Серійний номер: ДСФМУ-ДК-2024-010
Липень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Стратегічні комунікації ЄС на підтримку санкцій проти Росії

Що є ключем до боротьби з обходом санкцій? Санкційна дипломатія.

Дізнайтеся більше про те, як ЄС використовує стратегічні комунікації, щоб переконати треті країни співпрацювати щодо дотримання санкцій.

Новий документ від Balázs Gyimesi «Розробка санкцій: Стратегічні комунікації ЄС на підтримку санкцій проти Росії» демонструє, як:

🌍 ЄС використовує підхід «батога та пряника», щоб попередити треті країни про потенційні негативні економічні наслідки спроб обійти санкції, одночасно вихваляючи тих, хто зобов'язується впоратися з цією проблемою.

🌐 У той час як ЄС може очікувати, що країни-кандидати приєднаються до санкцій у рамках процесу вступу, для країн, які не є кандидатами, зусилля щодо вирішення проблеми обходу вважаються достатнім політичним кроком.

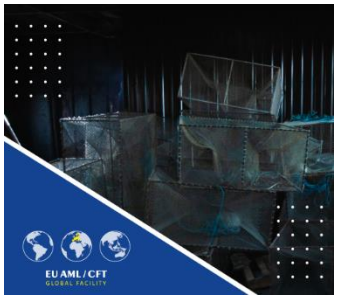
EU Стратегія санкційної дипломатії ЄС посилається на дії Росії щодо вторгнення в Україну, щоб кинути виклик російському наративу в третіх країнах.

♟️⚖️ Хоча цінності відіграють менш важливу роль, ніж інтереси, у комунікаційній стратегії ЄС щодо санкцій, вони є цінним інструментом формування рамок, пов'язаних із нормами міжнародного права.

https://static.rusi.org/eu-strategic-communications-to-support-sanctions-v-russia.pdf

Прозорість бенефіціарної власності для боротьби з незаконним, незареєстрованим і нерегульованим рибальством

EU Global Facility випустив свій останній документ, який заглиблюється в нагальну проблему незаконного, незареєстрованого та нерегульованого (ННН) рибальства. Це питання є не лише проблемою навколишнього середовища, але й серцевиною відмивання коштів, що впливає на природні та фіскальні ресурси юрисдикцій у всьому світі.



Цей документ досліджує:

📝 Вирішальний зв'язок між незаконним виловом риби та захистом навколишнього середовища.

📝 Як прозорість бенефіціарної власності (БВ) може зменшити ці ризики та проблеми.

📝 Необхідність спільного підходу із залученням учасників сфери ПВК/ФТ як з державного, так і з приватного секторів, реєстрів БВ, правоохоронних органів і судової системи.

📝 Недоліки поточної міжнародної та національних систем щодо вирішення проблеми з ННН-рибальством.

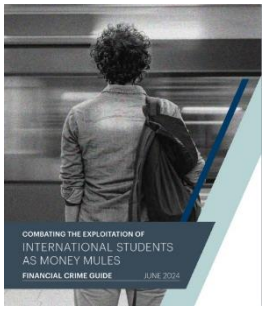
Чого прагне досягти цей документ?

✓ Надати початкове відображення проблеми БВхННН

✓ Започаткувати взаємодію та обговорення з партнерами, як у межах, так і за межами ЄС, щодо просування цієї важливої роботи.

https://bit.ly/3Kx6CT6

Боротьба з експлуатацією іноземних студентів як грошових мулів



AUSTRAC випустив посібник із фінансових злочинів для боротьби з використанням рахунків осіб, які переказують або переміщують незаконно придбані гроші від імені іншої особи.

У посібнику зазначено, що це може відбуватися різними способами, будь то фізична готівка, через банківські перекази, отримання та внесення касових чеків, цифрова валюта, використання передплачених дебетових карток або через постачальників послуг грошових переказів.

Така особа може переміщувати гроші, використовуючи особистий банківський рахунок чи рахунок компанії, рахунок іншої особи, або може отримати вказівку зареєструвати компанію, а потім відкрити банківський рахунок компанії.

Деякі з червоних прапорців включають:

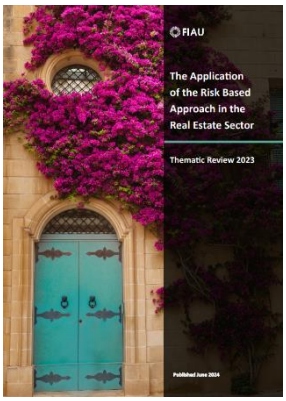
- Обіг готівки – внески готівки на різні рахунки протягом певного короткого періоду часу.
- Один вкладник робить внески на кілька рахунків.
- Єдиний рахунок для отримання внесків від кількох вкладників.
- Часті внески або зняття в одному відділенні, банкоматі, місці або передмісті.

Підзвітні суб'єкти, які надають визначені послуги, що є вразливими до вищезазначеного, мають брати до уваги свою оцінку ризику і відповідні засоби контролю, щоб перешкоджати та стримувати цю діяльність.

https://bit.ly/3VrQatM

Застосування ризик-орієнтованого підходу в сфері нерухомості

Документ є тематичним оглядом підготовленим FIAU (Financial Intelligence Analysis Unit) Мальти. Огляд стосується застосування ризик-орієнтованого підходу у секторі нерухомості та оцінює відповідність нотаріусів і агентів з нерухомості до обов'язків, встановлених Регламентом PMLFTR (Prevention of Money Laundering and Funding of Terrorism Regulations).



Метою огляду було оцінити, як нотаріуси та агенти з нерухомості застосовують ризик-орієнтований підхід при наданні послуг купівлі-продажу нерухомості. Огляд охоплював 20 суб'єктів (15 нотаріусів та 5 агентів з нерухомості), які здійснювали угоди протягом другого кварталу 2023 року. Оцінка проводилася на основі випадкових транзакцій, що відбулися між 1 квітня 2021 та 31 березня 2023 року.

Ключові висновки

- Політики та процедури: Усі суб'єкти мали письмові політики та процедури, однак часто вони були занадто загальними.
- Оцінка ризиків клієнтів: У більшості випадків процедури оцінки ризиків були наявні, але іноді вони проводилися з затримкою або взагалі не проводилися.
- Ідентифікація та верифікація клієнтів: Більшість суб'єктів виконували процедури ідентифікації та верифікації належним чином, хоча були виявлені випадки невиконання цих обов'язків.
- Джерела багатства: Інформація про джерела багатства збиралася в більшості випадків, але іноді ця інформація була неповною або не відповідала рівню ризику.
- Політично значущі особи (PEPs): 80% суб'єктів мали процедури визначення PEPs, але лише 60% мали процедури для управління ризиками, пов'язаними з PEPs.

Рекомендації

- Посилення та конкретизація політик та процедур.
- Проведення оцінки ризиків до завершення угод.
- Збір достатньої інформації та документації про джерела багатства відповідно до рівня ризику.
- Ретельна перевірка статусу PEP та застосування відповідних заходів для зниження ризиків.

Документ закликає нотаріусів та агентів з нерухомості ознайомитися з висновками огляду та внести відповідні зміни до своїх процедур для підвищення ефективності управління ризиками.

https://fiaumalta.org/app/uploads/2024/06/The-Application-of-the-Risk-Estate-Sector.pdf

Синтетичні наркотики у Східній та Південно-Східній Азії: Останні події та проблеми

Звіт УНЗ ООН (UNODC) досліджує питання синтетичних наркотиків в Східній та Південно-Східній Азії. Дослідження проказує, що за 2023 рік обсяги вилученого метамфетаміну в регіоні досягли рекордного рівня - було конфісковано 190 тонн цього наркотику.

Злочинці дедалі більше використовують торгівельну інфраструктуру регіону, поєднуючи наземні маршрути контрабанди з морськими шляхами, зокрема через Затоку Таїланду та нижній регіон Меконгу. Протягом 2023 року було зафіксовано численні вилучення великих партій метамфетаміну та кетаміну, часто разом з іншими наркотиками, що транспортувалися цими маршрутами. Ціни на метамфетамін в регіонах виробництва впали до 400 доларів США за кілограм, що свідчить про значне зростання виробництва та сильну пропозицію на ринку.

У звіті підкреслюються фінансові злочини, пов'язані з виробництвом і торгівлею наркотиками. Організовані злочинні групи використовують прогалини в регулюванні та управлінні для збільшення виробництва і контрабанди наркотиків, зокрема метамфетаміну. Вони знижують витрати на виробництво за рахунок використання неконтрольованих хімікатів, що сприяє зниженню цін і підвищенню доступності наркотиків. Ця діяльність підриває економічну стабільність регіону та створює значні ризики для суспільства.

ООН закликає до міжнародної співпраці для подолання цих викликів та підтримки платформ для обговорення прогалин і розробки рішень у регіоні Меконгу.

https://bit.ly/45emBz9

Проект технічних стандартів, що визначають певні вимоги щодо конфлікту інтересів для постачальників послуг криптовалютних активів відповідно до MiCA

(Стаття 72) Звіт про технічні стандарти (RTS) має на меті визначити вимоги щодо виявлення, запобігання, управління та розкриття конфліктів інтересів для постачальників послуг крипто-активів (CASPs).

🔻Джерела конфлікту інтересів:

Конфлікти можуть виникати через різні відносини, приналежності або численні функції, які виконують CASP, наприклад вертикально інтегровані послуги або надання різних послуг з криптоактивами одночасно.

🔻Рамки:

RTS черпає натхнення з існуючих структур, таких як MiFID II і CRD для інвестиційних компаній, і включає принципи з Керівництва EBA щодо внутрішнього управління та стандартів IOSCO.

🔻Вимоги до розкриття інформації:

CASP повинні розкривати конфлікти інтересів чітко та детально, враховуючи природу своїх клієнтів, і гарантувати, що ця інформація є доступною та зрозумілою.

🔻Принцип пропорційності:

Політики та процедури повинні враховувати масштаб, характер і діапазон послуг, що надаються CASP. Цей принцип забезпечує гнучкість, але вимагає належних ресурсів, спрямованих на управління конфліктами інтересів.

🔻Політика винагороди:

CASP повинні забезпечити, щоб їхня політика винагороди не створювала конфлікту інтересів і дозволяла працівникам виконувати свої обов'язки незалежно та об'єктивно.

🔻Конкретні заходи:

У випадках, коли конфлікт інтересів не можна врегулювати в рамках однієї організації, можуть знадобитися такі заходи, як відокремлення конфліктуючих служб в окремі юридичні особи.

RTS включає відгуки зацікавлених сторін і наголошує на відповідності принципу пропорційності. Були внесені корективи, щоб гарантувати, що CASP виділяють відповідні ресурси, не накладаючи при цьому на них надмірного тягаря.

https://bit.ly/3x6fJXU

РЕГУЛЮВАННЯ

Закони Китаю про ПВК в контексті боротьби з незаконною торгівлею об’єктами дикої природи: Порівняльний аналіз національного законодавства США, Великобританії та Китаю

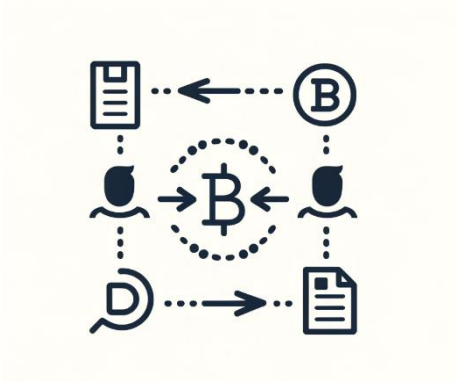
Незаконна торгівля об'єктами дикої природи стала четвертим за величиною транснаціональним організованим злочином після торгівлі наркотиками, зброєю та людьми. Злочинні синдикати використовують складні мережі, які включають браконьєрів, посередників, контрабандистів, транспортерів і торговців для здійснення своїх незаконних дій. Вони також залучають фінансові та нефінансові приватні сектори для незаконного переміщення, приховування та відмивання значних потоків нелегальних фінансів, як всередині країни, так і за кордоном.

У січні 2022 року 11 урядових агенцій Китаю, включаючи Народний банк Китаю, Міністерство громадської безпеки та Генеральну адміністрацію митниці, спільно видали Трирічний план дій щодо боротьби зі злочинами відмиванням коштів (2022-2024). Цей план передбачає проведення паралельних розслідувань як предикатних злочинів, так і злочинів з відмиванням коштів відповідно до закону.

Цей звіт оцінює придатність поточних китайських нормативних актів і Закону Китаю про боротьбу з відмиванням коштів (2006) для боротьби зі злочинами, пов’язаними з об'єктами дикої природи, порівнюючи їх з більш розвиненими системами США та Великобританії. Оцінюються три аспекти: законодавство та його виконання; нагляд і управління; та міжнародне співробітництво.

https://bit.ly/4eb4XQH

Стандарти обміну повідомленнями



🌐 Робоча група зі стандартів interVASP (ISWG) випустила оновлення стандарту обміну повідомленнями interVASP 101 (IVMS 101), універсального стандарту для постачальників послуг віртуальних активів (VASP) для передачі необхідної інформації про відправника та отримувача.

Спочатку розроблений міжгалузевою групою зі 130 технічних експертів і випущений у травні 2020 року, IVMS 101 забезпечує вимоги FATF до VASP передавати та отримувати особисту інформацію про відправника та отримувача з кожною криптовалютною транзакцією, відомою як Travel Rule. Відтоді вона стала основною моделлю даних для провідних постачальників рішень Travel Rule.

ISWG зібралася у квітні 2023 року, щоб вирішити:

📌 різні помилки,

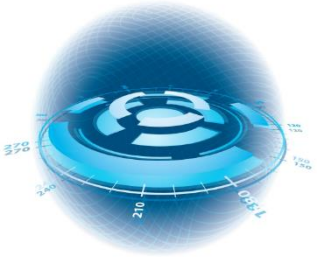
📌 труднощі впровадження та

📌 вдосконалення, які були визначені та запропоновані експертами з технічної тематики під час процесу прийняття.

Проект запропонованих змін до IVMS 101.2013 було оприлюднено для консультацій у липні 2023 року. Зараз ISWG ратифікувала запропоновані зміни, щоб забезпечити більш зручну, ефективну та повну універсальну загальну мову для передачі даних, передбачених Travel Rule.

https://www.intervasp.org/#

Закон про штучний інтелект, квітень 2024 р. Європейське всеосяжне регулювання ШІ



Документ описує нове регулювання штучного інтелекту (ШІ) в Європейському Союзі, яке має на меті забезпечити людсько-центроване та довірче використання ШІ. Основна мета цього регулювання полягає в захисті здоров'я, безпеки, фундаментальних прав, демократії, верховенства права та навколишнього середовища від потенційно шкідливих ефектів ШІ, а також у підтримці інновацій, особливо серед малих та середніх підприємств (МСП) Європи.

Закон застосовується до всіх ШІ-систем, які використовуються в ЄС, включаючи моделі з фундаментальними і загальними цілями, незалежно від їхнього місцезнаходження. Він базується на ризик-орієнтованому підході, класифікуючи ШІ-системи за категоріями ризику: неприйнятний ризик, високий ризик, мінімальний ризик. Ці категорії визначають вимоги до відповідності, такі як заборона, декларація відповідності, вимоги до прозорості або добровільні стандарти.

Регулювання набуде чинності через 20 днів після перекладу на всі офіційні мови ЄС, що очікується в середині червня 2024 року. Контроль за дотриманням регулювання здійснюватимуть національні наглядові органи у співпраці з органами ЄС. За порушення передбачено штрафи до 35 мільйонів євро або 7% глобального обороту для випадків забороненого використання, 15 мільйонів євро або 3% для інших порушень, та 7,5 мільйонів євро або 1,5% за помилки в звітності.

Регулятивний акт також визначає підходи до класифікації ризиків. Неприйнятний ризик включає масове спостереження, категоризацію за біометричними даними, розпізнавання емоцій на робочих місцях та соціальне оцінювання, що є забороненими випадками використання ШІ. Високий ризик охоплює ШІ-системи, що використовуються в критичній інфраструктурі, медичних приладах, управлінні працівниками, доступі до основних послуг, правоохоронних органах та управлінні міграцією. Мінімальний та обмежений ризик включає ШІ-системи для внутрішнього використання та процедурних завдань, такі як чат-боти та рекомендаційні системи.

Документ детально описує регуляторні вимоги, обов'язки провайдерів, механізми моніторингу та забезпечення відповідності, а також систему штрафів за порушення. Це регулювання покликане забезпечити безпеку та довіру до ШІ в Європейському Союзі, сприяючи інноваціям та захисту прав громадян.

https://bit.ly/3Rdamx6

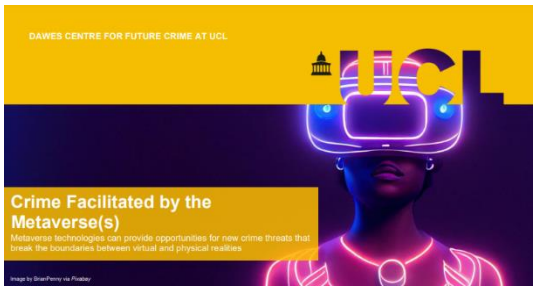
Регулювання з ПВК в Австралії

У глобальному фінансовому середовищі, яке дедалі більше вимагає прозорості та належної обачності, Австралія була на передньому краї запровадження суворих правил з ПВК. Ці норми є не лише життєво важливими для боротьби з відмиванням коштів і фінансуванням тероризму, але й стали ключовими показниками надійності законодавства в країні. ⚠

https://bit.ly/4aUU2bb

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Злочинb, створений за допомогою Метавсесвіту(ів)



Брифінг від Центру майбутніх злочинів (UCL) Великобританії досліджує можливості та ризики, пов'язані з розвитком метавсесвіту – технологій, що об'єднують фізичні та віртуальні середовища для різних цілей, від ігор до роботи. Хоча ці технології можуть значно покращити багато аспектів життя, вони також створюють нові можливості для злочинів.

Метавсесвіт створює умови для нових типів злочинів, які виходять за межі традиційного інтернет-злочинства. Злочини можуть включати використання дитячого сексуального контенту, фінансове шахрайство в метавсесвіті, переслідування, зловживання особистими даними та радикалізацію. У звіті описано 32 потенційні загрози, з яких 10 найризикованіших проаналізовано докладніше. Для боротьби з цими загрозами необхідно вдосконалювати законодавство та регулювання.

У звіті обговорюються актуальні британські правові рамки, включаючи Закон про безпеку в інтернеті 2023 року, який вводить обов'язок провайдерів інтернет-послуг забезпечувати безпеку користувачів та мінімізувати ризики злочинної діяльності. Автори зазначають, що для ефективного запобігання злочинам у метавсесвіті потрібно створювати комплексні стратегії, залучаючи широкий спектр втручань та використовуючи існуючі правові інструменти.

https://www.ucl.ac.uk/future-crime/sites/future_crime/files/metaversepolicybriefing_15_may2024.pdf

Рибальські човни та вантажні судна: як колумбійський кокаїн подорожує світом

Стаття досліджує способи перевезення колумбійського кокаїну по всьому світу, використовуючи витоки з документів прокуратури для заповнення прогалин в офіційній статистиці. За період з 2016 по квітень 2022 року журналісти виявили 1764 окремі випадки перевезення кокаїну з Колумбії, три чверті з яких були здійснені на малих суднах, таких як рибальські човни та траулери. Близько 431 випадок пов'язаний з великими суднами, що перевозили 264,8 метричних тонн кокаїну. Найчастіше контрабанду виявляли в Бельгії та Іспанії.

У статті детально розглядаються фінансові злочини, пов'язані з транспортуванням кокаїну з Колумбії. Витоки з документів прокуратури показали, що наркоторговці використовують складні схеми для фінансових махінацій, включаючи підроблені компанії та підставних імпортерів. Наприклад, одна така підставна компанія використовувалася для перевезення кокаїну, замаскованого під звичайний вантаж. Зловмисники часто використовують великі контейнерні судна, що належать великим судноплавним компаніям, для перевезення великих партій наркотиків, що ускладнює виявлення контрабанди та фінансових потоків, пов'язаних із цими злочинами.

Складність боротьби з контрабандою підсилюється використанням великих контейнерних суден, що надають можливість переміщувати наркотики великими партіями, а також новими методами контамінації, які стають все більш складними. Витоки документів також розкрили, що деякі наркоторговці віддають перевагу певним судноплавним компаніям та докам.

https://bit.ly/3yNvW4J

Польський бізнесмен заробляє мільйони на фірмі, яка працює з путінською росією

Стаття розслідує діяльність польського бізнесмена Анджея Манковського, який через свою компанію AMT Group отримав майже 3 мільйони доларів від московських компаній, що мають зв’язки з режимом Путіна та підпадають під санкції США та ЄС.

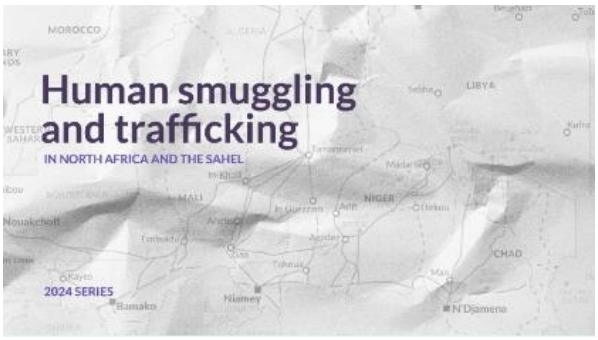
Після повномасштабного вторгнення Росії в Україну в лютому 2022 року, ім'я Андрея Манковського, польського бізнесмена та громадянина Франції, зникло з веб-сайту московської IT-компанії AMT Group, де він раніше був зазначений як президент. Однак журналісти виявили, що Манковський продовжує отримувати значні доходи від цієї компанії, яка співпрацює з російськими банками та іншими організаціями, що підпадають під санкції США та ЄС. Витоки даних показали, що він отримав майже 3 мільйони доларів у вигляді платежів від AMT Group та пов'язаної компанії AMT Group Telecom з 2022 по 2024 рік.

Розслідування виявило складну мережу компаній, пов'язаних з Манковським, що ускладнює відстеження фінансових потоків. Ця мережа включає компанії, зареєстровані в різних юрисдикціях, включаючи Люксембург та Острів Гернсі, що є податковою гаванню. Журналісти встановили, що основним власником цих компаній є Манковський, але через складність корпоративної структури, деталі власності та фінансів залишаються непрозорими. Таким чином, Манковський використовував складну мережу компаній для приховування реальних джерел фінансування, що ускладнює відстеження потоків грошей та піднімає питання щодо легітимності його доходів.

Після початку війни в Україні, AMT Group отримала мільйони доларів від компаній, що перебувають під санкціями, включаючи виробників ядерних боєголовок та технологій для військових літаків. Манковський також отримав виплати, що можуть порушувати санкції ЄС, якщо він є кінцевим бенефіціаром компанії, яка підтримує російську військову машину.

https://bit.ly/4c8MF0J

Контрабанда та торгівля людьми в Північній Африці та Сахелі



Цикл досліджень "Human smuggling and trafficking in the Sahel - 2024" досліджує зростаючу роль Північної Африки та регіону Сахель у контрабанді та торгівлі людьми з кінця 1990-х років. Ці регіони є ключовими коридорами для мігрантів з Африки на південь від Сахари, Південної Азії та Близького Сходу, які прямують до Європи. Дослідження висвітлюють політичні, економічні та безпекові зміни, що спричинили зсуви у міграційних потоках та діяльності контрабандистів, включаючи внутрішні конфлікти та політичну нестабільність. Основні країни досліджень включають Лівію, Туніс, Марокко, Малі, Нігер, Чад та Судан.

Перше дослідження з циклу зосереджується на питанні торгівлі людьми в Малі. У 2023 році політична та безпекова ситуація в північному Малі суттєво змінилася через вихід місії ООН MINUSMA, що призвело до відновлення бойових дій між різними угрупованнями, включаючи урядові сили Малі (FAMa) та підтримувану Росією групу Вагнера.

Внутрішні конфлікти та міжнародна ізоляція посилили економічний тиск, що змусило багатьох людей шукати кращих умов життя за кордоном. Використання дронів та авіаударів FAMa і Вагнера значно ускладнило ситуацію для мігрантів та контрабандистів.

Це дослідження підкреслює необхідність міжнародної співпраці для ефективної боротьби з контрабандою та торгівлею людьми, а також надання допомоги постраждалим мігрантам.

https://bit.ly/3KtIYHc

Майбутнє біткоїна №2: токени

Документ "The Future of Bitcoin #2: Tokens" представляє всебічний аналіз сучасних тенденцій та майбутніх перспектив у розвитку токенів на базі блокчейну Bitcoin. Основний акцент зроблено на появі нового протоколу Runes, розробленого Casey Rodarmor, який пропонує більш ефективний спосіб створення замінних токенів порівняно з попередніми стандартами, такими як BRC-20.

Звіт розпочинається з опису важливих віх у розвитку Bitcoin, зокрема появи Ordinals та Inscriptions, які дозволили створювати цифрові артефакти або NFT на основі Bitcoin. Цей процес, відомий як Ordinal Theory, надає кожному сатоші унікальний ідентифікатор, що дозволяє вписувати текст, зображення, відео та інший контент безпосередньо у блокчейн Bitcoin.

Протокол BRC-20, що виник на основі Ordinals, дозволив створювати замінні токени, використовуючи текстові дані JSON, що вписуються в сатоші. Однак, протокол Runes представляє новий підхід, який не залежить від Ordinals та забезпечує більшу ефективність у використанні блокового простору. Runes використовують модель UTXO Bitcoin, де кожна транзакція може містити не лише сатоші, а й баланси замінних токенів.

Однією з ключових особливостей Runes є їх здатність працювати без змін у програмному забезпеченні або правилах консенсусу Bitcoin. Це робить їх більш сумісними з існуючими протоколами Bitcoin, такими як гаманці, мости та рішення для масштабування. Крім того, Runes менш схильні до створення блокчейн-завантаження порівняно з BRC-20, що робить їх більш ефективними.

Важливим аспектом є вплив Runes на ринок Bitcoin. Від моменту запуску, вони спричинили значне збільшення транзакцій та комісій у мережі, що сприяє вирішенню довгострокових питань безпеки Bitcoin. Звіт прогнозує, що майбутнє Runes залежатиме від їх здатності інтегруватися з існуючою інфраструктурою та від їхньої привабливості для нових користувачів та розробників.

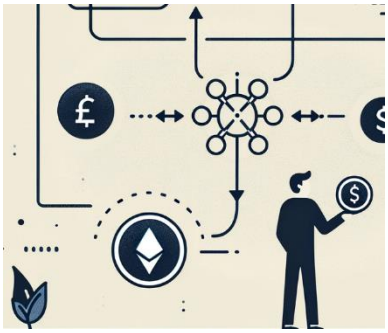
У заключних думках наголошується, що поява Runes, Ordinals, Inscriptions та BRC-20 значно вплинули на екосистему Bitcoin, створюючи нові типи транзакцій та стимулюючи розвиток мережі. Важливо буде спостерігати за тим, як Runes інтегруються та розвиваються в майбутньому, і чи зможуть вони досягти або перевершити успіх своїх попередників.

https://www.binance.com/en/research/analysis/the-future-of-bitcoin-2-tokens

Кредитне плече DeFi

📉 Всупереч поширеній думці, кредитування DeFi не характеризується надмірним кредитним плечем. Користувачі віддають перевагу управлінню ризиками, про що свідчать останні дослідження. 💡

У цьому документі BIS розглядаються тонкощі кредитного плеча DeFi, використовуючи дані на рівні гаманця з основних платформ кредитування.



▶ Результати показують, що загальне кредитне плече зазвичай знаходиться в діапазоні від 1,4 до 1,9.

▶ Цікаво, що найбільші та найактивніші користувачі постійно демонструють вище плече порівняно з іншими.

На динаміку кредитного плеча в першу чергу впливають вимоги співвідношення позики до вартості, ставки позики, коливання ринку криптовалют і настрої інвесторів.

▶ Вище плече позичальника, як правило, знижує стійкість кредитування, зокрема збільшуючи частку непогашеної заборгованості, що наближається до ліквідації.

▶Перед потенційною ліквідацією позичальники з високим кредитним плечем часто вдаються до волатильної застави.

https://www.bis.org/publ/work1171.pdf

Модернізація основних банківських систем

Цей документ детально описує важливість і процеси модернізації основних банківських систем (CBS), що є критично важливими для збереження конкурентоспроможності та адаптивності банків у сучасному цифровому світі. Основна увага приділяється необхідності переходу від застарілих систем до сучасних, які здатні забезпечити безперебійний цифровий досвід для клієнтів, зниження витрат і підвищення операційної ефективності.

Модернізація основних банківських систем є відповіддю на виклики, що стоять перед традиційними банками, зокрема жорстко закодовані правила та слабка документація, які ускладнюють інтеграцію з новітніми технологіями та платформами. У документі підкреслюється, що сучасні CBS дозволяють банкам пропонувати безперебійні та персоналізовані послуги, сприяти інноваціям і гнучкості у швидкому реагуванні на зміни ринку, покращувати операційну ефективність, забезпечуючи при цьому відповідність постійно змінюваним регуляторним вимогам.

Впровадження сучасних рішень у CBS сприяє зниженню операційних витрат шляхом усунення монолітних структур, забезпечення обробки транзакцій у реальному часі, що підвищує задоволеність клієнтів і продуктивність співробітників. Архітектура мікросервісів дозволяє банкам швидко впроваджувати зміни і адаптуватися до ринкових умов, забезпечуючи легку масштабованість для різних обсягів транзакцій або розширення бізнесу. Крім того, модернізація відкриває нові можливості для відкритого банкінгу, сприяючи співпраці та доступу до інноваційних технологій.

Документ також обговорює різні підходи до модернізації, включаючи повну заміну системи, поступове оновлення компонентів або створення нових банківських систем з нуля. Використання хмарних технологій і сервісно-орієнтованих платформ забезпечує гнучкість і доступність для банків різного масштабу, дозволяючи їм більш ефективно відповідати на потреби клієнтів і вимоги регуляторів.

Значна увага приділяється тенденціям та викликам, з якими стикається банківський сектор. Розвиток фінансових технологій (FinTech) в Індії створює додаткові вимоги до банків для впровадження сучасних технологій. Регуляторні зміни, такі як захист прав споживачів та екологічні

вимоги, також підштовхують банки до модернізації. Конкуренція з боку технологічно підкованих стартапів і нео-банків вимагає від традиційних банків адаптивності та інноваційності.

У підсумку, модернізація основних банківських систем є не лише технологічним викликом, а й стратегічним кроком для забезпечення конкурентоспроможності, відповідності регуляторним вимогам і задоволення очікувань клієнтів у цифрову епоху. Ефективне управління змінами і залучення зацікавлених сторін є ключовими факторами успіху в цій трансформації, що підкреслює важливість комплексного підходу до модернізації банківських систем.

https://bit.ly/4e9l1Th

Як Закон Індії про ПВК бореться з фінансовими злочинами, нещодавні нормативні зміни та вдосконалені рішення для боротьби з відмиванням коштів.

Стаття описує, що таке відмивання коштів, процес приховування незаконно отриманих коштів через різні фінансові системи та транзакції. Це кримінальна діяльність, яка може серйозно вплинути на фінансову систему, підтримуючи інші злочини, такі як тероризм і торгівля людьми, та шкодячи загальній економіці. Уряди, включаючи Індію, впровадили закони для боротьби з відмиванням коштів. В Індії це законодавство представлено Законом (PMLA), який був прийнятий у 2002 році та набрав чинності 1 липня 2005 року.

PMLA надає повноваження Директору ПФР та Директору з правозастосування для боротьби з відмиванням коштів. Основні положення закону включають боротьбу через встановлення правил для фінансових установ, зобов'язання для банків і фінансових інститутів щодо перевірки особи клієнтів, ведення записів і надання інформації ПФР, а також конфіскацію активів, отриманих в результаті відмивання коштів.

З моменту свого прийняття PMLA зазнав кілька змін для посилення своєї ефективності та адаптації до нових форм відмивання коштів. Серед нових положень - боротьба з фінансуванням тероризму та міжнародним відмиванням коштів.

Незважаючи на свої досягнення, PMLA стикається з проблемами у впровадженні через складнощі фінансової системи та постійно змінюваних методик відмивання коштів. Критики вказують на можливі лазівки, які можуть бути використані злочинцями, підкреслюючи необхідність постійних оновлень і пильності.

У статті також порівнюються PMLA з законами в інших країнах, де основні цілі залишаються схожими, але можуть відрізнятися рівнем жорсткості регуляцій. Використання технологій, таких як штучний інтелект і машинне навчання, допомагає у виявленні та запобіганні відмиванню коштів за допомогою аналізу даних у реальному часі, розпізнавання патернів і виявлення аномалій.

Стаття також наголошує на важливості співпраці між фінансовими установами, регуляторними органами та постачальниками технологій для обміну інформацією та кращими практиками у боротьбі з відмиванням коштів. Суворі заходи щодо дотримання регуляторних вимог і нещодавні зміни в PMLA спрямовані на посилення ПВК в Індії, що включає зниження критерію володіння акціями для визначення бенефіціарів до 10% і розширення вимог KYC на криптобіржі.

https://bit.ly/3VwsAfo

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

Боротьба з особами, які перебувають в міжнародному розшуку

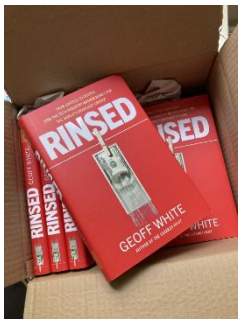
🎙 Окремі високоризикові злочинці становлять одну з найбільших загроз для безпеки Європи.

Ключові лідери злочинних організацій можуть брати участь у багатьох незаконних схемах одночасно, а це означає, що арешт однієї "цінної" цілі може звести нанівець кілька злочинних операцій.

У цьому епізоді The Europol Podcast Європол і An Garda Síochána розповідають, як вони протидіють небезпечним міжнародним втікачам, у цьому випадку на прикладі картелю Кінахан.

https://www.europol.europa.eu/media-press/europol-podcast/episode-14-fighting-international-fugitives

Rinsed



Книга "Rinsed" авторства Джеффа Уайта досліджує, як технології революціонізують індустрію відмивання грошей. У цій захоплюючій роботі автор розкриває, як організовані злочинці та висококваліфіковані кіберзлочинці об'єднують зусилля, створюючи складні віртуальні машини для відмивання грошей, які важко виявити правоохоронним органам. Книга містить вражаючі історії та інтерв'ю з інсайдерами на всіх рівнях системи, демонструючи, як злочинці використовують сучасні технології для уникнення покарання. "Rinsed" розглядає технологічний вплив на світ фінансових злочинів та буде опублікована в червні 2024 року.

https://www.amazon.co.uk/dp/0241624835

ІНШІ НОВИНИ

Боротьба з мовчазною загрозою шахрайства: посилення реагування Великобританії

У статті розглядається реакція Великобританії на загрозу шахрайства, яке вважається "тихою загрозою" для національної безпеки. Після втраченої декади 2010-х років, уряд почав активніше боротися з шахрайством, запровадивши першу стратегію боротьби з шахрайством у 2023 році. Описуються заходи, включаючи нові законодавчі ініціативи, міжнародні саміти та посилення внутрішніх заходів. Пропонується посилити роль керівництва, збільшити фінансування та забезпечити більш ефективну координацію заходів.

https://bit.ly/3XdQX2y

Придушення постачальників послуг грошових мулів, які відмили понад 10 мільйонів євро

Європол провів масштабну операцію, спрямовану на придушення діяльності "грошових мулів" — осіб, які використовуються злочинцями для відмивання грошей. В результаті цієї операції було виявлено та заарештовано 20 осіб, підозрюваних у відмиванні понад 10 мільйонів євро. Операція охопила декілька країн Європи, включаючи Францію, Італію та Румунію, де правоохоронці провели обшуки і арешти. Було проведено понад 20 обшуків у житлових та комерційних приміщеннях, в ході яких вилучили значну кількість електронних пристроїв, коштовностей та криптовалют. Заарештовано 20 осіб, включаючи організаторів цієї схеми. Серед арештованих — як основні фігуранти, так і допоміжні особи, які виконували роль "мулів". Операція була результатом тісної співпраці між національними правоохоронними органами та Європолом. Учасники операції обмінювалися інформацією та координували дії для ефективного виявлення та ліквідації злочинних мереж. Європол продовжує співпрацювати з міжнародними партнерами для запобігання фінансовим злочинам, і плануються подальші розслідування для виявлення інших учасників і організаторів схем відмивання грошей.

https://bit.ly/3V5jSn6

Санкційний огляд за травень 2024

✍🌎EUСтежити за розвитком подій у просторі санкцій ЄС може бути складним завданням. З «**This Month in EU Sanctions**» я пропоную підсумок останніх новин, оновлень і думок. Вийшов перший випуск бюлетеня.

https://bit.ly/3XdN4Ld

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:

- 🏛 Палата представників США проголосувала за закон про криптовалюти
- SEC схвалює зміну правил, прокладаючи шлях для Ether ETF
- Пік відкликання криптовалютних ліцензій у Гонконзі
- Поліція припиняє криптошахрайство в Малайзії
- Південна Африка приймає цифрове майбутнє
- Збалансування криптомайнінгу та енергоспоживання в ОАЕ
- 💰 7,5 років ув'язнення у справі про відмивання коштів через криптовалюту на 5 мільярдів фунтів стерлінгів

https://bit.ly/3VvF72x

Прогнозується, що світовий ринок програмного забезпечення для ПВК у середньорічному темпі зросте на 5,4% у період з 2024 по 2031 рік.

Стаття описує ринок програмного забезпечення для ПВК, який зазнав значного зростання в останні роки завдяки розширенню присутності на ринку та розширенню продуктів. Основні причини зростання ринку включають посилення уваги до регуляторної відповідності, зростання фінансових злочинів і технологічний прогрес. Прогнозується, що ринок AML Software зростатиме на 5,4% у період з 2024 по 2031 роки, в основному через зростання цифрових платежів і онлайн-банкінгу.

Основні тенденції ринку AML Software включають інтеграцію штучного інтелекту та машинного навчання для підвищення точності виявлення, впровадження хмарних рішень для гнучкості та масштабованості, а також розробку інструментів моніторингу в реальному часі. Ринок поділяється на два типи рішень: хмарні та локальні, кожне з яких має свої переваги щодо гнучкості та безпеки даних.

Ринок AML Software обслуговує різні рівні фінансових установ, від великих міжнародних банків до місцевих кредитних спілок, допомагаючи їм дотримуватися нормативних вимог і виявляти підозрілу діяльність. Географічно ринок швидко зростає в Північній Америці, Європі, Азіатсько-Тихоокеанському регіоні, Латинській Америці та на Близькому Сході та в Африці через зростання цифрових транзакцій і суворі регуляторні вимоги.

Основні гравці на ринку, такі як Oracle, Thomson Reuters, Fiserv і SAS, домінують завдяки своїм передовим технологіям і рішенням. Вони зосереджуються на впровадженні більш просунутих технологій, таких як штучний інтелект і блокчейн, для покращення процесів виявлення та підвищення безпеки.

Ринок AML Software продовжує еволюціонувати, впроваджуючи нові технології та вдосконалюючи існуючі рішення для ефективної боротьби з відмиванням грошей та фінансуванням тероризму.

https://bit.ly/4bRschi

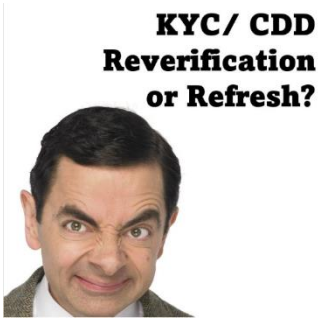
ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Новий орган влади ЄС з питань ПВК

ЄС посилює боротьбу з відмиванням коштів і фінансуванням тероризму шляхом створення нового органу з протидії відмиванню коштів (AMLA). Це агентство матиме вирішальне значення для забезпечення правильного та послідовного застосування правил ЄС.

https://europa.eu/!wyFGqq

Повторна перевірка KYC/ CDD та/або оновлення



З'явився тригер для оновлення ⚡ KYC/CDD клієнта, давайте подивимося, що ви можете зробити.

Давайте повернемося до перших принципів і того, що ми намагаємося зробити. Ми хочемо переконатися, що ми найкраще розуміємо про клієнта:

- Характер і мету відносин
- Ризик, який може представляти цей клієнт
- Зібрана інформація дозволяє нам зрозуміти та оцінити рівень ризику, який становить цей клієнт
- Надана інформація є правдивою та актуальною

Що нам тепер робити **?**

✅ Повинно бути чітко визначено, що і коли потрібно запитати з клієнта (це включає в себе те, чи можете ви сформувати основу для обґрунтованої підозри)

✅ Зібрана інформація має бути підтверджена надійним і незалежним джерелом

✅ Ви повинні знати, як реагувати на будь-які розбіжності, які виникають у цьому процесі

Не забувайте

🔥 Ваші співробітники повинні розуміти ці процеси ідентифікації клієнтів

🔥 Ви повинні враховувати виявлені ризики ВК/ФТ

🔥 Що це стосується вашого бізнесу та будь-яких агентів/брокерів/посередників або аутсорсингових сторін, яких ви використовуєте

🔥 Це застосовується до як існуючих, так і нових клієнтів

Що таке фінансування розповсюдження

Фінансування розповсюдження (ФР) передбачає фінансову підтримку розповсюдження зброї масового знищення (ЗМЗ). Це включає фінансову діяльність, яка дозволяє придбання, розробку, володіння або використання такої зброї державами чи недержавними суб'єктами. ФР становить загрозу глобальній безпеці та фінансовій стабільності, оскільки кошти можна залучати як законними,

так і нелегітимними каналами, використовуючи вразливі місця в міжнародних фінансових системах.

Важливість для ПВК

1. Ухилення від санкцій: визначені фізичні та юридичні особи, часто пов'язані з такими країнами, як Північна Корея та Іран, намагаються уникнути цільових фінансових санкцій за допомогою складних мереж фінансових транзакцій та перевезень. Це може передбачати використання підставних компаній і проведення транзакцій через юрисдикції зі слабким контролем за ПВК/ФТ.

2. Галузеві ризики: Особливо вразливими є різні сектори, зокрема фінансових послуг, торгівлі товарами подвійного призначення (предмети, які можна використовувати як у цивільних, так і у військових цілях), а також морський сектор. Наприклад, трасти та постачальники послуг компаніям (TCSP) можна використовувати для створення установ, які приховують зв'язки із визначеними особами або організаціями.

3. Складні транзакції: мережі підтримки розповсюдження часто використовують посередників та складні корпоративні структури, щоб приховати бенефіціарну власність і характер своєї діяльності. Це ускладнює моніторинг фінансових установ та ідентифікацію підозрілих транзакцій, пов'язаних з розповсюдженням.

4. Посилена належна перевірка: фінансові установи повинні прийняти заходи з посиленої перевірки для виявлення та зменшення ризиків ФР. Це включає ретельну перевірку клієнтів, моніторинг транзакцій і розуміння характеру ділової діяльності клієнтів. Ці кроки мають вирішальне значення для запобігання використанню коштів для фінансування розповсюдження.

Наслідки ігнорування ризиків ФР

1. Санкції та репутація: установи, які не ідентифікують і не пом'якшують ризики ФР, можуть зіткнутися з юридичними санкціями та шкодою репутації. Регуляторні органи можуть застосовувати суворі покарання, включно з відкликанням ліцензій на діяльність.

2. Системні ризики: відсутність розуміння ризиків ФР може наражати глобальну фінансову систему на серйозні загрози, компрометуючи економічну безпеку та стабільність. Мережі розповсюдження зброї масового знищення можуть продовжувати фінансувати незаконну діяльність, збільшуючи ризик виникнення нових конфліктів та нестабільних регіонів.

Шахрайство та програми комплаєнсу

Програми комплаєнсу мають важливе значення для зниження ризику шахрайства. Усуваючи або пом'якшуючи фактори, які сприяють шахрайству, програми комплаєнсу можуть допомогти захистити компанії від фінансових втрат, шкоди їхній репутації та юридичної відповідальності. Програми комплаєнсу відіграють вирішальну роль у захисті компаній від згубних наслідків шахрайства. Ось як вони цього досягають:

Зменшення можливостей для шахрайства:

- Внутрішній контроль. Встановлюючи чіткі та добре визначені політики та процедури, програми комплаєнсу створюють рамки, які ускладнюють здійснення шахрайських дій. Це включає розподіл обов'язків, контроль доступу та належне ведення записів;
- Навчання та підвищення обізнаності: навчання співробітників щодо ризиків шахрайства та червоних прапорців дає їм змогу виявляти підозрілу поведінку та повідомляти про неї. Це сприяє формуванню культури етичної поведінки, знижуючи ймовірність участі людей у шахрайських діях.

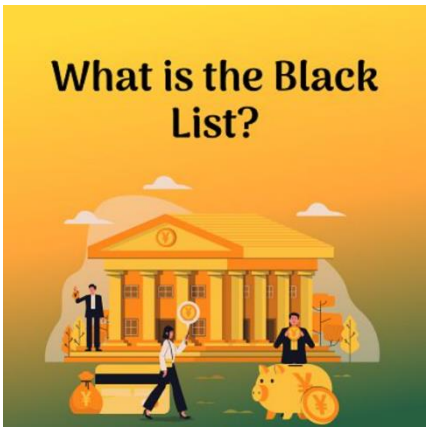
Пом'якшення впливу шахрайства:

- Раннє виявлення: програми комплаєнсу часто включають механізми моніторингу, такі як аналіз даних і внутрішні аудити. Ці інструменти допомагають виявляти шахрайські дії на ранніх стадіях, мінімізуючи потенційні фінансові втрати;
- Системи звітності: встановлення чітких каналів для повідомлення про підозри в шахрайстві заохочує людей висловлювати свої занепокоєння, що дозволяє швидко розслідувати та вжити заходів для виправлення ситуації;
- Правовий захист: Надійна програма комплаєнсу демонструє прихильність компанії етичній поведінці та дотриманню правил. Це може пом'якшити юридичні наслідки у випадку шахрайства.

Загалом, переваги впровадження сильної програми комплаєнсу набагато переважують витрати. Вона діє як проактивний щит від шахрайства, захищаючи фінансовий добробут, репутацію та статус компанії.

Корпоративне шахрайство є серйозною проблемою, яка може мати руйнівний вплив на доходи, репутацію та навіть безперервність організації. Таким чином, компанії повинні вживати заходи для усунення, боротьби та пом'якшення ризику шахрайства у своїй організації.

Що таке чорний список



Чорний список - це перелік осіб, груп або організацій, які вважаються небажаними або яким заборонено користуватися певними привілеями або можливостями. Це перелік людей, організацій або країн, яких інші уникають або залишають поза увагою через їхню ймовірну участь в аморальній або неетичній поведінці. Чорний список розглядається як форма помсти, покликана спричинити фінансові труднощі для людей, занесених до Чорного та Сірого списків FATF.

Що таке чорний список FATF?

Чорний список FATF, який офіційно називається "Список юрисдикцій з високим рівнем ризику, що підлягають заклику до дій" (скорочено - "Заклик до дій"), - це список, який веде FATF. Задля глобальної справедливості FATF щороку публікує два списки, в яких зазначаються юрисдикції, які, на її думку, мають недоліки у своїх системах комплаєнсу.

До Чорного списку FATF країни потрапляють, коли вони не усувають належним чином серйозні недоліки у своїх системах протидії відмиванню коштів та фінансуванню тероризму, як це визначено за результатами оцінок FATF. Ці недоліки можуть бути пов'язані з недостатніми законами, правилами, методами правозастосування або відсутністю рішучості ефективно боротися з фінансовими правопорушеннями.

1. Корейська Народно-Демократична Республіка (КНДР)

Позиція FATF щодо Північної Кореї залишається незмінною з 2011 року, радячи країнам-членам Групи та всім регіонам уважно стежити за діловим співробітництвом та угодами.

2. Іран

У жовтні 2019 року FATF рекомендувала всім країнам запровадити вдосконалені системи звітності про фінансові операції, вимагати більш ретельного зовнішнього аудиту для фінансових установ, що мають філії та дочірні компанії в Ірані, та посилити нагляд за філіями та дочірніми компаніями фінансових установ в Ірані.

3. М'янма

У 2020 році М'янма взяла на себе зобов'язання вирішити свої проблеми за допомогою запропонованого плану дій. План дій мав завершитися у вересні 2021 року. FATF визначила, що необхідні додаткові заходи, у зв'язку з повільним прогресом і недостатньою увагою до більшості пунктів плану дій. Це відповідає протоколам Групи, які закликають членів Групи та інші країни впроваджувати більш жорсткі заходи належної перевірки з урахуванням ризику, який становить М'янма.

Наслідки для країн, внесених до Чорного списку

Внесення країн до Чорного списку FATF призводить до серйозних наслідків для цих країн. Його результатом може стати

1. Економічні санкції
2. Посилена регуляторна перевірка
3. Перешкоди для міжнародної торгівлі та фінансових операцій

Фінансові установи повинні проявляти підвищену обережність при здійсненні операцій з країнами з "чорного списку" для того, щоб ефективніше управляти ризиками.

Що таке RegTech

Регуляторні технології, які часто називають RegTech, представляють нішу технологічних рішень, спеціально розроблених для допомоги в дотриманні регуляторних вимог у різних секторах. Вони використовують передові технології, такі як штучний інтелект, великі дані, машинне навчання та хмарні обчислення для автоматизації процесів дотримання вимог, тим самим підвищуючи точність і знижуючи ризики.

Чому RegTech важливий?

Регуляторні технології важливі, оскільки вони допомагають фінансовим установам дотримуватися нормативних вимог і ефективніше виправляти потенційні невідповідності. Ця технологія дозволяє швидко обробляти великі обсяги даних, що може бути складним завданням для звичайної комплаєнс-команди.

Вони покращують внутрішню діяльність компанії, підвищуючи її здатність вирішувати проблеми з дотриманням нормативних вимог, а також забезпечують захист від різних ризиків.

Крім того, RegTech підвищує точність, пропонуючи більш впорядкований і спрощений процес, ніж традиційні ручні методи, тим самим зменшуючи ймовірність людської помилки. Регулярні звіти та точна інформація сприяють створенню більш прозорої культури комплаєнсу в організації.

Застосування RegTech

Завдяки технологічним інноваціям для впровадження RegTech відкрився цілий ряд сфер застосування, серед яких управління капіталом, кібербезпека, управління ризиками, операційна діяльність, регуляторна звітність та інші. Розглянемо три ключові категорії.

Управління ризиками

Ризики швидко розвиваються, і їх взаємодія може мати значний вплив на бізнес-операції. Включення RegTech у стратегії управління ризиками надає перевагу, необхідну для пом'якшення та управління цими ризиками за допомогою винахідливих, заснованих на даних рішень. RegTech змінює правила гри в управлінні різними функціями ризик-менеджменту.

Кілька прикладів застосування RegTech в управлінні ризиками включають, зокрема, управління кіберризиками, управління кредитними ризиками, управління ринковими ризиками, управління ризиками шахрайства та управління репутаційними ризиками, але не обмежуються ними.

Врядування

Безсумнівно, ефективне управління має вирішальне значення для того, щоб будь-яка регульована організація працювала відповідально, етично та прозоро. Це передбачає створення політик, процедур і засобів контролю, які є основою для прийняття рішень, управління ризиками та підзвітності.

Законодавча відповідність

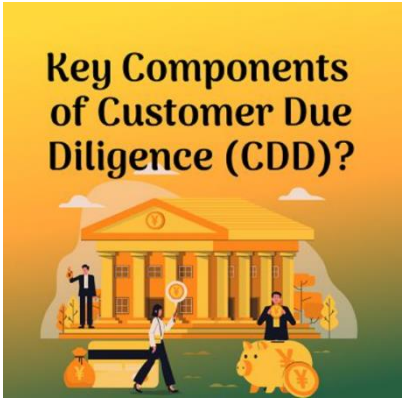
В основі місії RegTech лежить дотримання регуляторних вимог. Наприклад, в Індії дотримання вимог законодавства складається з трьох елементів - ведення реєстру регуляторних зобов'язань, управління ідентифікаційними даними та подання регуляторної звітності. Ці компоненти забезпечують дотримання регуляторного ландшафту і є фундаментальними для будь-якого рішення RegTech.

Використання анонімних типів активів: приклад протидії відмиванню коштів

Стаття описує випадок підозрілого обміну валюти в тихоокеанській країні, який призвів до розслідування можливого відмивання коштів. Новий клієнт, Джон, обміняв 2000 доларів США у європейській валюті на місцеву валюту та відкрив рахунок у банку, де негайно вніс ці кошти, а через кілька днів частина з них була знята готівкою. Інший підозрілий випадок стався, коли його кузина Сара намагалася внести 72 000 доларів США у європейській валюті в інший банк, але їй відмовили через незрозуміле походження коштів. Пізніше Джон і ще один кузен, Майк, здійснили аналогічні операції в різних банках. Після аналізу було виявлено зв'язок між цими особами та можливу участь у міжнародному наркотрафіку. Стаття також надає рекомендації для відповідальних працівників щодо посилення контролю за транзакціями і співпраці з правоохоронними органами.

https://bit.ly/3yRfPmL

Ключові компоненти належної перевірки клієнтів



Практики CDD можуть відрізнятися в різних компаніях, але всі підзвітні суб’єкти повинні включити кілька основних елементів у свою політику та процедури з CDD.

Ці фундаментальні елементи наступні:

1. Фінансові установи повинні збирати та підтверджувати конкретні дані клієнтів, такі як ім’я, адреса, дата народження та документи, що посвідчують особу, щоб підтвердити зібрані дані.

2. Фінансові установи повинні оцінювати рівень ризику кожного клієнта, враховуючи різні фактори, такі як їхня діяльність, джерело доходу та місце проживання. Для клієнтів, які мають більшу ймовірність виникнення проблем, необхідні більш суворі процедури належної перевірки.

3. Фінансові установи повинні контролювати діяльність своїх клієнтів, щоб виявити будь-які незвичні закономірності. Вони можуть включати значні транзакції, регулярні надходження чи відтоки, або взаємодію з країнами чи організаціями, які становлять значну загрозу.

4. Безперервна належна перевірка є важливою протягом усього періоду ділових відносин, від початку до кінця. Постійний моніторинг допомагає виявити можливу підозрілу поведінку та підтверджує точність даних клієнта. Це передбачає відстеження покупок клієнта, оновлення його профілю за потреби та проведення регулярних перевірок інформації.

5. Цілі фінансових установ, які здійснюють ретельну перевірку клієнта, полягають у відповідності правовим і регулятивним стандартам і покращенні своєї здатності виявляти та припиняти фінансові злочини.

6. Усі працівники, які працюють із CDD у банківській сфері, повинні пройти відповідну підготовку щодо дотримання правил і процесів. Завдяки цьому кожен зрозуміє, наскільки важлива CDD, і зможе помітити будь-яку дивну поведінку та повідомити про неї.

🎮 Відеоігри: нові можливості для відмивання коштів 🐦‍🔥

🐝 Відеоігри… це новий шлях для злочинців, терористів та інших незаконних осіб для збору, відмивання та ліквідації коштів.

🐦‍🔥Віртуальні валюти та цифрові активи в цих іграх, які купуються за реальні гроші, створили здебільшого нерегульований ринок, готовий для незаконної фінансової діяльності.

«Відмивання грошей у відеоіграх не є гіпотетичним ризиком. Протягом останніх двох десятиліть злочинці відмивали гроші за допомогою таких популярних відеоігор, як Roblox, World of Warcraft, Fortnite, Eve Online, Counter-Strike та Second Life — це лише кілька із сотень ігор, які видаються сприйнятливими до відмивання грошей».

🪽Процес відмивання коштів у відеоіграх зазвичай складається з трьох етапів:

1. Купуйте віртуальні активи або валюту за кошти, отримані незаконним шляхом

2. Перенесіть ці елементи на інший обліковий запис

3. Продавайте товари на публічних або незаконних вторинних ринках за фіксовану валюту

🕵 Порушення Керівних принципів ПВК/ФТ 🕵

Ця методологія явно порушує керівні принципи протидії відмиванню коштів і фінансуванню тероризму (ПВК/ФТ). Відсутність нагляду та регулювання в економіці відеоігор дозволяє злочинцям швидко відмивати великі суми за допомогою тисяч дрібних транзакцій, метод, знайомий деяким терористичним групам. 😳

У статті The Lawfare Institute згадується, що FATF закликала країни-члени боротися з незаконним фінансуванням через «нові технології», включаючи відеоігри. Однак більшість урядів намагаються регулювати постачальників послуг віртуальних активів (VASP), зосереджуючись насамперед на цінних паперах та активах на основі блокчейну, ігноруючи загрози, які створює економіка відеоігор. 🙈

🎯 Важливість висвітлення цього забутого сектору 🎯

🚧Оскільки уряди продовжують закривати традиційні шляхи фінансування тероризму, екстремістські групи довели свою майстерність у інноваціях і пошуку нових способів збору,

доступу та ліквідації коштів. Оскільки багато екстремістів уже знайомі з відеоіграми, ці нерегульовані ринки можуть стати для них наступним варіантом ведення фінансової діяльності. ☹

Вкрай важливо, щоб уряди, FATF та інші організації, які борються з відмиванням коштів і фінансуванням тероризму, серйозно поставилися до цієї загрози. Запроваджуючи правила протидії відмиванню коштів та фінансуванню тероризму та найкращі практики в індустрії відеоігор, ми можемо виявляти та стримувати фінансування тероризму, ускладнюючи зловмисникам використання цих віртуальних економік. 💪

Як визначити джерело коштів у криптовалюті

У кожному нормативному акті про боротьбу з відмиванням коштів підзвітні установи зобов'язані визначати джерело коштів або джерело багатства в конкретних ситуаціях і завжди у випадку клієнтів із високим ризиком.

Речі стають ще більш складними, коли ми говоримо про визначення джерела коштів або багатства в криптовалюті.

Чому?

Оскільки блокчейн — це публічна книга з псевдонімними адресами, відстежити джерело коштів складніше, ніж у традиційних банківських операціях.

Ось кілька найкращих практик щодо визначення джерела коштів у криптовалюті:

✓ Фінансові/банківські звіти:

Кошти, які використовуються для покупки криптовалюти, часто надходять із традиційних фінансових установ і надходять на централізовані біржі. Якщо це те, що говорить клієнт, ви зможете побачити транзакцію в будь-якій фінансовій/банківській виписці. Покупки за готівку становлять більшу проблему. У таких випадках перегляньте дані про зняття готівки у виписці.

✓ Документація постачальника послуг:

Постачальники послуг, такі як біржі криптовалют і платформи P2P, діють як посередники. Вони ведуть детальний облік транзакцій, включаючи джерело коштів, внесених їхніми клієнтами. Такі записи можуть дати пояснення щодо джерела коштів.

✓ Майнінг:

Клієнти, які беруть участь у майнінг-пулах, можуть надати історію виплат для встановлення джерела коштів. Для самостійних майнерів вимагайте квитанції про покупку обладнання та рахунки за комунальні послуги з відображенням високого споживання електроенергії. Це часто може виправдати вимогу клієнта, що кошти є доходами від майнінгу.

✓ Трудові договори:

Деякі фахівці отримують криптовалютні платежі за консультаційні чи маркетингові послуги. У трудових угодах зазвичай вказуються деталі оплати. У деяких випадках таких контрактів або підтвердження платежів може бути достатньо.