Серійний номер: ДСФМУ-ДК-2024-023
Вересень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Національна стратегічна оцінка 2024: Зростання організованої злочинності та нові загрози для безпеки Великобританії

Звіт представляє **Національну стратегічну оцінку (NSA) 2024 щодо серйозної та організованої злочинності у Великобританії**, яку підготувало Національне агентство з боротьби зі злочинністю (NCA). Цей документ висвітлює основні загрози для національної безпеки Великобританії, такі як кібератаки, наркотрафік, відмивання грошей, сучасне рабство та торгівля людьми. Оцінка також аналізує вплив технологій, міжнародних конфліктів і взаємозв'язків між злочинними угрупованнями.

Ключові моменти:

Зростання загрози від організованої злочинності: Основною рушійною силою злочинності стає цифровізація та зростаюча кількість людей, що проводять більше часу в інтернеті. Це призводить до зростання кіберзлочинності, шахрайства та сексуальної експлуатації дітей.

Загрози від наркотиків: Протягом 2023 року загроза, пов'язана з наркотиками, значно зросла. Збільшення виробництва кокаїну та складного синтетичного ринку наркотиків призвело до зростання доступності та небезпеки наркотиків. Це включає посилення торгівлі опіоїдами та канабісом, що негативно впливає на здоров'я суспільства.

Кіберзлочинність: Кіберзагрози, зокрема програми-вимагачі, залишаються одним із найбільш небезпечних викликів. Інциденти з використанням програм-вимагачів збільшилися на 103% порівняно з 2022 роком. Кіберзлочинці продовжують використовувати складніші методи, такі як клонування голосу та deepfake, для вчинення шахрайства та крадіжки інформації.

Використання криптовалют для відмивання грошей: У 2023 році спостерігалося збільшення використання криптовалют для відмивання грошей. Британські структури продовжують бути ключовими у міжнародному відмиванні коштів. Оцінюється, що щорічно через Великобританію відмиваються до £100 мільярдів.

Модернізація методів злочинності: Використання сучасних технологій, таких як штучний інтелект та 3D-друк, дозволяє злочинцям швидше адаптуватися та розширювати свої операції. Це включає створення складніших злочинних схем і нових методів обходу закону.

Збільшення трафіку людей та сучасного рабства: Злочинні угруповання продовжують використовувати людей для примусової праці та сексуальної експлуатації. Відзначається також зростання дитячого рабства та вербування дітей для розповсюдження наркотиків.

Загрози на кордоні: Організовані злочинні угруповання використовують слабкі місця на кордонах для контрабанди товарів, зокрема наркотиків та зброї, що продовжує створювати значні виклики для правоохоронних органів.

Висновки:

Незважаючи на успіхи в боротьбі з окремими злочинними операціями, загрози від організованої злочинності у Великобританії продовжують зростати. Технологічні досягнення дозволяють злочинцям розвивати нові методи, включаючи кіберзлочинність, фінансові махінації та експлуатацію людей.

http://surl.li/hjmlvf

Професійні відмивачі грошей: галузі, способи діяльності та зв'язки зі злочинними мережами

Документ ПФР Швеції аналізує діяльність професійних відмивачів коштів (PMLs), які спеціалізуються на систематичному відмиванні коштів для злочинних мереж. Професійні відмивачі коштів є критично важливими для організованої злочинності, оскільки допомагають управляти незаконними доходами, зменшуючи ризик для злочинців. PMLs працюють у різних секторах, таких як банки, нерухомість, юридичні послуги та криптовалютні біржі. Окрім індивідуальної діяльності, існують цілі мережі PMLs, включаючи системи «хавала», які використовуються для переведення коштів та ухилення від контролю фінансових інституцій.

Документ підкреслює, що сучасні злочинні мережі стають більш професійними та організованими, й все частіше купують послуги відмивання коштів як частину своїх злочинних операцій. Розвиток глобалізації та цифрових фінансових технологій зробив відмивання коштів центральним елементом майже кожного виду організованої злочинності. PMLs використовують легальні економічні структури для приховування незаконних операцій, що ускладнює їх виявлення правоохоронними органами та фінансовими інституціями.

Висновки

Професійні відмивачі коштів відіграють центральну роль у підтримці діяльності організованих злочинних угруповань, полегшуючи переміщення кримінальних доходів через різні схеми. Їх діяльність робить злочинні мережі більш стійкими до виявлення та руйнування. Важливо посилити заходи протидії PMLs, оскільки їх ліквідація може мати серйозний вплив на стабільність всієї кримінальної інфраструктури. Особливу загрозу становлять ті PMLs, які мають професійну кваліфікацію (наприклад, юристи або банкіри), оскільки їхня діяльність поєднує законні та нелегальні операції.

http://surl.li/lsdxce

Використання даних та захист конфіденційності у CBDC

Документ від Міжнародного валютного фонду (МВФ) досліджує потенційний вплив цифрових валют центральних банків (CBDC) на захист конфіденційності користувачів, а також на використання персональних даних у макроекономічних цілях. Впровадження CBDC супроводжується ризиками щодо зберігання та управління великими обсягами особистої інформації, включаючи фінансові транзакції, що може призвести до загроз для приватності користувачів.

Документ підкреслює необхідність інтеграції принципів "конфіденційність за дизайном" та технологій PET для балансування між інноваціями та захистом конфіденційності.

Центральні банки повинні знайти оптимальний баланс між використанням даних для економічного аналізу та забезпеченням конфіденційності. Використання таких даних може сприяти розвитку нових макроекономічних політик і підвищити конкурентоспроможність цифрових валют. Однак важливо впроваджувати системи з високим рівнем захисту від витоків даних, кібератак та інших загроз, що можуть підірвати довіру до CBDC. Рекомендується використовувати технології PET, які забезпечують анонімність транзакцій і мінімізують збір персональних даних.

Висновок

У висновках документу наголошується на тому, що впровадження цифрових валют центральних банків (CBDC) потребує уважного підходу до захисту конфіденційності користувачів. Важливо забезпечити баланс між ефективним використанням даних для економічного розвитку та безпекою особистої інформації. Використання технологій, що підвищують конфіденційність (PET), а також впровадження принципу "конфіденційність за дизайном" є критичними для збереження довіри громадськості до CBDC. Ризики, пов'язані з витоками даних або кіберзлочинністю, можуть звести нанівець переваги впровадження цифрових валют, якщо не буде забезпечено належний захист приватності.

http://surl.li/cebiej

РЕГУЛЮВАННЯ

Запуск 2024 Digital Assets Framework у Катарі

1 вересня 2024 року Катар зробив важливий крок у напрямку впровадження інноваційних цифрових технологій у свій фінансовий сектор. Центральний банк Катару (QCB), Катарський фінансовий центр (QFC) та його регуляторний орган (QFCRA) запровадили нову нормативну базу для цифрових активів — QFC Digital Assets Framework 2024. Цей документ встановлює правові та регуляторні основи для створення і регулювання цифрових активів у межах Катару, забезпечуючи прозорість та безпеку для всіх учасників ринку.

Нова нормативна база для цифрових активів стала результатом всебічного співробітництва з представниками фінансового, технологічного та юридичного секторів, як на місцевому, так і на міжнародному рівнях. Основою для розробки цієї рамкової бази слугувала стратегія розвитку фінансового сектору, яка була оголошена Центральним банком Катару.

Основні положення QFC Digital Assets Framework 2024:

- **Токенізація активів:** Встановлюються правила токенізації активів, що включають процес створення токенів, їх юридичне визнання, права власності на токени та активи, що ними представлені, механізми зберігання токенів, їх передачу та обмін. Ці положення забезпечують високий рівень захисту прав споживачів та інвесторів.
- **Смарт-контракти:** Визнання смарт-контрактів на юридичному рівні, що дозволяє забезпечити автоматичне виконання угод та зобов'язань за умови дотримання всіх необхідних вимог.
- **Довіра та прозорість:** QFC Digital Assets Framework спрямована на створення інфраструктури, яка забезпечить довіру та впевненість серед усіх учасників ринку. Це включає суворі вимоги до технологічної інфраструктури та високі стандарти безпеки.
- **Регулювання діяльності з інвестиційними токенами:** У межах нової нормативної бази було впроваджено інвестиційні токени, що представляють собою токени, які можуть включати права на цінні папери або інші фінансові інструменти. Діяльність, пов'язана з цими токенами, підлягає жорсткому регулюванню.

Ліцензування та авторизація постачальників токен-сервісів (TSP)

Після запуску QFC Digital Assets Framework компанії можуть подавати заявки на отримання ліцензій для виконання діяльності як постачальники токен-сервісів (TSP). Всі TSP повинні отримати відповідні ліцензії та авторизації від QFCRA для ведення діяльності з токенами. Для діяльності з інвестиційними токенами потрібна додаткова авторизація.

Заборонені токени

Важливим аспектом нової нормативної бази є чітке визначення типів токенів, які виключені з регулювання або заборонені до обігу в межах Катару. Це включає криптовалюти, що використовуються як замінники фіатних валют, або стейблкоїни, що використовуються як платіжний засіб.

Основні нормативні документи

Запровадження цифрових активів у Катарі ґрунтується на кількох ключових законодавчих актах та регуляторних документах, які встановлюють правила для учасників ринку та визначають права й обов'язки всіх сторін.

1. **Digital Asset Regulations 2024**

Digital Asset Regulations 2024 є основним нормативним документом, який регулює використання цифрових активів у межах Катарського фінансового центру (QFC). Цей документ визначає ключові поняття, такі як дозволені токени (permitted tokens), правила їх створення, володіння, передачі та анулювання. Digital Asset Regulations встановлює чіткі вимоги до ліцензування токен-сервісів (TSP) і описує, які токени виключені з регуляторного поля, включаючи криптовалюти, що використовуються як платіжний засіб або замінники фіатних валют. Цей регламент служить основою для формування безпечного та прозорого середовища для цифрових активів у Катарі.

https://qfcra-en.thomsonreuters.com/sites/default/files/net_file_store/QFCRA_15128_VER1.pdf

2. **Investment Token Rules 2024 (TOKN)**

Investment Token Rules 2024 (TOKN) є документом, що регулює діяльність з інвестиційними токенами, які представляють права на цінні папери або інші фінансові інструменти. Цей документ визначає, що таке інвестиційний токен, які види діяльності з такими токенами підлягають регулюванню, а також встановлює вимоги до ліцензування. Investment Token Rules також містять положення про заборону діяльності з певними токенами, які не відповідають встановленим критеріям, та надають регуляторному органу QFCRA право забороняти певні види діяльності з такими токенами у межах QFC.

https://qfcra-en.thomsonreuters.com/sites/default/files/net_file_store/QFCRA_15114_VER1.pdf

3. **Token service provider guidelines**

Token Service Provider Guidelines є керівництвом, яке надає інструкції для компаній, що бажають отримати ліцензію на надання послуг із токенами у межах QFC. Цей документ містить докладні пояснення щодо вимог до ліцензування, процесу подачі заявки та критеріїв, які повинні виконати компанії для отримання відповідної авторизації. Також у керівництві описані процедури, пов'язані з різними видами послуг, такими як валідація токенів, їхнє створення, зберігання, обмін та передача. Це керівництво спрямоване на забезпечення відповідності компаній найкращим міжнародним стандартам при роботі з цифровими активами.

http://surl.li/qwubai

4. **User Guide**

Гайд користувача є покроковим керівництвом, що допомагає компаніям зрозуміти процес встановлення та ведення діяльності як постачальника токен-сервісів у QFC. Цей посібник містить інформацію про переваги створення бізнесу в QFC, включаючи доступ до міжнародних ринків, правові та податкові пільги, 100% іноземну власність та конкурентоспроможну податкову систему. Посібник також охоплює процес подачі заявки на ліцензію, структуру зборів та відповіді на поширені запитання, що можуть виникнути у компаній, які планують працювати у сфері цифрових активів у Катарі.

http://surl.li/etivna

Висновок

Запровадження QFC Digital Assets Framework 2024 є важливим кроком для розвитку цифрової економіки в Катарі. Ця нормативна база створює умови для безпечного та прозорого розвитку ринку цифрових активів, залучення інвестицій та стимулювання інновацій у фінансовому секторі. Суворі регуляторні вимоги, інтеграція новітніх технологій та високі стандарти безпеки забезпечать стабільний розвиток цього сектору відповідно до міжнародних найкращих практик та стандартів.

Заява Вольфсберзької групи щодо Повідомлення FinCEN про запропоновані норми для Правила програм з ПВК

Документ є листом-зверненням Wolfsberg Group до FinCEN щодо запропонованого правила для Програми протидії відмиванню коштів (AML Program Rule) у рамках AML Act 2020. **Wolfsberg Group** вітає спрямування нового правила на підвищення ефективності AML-програм, однак **висловлює занепокоєння, що запропоновані зміни можуть ненавмисно призвести до зосередження на технічній відповідності замість ефективного управління ризиками**. Група наголошує на необхідності чітко визначити принципи ефективності AML-програм, щоб сприяти досягненню реальних результатів у боротьбі з фінансовими злочинами. Вона також рекомендує FinCEN забезпечити фінансовим установам більшу гнучкість у проведенні процесів оцінки ризиків, а також переглянути вимоги щодо ресурсів та інноваційних технологій у сфері AML/CFT.

Ключові висновки:

1. **Пріоритетність високоризикових клієнтів та операцій:**

Wolfsberg Group наполягає на тому, що для ефективного управління ризиками фінансовим установам слід переорієнтовувати свої ресурси з діяльності, яка пов'язана з низьким рівнем ризику, на високоризикові операції та клієнтів. У документі зазначається, що поточна редакція запропонованого правила FinCEN може бути інтерпретована таким чином, що всі клієнти, незалежно від рівня ризику, повинні отримувати однаковий рівень уваги. Це суперечить концепції ризик-орієнтованого підходу, який є основоположним у сучасних програмах протидії відмиванню грошей. Група пропонує внести до правила уточнення, яке дозволить фінансовим установам спрямовувати більше ресурсів на контроль високоризикових клієнтів і операцій, як того вимагає Закон про AML 2020.

2. **Гнучкість у процесах оцінки ризиків:**

Група підкреслює, що запропоноване правило має забезпечити фінансовим установам можливість самостійно визначати, яким чином проводити оцінку ризиків, як часто її оновлювати та які процеси включати до ризик-орієнтованої програми. Важливо, щоб кожна фінансова установа могла адаптувати свою програму до специфічних загроз, пов'язаних із її бізнес-моделлю, розміром та регіоном діяльності. Це дозволить уникнути підходу "галочок" і створить більш гнучкі та ефективні AML/CFT програми, які можуть реагувати на зміни в ризиках в реальному часі. Wolfsberg Group вважає, що фокус на єдиній оцінці ризиків обмежує гнучкість і знижує ефективність управління ризиками, оскільки цей підхід більше орієнтований на минулі події, а не на активне управління ризиками.

3. **Підтримка інновацій у сфері AML/CFT:**

Wolfsberg Group закликає FinCEN активно заохочувати фінансові установи до впровадження інноваційних технологій для підвищення ефективності боротьби з фінансовими злочинами. Група наголошує, що існують перешкоди для інновацій, такі як очікування регуляторів щодо "паралельного запуску" нових і старих систем або моделі управління ризиками, що можуть гальмувати інноваційні процеси. У цьому контексті група рекомендує внести до правила положення, яке б дозволило установам використовувати інновації без необхідності дотримуватись надмірних вимог, що не завжди враховують реальні загрози. Заохочення інновацій може зробити програми протидії фінансовим злочинам більш ефективними та гнучкими.

4. **Чітке визначення принципів ефективності:**

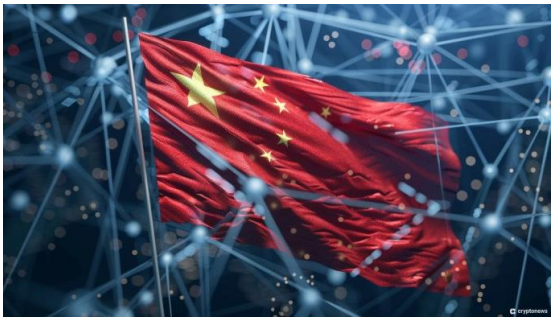
Документ наголошує на важливості чіткого визначення, що означає "ефективність" для AML/CFT програм. Це дозволить фінансовим установам, правоохоронним органам і регуляторам мати єдине розуміння того, якими мають бути результати ефективної програми. Wolfsberg Group пропонує, щоб FinCEN розробило чіткі принципи ефективності, що включали б оцінку ризиків, управління загрозами та зворотний зв'язок із правоохоронними органами. Група також звертає увагу на те, що ефективна AML-програма не може гарантувати відсутність усіх фінансових злочинів, оскільки програми повинні бути спрямовані на управління ризиками, а не на повне їх викорінення. Важливо, щоб регулятори визнавали, що певний рівень ризику є прийнятним у рамках ризик-орієнтованого підходу.

5. **Пролонгований термін впровадження:**

Wolfsberg Group вважає, що шість місяців, запропонованих FinCEN для впровадження нових правил, є недостатнім терміном для реалізації таких значних змін. Група пропонує продовжити цей термін до двох років, щоб фінансові установи могли належним чином підготуватися до нових вимог. Важливо, щоб зміни не призводили до негативних наслідків через поспіх або недоотриману інформацію. Крім того, для повної реалізації реформи AML потрібні додаткові зміни, такі як вдосконалення правил подачі звітів про підозрілу діяльність (SAR) і валютні операції (CTR), оновлення навчальних програм для працівників та забезпечення зворотного зв’язку між правоохоронними органами та фінансовими установами.

https://dev.wolfsberg-group.org/news/73

Нове правове регулювання відмивання грошей у Китаї: посилення відповідальності та боротьба з використанням віртуальних активів



19 серпня 2024 року Верховний народний суд і Верховна народна прокуратура Китаю оприлюднили спільні судові роз'яснення щодо застосування закону в справах про відмивання грошей. Це рішення спрямоване на посилення боротьби з відмиванням грошей шляхом чіткого визначення критеріїв злочинних дій, таких як "самовідмивання" і "чужого відмивання", а також оновленням підходів до покарання за тяжкі злочини, включаючи використання новітніх фінансових технологій для приховування доходів.

Ключові моменти:

Чіткі критерії для визначення злочинів: Роз'яснення розрізняють "самовідмивання" (коли особа приховує доходи від власних злочинів) та "чужого відмивання" (коли одна особа допомагає приховати незаконні доходи іншої). Вони також встановлюють стандарти для оцінки суб'єктивної обізнаності злочинця про незаконність отриманих доходів. Враховуються такі фактори, як кількість доходів, спосіб їх переведення та професійний досвід особи.

Тяжкі злочини та покарання: Відмивання грошей на суму понад 5 мільйонів юанів або завдання шкоди на суму понад 250 тисяч юанів визначається як тяжкий злочин. Також злочини, пов’язані з декількома випадками відмивання або відмовою співпрацювати у поверненні коштів, потрапляють до категорії тяжких. Вироки за такі злочини можуть досягати п’яти років ув’язнення або більше, а також штрафи у великих розмірах.

Використання віртуальних активів: У роз'ясненнях наголошено на тому, що використання віртуальних активів для приховування або переведення доходів також є способом відмивання грошей. Віртуальні активи тепер офіційно розглядаються як частина механізмів фінансових

шахрайств, що охоплюють криптовалютні транзакції, обмін фінансовими активами та інші технологічні методи.

Посилена співпраця між органами: Важливим елементом нових правил є створення механізмів співпраці між різними державними структурами для ефективнішої боротьби з відмиванням грошей. У рамках цих заходів був розроблений принцип "одна справа — два розслідування", що дозволяє одночасно розглядати як основний злочин, так і пов'язані з ним фінансові операції. Наприклад, у Гуандуні запроваджено правило "три обов'язкові етапи", щоб полегшити виявлення злочинів у фінансовій сфері.

Правовий захист: У разі активного співробітництва з владою, наприклад, повернення незаконних доходів або надання свідчень, обвинувачені можуть отримати полегшене покарання. Крім того, легкі порушення або малозначні випадки можуть призвести до відмови від кримінального переслідування.

Покарання для організацій: Компанії, причетні до відмивання грошей, також можуть нести відповідальність. Якщо злочин скоюється через організацію, ця структура підлягає штрафу, а керівники можуть нести особисту відповідальність.

Висновки:

Оприлюднені роз'яснення є значним кроком у боротьбі з відмиванням грошей у Китаї. Вони спрямовані на вдосконалення правових норм, підвищення ефективності правосуддя та зменшення використання нових фінансових технологій для незаконної діяльності. Чіткі визначення критеріїв злочину, підходи до розслідування і співпраця між державними органами мають сприяти ефективнішій боротьбі з фінансовими злочинами.

http://surl.li/rxnxlq

Розуміння відповіді ЄС на відмивання коштів: Новий пакет ЄС щодо боротьби з відмиванням коштів

Документ є оглядом заходів Європейського Союзу (ЄС) щодо протидії відмиванню грошей та фінансуванню тероризму. Він **описує, як злочинці використовують складні методи для перетворення "брудних" грошей у легальні доходи**, що створює значні загрози для фінансової стабільності та безпеки суспільства. ЄС активно реагує на ці виклики, удосконалюючи свої законодавчі механізми та створюючи нові інституції, як-от Управління з боротьби з відмиванням грошей (AMLA) у Франкфурті, яке займатиметься координацією та наглядом за дотриманням правил боротьби з фінансовими злочинами в усіх країнах-членах. **Документ охоплює етапи процесу відмивання грошей та наголошує на важливості міжнародної співпраці, зокрема через FATF, Europol, Interpol та інші організації, щоб протидіяти глобальним фінансовим злочинам. Також аналізуються ключові зміни, запроваджені ЄС у законодавстві, зокрема щодо криптовалют та цифрових активів, що ускладнюють відстеження фінансових потоків**.

Ключові висновки:

1. **Складність і еволюція методів відмивання грошей:** Злочинці використовують складні багатоступеневі методи, щоб приховати походження грошей, включаючи використання криптовалют та цифрових активів. Це створює значні труднощі для правоохоронних органів і фінансових установ, оскільки швидкість та анонімність операцій ускладнюють відстеження фінансових потоків.

2. **Важливість міжнародної співпраці:** Відмивання грошей є глобальною проблемою, і для її ефективної протидії потрібна тісна співпраця між міжнародними організаціями та національними урядами. FATF, Interpol, Europol та інші організації забезпечують координацію та спільні дії для відстеження та запобігання фінансовим злочинам.
3. **Реформа законодавства ЄС:** ЄС продовжує реформувати свої закони з ПВК/ФТ, запроваджуючи новий регуляторний пакет, що включає нову директиву та регламент, який стосується криптовалют та цифрових активів. Створення AMLA у Франкфурті дозволить централізувати нагляд і забезпечить єдині правила боротьби з відмиванням грошей по всьому ЄС, що усуне проблеми з неоднорідною імплементацією правил у різних країнах-членах.
4. **Інновації та технології:** Документ підкреслює важливість врахування нових викликів, таких як цифрові фінанси та криптовалюти, які використовуються для відмивання грошей і фінансування тероризму. ЄС відповідає на ці виклики шляхом удосконалення регулювання щодо криптоактивів та посилення вимог до прозорості фінансових операцій.
5. **Усвідомлення ризиків для суспільства:** Відмивання грошей негативно впливає на суспільство, підриваючи легальні фінансові структури та загрожуючи економічній стабільності. Важливо, щоб громадськість та уряди розуміли серйозність цієї проблеми і підтримували глобальні зусилля щодо боротьби з цим злочином.

https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762387/EPRS_BRI(2024)762387_EN.pdf

САНКЦІЇ

Аналіз нещодавніх санкцій Великобританії

31 липня 2024 року уряд Великої Британії представив значне оновлення свого санкційного режиму, спрямованого на Росію, шляхом прийняття Положення про Росію (Санкції) (Вихід з ЄС) (Поправка) (№ 3) 2024 року. **Ця поправка є найвагомішим розширенням критеріїв для визначення осіб та організацій для заморожування активів з моменту впровадження санкційних положень Великобританії щодо Росії у 2019 році**.

Розширені критерії для санкцій

Поправка значно розширює визначення того, хто вважається «залученою особою», збільшуючи таким чином коло потенційних цілей для санкцій. Раніше санкції здебільшого були зосереджені на тих, хто безпосередньо сприяв дестабілізації України або загрожував її суверенітету. **Нові правила розширюють сферу дії, включаючи осіб або організації, які мають непряме відношення, наприклад, тих, хто займає ключові посади в організаціях, пов'язаних з дестабілізуючими діями, або тих, хто надає фінансову підтримку чи ресурси російському уряду**.

Це розширення означає, що під загрозою санкцій може опинитися ширше коло осіб, включно з тими, хто не перебуває у Великій Британії або не має прямої причетності до ситуації. **Особливо примітним є включення фінансових послуг та економічних ресурсів до критеріїв, що може зачепити іноземні організації, які займаються законною діяльністю, але опосередковано приносять користь Росії**.

Потенційний вплив та виклики

Розширення цих критеріїв, ймовірно, матиме значний вплив на світовий бізнес, особливо на ті компанії, що працюють у секторах, які мають непрямі зв’язки з російськими інтересами. Ці зміни додають новий рівень складності та вимагають посиленої перевірки, оскільки компаніям тепер необхідно ретельно оцінювати свої зв'язки, щоб випадково не потрапити під дію санкцій Великобританії.

Хоча ці зміни офіційно не названі вторинними санкціями, їхній ефект схожий на такі заходи. Тепер уряд Великобританії може впливати на організації за межами своєї юрисдикції, що нагадує підхід США щодо санкцій проти таких країн, як Іран. Це може створити значні юридичні та операційні виклики для міжнародного бізнесу, особливо стосовно дотримання вимог та управління ризиками.

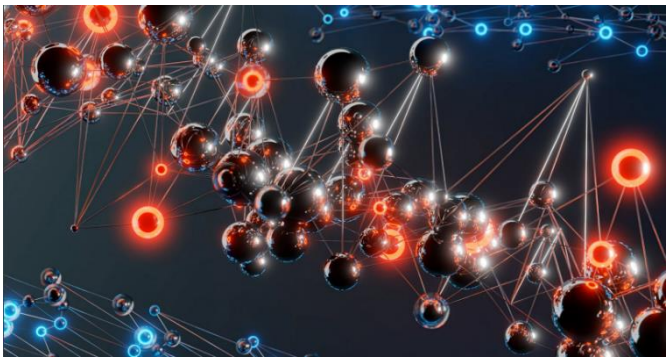
Висновок

Поправка № 3 є стратегічною ескалацією санкційного режиму Великої Британії, що узгоджується з ширшими зусиллями країн G7 щодо економічної ізоляції Росії. Однак повні наслідки цих змін стануть очевидними лише тоді, коли Великобританія почне застосовувати нові критерії для визначення осіб та організацій.

https://www.legislation.gov.uk/uksi/2024/834/made

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Масштабування генеративного ШІ в банківській справі: вибір найкращої операційної моделі



Документ від McKinsey, присвячений впровадженню генеративного штучного інтелекту (gen AI) у банківській сфері. Він аналізує, як правильно обрати операційну модель для масштабування gen AI у фінансових установах. Gen AI може значно підвищити ефективність і продуктивність банківського сектору, додаючи до $200-340 мільярдів щорічної вартості. Однак існують виклики, пов'язані з впровадженням цієї технології, включаючи ризики помилок, упередженості, безпеки та управління. **Документ детально розглядає різні операційні моделі, від централізованої до децентралізованої, і наводить аргументи на користь вибору центрально-координованого підходу на ранніх етапах впровадження gen AI.** Основна ідея полягає в тому, що правильна операційна модель має підтримувати ефективне масштабування технології, враховуючи структуру і культуру організації.

Ключові висновки:

1. **Централізація як ключ до успіху:** Документ підкреслює важливість централізованої операційної моделі на початкових етапах впровадження gen AI у банківському секторі. Централізоване управління дозволяє краще розподілити обмежені ресурси, такі як висококваліфіковані кадри, ефективніше відстежувати технологічні новинки та приймати ключові рішення, що стосуються технологічної архітектури, провайдерів хмарних послуг, фінансування та партнерств. Такий підхід дозволяє швидше перейти від експериментальних проектів до масштабування рішень, що мають значний вплив на бізнес.
2. **Гнучкість і адаптивність операційної моделі:** Незважаючи на переваги централізації, документ визнає, що в міру дозрівання технології gen AI можливий перехід до більш федеративної моделі управління. Це означає, що різні підрозділи організації можуть брати на себе більшу відповідальність за розробку та впровадження gen AI-рішень, зберігаючи при цьому централізоване управління стандартами безпеки, управління ризиками та технологічною архітектурою.
3. **Стратегічна важливість операційної моделі:** Правильно обрана операційна модель має бути тісно пов'язана зі стратегією компанії та її організаційною структурою. Це дозволяє не лише ефективно масштабувати gen AI, але й максимально інтегрувати цю технологію в усі аспекти бізнесу. Організації повинні розробляти операційні моделі, що дозволяють ефективно керувати ген AI-ініціативами на всіх рівнях, забезпечуючи їх відповідність стратегічним цілям компанії.
4. **Ризики децентралізації:** Документ також вказує на потенційні ризики, пов'язані з децентралізованим підходом до впровадження gen AI. Незалежні підрозділи, які керують власними gen AI-проектами, можуть не мати достатнього доступу до передових знань і найкращих практик, які можна отримати від централізованої команди. Це може призвести до того, що проекти залишаться на експериментальному етапі і не будуть масштабовані, що знижує ефективність і цінність ген AI для всієї організації.
5. **Необхідність інтеграції управління ризиками:** Впровадження gen AI вимагає ретельного управління ризиками, включаючи захист даних, запобігання порушенням інтелектуальної власності та забезпечення відповідності регуляторним вимогам. Централізоване управління ризиками дозволяє ефективніше реагувати на нові загрози та підтримувати високий рівень безпеки в умовах швидко змінюваного технологічного ландшафту.

Таким чином, документ підкреслює важливість ретельного планування і вибору операційної моделі для ефективного впровадження gen AI в банківській сфері, акцентуючи на важливості балансу між централізацією та гнучкістю, що дозволяє швидко адаптуватися до змінних умов та максимально використовувати потенціал цієї технології.

http://surl.li/uzhebe

Діяльність Північної Кореї в секторі казино та ігор: як реагують юрисдикції?

Документ розглядає участь Північної Кореї у гральному секторі, зокрема в казино, з метою генерації та відмивання коштів для фінансування програм зі створення зброї масового знищення (ЗМЗ). Він аналізує загрози, пов'язані з використанням грального бізнесу для ухилення від санкцій, зокрема за допомогою криптовалют. Дослідження підкреслює необхідність для юрисдикцій враховувати ці ризики у своїх національних оцінках ризиків. Автори також розглядають роль "джанкетів" (гральних агентів) і організованої злочинності в схемах відмивання грошей та фінансування розповсюдження ЗМЗ, а також пропонують стратегії для мінімізації цих ризиків. Основна мета роботи – надання рекомендацій для юрисдикцій щодо управління ризиками у гральному секторі з акцентом на ухиляння від санкцій через казино.

Ключові висновки:

1. **Активне використання Північною Кореєю грального сектору для фінансування програм ЗМЗ**

Північна Корея успішно експлуатує слабкості в регуляторному середовищі грального бізнесу (як наземного, так і онлайн казино) для отримання та відмивання коштів, які потім використовуються для фінансування програм зі створення зброї масового знищення (ЗМЗ). Використання криптовалют робить такі схеми більш складними для відстеження, оскільки криптовалюти дозволяють приховати походження коштів. Це створює значні загрози для міжнародної безпеки, оскільки юрисдикції можуть не усвідомлювати повного масштабу цих загроз.

2. **Роль джанкет-операторів у схемах відмивання грошей**

Джанкет-оператори, які діють як посередники між гравцями та казино, можуть бути використані для відмивання коштів у складних схемах, включаючи використання криптовалют. Джанкет-структури часто є недостатньо регульованими, що дозволяє операторам ухилятися від належної перевірки походження коштів. Вони можуть діяти як частина транскордонної тіньової банківської системи, переміщуючи нелегальні активи через кілька юрисдикцій, ускладнюючи контроль та моніторинг.

3. **Необхідність посилення нагляду за гральним сектором**

Юрисдикції повинні переглянути свої регуляторні механізми, щоб включити до них чіткі процедури ліцензування та моніторингу діяльності казино, зокрема щодо використання джанкетів та криптовалют. Багато юрисдикцій мають слабкий або відсутній нагляд за діяльністю джанкет-операторів, що створює вразливості для відмивання грошей. Такі регуляторні недоліки можуть використовуватися Північною Кореєю для ухилення від міжнародних санкцій.

4. **Зростаюча загроза криптовалют у казино**

Використання криптовалют у казино зростає, що створює нові ризики для відмивання коштів та фінансування ЗМУ. Криптовалюти надають можливість проводити анонімні транзакції, які важко

відстежити за допомогою традиційних методів моніторингу фінансових потоків. Юрисдикції повинні включати вимоги до криптовалют у свої регуляторні рамки для грального бізнесу, щоб мати змогу відстежувати транзакції за допомогою аналітичних інструментів блокчейну.

5. **Необхідність міжнародної співпраці для протидії загрозам**

Щоб ефективно боротися з відмиванням грошей та фінансуванням розповсюдження ЗМЗ через казино, потрібна тісна співпраця між юрисдикціями, гральними компаніями, криптовалютними біржами та аналітичними компаніями, що спеціалізуються на блокчейні. Лише за допомогою міжнародної координації можна забезпечити запобігання зловживанню криптовалютами та казино для ухилення від санкцій. Спільні зусилля дозволять виявляти і припиняти діяльність, спрямовану на приховування незаконних фінансових потоків, пов'язаних із Північною Кореєю та іншими підсанкційними державами.

6. **Впровадження найкращих практик і рекомендацій для зменшення ризиків**

Документ наголошує на важливості впровадження юрисдикціями чітких правил щодо ідентифікації джерел коштів і багатства, що використовуються в гральному секторі. Юрисдикції повинні вимагати від казино детального розкриття інформації про походження коштів клієнтів, включаючи джанкет-операторів, та запроваджувати постійний моніторинг транзакцій. Це сприятиме зниженню ризиків зловживання казино для відмивання коштів та фінансування програм ЗМЗ.

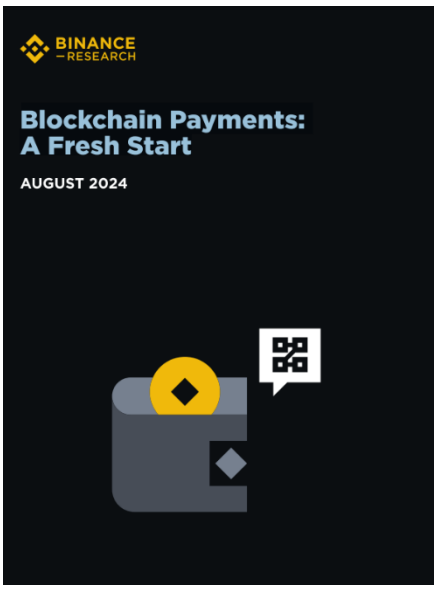
7. **Посилення контролю за використанням криптовалют у гральному секторі**

Юрисдикції повинні вимагати від казино, які використовують криптовалюти, дотримуватися додаткових умов ліцензування, таких як обмеження видів дозволених криптовалют, використання аналітичних інструментів блокчейну для відстеження транзакцій та встановлення порогових лімітів для операцій із криптовалютами. Це зменшить ризики використання криптовалют для ухилення від санкцій та фінансування незаконних операцій.

Ці висновки підкреслюють необхідність посилення глобального нагляду за гральним сектором та вжиття заходів для боротьби з ризиками, пов'язаними з відмиванням грошей, фінансуванням тероризму та фінансуванням розповсюдження ЗМЗ, зокрема в контексті нових фінансових технологій, таких як криптовалюти.

https://static.rusi.org/north-korean-activity-in-casino-gaming-industry_0.pdf

Блокчейн-платежі: новий початок



Документ "Blockchain Payments: A Fresh Start" детально аналізує сучасний стан глобальних платіжних систем, які здебільшого працюють на застарілих технологіях 50-річної давності. Він наголошує на складнощах міжнародних транзакцій, що включають значні витрати та затримки через участь численних посередників. Блокчейн пропонується як нова платіжна інфраструктура, що може усунути ці недоліки, надаючи майже миттєві та менш витратні транзакції з більшою прозорістю. Документ також висвітлює впровадження таких рішень, як стабільні монети (stablecoins), які забезпечують стабільну вартість активів для обробки платежів на блокчейнах. Особливу увагу приділено перспективам використання публічних блокчейнів для міжнародних розрахунків і пілотним проектам, наприклад, Visa та Crypto.com, що вже успішно застосовують блокчейн для зменшення витрат на трансакції.

Документ також звертає увагу на основні виклики, з якими стикається блокчейн-індустрія в контексті платежів. Це питання масштабованості, складність використання для середньостатистичних користувачів і регуляторна невизначеність, яка заважає

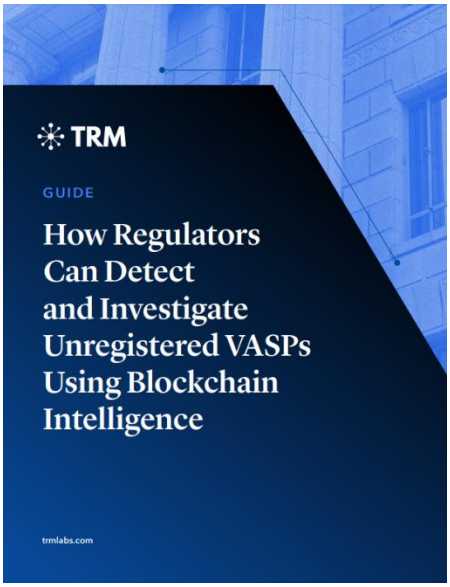
масовому впровадженню технології. Однак, незважаючи на ці проблеми, автори прогнозують, що блокчейн стане ключовим елементом майбутньої глобальної платіжної інфраструктури, оскільки він дозволяє знизити витрати, прискорити розрахунки та усунути залежність від банківських систем, особливо у міжнародних переказах і грошових відправленнях.

Висновки

Блокчейн-технології можуть радикально змінити індустрію платежів, усунувши посередників і знизивши витрати на транзакції, особливо в міжнародних розрахунках та переказах. Поточні проблеми, такі як масштабованість і регуляторна невизначеність, є головними бар'єрами для масового впровадження, але розвиток інфраструктури і технологій, таких як стабільні монети та Layer-2 рішення, може подолати ці виклики. Блокчейн також пропонує більше прозорості та безпеки порівняно з традиційними платіжними системами, що робить його привабливою альтернативою в довгостроковій перспективі.

https://public.bnbstatic.com/static/files/research/blockchain-payments-a-fresh-start.pdf

Як регулятори можуть виявляти та розслідувати діяльність незареєстрованих VASP за допомогою Blockchain Intelligence



Документ "Detect and Investigate Unregistered VASPs Using Blockchain Intelligence" аналізує проблеми, пов'язані з незареєстрованими постачальниками послуг віртуальних активів (VASPs) та пропонує практичні рішення для їх виявлення за допомогою інструментів блокчейн-розвідки. Незареєстровані VASPs, які часто працюють без ліцензії, піддають систему ризикам відмивання коштів і фінансування тероризму, оскільки вони не дотримуються вимог ПВК/ФТ. У документі детально описані методи аналізу транзакцій, зокрема виявлення прихованих зв'язків із ліцензованими VASPs та аналіз часових рамок транзакцій, що дозволяє відстежувати незаконну діяльність у фінансовій системі.

Для регуляторів пропонується низка ефективних інструментів, включаючи використання блокчейн-розвідки для аналізу ліквідності, місцезнаходження та взаємодії між платформами. Завдяки цьому можна виявляти "паразитарні" сервіси, які використовують інфраструктуру інших платформ без згоди, а також аналізувати операції та перевіряти відповідність діяльності вимогам юрисдикції.

Висновки

Незареєстровані VASPs становлять значну загрозу для фінансової безпеки через відсутність вимог щодо дотримання правил боротьби з відмиванням коштів (ПВК) і фінансуванням тероризму (ПФТ). Використання інструментів блокчейн-розвідки дозволяє регуляторам ідентифікувати потенційні загрози, перевіряти джерела ліквідності та аналізувати поведінку транзакцій для виявлення незаконної діяльності. Розслідування часто включають аналіз транзакційних часових рамок та зв'язків із ліцензованими VASPs, що дозволяє регуляторам виявляти нелегальні операції навіть у складних схемах.

http://surl.li/gneaqi

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

Курс щодо Travel Rule

Цей навчальний курс зосереджений на виконанні вимог "Travel Rule", що стосується обміну інформацією між фінансовими установами під час переказу активів. Правило є обов'язковим у багатьох юрисдикціях. Курс охоплює основні аспекти імплементації Travel Rule, зокрема:

-Як забезпечити відповідність міжнародним стандартам.
-Інструменти для ефективної передачі інформації між учасниками транзакцій.
-Вимоги до зберігання та передавання даних про відправника та отримувача.
-Приклади із практики та кейси, пов'язані з відмиванням грошей та фінансуванням тероризму.

Навчальний курс вже доступний для реєстрації.

Цей курс організовує команда Sumsub, яка спеціалізується на рішеннях для KYC/AML, відомих своєю експертизою у сфері ПВК/ФТ. Одним із ключових тренерів є Делфін Форма (Delphine Forma), яка має багаторічний досвід роботи в галузі дотримання міжнародних норм у фінансових інституціях.

Кому може бути корисний цей курс? Курс орієнтований на:

- Працівників фінансових установ, які відповідають за дотримання норм ПВК/ФТ.
- Спеціалістів у сфері криптовалют та фінтех-індустрії.
- Compliance officers, які хочуть поглибити свої знання щодо Travel Rule.
- Фахівців, які прагнуть залишатися в курсі актуальних міжнародних вимог.

http://surl.li/gzyqcn

ПВК у 2024 році: ШІ, регулювання та що далі

Світ боротьби з відмиванням грошей швидко розвивається, і 2024 рік принесе значні зміни, які вплинуть на всіх у фінансовому секторі.

Від нового органу Європейського Союзу з питань ПВК до розвитку штучного інтелекту у виявленні підозрілих дій, ландшафт змінюється швидше, ніж будь-коли раніше.

🔍 **Основні ідеї, розглянуті в цьому відео:**

- ✓ Регуляторна реформа: дізнайтеся, як нові норми ЄС підвищують ставки щодо комплаєнсу.
- ✓ Штучний інтелект у сфері ПВК: дізнайтеся, як штучний інтелект революціонізує спосіб виявлення та запобігання фінансовим злочинам.
- ✓ Інтегровані процеси: розумійте важливість об'єднання зусиль з ПВК у різних системах.
- ✓ Комплаєнс криптосфери: правила щодо цифрових активів посилюються.
- ✓ Хмарні обчислення в ПВК: дізнайтеся, як хмарні сервіси змінюють стратегії відповідності.

https://www.youtube.com/watch?v=idDzJTPh604

ІНШІ НОВИНИ

Міжнародна загроза сексторції: зростання злочинів проти підлітків та боротьба за справедливість

Стаття стосується проблеми сексторції (секс-шантажу) — поширеної форми онлайн-злочинів, коли шахраї змушують жертв надсилати інтимні фотографії або відео, а потім шантажують їх, вимагаючи гроші під загрозою публікації цих матеріалів. Увага приділяється тому, як міжнародні кіберзлочинці, переважно з Західної Африки, стали основними виконавцями цього злочину. Національне кримінальне агентство Великої Британії (NCA) попереджає, що такі злочинці не захищені від екстрадиції та можуть бути притягнуті до відповідальності у Великій Британії.

Ключові моменти:

Проблема сексторції серед молоді: Спостерігається зростання кількості випадків, коли молоді люди стають жертвами онлайн-шахраїв. Особливо постраждалими є підлітки, які обманом спонукаються до надання інтимних матеріалів. Злочинці погрожують поширенням цих матеріалів, якщо не отримають викупу.

Міжнародний характер злочину: Шахраї переважно базуються у Західній Африці, і NCA працює над екстрадицією таких злочинців. NCA наголошує, що вони не уникнуть відповідальності у Великій Британії, навіть якщо перебувають за межами країни.

Наслідки для жертв: У статті наводяться приклади трагічних випадків, коли підлітки вкоротили собі віку через тиск і шантаж. Наприклад, йдеться про Дінала Де Алвіса та Мюррея Доуї, які загинули після того, як їх шантажували онлайн-злочинці.

Поширення контенту про сексторцію: В мережі є легко доступні онлайн-ресурси, що пропонують інструкції для шахраїв щодо здійснення сексторції, навіть із детальними відеоуроками за окрему плату.

Статистичне зростання сексторції: Фонд Internet Watch Foundation (IWF) повідомив про 19-відсоткове зростання кількості випадків сексуального шантажу, пов'язаного з фінансовими вимогами, у перші шість місяців 2024 року порівняно з аналогічним періодом попереднього року. Особливо зросла кількість жертв серед дівчаток.

Співпраця на міжнародному рівні: NCA активно співпрацює з міжнародними партнерами для боротьби з цими злочинами, що включає обмін досвідом та спільні заходи проти кіберзлочинців.

Потреба у політичних діях: Організації та активісти закликають уряд до рішучих дій, аби зупинити зростання випадків сексторції. Особливо важливим є підвищення обізнаності серед населення та розширення заходів для захисту молоді.

http://surl.li/wbrftv

Рай для контрабандистів: Румунська держава не повертає гроші, отримані від незаконної торгівлі наркотиками

Дослідження окреслює систематичну проблему неспроможності румунських правоохоронних органів ефективно боротися з наркоторгівлею та відмиванням грошей. Хоча країна має інструменти для відстеження та конфіскації доходів від наркоторгівлі, використання цих інструментів є дуже обмеженим. Влада визнає проблему, але дієвих заходів недостатньо. Ситуація посилюється через

нестачу ресурсів для правоохоронців, слабке застосування законодавства та недоліки в судовій системі.

Ключові моменти:

Недооцінка загрози: У звіті Moneyval 2023 року загрозу від наркоторгівлі було оцінено як «середню», зважаючи на невелику кількість складних випадків. Однак експерти зазначають, що це є хибною оцінкою, оскільки ситуація є набагато складнішою. Влада аргументує свою позицію тим, що більшість злочинів у сфері наркоторгівлі є локальними, а значна частина прибутків отримується за кордоном. Проте проблема стала більш актуальною після трагедії 2 травня 2023 року, коли підлітки загинули через водія, який був під впливом наркотиків, що привернуло увагу до проблеми.

Слабка робота в конфіскації активів: Агенція ANABI, яка займається конфіскацією та управлінням злочинними доходами, визнала, що не веде окремих статистик за категоріями злочинів, що значно ускладнює відстеження доходів від наркоторгівлі. Відсутність належних даних щодо конфіскацій підриває здатність влади боротися з відмиванням грошей та не дозволяє відстежувати ефективність боротьби з фінансовими потоками, пов'язаними з наркоторгівлею.

Нестача ресурсів у правоохоронців: У звіті DIICOT 2023 року зазначено, що прокуратура потребує більш активного використання паралельних фінансових розслідувань, щоб запобігти поверненню кримінальних доходів до легальної економіки. Однак недостатня кількість прокурорів і велика кількість справ робить цей процес неефективним. Наприклад, у 2023 році DIICOT мала лише 19 прокурорів, які розслідували 7,000 справ, пов’язаних з наркоторгівлею, що значно перевищує можливості персоналу.

Недоліки у судовій системі: Румунські суди не мають належної статистики щодо злочинів, пов’язаних одночасно з наркоторгівлею та відмиванням грошей. Через відсутність відповідної інформації складно оцінити, скільки справ було успішно завершено і які суми грошей вдалося конфіскувати.

Ситуація в порту Констанца: Порт Констанца, один з найважливіших стратегічних об’єктів, через який проходять значні обсяги наркотрафіку, не забезпечений належними ресурсами для боротьби з цією проблемою. За останні роки не було жодного великого вилучення наркотиків, хоча звіти Європейського центру моніторингу наркотиків свідчать про те, що порти на Балканах стають основними маршрутами для наркотрафіку.

Висновки:

Румунська держава стикається зі значними викликами у боротьбі з наркоторгівлею та відмиванням грошей. Основними проблемами є недооцінка загроз, недостатня кількість ресурсів у правоохоронців та судової системи, а також відсутність ефективних інструментів для конфіскації незаконних доходів. Попри намагання вирішити проблему на рівні політики, реальних змін поки не досягнуто.

http://surl.li/xgwsbf

Тріади та мистецтво відмивання грошей Макао

В статті досліджується, як тріади, організовані злочинні групи, активно беруть участь у відмиванні грошей у Макао через гральну індустрію. Макао, будучи найбільшим центром казино у світі, приносить мільярди доларів прибутку, але також є ключовою ланкою в нелегальних фінансових потоках.

Хоча китайський уряд запровадив жорсткі заходи для боротьби з відмиванням грошей, тріади продовжують шукати шляхи для обходу правил, використовуючи валютний обмін та нелегальні фінансові операції.

Ключові моменти:

Макао як світовий центр грального бізнесу: Гральна індустрія Макао є найбільш прибутковою у світі, забезпечуючи приблизно 36,2 мільярда доларів США щорічно. Основними гравцями на цьому ринку є великі американські компанії, зокрема такі, як Galaxy Casino, Las Vegas Sands, Melco Resorts та Wynn Resorts. Після пандемії COVID-19 Макао відновило свій дохід, що досягає рівнів до пандемії.

Контроль тріад: Тріади, особливо в Макао та Гонконзі, відіграють ключову роль у відмиванні грошей через гральні операції. Вони контролюють обмін валюти, який використовується для незаконних фінансових потоків. Китайські громадяни мають обмеження на обмін валюти на суму до 50,000 доларів США на рік, що змушує багатьох шукати нелегальні шляхи для проведення великих фінансових операцій.

Китайська боротьба з тріадами: У 2021 році уряд Китаю розпочав масштабну операцію проти нелегальних "Junket" операцій, які організовували тріади для залучення багатих клієнтів до нелегальних азартних ігор. Junkets, які забезпечували близько 50% доходу казино, були закриті. Влада Макао також почала активніше боротися з нелегальним обміном валют, що додатково ускладнило життя тріадам.

Негативний вплив на індустрію: Закриття Junkets і посилення контролю за гральною діяльністю призвели до спаду на ринку азартних ігор у Макао. Це спричинило падіння акцій провідних операторів казино, що стало негативною новиною для інвесторів. Попри це, експерти вважають, що гральний бізнес у Макао здатен відновитися, оскільки тріади та інші нелегальні структури завжди знаходять способи адаптуватися до нових реалій.

Реакція влади: Влада Макао минулого року заарештувала близько 10,000 людей, пов'язаних із незаконними операціями обміну валюти. Було встановлено нові закони, згідно з якими порушників можуть ув'язнити на термін до 5 років, а також заборонити відвідувати казино на строк від 2 до 10 років.

Майбутнє боротьби з відмиванням грошей: Хоча китайська влада та уряд Макао здійснюють жорсткі заходи для боротьби з відмиванням грошей, досвід показує, що тріади та інші кримінальні організації швидко адаптуються до нових умов. Тож боротьба з цим явищем продовжиться, але очікується, що тріади зможуть знайти нові способи для обходу законодавства.

https://igamingfuture.com/triads-macau-money-washing/

ОАЕ запроваджує Національну стратегію боротьби з відмиванням коштів та фінансуванням тероризму

В ОАЕ запустили національну стратегію боротьби з відмиванням коштів і фінансуванням тероризму. Цей всеосяжний план спрямований на покращення правової та нормативної бази країни, покращення співпраці між різними державними установами та посилення міжнародної співпраці. Ця стратегія є частиною ширших зусиль ОАЕ щодо захисту своєї фінансової

системи та економіки від незаконної діяльності, забезпечуючи відповідність світовим стандартам.

http://surl.li/addtug

PEP не всі однакові. Чому?

Стаття під назвою "PEPs are not all the same. Why?" аналізує різні категорії політично значущих осіб (PEPs, Politically Exposed Persons) і підкреслює важливість диференційованого підходу до управління ризиками, пов'язаними з такими особами. У статті наголошується, що не всі PEP мають однаковий рівень ризику, оскільки їх вплив, роль і рівень доступу до фінансових ресурсів можуть сильно варіюватися залежно від їхньої позиції та функцій. Стаття акцентує увагу на тому, що для ефективного управління ризиками важливо не лише відзначати факт, що особа є PEP, а й детально аналізувати її рівень впливу та зв'язки, щоб правильно оцінити ризики відмивання грошей або корупції.

https://www.sgrcompliance.com/peps-are-not-all-the-same-why/

Марихуана та мексиканські картелі: всередині приголомшливого зростання кількості китайських відмивачів грошей

Стаття розглядає значну роль китайських організованих злочинних угруповань у відмиванні грошей для мексиканських наркокартелів, особливо у контексті виробництва марихуани. Зазначається, що мексиканські картелі, зокрема ті, що займаються наркотрафіком, активно використовують китайські злочинні структури для маскування нелегальних доходів. За допомогою складних фінансових схем і криптовалют китайські угруповання ефективно переводять гроші через міжнародні канали, що ускладнює їхнє відстеження. Однією з ключових особливостей є використання криптовалют та легальних фінансових установ для переміщення великих обсягів "брудних" грошей через системи, що створюють видимість легальних операцій.

Китайські гроші грають важливу роль у спрощенні доступу до прекурсорів, необхідних для виготовлення метамфетаміну та інших наркотиків, якими торгують мексиканські картелі. Злочинні групи використовують також законні торгові операції, такі як імпорт і експорт товарів, для проведення нелегальних фінансових операцій, включаючи розрахунки за наркотики. Стаття звертає увагу на тісний зв'язок між фінансовими та злочинними операціями, а також на складність їх виявлення через використання новітніх технологій.

Китайські злочинні угруповання також використовують шахрайські схеми з кредитними картками, підробки документів та фіктивні компанії для відмивання грошей, що значно ускладнює правоохоронцям можливість відстежувати ці операції.

http://surl.li/swqanr

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Навігація у складному ландшафті санкцій у європейських країнах: ключові міркування для бізнесу

Останніми роками ландшафт міжнародних санкцій стає дедалі заплутанішим, і європейські країни відіграють ключову роль у формуванні та забезпеченні цих заходів. Для компаній, які працюють за кордоном, розуміння та дотримання правил санкцій у Європі є надзвичайно важливим, ніж будь-коли. Ця стаття має на меті пролити світло на поточний стан санкцій у європейських країнах і запропонувати вказівки щодо того, як підприємства можуть орієнтуватися у цьому складному регуляторному середовищі.

1. Еволюція режиму санкцій у Європі

Європейські санкції часто є результатом колективних рішень, прийнятих Європейським Союзом (ЄС) та його державами-членами у відповідь на геополітичні події, порушення прав людини та інші важливі проблеми. Ці санкції можуть включати заморожування активів, заборону на поїздки, обмеження торгівлі тощо. Останні події призвели до посилення санкцій проти таких країн, як Росія, Білорусь та Іран, що відображає позицію Європи щодо глобальних конфліктів і політичних розбіжностей.

Ключовий висновок: європейські санкції динамічні та часто оновлюються. Підприємства повинні бути в курсі змін, щоб уникнути ненавмисних порушень.

2. Розуміння системи санкцій ЄС

Система санкцій ЄС в першу чергу регулюється:

- Регламентами та рішеннями: вони є юридично обов'язковими до виконання та визначають особливості накладених санкцій.
- Спільною зовнішньою політикою та політикою безпеки (CFSP): ця структура окреслює зовнішню політику ЄС та стратегію санкцій.
- Картою санкцій ЄС: Європейська зовнішня діяльність (EEAS) веде онлайн-карту, щоб допомогти компаніям і окремим особам орієнтуватися в поточному ландшафті санкцій.

Ключовий висновок: ознайомтеся з правовими текстами та ресурсами ЄС, щоб забезпечити відповідність останнім нормам.

3. Виклики комплаєнсу для компаній

Підприємства стикаються з кількома викликами, коли мають справу з європейськими санкціями:

- Визначення сфери застосування: розуміння того, які правила застосовуються та як вони впливають на вашу діяльність.
- Скринінг та належна перевірка: забезпечення того, щоб ані ваші ділові партнери, ані ваші операції не підпадали під санкції.

Ключовий висновок: запроваджуйте надійні програми відповідності, включаючи регулярне навчання персоналу та комплексні процедури перевірки.

4. Майбутнє санкцій у Європі

Траєкторія європейських санкцій, ймовірно, продовжуватиме розвиватися у відповідь на глобальні політичні події. Відданість ЄС правам людини та міжнародному праву свідчить про те, що санкції залишатимуться ключовим інструментом у його зовнішньополітичному арсеналі. Підприємства повинні передбачити посилення контролю та адаптуватися до нових нормативних умов у міру їх появи.

Ключовий висновок: залишайтеся гнучкими та готовими до змін, дотримуючись проактивної стратегії відповідності та зміцнюючи відносини з юридичними та регуляторними експертами.

Ключові етапи процесу EDD

1. **Оцінка ризиків**
   - Ризикоорієнтований підхід: Розроблення складної системи рейтингів ризиків, враховуючи тип клієнта, географічне розташування, обсяги транзакцій і їх складність.
   - Червоні прапори: Визначення чітких ознак високого ризику, такі як високоризикові юрисдикції, політично значущі особи (PEPs) або складні корпоративні структури.
   - Порогові значення: Встановлення чітких порогів для запуску EDD на основі результатів оцінки ризиків.
2. **Ідентифікація та перевірка клієнтів (CIV)**
   - Встановлення бенефіціарної власності: Використання строгих методів для ідентифікації та перевірки кінцевих бенефіціарних власників (КБВ).
   - Ідентифікація PEP: Використання комплексних баз даних PEP та інструменти перевірки для виявлення потенційних PEP або їх близьких асоційованих осіб.
   - Перевірка у ЗМІ: Проведення детального пошуку у ЗМІ, щоб виявити негативну інформацію про клієнтів, директорів або бенефіціарних власників.
3. **Постійний моніторинг**
   - Моніторинг транзакцій: Впровадження передових систем моніторингу транзакцій для виявлення незвичайних моделей та високоризикових дій.
   - Аналіз поведінки клієнтів: Аналіз поведінки клієнтів протягом часу, щоб виявляти зміни, які можуть свідчити про підвищений ризик.
   - Зміни в регулюванні: Необхідно бути в курсі змін у нормативних вимогах і відповідно налаштовувати параметри моніторингу.
4. **Аналіз транзакцій**
   - Підозрілі транзакції (SAR): Розроблення чітких інструкцій для виявлення підозрілих транзакцій та подання звітів SAR.
   - Управління випадками: Впровадження системи управління справами для відстеження та розслідування підозрілих випадків.
   - Встановлення протоколів для обміну інформацією з правоохоронними органами та іншими відповідними інституціями.
5. **Перевірка PEP і санкцій**
   - Оновлення баз даних: Регулярне оновлення списків PEP і санкцій, щоб забезпечити точну перевірку.
   - Управління помилковими спрацьовуваннями: Розроблення процедури для зменшення кількості помилкових спрацьовувань і оптимізації процесу перевірки.
   - Обсяг перевірки: Визначення відповідного обсягу перевірки, включаючи дочірні компанії, афілійовані організації та пов'язані сторони.
6. **Документація та зберігання записів**
   - Політика збереження: Встановлення чіткої політик щодо зберігання документації EDD відповідно до регуляторних вимог.
   - Доступність: Забезпечення легкого доступу до файлів EDD для аудитів, розслідувань та регуляторних перевірок.
   - Безпека даних: Впровадження надійних заходів безпеки для захисту конфіденційної інформації клієнтів.

7. **Навчання та підвищення обізнаності**
   - Навчання персоналу: Забезпечення всебічного навчання з питань EDD для всіх відповідних співробітників, включаючи інтеграцію нових працівників та постійне навчання.
   - Навчання за ролями: Адаптація навчальних програм до конкретних ролей і обов'язків в організації.

Що таке Wash Trading?

Wash trading — це тактика маніпулювання ринком, коли той самий актив купується та продається одночасно однією особою, що створює оманливу картину вартості активу.

Така практика зустрічається у традиційних цінних паперах, а також на нових ринках, таких як криптовалюти та NFT.

Мета?

Вводити інших в оману, щоб вони повірили в реальний інтерес до активу, підвищуючи його ціну або обсяг торгів.

Як це працює:

↳ Трейдер або іноді кілька трейдерів, які змовляються разом, купують і продають той самий актив одночасно, створюючи хибне враження високого попиту.

↳ Ціна активу штучно завищена, що робить його більш привабливим, ніж він є насправді, що спонукає більше інвесторів купувати його.

↳ Коли ціна зростає, зловмисники продають з прибутком, знижуючи ціну та залишаючи іншим інвесторам нікчемні активи.

Чому це нелегально:

↳ Підробна торгівля є формою маніпулювання ринком і основним злочином для відмивання грошей у багатьох юрисдикціях.

Суб’єкти, які пропонують цінні папери, тобто брокери-дилери, згідно із законодавством зобов’язані впроваджувати надійні заходи ринкового нагляду для виявлення та запобігання маніпулюванню ринком, у тому числі wash trading. Невиконання цього не лише підриває довіру інвесторів, але й наражає компанію на суворі регуляторні санкції.