціональна оцінка ризиків ЄС (SRA) викриває ризики відмивання коштів у футболі.

Основні вразливості:

💰 Великі обсяги транзакцій: глобальний ринок ставок на 1,7 трильйона доларів створює сприятливий ґрунт для злочинців, які можуть маніпулювати результатами матчів і відмивати кошти через онлайн-платформи.

🕵️‍♀️ Непрозорі грошові потоки: трансфери гравців, права на зображення та спонсорство часто включають офшорні рахунки та транзакції третіх сторін, що ускладнює відстеження незаконних коштів.

SRA малює тривожну картину:

🔑 Проникнення організованої злочинності: операція Matrioskas викрила російську мафіозну групу, яка відмивала мільйони через португальський клуб через завищені трансферні комісії та транскордонні потоки.

💻 Платформи для договірних матчів і ставок: злочинні організації використовують договірні матчі та платформи для он-лайн ставок з метою отримання незаконних прибутків шляхом маніпуляції результатами.

⛓️ Синергія з іншими злочинами: відмивання коштів у футболі часто пов’язане з торгівлею наркотиками, контрабандою та іншою серйозною кримінальною діяльністю

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Як можна зловживати компаніями-оболонками в незаконних цілях

Компанія-оболонка або корпорація — це організація з обмеженою відповідальністю, яка не має фізичної присутності в своїй юрисдикції, немає працівників і не здійснює комерційної діяльності.

Компанії-оболонки також називають міжнародними бізнес-компаніями, компаніями особистого інвестування, підставними компаніями або компаніями «поштової скриньки». 🐚

Panama Papers: Реальний сценарій

Panama Papers, масовий витік фінансових документів у 2016 році, викрив широке використання компаній-оболонок і офшорних рахунків політиками, великими бізнесами та знаменитостями для ухилення від податків і приховування незаконних багатств.

Одним із заарештованих і засуджених у результаті витоку інформації був Річард Гаффі, американський бухгалтер.

Гаффі радив клієнтам:

❌ створювати компанії-оболонки з його допомогою.

❌ фальсифікувати записи про власність, стверджуючи, що мати його клієнта, літня громадянка Гватемали (не зобов’язана сплачувати податки США), була власником, тоді як його клієнт (платник податків США) фактично контролював компанію.

❌ Ці компанії-оболонки використовувалися для утримання активів та інвестицій клієнтів, фактично приховуючи їх від Служби внутрішніх доходів (IRS), органу, відповідального за дотримання та стягнення податків у США.

❌ Для одного клієнта Гаффі створив фіктивний продаж компанії, щоб пояснити репатріацію коштів до США, уникаючи належної податкової звітності.

Гаффі був засуджений до 48 місяців ув'язнення, а також зобов'язаний виплатити приблизно 9 мільйонів доларів у якості реституції та конфіскації.

У цій схемі переважало використання компаній-оболонок, що вказувало на те, як ними можна зловживати в незаконних цілях.

Незважаючи на те, що це не завжди незаконно, компанії-оболонки традиційно використовували для незаконної діяльності, включаючи відмивання коштів, і все ще використовують!

Три етапи відмивання коштів

Існує 3 етапи відмивання коштів:

Етап 1: Розміщення

Етап 2: Розшарування

Етап 3: Інтеграція

Кожен етап відмивання коштів служить унікальній меті та ставить перед злочинцями свій набір проблем. Розуміння цих етапів має вирішальне значення для розуміння складності схем відмивання коштів і розробки ефективних стратегій боротьби з цими фінансовими злочинами.

Етап 1: Розміщення

Першим етапом процесу відмивання коштів є «розміщення». Цей етап передбачає введення незаконно отриманих грошей, які часто називають «брудними грошима», у законну фінансову систему. Це можна зробити за допомогою різних методів, таких як розбиття великих сум готівки на менш помітні менші суми, які потім вносяться безпосередньо на банківський рахунок, або використовуються для придбання фінансових інструментів, таких як чеки чи платіжні доручення.

Інші методи розміщення включають змішування незаконної готівки з законними комерційними надходженнями, використання фальшивих рахунків-фактур і навіть фізичне переміщення невеликих сум готівки за кордон і розміщення їх на рахунках в іноземних банках.

Етап 2: Розшарування

Другий етап, відомий як «розшарування», передбачає переміщення розміщених коштів у фінансовій системі за допомогою складних транзакцій і бухгалтерських маневрів, щоб ускладнити відстеження джерела. Це може включати переказ грошей між кількома банківськими рахунками, часто в різних юрисдикціях, використання компаній-оболонок або купівлю та продаж різних типів активів.

У деяких випадках злочинці використовують цифрові валюти, щоб ще більше приховати слід грошей. Основна мета на цьому етапі полягає в тому, щоб створити заплутану мережу фінансових операцій, яка ускладнює спроби відстеження з боку правоохоронних органів.

Етап 3: Інтеграція

Останнім етапом відмивання коштів є «інтеграція». На цьому етапі відмиті гроші, які тепер виглядають законними, знову вводяться в економіку. Це часто досягається через інвестиції в нерухомість, розкішні активи або бізнес-підприємства. На даний момент кошти, схоже, були отримані з законних джерел, що ускладнює органам влади розрізнення між законними та незаконними активами.

Список Спеціально Визначених Осіб (SDN List)

Список спеціально визначених громадян (SDN) ведеться Офісом з контролю за іноземними активами (OFAC) Міністерства фінансів США. У цей список включені особи, групи та суб'єкти, що підлягають економічним санкціям США через їхню участь у таких діяльностях, як тероризм, наркотрафік, поширення зброї масового знищення або інші дії, які вважаються шкідливими для національної безпеки або зовнішньополітичних інтересів США.

Список SDN є загальнодоступним і важливим для американських громадян, банків і фінансових установ для визначення заборон або необхідності отримання ліцензій для здійснення транзакцій з перерахованими особами. Кожен запис містить детальну інформацію, таку як ім'я, псевдоніми, адреси, громадянство, паспортні дані та правову основу для включення до списку.

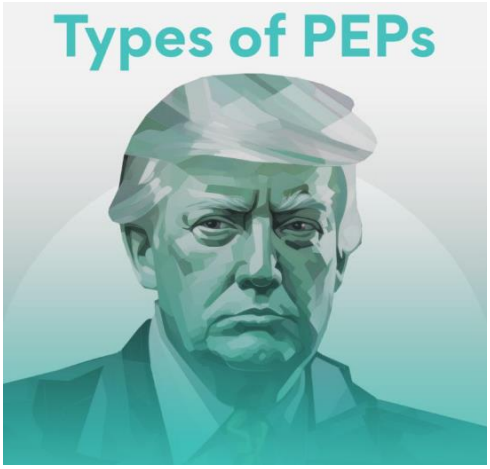
Фінансові інституції та компанії повинні перевіряти відповідність списку SDN, щоб уникнути ведення операцій з підсанкційними сторонами. Недотримання може призвести до серйозних штрафів, включно з фінансовими штрафами та правовими наслідками.

Список є всеохоплюючим, постійно оновлюється і включає різноманітні підсанкційні сторони з різних країн. Ці особи та суб'єкти можуть бути залучені до тероризму, наркотрафіку, порушення прав людини або дій, що підривають демократію або правовий порядок.

Список SDN доступний на веб-сайті OFAC. Дотримання списку обов'язкове для громадян США, постійних резидентів, суб'єктів всередині США, американських корпорацій, їхніх міжнародних філій, а також певних іноземних дочірніх компаній, які контролюються США.

Підсумовуючи, список SDN є динамічним інструментом, який використовує уряд США для втілення своїх зовнішньополітичних та національних безпекових цілей через економічні санкції щодо певних осіб та суб'єктів.

Типи PEP



🔐 Навігація в заплутаному світі протидії відмиванню коштів (AML) означає розуміння складності 🫆політично значущих 'осіб (PEPs). Ці особи, які часто займають впливові посади, потенційно можуть становити більший ризик ПВК через свою здатність і можливості розкрадати кошти або брати участь у корупційній діяльності. 🏛✨

Ось короткий огляд різних типів публічних діячів:

● Іноземні публічні діячі:

Особи, які займають високі державні посади або ролі в інших країнах.

Вони вважаються високоризиковими ⚠, оскільки установи можуть не мати інформації з перших рук про дохід на конкретній посаді, і їм може бути важче оцінити інформацію під час започаткування або моніторингу ділових відносин з клієнтами.

● Національні публічні діячі:

Це особи, які займають важливі державні посади всередині вашої країні.

Хоча ризик, який вони становлять, зазвичай вважається нижчим, ніж ризик іноземних публічних діячів, вони все одно вимагають ретельного моніторингу. Суб'єкт господарювання повинен проводити оцінку ризиків у випадку національних публічних діячів та здійснювати ризик-орієнтовану належну перевірку.

● Публічні діячі Міжнародних організацій:

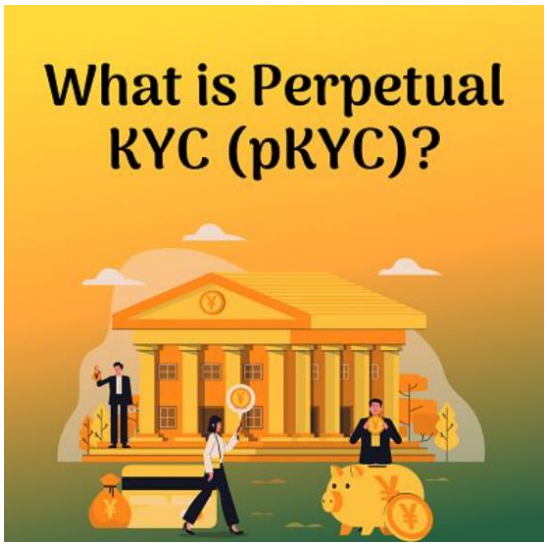
Ці публічні діячі пов'язані з міжнародними організаціями, такими як ООН або НАТО, і можуть мати доступ до великих коштів💰, які можуть бути незаконно привласнені. Суб'єкти господарювання повинні проводити оцінку ризиків у випадку публічних діячів міжнародної організації, щоб зрозуміти ризики, пов'язані з клієнтом.

● Члени родини та пов'язані з публічними діячами особи:

Значні ризики для суб'єкта становлять не лише самі публічні діячі - їхні найближчі родичі та близьке оточення також вважаються ризикованими, оскільки їх можна використовувати як посередників для відмивання коштів. До членів сім'ї та пов'язаних осіб треба ставитися так само як і до PEP.

💡 Розуміючи ці профілі ризиків, спеціалісти з комплаєнсу та боротьби з відмиванням коштів можуть запровадити відповідні заходи для запобігання фінансовим злочинам.

Вічний KYC



Вічний KYC (pKYC) – це постійний моніторинг та оновлення інформації про клієнтів у режимі реального часу, на відміну від традиційного методу періодичної перевірки KYC. Цей інноваційний підхід до перевірки клієнтів дозволяє фінансовим установам підтримувати актуальну інформацію про своїх клієнтів та оперативно виявляти та реагувати на зміни ризиків.

Завдяки використанню передових технологій, таких як штучний інтелект, машинне навчання та аналітика великих даних, pKYC може допомогти командам з дотримання нормативних вимог виявляти та запобігати фінансовим злочинам, підвищувати операційну ефективність та покращувати якість обслуговування клієнтів.

Впровадження підходу, заснованого на вічному KYC, може дати фінансовим установам низку ключових переваг, у тому числі:

Підвищення рентабельності

Впровадження рішень KYC та підтримання відповідності нормативним вимогам, що постійно змінюються, може бути дорогим для фінансових установ. Застосовуючи підхід, заснований на вічному KYC, організації можуть скоротити необхідність у періодичних перевірках та пов'язані з ними витрати, що призведе до підвищення рентабельності.

Підвищена якість даних

Вічна перевірка KYC вимагає доступу до великих обсягів даних з різних джерел, що дозволяє фінансовим установам отримати цінні відомості про поведінку клієнтів та потенційні ризики. Крім того, аналіз підозрілих операцій у режимі реального часу сприяє підвищенню безпеки та ранньому виявленню потенційних загроз.

Зниження ризиків

Постійне оновлення інформації про клієнтів та профілів ризику дозволяє фінансовим установам краще управляти ризиками та знижувати ймовірність фінансових злочинів. На відміну від цього, періодичні перевірки KYC можуть призвести до застаріння інформації та збільшення ризику між циклами перевірок.

Оптимізований процес виправлення помилок

Вічний KYC усуває необхідність у трудомісткому та ресурсомісткому процесі виправлення KYC, оскільки інформація про клієнтів постійно оновлюється та підтримується. Це призводить до більш ефективного та економічного процесу дотримання нормативних вимог.

Покращений клієнтський досвід

pKYC спрощує процес залучення клієнтів та перевірки благонадійності, зводячи до мінімуму необхідність періодичного запиту документації та зменшуючи протиріччя клієнтів. Крім того, постійне оновлення інформації про клієнта в реальному часі дозволяє фінансовим установам забезпечити більш персоналізований та ефективний клієнтський досвід.

Основні функції AI-рішень та їх потенційне застосування для KYC

Малюнок показує схему основних функцій та застосувань ШІ-рішень у процесах KYC-AML. Він описує різні особливості, такі як Центральний Дата-пул, Автоматизація Робочих Процесів, Аналіз

Неструктурованих Даних, Аналіз Зв'язків та Розпізнавання паттернів. Для кожної функції вказані її переваги та потенційні застосування, включно з удосконаленням нагляду за клієнтами, моніторингом транзакцій, звітністю, ідентифікацією ризиків та виявленням шахрайства.

Feature	Advantages	Applications
Central Data Pool	• Holistic customer view • Ease of analysis and referencing	• Customer review, Alert investigation, Client experience
Intelligent Data	• Context aware data helping achieve better and faster investigation results • Fulfil data and regulatory gaps	• Alert investigation • Compliance and Reporting
Policy Definition and Implementation	• Scan and understand regulatory changes • Identify gaps in information collection process and generate alerts for completing the process	• KYC-AML policy
Workflow Automation	• Analysing documents, behaviour, patterns from multiple places • Generating documents, reports, audit trails and notifications; task assignments • Dashboards for information aggregation and reporting	• Complete KYC-AML value chain
Unstructured Data Analysis	• Analyze news, social media and web information, linguistic analysis • Analyze long lists • Analyze employee communication	• KYC, UBO identification and ongoing monitoring • Watchlist filtering • Internal fraud analysis
Link Analysis	• Identify customer links with bad actors • Identify customer links with dubious jurisdictions, companies, UBOs	• KYC review
Pattern Recognition	• Patterns in customer behaviour • Simplify questionnaire based on previous response	• AML, anti-fraud, alert investigation • KYC, on-going review, client experience

Що таке OCR для KYC?

OCR for KYC — це технологія, яка дозволяє автоматично отримувати дані із зображень і документів, наприклад ідентифікаційних карток. Технологію перевірки документів OCR можна використовувати для вилучення даних та ідентифікаційної інформації про клієнта, щоб підтвердити автентичність особи та перевірити, чи є вона у відповідних списках спостереження. З іншого боку, інтелектуальна обробка документів (IDP) робить крок уперед, не лише збираючи дані, але й розуміючи та обробляючи їх. IDP використовує такі технології, як машинне навчання, обробка природної мови та OCR, щоб витягувати, класифікувати та розуміти дані з різних типів документів, додаючи ще один рівень ефективності та точності процесу KYC.

Переваги використання OCR для KYC

У сучасному суспільстві більшість людей матимуть якийсь цифровий документ, що посвідчує особу, наприклад водійські права чи паспорт. Використання оптичного розпізнавання символів для KYC дозволяє компаніям швидко й точно зчитувати витягнуті дані з цих документів без ручного введення, що може зайняти багато часу та бути схильним до людських помилок. OCR для KYC

скорочує час, витрачений на перевірку інформації про клієнтів, дозволяючи компаніям і фінансовим установам зосередитися на інших сферах своєї діяльності.

Інтеграція IDP у процес KYC може ще більше оптимізувати роботу. Розуміючи та обробляючи отримані дані, IDP може автоматизувати процеси прийняття рішень, зменшуючи потребу в людському втручанні та додатково знижуючи ризик помилок.

Крім того, використання OCR та IDP для KYC допомагає усунути ризик шахрайства. Маючи можливість автоматично розпізнавати та розуміти документи, що посвідчують особу, за допомогою OCR для KYC, компанії можуть переконатися, що вся інформація про клієнтів є правильною та актуальною до здійснення будь-яких транзакцій. Це покращує відповідність нормам AML і процесу вилучення даних, а також допомагає захистити клієнтів від крадіжки особистих даних або інших шахрайських дій.

Проблеми використання OCR для KYC

Незважаючи на численні переваги використання OCR для KYC для автоматизації процесів KYC, з цим пов'язані деякі проблеми. По-перше, технологія OCR може потребувати допомоги з документами, які були пошкоджені або підроблені, оскільки система може не мати змоги отримати точні дані. Крім того, великі обсяги даних можуть спричинити сповільнення системи та вплинути на загальну продуктивність. Нарешті, існує також ризик витоку даних, якщо системи безпеки не реалізовані належним чином.

Ось чому інвестування в надійне програмне забезпечення OCR та IDP і забезпечення протоколів безпеки для захисту даних клієнтів є важливими.

Блог AML UAE надає рекомендації щодо сфери ПВК/ФТ у ОАЕ

Всеохоплююча політика, процедури та засоби контролю з ПВК: сприяння боротьбі з відмиванням коштів, а також Посібник із перевірки ідентифікаційних даних: найкращі практики та інструменти.

Ці матеріали надають підзвітним суб'єктам ОАЕ ключові знання, які допоможуть відповідати їхнім правовим зобов'язанням відповідно до законодавства з ПВК/ФТ/ФР.

https://amluae.com/comprehensive-aml-policies-procedures-and-controls-bolstering-aml-efforts/

https://amluae.com/a-complete-guide-to-id-verification-best-practices-and-tools/

Незаконна торгівля об'єктами дикої природи: як?

33-річний громадянин Китаю намагався контрабандою переправити 43 австралійських ящірки (включно з синьоязичними сцинками, гальковими сцинками та східними водяними драконами) до Гонконгу та був заарештований.

Він спробував це зробити, сховавши їх у посилках у поштових відділеннях Сіднея та Вуллонгонга з грудня 2023 року по січень 2024 року. Рептилії були знайдені схованими в пластикових контейнерах, зав'язаними всередині шкарпеток і оточеними пластиковими дитячими іграшками. Деякі були вставлені в гумових іграшкових тварин.

Незаконна торгівля дикими тваринами є загальновизнаним злочином.

Відповідно до звіту FATF «Відмивання коштів і незаконна торгівля дикими тваринами» (2020), глобальна незаконна торгівля дикими тваринами оцінюється у $7-23 мільярди щорічно.

Це робить її однією з найприбутковіших форм транснаціональної організованої злочинності, яка стоїть поряд з торгівлею наркотиками, контрабандою зброї та торгівлею людьми.

Чому нас це має хвилювати

- Незаконна торгівля дикою природою становить значну загрозу біорізноманіттю, ведучи багато видів до зникнення.
- Дика природа відіграє вирішальну роль у підтримці екологічної рівноваги та функціонування екосистем.
- Дика природа має економічну цінність для економіки. Екотуризм, спостереження за дикою природою та діяльність на природі сприяють місцевій економіці.
- Незаконна торгівля дикими тваринами може становити загрозу для здоров'я населення, сприяючи поширенню зоонозних захворювань від тварин до людей.

Методи торгівлі дикими тваринами

Постає питання: як цим людям вдається здійснювати незаконну торгівлю дикими тваринами?

- Браконьєрство
- Контрабанда
- Використання незаконних мереж торгівлі
- Корупція
- Підроблена документація
- Підставні компанії
- Онлайн-платформи