Серійний номер: ДСФМУ-ДК-2024-018
Липень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Питання та відповіді щодо впровадження Регламенту про миттєві платежі (IPR).

Європейська Комісія опублікувала запитання та відповіді щодо впровадження **Регламенту миттєвих платежів (IPR). IPR набув чинності 8 квітня 2024 року, і перший набір зобов'язань для постачальників платіжних послуг (PSP) потрібно буде виконувати з 9 січня 2025 року**. Питання та відповіді є результатом двох онлайн-семінарів, організованих службами Комісії з органами влади держав-членів та зацікавленими сторонами 30 квітня та 29 травня 2024 року відповідно з метою обговорення низки положень IPR.

Регламент вносить зміни до низки інших нормативних актів, зокрема до Регламенту SEPA, Регламенту про транскордонні платежі (CBPR), Директиви про остаточність розрахунків (SFD) та Другої Директиви про платіжні послуги (PSD2). **Документ складається з роз'яснень, наданих Генеральним директоратом з фінансової стабільності, фінансових послуг та Союзу ринків капіталу (DG FISMA).** Метою документа є широке розповсюдження результатів цих обговорень серед зацікавлених сторін.

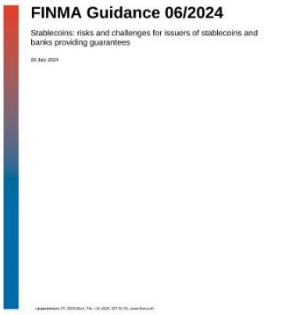
Ключові висновки:

1. **Охоплення регламенту**: Регламент про миттєві платежі стосується тільки переказів у євро. Інші валюти не підпадають під його дію.
2. **Обов'язковість для постачальників платіжних послуг (PSP)**: Всі PSP, що пропонують послуги з надсилання та отримання переказів у євро, повинні також надавати послуги миттєвих переказів у євро.
3. **Винятки з регламенту**: Деякі транзакції, такі як великі платежі, що обробляються через системи платежів великого обсягу (LVPS), не підпадають під дію регламенту.
4. **Вимоги до платіжних рахунків**: Миттєві перекази можуть виконуватися тільки з платіжних рахунків. Інші типи рахунків, такі як довірчі або заставні рахунки, повинні розглядатися в індивідуальному порядку, щоб визначити, чи підпадають вони під визначення платіжних рахунків.
5. **Інформація для користувачів платіжних послуг (PSU)**: PSU повинні мати можливість вибору між звичайними та миттєвими переказами. PSP повинні інформувати PSU про статус виконання миттєвих переказів протягом 10 секунд після отримання платіжного доручення.

6. **Інтеграція нових технологій**: PSP, які не мають електронних каналів для надання платіжних послуг, не зобов'язані створювати такі канали спеціально для миттєвих платежів, якщо вони не надають послуги звичайних переказів через електронні канали.
7. **Відповідальність за виконання платежів**: У випадку невиконання миттєвого платежу вчасно, PSP платника зобов’язаний негайно відшкодувати суму платежу.

http://surl.li/dswvdl

Стейблкоїни: ризики та виклики для емітентів стейблкоїнів та банків, що надають гарантії



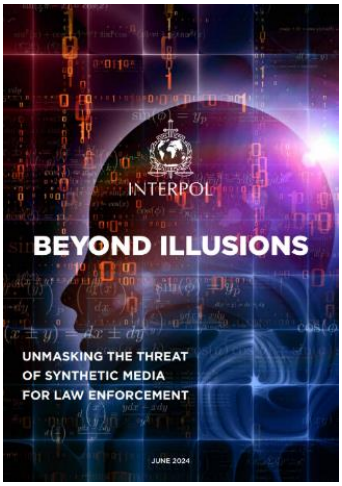
Документ «Стейблкоїни: ризики та виклики для емітентів стейблкоїнів та банків, що надають гарантії» від швейцарського регулятора фінансових ринків (FINMA) обговорює питання, пов’язані з випуском стейблкоїнів та участю банків у забезпеченні гарантій щодо таких активів. Зокрема, він охоплює правову класифікацію стейблкоїнів, питання боротьби з відмиванням грошей (ПВК) та регулювання відповідно до банківського законодавства. В документі зазначається, що проєкти з випуску стейблкоїнів зазвичай переслідують мету забезпечення платіжного засобу з низькою волатильністю цін за рахунок прив’язки до реальних активів, таких як національні валюти. Також розглядаються питання, пов’язані з репутаційними ризиками для банків, що надають гарантії по стейблкоїнах.

Ключові висновки:

1. **Правова класифікація стейблкоїнів**: Вони можуть бути класифіковані як депозити за банківським законодавством або як колективні інвестиційні схеми, залежно від способу управління активами.
2. **Протидія відмиванню коштів**: Стейблкоїни підпадають під дію законодавства про ПВК/ФТ через їхній потенціал для використання у злочинних цілях, зокрема для обходу санкцій та фінансування тероризму.
3. **Регулювання за банківським законодавством**: Випуск стейблкоїнів може вимагати банківської ліцензії, якщо не використовується механізм гарантії дефолту, наданий банком.
4. **Репутаційні ризики**: Банки, що надають гарантії за стейблкоїнами, можуть стикатися з репутаційними ризиками та юридичними проблемами у разі порушень законодавства у сфері ПВК/ФТ з боку емітентів стейблкоїнів.
5. **Потреба в регулюванні**: Визнана необхідність перегляду законодавчих винятків для забезпечення належного захисту інвесторів.

http://surl.li/rlrigy

Поза межами ілюзій: викриття загрози синтетичних (фальшивих) медіа для правоохоронних органів



Документ під назвою "Beyond Illusions: Unmasking the Threat of Synthetic Media for Law Enforcement" аналізує зростаючу загрозу, що представляє собою синтетичні (фальшиві) медіа. З розвитком технологій штучного інтелекту (ШІ) синтетичні медіа, включаючи глибинні фейки (deepfakes), синтетичне аудіо, згенеровані тексти та синтетичні ідентифікаційні документи, стають все більш складними та доступними. Це створює значні виклики для правоохоронців у перевірці автентичності медіа контенту та проведенні розслідувань.

Документ детально розглядає різні типи синтетичних медіа та технології, що лежать в їх основі, такі як генеративні мережі (GANs), дифузійні моделі та автоенкодери. Він також описує, як ці технології можуть бути використані для підвищення можливостей правоохоронних органів, зокрема для створення монтажів, підтримки агентів під прикриттям та тренувань. Однак, основна увага приділяється викликам, пов'язаним з автентифікацією доказів, ідентифікацією жертв, дезінформацією, пропагандою та питаннями конфіденційності.

Документ також розглядає техніки розслідування та судово-медичних експертиз, включаючи аналіз метаданих, зворотній пошук зображень та лінгвістичний аналіз. Він описує новітні технологічні рішення для виявлення синтетичних медіа, такі як моделі глибокого навчання, пояснювальний ШІ, аналіз структури файлів, біологічні сигнали та статистичний аналіз на піксельному рівні.

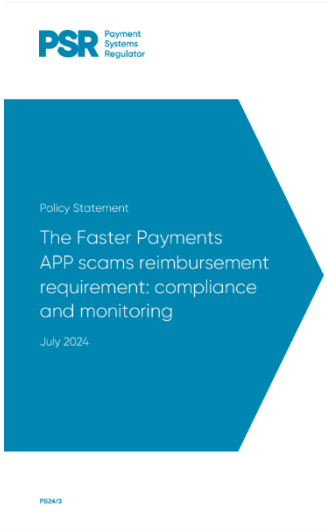
Наостанок, документ обговорює нормативні та політичні питання, пов'язані з інтелектуальною власністю та відповідальним використанням ШІ, та висвітлює роль Інтерполу в дослідженні синтетичних медіа та підтримці правоохоронних органів країн-членів.

Ключові висновки

- **Складність автентифікації**: Синтетичні медіа можуть значно ускладнити процес перевірки автентичності доказів, що може призвести до появи фальшивих доказів у судових процесах.
- **Вплив на розслідування:** Використання синтетичних медіа для ідентифікації жертв та в рамках дезінформаційних кампаній створює нові виклики для правоохоронців у зборі та перевірці доказів.
- **Технічні рішення:** Для боротьби із загрозами синтетичних медіа необхідно впроваджувати новітні технологічні рішення, такі як моделі глибокого навчання та пояснювальний ШІ.
- **Співпраця та обмін знаннями:** Вирішення проблем, пов'язаних з синтетичними медіа, потребує тісної співпраці між країнами, приватним сектором та академічними інститутами для обміну знаннями та передовими технологіями.
- **Роль Інтерполу:** Інтерпол має відігравати ключову роль у дослідженні та протидії загрозам, що представляють синтетичні медіа, надаючи підтримку країнам-членам у розробці та впровадженні відповідних заходів.

http://surl.li/nvhclx

Повернення коштів за шахрайські операції: Вимоги та рекомендації PSR



Документ "The Faster Payments APP scams reimbursement requirement: compliance and monitoring" від Регулятора платіжних систем Великобританії (PSR) детально описує нову політику щодо відшкодування збитків від шахрайства з авторизованими платіжними переказами (APP). Основні положення включають вимоги до постачальників платіжних послуг (PSP) реєструватися в Pay.UK до 20 серпня 2024 року. PSP мають регулярно звітувати про транзакційні дані, щоб моніторити дотримання нових правил, і повинні інформувати споживачів про їхні права та обов'язки в рамках цієї політики. Ця ініціатива спрямована на підвищення прозорості та справедливого розподілу відповідальності за шахрайські операції.

В документі також зазначено, що PSP мають запровадити ефективні заходи щодо запобігання шахрайству, що включає покращення процесів верифікації транзакцій та посилення моніторингу підозрілих дій. Звіти мають подаватися щомісяця, і вони допоможуть у виявленні тенденцій шахрайства та оцінці ефективності впроваджених заходів.

Політика також включає положення про те, що споживачі повинні бути повністю обізнані про свої права на відшкодування у випадку шахрайства. Вона передбачає, що PSP повинні забезпечити доступність інформації про процеси подачі скарг і вимог на відшкодування, а також сприяти підвищенню фінансової грамотності споживачів щодо захисту їхніх фінансових інтересів.

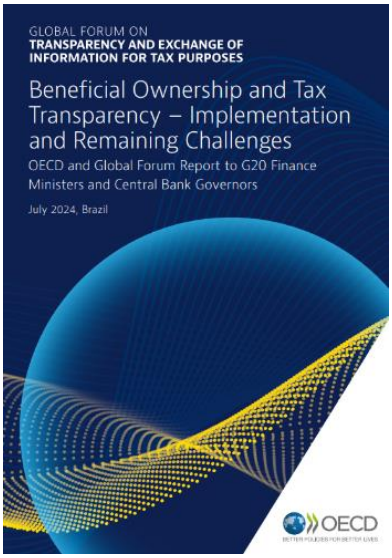
Впровадження цих вимог почнеться з 7 жовтня 2024 року, що надасть PSP час для адаптації своїх систем та процесів відповідно до нових стандартів. Очікується, що ця політика зменшить рівень шахрайства та підвищить довіру споживачів до платіжних систем.

Ключові висновки:

- **Реєстрація PSP:** Всі постачальники платіжних послуг, що підпадають під дію політики, повинні зареєструватися в Pay.UK до 20 серпня 2024 року. Це забезпечить створення реєстру для обміну контактними даними та спрощення комунікації щодо шахрайських претензій.
- **Щомісячне звітування:** PSP повинні подавати щомісячні звіти до Pay.UK, починаючи з 7 жовтня 2024 року, щоб забезпечити моніторинг дотримання правил повернення коштів.
- **Впровадження RCMS**: Pay.UK впровадить систему управління претензіями щодо відшкодування (RCMS), яку повинні будуть використовувати всі учасники системи Faster Payments до 1 травня 2025 року. Це полегшить управління претензіями та забезпечить дотримання вимог щодо звітності.
- **Запобігання шахрайству:** PSP повинні впровадити ефективні заходи щодо запобігання шахрайству, покращити процеси верифікації транзакцій та посилити моніторинг підозрілих дій.
- **Обізнаність споживачів:** PSP зобов'язані інформувати споживачів про їхні права на відшкодування коштів у випадку шахрайства. Це включає забезпечення доступності інформації про процеси подачі скарг і вимог на відшкодування, а також підвищення фінансової грамотності споживачів щодо захисту їхніх фінансових інтересів.
- **Дата початку дії вимог:** Вимоги почнуть діяти з 7 жовтня 2024 року, що дає PSP час для адаптації своїх систем до нових стандартів.
- **Моніторинг та звітність:** Pay.UK буде відповідальний за моніторинг дотримання правил повернення коштів, і у випадку виявлення невідповідності вимогам буде вживати відповідні заходи.

http://surl.li/kdgfra

Бенефіціарна власність та прозорість оподаткування – реалізація та виклики, що залишаються



Документ OECD аналізує стан бенефіціарної власності та податкової прозорості у світі. Він розроблений у відповідь на запити G20 і **включає оцінку виконання стандартів прозорості, проблеми, що залишаються, та рекомендації щодо покращення ситуації**. Основна увага приділяється тому, як різні країни виконують вимоги щодо розкриття інформації про бенефіціарних власників юридичних осіб, правових утворень та банківських рахунків.

Ключові висновки:

- **Значення прозорості бенефіціарної власності:** Прозорість бенефіціарної власності є ключовою для забезпечення податкової справедливості та боротьби з фінансовими злочинами. Відсутність прозорості сприяє ухиленню від сплати податків, корупції та відмиванню грошей.
- **Виконання стандартів:** Більшість країн запровадили законодавчі рамки для забезпечення прозорості бенефіціарної власності, але практична реалізація часто стикається з проблемами. Приблизно половина з 112 оцінених юрисдикцій мають серйозні недоліки у своїй правовій базі або в ефективному виконанні вимог.
- **Проблеми та виклики:** Основні проблеми включають слабке законодавство, низьку якість даних та недостатній нагляд і контроль. Навіть у юрисдикціях, де законодавча база є адекватною, існують значні проблеми з її практичною реалізацією.
- **Підходи до забезпечення прозорості:** Найкращі результати досягаються юрисдикціями, які використовують багатопрофільний підхід до збору інформації про бенефіціарну власність, що включає систему ПВК/ФТ, вимоги до самих суб'єктів та централізовані реєстри.
- **Співпраця з FATF:** FATF та Глобальний форум тісно співпрацюють у питаннях бенефіціарної власності, що забезпечує узгодженість та підвищує ефективність реалізації міжнародних стандартів.
- **Майбутні напрями розвитку:** Необхідно продовжувати роботу з удосконалення правових рамок, зміцнення наглядових механізмів та розширення міжнародної співпраці для забезпечення повної прозорості бенефіціарної власності.

Документ підкреслює важливість подальшого розвитку механізмів збору та обміну інформацією про бенефіціарних власників, а також необхідність впровадження нових технологічних рішень для підвищення ефективності та прозорості у цій сфері.

http://surl.li/ozrmfr

Звіт про оцінку загрози тероризму в Сінгапурі за 2024 рік

Міністерство внутрішніх справ Сінгапуру оприлюднило оцінку загрози тероризму. **У звіті розглядаються як внутрішні, так і зовнішні загрози, оцінюючи рівень загрози як високий, але немає ознак неминучої атаки.**

Примітно, що звіт використовує тонкий і точний підхід до використання криптовалют, зазначаючи, що, хоча ми бачимо збільшення використання криптовалюти такими групами, як ІДІЛ, для збору та переказу коштів, **готівка та інші неофіційні системи переказу вартості залишаються переважаючим видом для фінансових операцій**.

Зокрема, у звіті зазначається: «Хоча криптовалюти все частіше використовуються, переважним засобом фінансових операцій ІДІЛ та його філіями залишаються готівкові кур'єри та неофіційні системи переказу вартості (хавала). Кошти надходять до бійців ІДІЛ та їхніх сімей у Сирії. У лютому 2024 року влада США повідомила, що ІДІЛ «переказувала кошти – до 20 000 доларів США (27 100 сінгапурських доларів) на місяць кожному – особам в таборі Al-Hol через посередників у Туреччині через систему hawala, а також через додатки для грошових переказів і криптовалюту».

Ключові висновки:

1. **Постійна загроза від ісламістських терористичних груп:** ІДІЛ та Аль-Каїда продовжують бути основними джерелами терористичної загрози, активно вербуючи нових членів і здійснюючи атаки в різних регіонах, включаючи Південно-Східну Азію.
2. **Вплив конфлікту між Ізраїлем та ХАМАС:** Останні події, пов'язані з конфліктом між Ізраїлем та ХАМАС, призвели до підвищення рівня саморадикалізації серед окремих осіб у Сінгапурі, зокрема серед молоді, що викликає занепокоєння.
3. **Саморадикалізація через інтернет:** Онлайн-екстремізм залишається головним драйвером терористичної загрози в Сінгапурі, з багатьма випадками саморадикалізації серед молодих людей, які піддаються впливу екстремістської пропаганди в інтернеті.
4. **Ультраправий екстремізм:** Ультраправий екстремізм також становить зростаючу загрозу, з випадками радикалізації серед молоді, що підкреслює необхідність моніторингу та протидії цьому явищу.
5. **Фінансування тероризму:** Сінгапур залишається потенційним джерелом фінансування тероризму через його статус глобального фінансового центру, незважаючи на відсутність недавніх випадків засудження за фінансування тероризму.
6. **Зусилля щодо підвищення готовності та співпраці:** Уряд Сінгапуру активно працює над підвищенням своєї готовності до терористичних атак, співпрацюючи з міжнародними партнерами та залучаючи громадськість через ініціативи, такі як SGSecure.

Звіт наголошує на важливості колективної пильності, готовності та співпраці всіх секторів суспільства для ефективної боротьби з тероризмом і підтримки безпеки в країні.

https://www.mha.gov.sg/docs/default-source/default-document-library/sttar-2024.pdf?sfvrsn=98ce88bd_3

РЕГУЛЮВАННЯ

Південна Корея: вступає в силу закон про регулювання ринків криптовалюти

Закон про захист користувачів віртуальних активів (Закон № 19563) (VAUPA), оприлюднений 18 липня 2023 року, набув чинності 19 липня 2024 року. Згідно з прес-релізом Комісії з фінансових послуг (FSC), **Закон має на меті «встановити здоровий порядок на ринку віртуальних активів і забезпечити захист користувачів». Криптовалютні біржі посилили свої системи контролю відповідності, щоб підготуватися до набуття чинності закону**.

Основні ознаки Закону

Є чотири ключові аспекти нового закону:

- **Що таке «віртуальні активи», на які поширюється дія закону**
- **Захист активів користувачів**
- **Регулювання недобросовісної торгової практики**
- **Нагляд, санкції та штрафи**

Визначення «віртуальних активів»

Закон визначає «віртуальні активи» в широкому сенсі як «електронні сертифікати (включно з усіма пов'язаними правами), які мають економічну цінність і які можна торгувати або передавати в електронному вигляді», але виключає певні активи, такі як продукти, які регулюються іншими законами, і цифрові валюти, випущені Банком Кореї. (VAUPA ст. 2, п. 1.)

Що стосується невзаємозамінних токенів (NFT), 10 червня 2024 року FSC і Служба фінансового нагляду Південної Кореї оголосили про нові керівні настанови для роз'яснення застосування VAUPA до NFT. Як резюмував FSC, наступні випадки будуть вважатися віртуальними активами відповідно до закону:

a) Коли ідентичні або схожі типи NFT випускаються у великих кількостях або серією. . . .
b) Коли можна розділити NFT. . . на фрактальні одиниці.
c) Коли можна використовувати NFT як прямий або непрямий спосіб оплати певних товарів або послуг.
d) Коли можна використовувати NFT як засіб обміну на віртуальні активи між невизначеними особами або коли його можна використовувати як засіб оплати за товари чи послуги, пов'язані з іншими типами віртуальних активів. . . .

Захист активів користувачів

Новий закон покладає обов'язки на постачальників послуг віртуальних активів (VASP) щодо захисту депозитів користувачів шляхом керування окремими рахунками та списком користувачів. (Статті 6, 7.) VASP несуть відповідальність за участь у програмах страхування або взаємодопомоги відповідно до керівних настанов у разі нещасних випадків, таких як злом або збій комп'ютера. (Стаття 8.) Вони також повинні зберігати записи про транзакції віртуальних активів протягом 15 років з моменту припинення відповідних транзакційних відносин. (Стаття 9.)

Регулювання недобросовісної торгової практики

Новий закон забороняє використання суттєвої непублічної інформації (ст. 10, п. 1), маніпулювання ринковими цінами (ст. 10, п. 2, 3), а також дії недобросовісної торгівлі, які можуть порушити ринковий порядок (ст. 10, п. 4). Ці положення подібні до паралельних положень Закону про фінансові інвестиційні послуги та ринки капіталу (Закон № 19263). Крім того, новий закон забороняє дискреційне блокування депозитів або зняття віртуальних активів (ст. 11) і вимагатиме від криптобірж створювати механізми моніторингу та повідомляти про підозрілу діяльність фінансовим органам влади (ст. 12).

Нагляд, санкції та штрафи

FSC може здійснювати нагляд за діями VASP та перевіряти їхні ділові відносини та фінансовий стан. (стаття 13.) Новий закон містить положення щодо розслідування та вжиття заходів у відповідь на недобросовісну торговельну практику (стаття 14) та заходів щодо порушників (стаття 15). Доступні механізми правозастосування включають покарання за недобросовісну торговельну практику (ст. 17), доручення наглядового органу (ст. 18), загальні положення про штрафи (ст. 19), конфіскацію та стягнення (ст. 20), спільні штрафні положення (ст. 21).), та адміністративні штрафи (ст. 22). Закон передбачає мінімальне покарання у вигляді позбавлення волі строком до одного року, але не передбачає максимального покарання за вказані порушення закону. (Стаття 19 (1).).

https://perma.cc/6VMU-AYVP

САНКЦІЇ

Санкції це штрафи або обмежувальні заходи, які накладаються однією або декількома країнами або міжнародними організаціями для досягнення політичних або безпекових цілей.

Вони часто використовуються як інструменти впливу на поведінку урядів, організацій або окремих осіб, які, як вважають, порушують міжнародні закони, беруть участь у незаконній діяльності або становлять загрозу миру та безпеці.

Санкції зазвичай накладаються для:

- Заохочення дотримання міжнародних законів і норм.
- Стримання агресивної чи протиправної поведінки.
- Покарання та ізолювання порушників.
- Захисту інтересів національної безпеки.

Санкції можуть бути введені в односторонньому порядку однією країною або багатосторонньо групами країн чи міжнародними організаціями, такими як ООН або Європейський Союз. Ефективність і вплив санкцій можуть бути різними, і вони часто залежать від політичних і правових міркувань.

Типи Санкцій

Економічні санкції

Економічні санкції — це заходи, що вводяться однією чи декількома країнами або міжнародними організаціями для обмеження економічної взаємодії з певною країною, юридичною чи фізичною особою. Ці санкції зазвичай використовуються як інструмент зовнішньої політики для досягнення певних цілей або для того, щоб змусити підсанкційну сторону змінити свою поведінку.

Нижче наведено деякі форми економічних санкцій:

1. **Торгівельні обмеження:** це передбачає обмеження або повну заборону імпорту чи експорту товарів і послуг між суб'єктами. Ці обмеження можуть включати тарифи, заборони на імпорт/експорт або квоти.
2. **Заморожування активів:** Економічні санкції можуть передбачати заморожування активів окремих осіб, організацій або чиновників, пов'язаних із підсанкційною країною. Це перешкоджає їм отримати доступ до своїх коштів або активів, які зберігаються в країні, що накладає санкції.
3. **Фінансові обмеження:** санкції можуть обмежувати або блокувати фінансові операції, включаючи банківські операції та використання міжнародних платіжних систем, що може ізолювати підсанкційну країну від глобальної фінансової системи.
4. **Заборона на поїздки:** особам, пов'язаним з підсанкційною країною, може бути заборонено здійснювати поїздки до країн, які накладють санкції, або здійснювати міжнародні поїздки в цілому.
5. **Ембарго на технології та зброю:** санкції можуть обмежити експорт певних технологій, військового обладнання або товарів подвійного призначення до підсанкційної країни.

Економічні санкції часто використовуються як невійськовий засіб тиску на країну, щоб вона дотримувалася міжнародних норм, змінила свою політику або подолала порушення прав людини.

Комплексні санкції

Комплексні санкції, також відомі як повні санкції, стосуються типу економічних санкцій, накладених на цільову країну, які **охоплюють широкий спектр економічної діяльності та секторів**. На відміну від цільових санкцій, які зосереджуються на конкретних особах, організаціях або секторах, комплексні санкції **є ширшими та впливають на всю економіку країни, щодо якої введено санкції**. Ці санкції можуть включати обмеження на торгівлю, фінансові операції, інвестиції, передачу технологій тощо.

Комплексні санкції часто впроваджуються декількома країнами або міжнародними організаціями та **спрямовані на здійснення значного економічного та політичного тиску на підсанкційну країну**. Мета полягає в тому, щоб змусити країну змінити свою поведінку, наприклад, припинити порушення прав людини, припинити агресивні військові дії або дотримуватися міжнародних норм і угод.

Комплексні санкції можуть мати далекосяжні наслідки для підсанкційної країни та її населення. Вони можуть призвести до економічних труднощів, перешкоджати розвитку та обмежувати доступ до основних товарів і послуг. Гуманітарні проблеми часто виникають через те, що ці санкції можуть негативно вплинути на звичайних громадян, що призводить до дебатів щодо етичних наслідків таких заходів.

Цільові санкції

Цільові санкції, також відомі як інтелектуальні санкції або вибіркові санкції, **є типом економічних або торговельних обмежень**, які накладаються однією або декількома країнами чи міжнародними організаціями **проти конкретних осіб, організацій або секторів у країні**. Ці заходи покликані звести до мінімуму несприятливий гуманітарний вплив на населення в цілому, одночасно націлюючись та чинячи тиск на конкретних осіб, групи чи види діяльності, які викликають занепокоєння міжнародної спільноти.

Нижче наведено деякі причини застосування цільових санкцій:

1. **Дипломатичні та політичні важелі:** цільові санкції часто використовуються для тиску на уряд або окремих осіб в уряді, щоб вони змінили свою поведінку, наприклад, припинили порушення прав людини, припинили підтримку тероризму або дотримувалися міжнародних угод.
2. **Вирішення конфліктів:** вони можуть бути використані для підтримки зусиль із вирішення конфліктів, націлюючись на осіб або організації, залучені в конфлікти, торгівлю зброєю або незаконну торгівлю природними ресурсами, що сприяє насильству.
3. **Боротьба з тероризмом:** цільові санкції можуть бути використані для зриву фінансового забезпечення і операцій терористичних організацій та окремих осіб.
4. **Нерозповсюдження:** вони можуть застосовуватися для запобігання розповсюдженню зброї масового знищення шляхом націлювання на осіб або організації, залучені до програм ядерної, хімічної чи біологічної зброї.
5. **Права людини:** Санкції можуть бути застосовані до осіб, відповідальних за порушення прав людини, включно з урядовцями та організаціями, причетними до репресій, тортур чи інших зловживань.
6. **Корупція та незаконна діяльність:** цілеспрямовані санкції можуть бути застосовані проти фізичних або юридичних осіб, залучених до корупції, відмивання коштів або іншої незаконної фінансової діяльності.

Ці санкції зазвичай передбачають заморожування активів цільових фізичних або юридичних осіб, накладення заборони на поїздки та обмеження їхнього доступу до фінансових послуг. Мета полягає

в тому, щоб змусити об’єкти санкцій змінити свою поведінку або дотримуватися міжнародних норм, не завдаючи великої шкоди населенню в цілому.

Секторальні санкції

Секторальні санкції — **це різновид цільових економічних санкцій**, які запроваджуються однією чи декількома країнами або міжнародними організаціями **щодо окремих секторів економіки країни, а не щодо країни в цілому чи окремих суб’єктів.** Ці санкції спрямовані чинити тиск на підсанкційну країну шляхом **обмеження її доступу до певних секторів, технологій або послуг**, мінімізуючи при цьому вплив на населення в цілому.

Секторальні санкції можуть бути спрямовані на різні галузі чи сектори, наприклад фінанси, енергетику, оборону чи технології. Обмеження, накладені на ці сектори, можуть включати обмеження на експорт, імпорт, інвестиції або передачу технологій. Ці заходи часто вживаються у відповідь на конкретні дії чи політику підсанкційної країни, такі як порушення прав людини, агресивні військові дії або порушення міжнародного права.

Метою секторальних санкцій є вплив на поведінку уряду країни або організацій, що працюють у цих секторах. Обмежуючи доступ до важливих ресурсів або технологій, секторальні санкції мають на меті створити економічний тиск і стимулювати підсанкційну країну змінити свою політику, брати участь у дипломатичних переговорах або дотримуватися міжнародних норм.

Секторальні санкції – це стратегічний підхід до міжнародної дипломатії, що дозволяє країнам реагувати на конкретні проблеми, не вдаючись до ширших санкцій, які можуть завдати шкоди населенню в цілому. Однак, як і інші форми санкцій, ефективність та етичні наслідки секторальних санкцій є предметом постійних дискусій у сфері міжнародних відносин.

Що таке первинні санкції

Первинні санкції - це економічні або дипломатичні заходи, що застосовуються однією країною або групою країн безпосередньо проти іншої країни, суб'єкта або окремої особи. У Сполучених Штатах Америки такі заходи зазвичай виконує OFAC, і вони можуть включати повні торгові ембарго, замороження або конфіскацію активів, заборону на подорожі для іноземних суб'єктів.

Санкції можуть проявлятися у різних формах:

- Торговельні обмеження: Обмеження на імпорт, експорт або інвестиції, що стосуються цільової країни або суб'єкта.
- Фінансові санкції: Замороження активів, заборона фінансових транзакцій або обмеження доступу до міжнародної банківської системи.
- Заборона на подорожі: Перешкоджання в'їзду або подорожі осіб, пов'язаних з цільовою країною або суб'єктом, через певні регіони.
- Ембарго на зброю: Обмеження на продаж, передачу або надання військового обладнання, зброї чи пов'язаних технологій.
- Дипломатичні заходи: Висилка дипломатів, закриття посольств або консульств або скорочення дипломатичних відносин.

Ці санкції накладаються з різних причин, включаючи реакцію на міжнародні злочини або загрози національній безпеці. Вони можуть призводити до обмежень у торгівлі, фінансових операціях, подорожах та інших видів взаємодії. Зазвичай мета таких санкцій - змусити цільову країну або суб'єкта змінити свою поведінку, таку як припинення порушень прав людини, підтримка тероризму або виконання міжнародних стандартів та угод.

Наприклад, сучасні санкції США спрямовані на такі країни, як Північна Корея, Куба, Сирія, Росія та конкретні китайські інтереси. Вони можуть приймати різні форми, такі як обмеження у торгівлі, фінансові санкції, подорожні заборони, ембарго на зброю та дипломатичні заходи.

Санкції можуть бути спрямовані на цілі країни або регіони, а також на конкретних осіб або суб'єктів. Уникнути санкцій можуть тільки особи, юридичні особи та організації, які перебувають під юрисдикцією США. Невиконання санкцій може призвести до великих фінансових штрафів або інших санкційних заходів.

https://bit.ly/4bD5r07

Що таке вторинні санкції

Вторинні санкції — це економічні заходи, що вводяться однією країною проти іноземних осіб чи компаній, які співпрацюють з країнами, що підпадають під первинні санкції. На відміну від первинних санкцій, що безпосередньо спрямовані на певну країну чи об'єкт, вторинні санкції впливають на третіх осіб, які взаємодіють з цими країнами. Такі санкції можуть включати обмеження на бізнес чи доступ до фінансової системи країни, що вводить санкції. Ці заходи зазвичай використовуються для стримування третіх осіб від шкідливих дій щодо інтересів підсанкційної країни.

https://bit.ly/3yiTaj8

ПРОВІДНА РОЛЬ ГОНКОНГУ В УХИЛЕННІ ВІД САНКЦІЙ

Розкрито ухилення від санкцій на мільярд доларів – як вантажовідправники з Гонконгу відправили російським покупцям товарів на 1,97 мільярда доларів. Фонд «Комітет свободи Гонконгу» (CFHK) опублікував звіт під назвою «Під гаванню: провідна роль Гонконгу в ухиленні від санкцій». Звіт проливає світло на **ключову роль Гонконгу в сприянні ухилення від санкцій для Росії, Ірану та Північної Кореї**.

Ось ключові висновки зі звіту.

1. **Значне зростання торгівлі з країнами, які перебувають під санкціями:**

Незважаючи на міжнародні санкції, торгівля між Гонконгом і такими країнами, як Росія, Північна Корея та Іран, значно зросла за останні роки. Після лютого 2022 року експорт напівпровідників із Гонконгу до Росії подвоївся до 400 мільйонів доларів, що зробило Гонконг ключовим постачальником.

2. **Критичні військові поставки:**

З серпня по грудень 2023 року 750 мільйонів доларів із 2 мільярдів доларів товарів, доставлених із Гонконгу до Росії, становили передові компоненти, життєво важливі для військових зусиль Росії. Ці поставки включали предмети високого пріоритету, такі як інтегральні схеми та інші передові технології, критичні для військових застосувань.

3. **Регуляторне середовище, що дозволяє ухилятися:**

М'яке регуляторне середовище Гонконгу сприяє легкому приховуванню корпоративної власності та швидкому створенню та закриттю компаній, які використовуються для ухилення від санкцій. Позиції уряду, включаючи заяву генерального директора Джона Лі в жовтні 2022 року, про те, що

територія не застосовуватиме глобальні санкції проти Росії, було достатньо, щоб підбадьорити тих, хто ухиляється від санкцій.

4. **Співучасть і бездіяльність уряду:**

Небажання уряду Гонконгу застосовувати міжнародні санкції, такі як санкції ООН, США та ЄС, зробило місто безпечним притулком для тих, хто ухиляється від санкцій. Резонансні справи, такі як причалювання яхти підсанкційного російського олігарха Олексія Мордашова, підкреслюють співучасть міста.

Детальні тематичні дослідження, висвітлені зі звітів.

- **Piraclinos Limited:**

Заявляла про продаж добрив і деревного вугілля, але було виявлено, що вона відправляє інтегральні схеми на мільйони доларів російській компанії, яка потрапила під санкції.

- **Arttronix International:**

Після накладення санкцій за постачання деталей для безпілотників до Ірану компанія розпустилася та знову з'явилася під новою назвою ETS International.

- **Співпраця HK Shipping Cooperation Limited і HK Petroleum Enterprises:**

Сприяли значним нафтовим угодам з іранською компанією Sahara Thunder, включаючи транспортування нафти з судна на судно.

У звіті пропонується запровадити жорсткі міжнародні заходи, такі як вторинні санкції щодо фінансових установ, і скоординований глобальний підхід для покращення правозастосування.

https://www.thecfhk.org/post/beneath-the-harbor

Індикатори обходу галузевих та цільових фінансових санкцій

Документ "Indicators of Sectoral and Targeted Financial Sanction Evasion" є методичним матеріалом, розробленим у співпраці латвійськими та міжнародними організаціями. Він **висвітлює важливість санкцій, типи санкцій та їхні цілі**, зокрема забезпечення міжнародного миру, безпеки та підтримки демократії. **Особлива увага приділяється санкціям, накладеним на Росію у відповідь на агресію проти України, та спробам їх обходу**. У документі представлено **аналіз даних про імпорт та експорт, а також підозрілих транзакцій**, що надаються латвійським ПВР, та включено **список індикаторів, які можуть свідчити про спроби обходу санкцій.**

Ключові висновки:

1. **Роль санкцій:** Санкції є важливим інструментом забезпечення міжнародного миру, безпеки та підтримки демократичних принципів. Вони можуть бути як фінансовими (цільовими), так і секторальними, що стосуються конкретних товарів чи послуг.
2. **Зростання кількості заморожених активів:** З 2014 по 2024 рік у латвійських фінансових установах значно збільшилася сума заморожених коштів у зв'язку з посиленням санкцій проти Росії. Станом на кінець 2014 року сума заморожених коштів у латвійських фінансових установах становила приблизно 11 мільйонів євро. Станом на 30 червня 2024 року ця сума збільшилася до приблизно 108 мільйонів євро. Значна частина цих коштів була заморожена у 2022 році через суттєві санкції, накладені на Росію з 23 лютого 2022 року.

3. **Основні загрози порушення санкцій:** Через географічне розташування та економічні зв'язки з Росією та Білоруссю, Латвія зазнає значних ризиків порушення санкцій, накладених на ці країни.
4. **Методи обходу санкцій:** У документі описуються різні методи, що використовуються для обходу санкцій, включаючи фіктивні зміни у структурі власності, транзит товарів через треті країни, заниження вартості товарів та інші. Зокрема, зазначається, що значна частина товарів, експортованих до третіх країн, у кінцевому підсумку опиняється в Росії, а деякі імпортовані товари з третіх країн насправді мають російське походження.
5. **Санкції проти Росії та Білорусі:** Після початку війни Росії проти України санкції були значно посилені. Латвійські установи виявили численні спроби обходу цих санкцій через інші країни.
6. **Важливість контролю та співпраці:** Для ефективної боротьби з обходом санкцій важливо впроваджувати відповідні контрольні заходи, перевіряти партнерів по бізнесу, підтверджувати кінцевих отримувачів товарів та перевіряти походження товарів.
7. **Зростання кількості підозрілих транзакцій:** Збільшення кількості звітів про підозрілі операції свідчить про активні спроби обходу санкцій. Це вимагає посиленої уваги та співпраці між різними установами для виявлення та припинення таких спроб. Аналіз цих звітів показує, що більшість транзакцій, пов'язаних з ухиленням від санкцій, надходять з Литви, Туреччини та Чехії, тоді як основні напрямки вихідних платежів з Латвії - Литва, Білорусь та Німеччина.

Цей документ є важливим ресурсом для розуміння та протидії спробам обходу санкцій, спрямованих на підтримку міжнародного права та безпеки.

http://surl.li/wtlgxd

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Звіт Numeral «Стан європейських платіжних операцій»

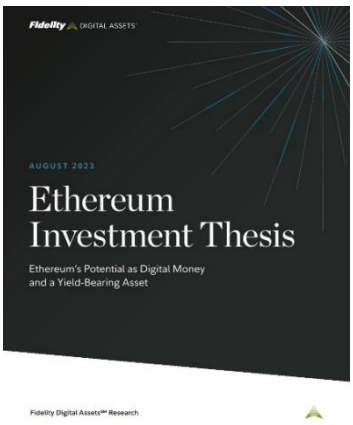
Документ представляє звіт про сучасний стан операцій з платежами в Європі, створений на основі опитування фінансових керівників з Франції, Великої Британії та Німеччини. У звіті висвітлюються ключові виклики, з якими стикаються компанії під час впровадження ефективних та масштабованих процесів обробки платежів, а також очікувані переваги від їх модернізації. Документ обговорює зростання ролі платежів у бізнесі та економіці, акцентуючи увагу на важливості автоматизації та централізації платіжних операцій. Крім того, звіт підкреслює бар'єри, що заважають модернізації, такі як складність інтеграції нових систем, безпекові ризики та інерційність корпоративного керівництва.

Ключові висновки:

1. Платіжні операції в багатьох компаніях залишаються фрагментованими і значною мірою ручними, що призводить до втрат часу та ефективності.
2. 88% керівників вважають, що модернізація платіжних операцій є критично важливою для бізнесу, з більшістю компаній, що планують інвестувати в ці оновлення протягом наступних 12 місяців.
3. Основні перешкоди для модернізації включають високі витрати, складність впровадження нових систем та потребу у навчанні ключових співробітників щодо важливості платіжних операцій.
4. Очікувані переваги від модернізації включають пришвидшення обробки платежів, зменшення кількості помилок, покращення досвіду клієнтів та загальне зниження витрат.
5. Документ наголошує на важливості автоматизації платіжних процесів для зменшення ручної роботи та підвищення ефективності, при цьому більшість компаній розглядає автоматизацію як ключовий елемент в майбутніх рішеннях.

https://www.numeral.io/guides/payment-operations-report-survey

Дослідження Fidelity Digital Assets «Інвестиційні тези про Ethereum»



Документ, підготовлений Fidelity Digital Assets «Інвестиційні тези про Ethereum» досліджує потенціал Ethereum як цифрової валюти та активу, що приносить дохід. У ньому розглядається, як Ethereum може функціонувати як платформа для розробки додатків, використовуючи ETH як засіб платежу, а також обговорюються фактори, що впливають на вартість токена ETH, включаючи використання мережі, динаміку попиту та пропозиції, а також технічні аспекти після переходу на механізм proof-of-stake.

Ключові висновки:

1. **Вартість ETH та Ethereum:** Вартість ETH як токена значною мірою залежить від використання блокчейн-системи Ethereum, особливо після впровадження механізму спалювання частини комісійних зборів, що зменшує загальну пропозицію ефіру.

2. **ETH як форма грошей:** Хоча ETH може розглядатися як форма грошей, він стикається зі значними труднощами у порівнянні з BTC, зокрема через відсутність обмеження максимальної пропозиції та часті технічні оновлення.

3. **Ризики та перспективи:** Основними ризиками є регуляторні питання та технічні ризики, пов'язані з регулярними оновленнями мережі. Однак, очікується, що зростання

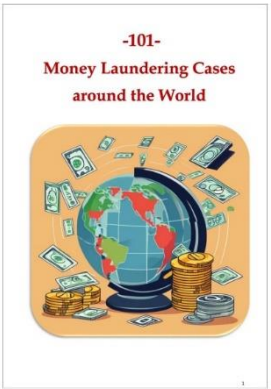
використання Ethereum та інтеграція з реальними активами можуть сприяти зростанню попиту на ETH.

4. **Ефір як дохідний актив:** Після переходу на proof-of-stake, ефір став приносити дохід за рахунок стейкінгу. Це створює нову модель оцінки вартості ETH через очікувані грошові потоки, зокрема на основі попиту на блокчейн-простір і платних транзакцій.

Документ також містить прогнозні моделі, які показують, як зростання використання мережі Ethereum може вплинути на вартість ефіру в майбутньому. В цілому, висновок документу вказує на те, що ETH має потенціал зростання вартості, проте існують значні ризики, пов'язані з регулюванням та технічними аспектами мережі.

https://fwc.widen.net/s/dlbgbmjqxs/fidelity-digital-assets---ethereum-investment-thesis

101 випадок відмивання коштів по всьому світу



Документ «101 випадок відмивання коштів по всьому світу» представляє собою збірку випадків відмивання коштів, що сталися у фінансових установах по всьому світу. Він охоплює низку резонансних скандалів, таких як випадок у Сінгапурі (2024), скандали з участю HSBC, Danske Bank, Deutsche Bank, Standard Chartered Bank та інших великих банків. У кожному випадку описані основні деталі скандалу, методи, які використовувалися для відмивання коштів, системні недоліки в банківських установах, а також нормативно-правові та репутаційні наслідки для залучених осіб та організацій.

Ключові висновки

1. **Системні недоліки:** Більшість випадків відмивання коштів стали можливими через слабкість контролю за дотриманням норм ПВК та низьку культуру дотримання регуляторних вимог у банках.
2. **Недостатня дія керівництва:** В багатьох випадках старше керівництво банків ігнорувало внутрішні попередження про підозрілі операції, що сприяло подальшому розвитку незаконної діяльності.
3. **Правові наслідки:** Банки та їх співробітники стикалися з серйозними правовими наслідками, включаючи значні фінансові штрафи, судові розгляди та в деяких випадках - тюремні терміни.
4. **Репутаційні втрати:** Всі залучені організації зазнали серйозних втрат своєї репутації, що призвело до втрати довіри з боку клієнтів і партнерів, а також до зниження вартості акцій.
5. **Необхідність реформ:** Багато випадків призвели до реформ у банківській системі, включаючи посилення контролю у сфері ПВК, покращення внутрішнього аудиту та підвищення відповідальності керівництва за дотримання нормативних вимог.

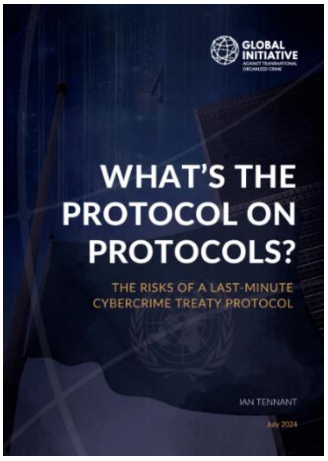
Цей документ підкреслює важливість суворого дотримання норм у сфері ПВК та співпраці з регуляторами для підтримання фінансової системи в безпеці та збереження довіри суспільства.

http://surl.li/zidpvy

Оцінка ризиків прийняття додаткових протоколів до міжнародної кіберзлочинної конвенції: Уроки з досвіду UNTOC

Документ "What's the Protocol on Protocols? The Risks of a Last-Minute Cybercrime Treaty Protocol" авторства Іана Теннанта, підготовлений Global Initiative Against Transnational Organized Crime,

аналізує ризики та можливості, пов'язані з прийняттям додаткових протоколів до міжнародної конвенції щодо кіберзлочинності, який зараз перебуває на стадії розробки в ООН. Цей документ був підготовлений напередодні фінальної сесії Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, яка відбувається з 29 липня по 9 серпня 2024 року в Нью-Йорку.



Документ досліджує досвід розробки додаткових протоколів до Конвенції ООН проти транснаціональної організованої злочинності (UNTOC), які були розроблені як частина початкового мандату Комітету Ad Hoc. Аналізуються політичні, практичні та юридичні аспекти, які забезпечили успішне прийняття протоколів UNTOC. Також розглядаються відмінності між поточною ситуацією та процесом розробки кіберзлочинної конвенції, зокрема те, що протоколи до UNTOC були частиною мандату з самого початку, а поточний комітет не має аналогічного мандату.

Ключові висновки

- **Відсутність консенсусу:** Протягом переговорів щодо кіберзлочинної конвенції не було досягнуто згоди щодо обсягу кримінальних дій, що охоплюються договором. Це призвело до продовження процесу переговорів до серпня 2024 року.
- **Пропозиція про додаткові протоколи:** Країни, які підтримують ширший обсяг конвенції, пропонують розпочати розробку додаткових протоколів, які б охоплювали додаткові злочини, навіть без остаточного тексту основної конвенції.
- **Уроки з UNTOC:** Протоколи до UNTOC були розроблені як частина початкового мандату комітету Ad Hoc, що дозволило ефективно узгодити основну конвенцію та додаткові протоколи. Однак політичні, практичні та юридичні обставини, які сприяли успіху UNTOC, відрізняються від поточної ситуації.
- **Ризики останньої хвилини:** Початок процесу розробки додаткових протоколів на такій пізній стадії переговорів, коли основний текст конвенції ще не узгоджено, може призвести до плутанини та підриву цілісності конвенції.
- **Політичний клімат:** Переговори щодо кіберзлочинної конвенції відбуваються в умовах поляризованого політичного клімату, де різні держави мають протилежні погляди на обсяг та цілі конвенції.
- **Важливість узгодження основної конвенції:** Комітет Ad Hoc має зосередитися на досягненні компромісу щодо основного тексту конвенції, перш ніж розглядати можливість додаткових протоколів.

Таким чином, документ підкреслює важливість обережного підходу до розробки додаткових протоколів до кіберзлочинної конвенції, враховуючи політичні та юридичні складнощі, пов'язані з цим процесом.

https://globalinitiative.net/analysis/risks-last-minute-un-cybercrime-treaty-protocol/

Comrades in Crime: Дослідження російськомовної незаконної криптоекосистеми

Вийшов **новий звіт TRM Labs** «Товариші по злочину: **дослідження російськомовної незаконної криптоекосистеми**» 📥 Російськомовні суб’єкти відіграють величезну роль у більшості типів кіберзлочинів із підтримкою криптографії, провідними типами є:

Програми-вимагачі: у 2023 році на російськомовні групи програм-вимагачів припало щонайменше 69% усіх криптовалютних надходжень від програм-вимагачів, що перевищило 500 мільйонів доларів США.

🛒 **Ринки Darknet**: російськомовні ринки darknet склали 95% усіх продажів наркотиків у криптовалюті в dark web у 2023 році.

🌐 **Санкції**: надходження лише до однієї російської криптобіржі, Garantex, склали 82% обсягів криптовалюти, що належать усім підсанкційним організаціям у всьому світі.

Але найбільше вражає те, що «з 2021 року щонайменше 85 мільйонів доларів було відправлено на гаманці, пов'язані як з російськими, так і з китайськими компаніями, які займаються виробництвом, транспортуванням і продажем військового обладнання та обладнання подвійного призначення та критичних компонентів."

https://www.trmlabs.com/comrades-in-crime-exploring-the-russian-speaking-illicit-crypto-ecosystem

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

Ризики фондів: як благодійні організації стають каналами для відмивання коштів

🌟 У цьому відео досліджується прихована вразливість благодійних фондів та їх ненавмисна роль у відмиванні коштів. Якщо ви берете участь у запобіганні фінансовим злочинам або дотриманні нормативних вимог, це обов'язково до перегляду! 🌐💼

💼 Що в цій серії?

- Розуміння того, як фонди можна використовувати для відмивання коштів 💰🏢
- Етапи відмивання коштів: розміщення, розшарування та інтеграція 🔺🔍
- Реальні приклади, що висвітлюють ризики ПВК, пов'язані з фондами 🌍🏭
- Необхідність глобальної стандартизації та розширеної нормативної бази 🌐📜

🔍 Чому варто дивитися?

- Отримайте уявлення про складні методи відмивання коштів через фонди
- Дізнайтеся про останні тенденції та нормативні прогалини у філантропічному секторі
- Відкрийте для себе ефективні стратегії пом'якшення ризиків фінансових злочинів, пов'язаних із фондами

💡 Хоча фонди, зосереджені головним чином на благодійних цілях, все частіше перевіряються на предмет можливого зловживання ними у відмиванні коштів. Розуміння цих ризиків і впровадження надійних профілактичних заходів є важливими для збереження їх доброчесності.

https://www.youtube.com/watch?app=desktop&v=5WoEqy7gwuY&feature=youtu.be

Журнал SARs in Action, випуск 26

Випуск 26 журналу "SARs in Action", опублікованого підрозділом фінансової розвідки Великобританії (UKFIU), охоплює різні аспекти, пов'язані з режимом підозрілих активностей. **Головними темами є вплив генеративного штучного інтелекту (GenAI) на загрозу шахрайства; подкаст UKFIU, присвячений сектору юридичних послуг та проблемам боротьби з відмиванням коштів; нові коди словника фінансування тероризму; а також індикатори ризику криптоактивів для фінансових установ**. Журнал також включає **приклади випадків успішного використання звітів про підозрілу діяльність (SARs)** у боротьбі з організованою злочинністю, а також **інформацію про цифрову трансформацію SARs**.

Ключові висновки:

1. **Загроза з боку генеративного штучного інтелекту (GenAI):** GenAI, зокрема великі мовні моделі (LLM), голосове клонування та deepfake, стали значною загрозою у сфері шахрайства. Ці технології використовуються для підвищення ефективності шахрайських схем, таких як інвестиційне шахрайство, шахрайство з романтичними стосунками та фішинг. GenAI також допомагає шахраям обходити системи модерації та покращувати свої навички анонімізації.

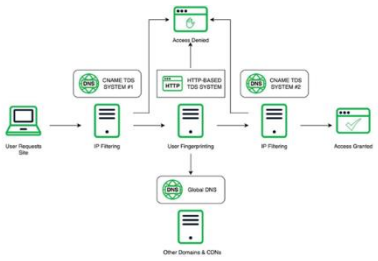
2. **Роль сектору юридичних послуг у системі з ПВК:** Подкаст UKFIU висвітлює основні виклики та можливості для юридичного сектору щодо дотримання вимог ПВК. Обговорюються ключові загрози, зони ризику та червоні прапорці, на які повинні звертати увагу фірми та практикуючі юристи.
3. **Нові коди словника фінансування тероризму:** UKFIU незабаром додасть нові коди словника для фінансування тероризму до порталу SAR, що допоможе тим, хто звітує більш ефективно класифікувати та звітувати про підозрілу діяльність, пов'язану з тероризмом.
4. **Індикатори ризику криптоактивів:** У рамках ініціативи об’єднаних керівників глобального податкового правозастосування (J5), UKFIU разом з HMRC надала фінансовим установам індикатори ризику для виявлення та звітування про відмивання грошей і незаконну діяльність з використанням криптоактивів.
5. **Успішні випадки використання SARs:** Журнал містить кілька прикладів, де інформація з SARs допомогла правоохоронним органам виявити та запобігти злочинній діяльності, включаючи відмивання коштів та шахрайство. Ці випадки підкреслюють важливість високоякісних SARs для боротьби з організованою злочинністю.
6. **Цифрова трансформація SARs:** Програма цифрової трансформації SARs досягла значного етапу, завершивши перехід на нові канали подання SARs через портал SAR та платформи Bulk API, що покращить здатність слідчих швидко ідентифікувати підозрілу діяльність та діяти на основі ключової інформації.

Цей випуск підкреслює важливість співпраці між різними секторами та організаціями у боротьбі з відмиванням грошей, фінансуванням тероризму та іншими формами фінансових злочинів.

https://www.nationalcrimeagency.gov.uk/who-we-are/publications/723-sars-in-action-issue-26/file

ІНШІ НОВИНИ

Експерти розкривають китайську кіберзлочинну мережу, яка стоїть за азартними іграми та торгівлею людьми



Стаття описує розкриття китайської кіберзлочинної мережі Vigorish Viper, яка займається азартними іграми та торгівлею людьми в Південно-Східній Азії. Ця група використовує передові технології для налаштування DNS, хостингу вебсайтів, платіжних систем і зашифрованих комунікацій. Вони спонсорують європейські футбольні клуби для реклами нелегальних азартних сайтів, використовуючи складну інфраструктуру для уникнення виявлення. Розслідування показали їх активне використання понад 170 000 доменних імен та залучення людей до примусової праці.

https://thehackernews.com/2024/07/experts-uncover-chinese-cybercrime.html

Нові виклики для FATF з новим Президентом

ФАТФ зустрічає нові виклики під час переходу до нової методології оцінки країн, керівництво якої тепер здійснює новий президент - Еліза де Анда Мадразо. Успадкувавши посаду від Раджа Кумара, Мадразо має перед собою багато завдань, особливо в умовах геополітичної нестабільності.

- Новий Президент та Її Пріоритети

Призначення Елізи де Анда Мадразо на посаду президента ФАТФ відбулося під час червневої пленарної сесії 2024 року. Вона приймає на себе керівництво в період, коли ФАТФ впроваджує нову методологію оцінювання країн - п'ятий раунд з моменту створення організації. Цей раунд оцінок має включати нову методологію, яка була оголошена в травні 2024 року. Зокрема, вона наголошує на ефективності та надає докладні вказівки для оцінювачів, щоб забезпечити послідовність результатів.

- Ефективність як Основний Пріоритет

Нова методологія підкреслює важливість досягнення ефективних результатів, зокрема у протидії фінансуванню розповсюдження. Зміни також включають розділення оцінки ефективності ризик-орієнтованого нагляду за фінансовим та нефінансовим секторами на дві окремі частини. Це допоможе чіткіше відслідковувати виконання вимог у різних секторах економіки.

- Неочікувані Наслідки

Одним з ключових пріоритетів для Елізи де Анда Мадразо є фінансова інклюзія. Вона активно підтримує зміни до Рекомендації 1, що стосуються ризик-орієнтованого підходу, з метою стимулювання використання спрощеної належної обачності (SDD) в умовах низького ризику відмивання грошей і фінансування тероризму. Це може сприяти залученню більшої кількості людей до формальної фінансової системи.

- Глобальна Кооперація

Однією з найбільших проблем ФАТФ залишається взаємодія між країнами Глобальної Півночі та Півдня. Країни Глобального Півдня, як правило, є членами регіональних організацій FATF-Style

Regional Bodies (FSRBs), а не повноправними членами ФАТФ. Вони часто відчувають, що їх голоси не мають належного впливу на рівні ФАТФ, і багато з них потрапляють до так званого "сірого списку" ФАТФ, що може мати серйозні наслідки для їх економік.

- Збереження Уваги до Важливих Питань

Президентство Раджа Кумара привернуло увагу до питання повернення активів, але результати були обмеженими. Лише менше 1% кримінальних доходів повертається. Еліза де Анда Мадразо планує продовжувати зосереджуватися на підвищенні ефективності глобальних механізмів повернення активів. Однак це залишається складною проблемою, і одні лише оновлення рекомендацій навряд чи вирішать її повністю.

- Вихід за Межі Боротьби з Відмиванням Грошей

З моменту створення ФАТФ у 1989 році її мандат значно розширився і тепер включає боротьбу з фінансуванням тероризму та фінансуванням розповсюдження. Протягом останніх років ФАТФ зосередилася на загрозах, що виникають від нових технологій, таких як краудфандинг. Зміни до Рекомендації 8 були спрямовані на баланс між боротьбою з фінансуванням тероризму та мінімізацією негативних наслідків для неприбуткового сектору.

Щодо фінансування розповсюдження, значні зміни до Рекомендації 1 були внесені у 2020 році. Вони вимагають від країн і зобов'язаних суб'єктів проведення оцінки ризиків фінансування розповсюдження. Проте, з моменту внесення цих змін, міжнародна система протидії фінансуванню розповсюдження зазнала суттєвих змін. Резолюція Ради Безпеки ООН 2231, яка регулювала іранську ядерну угоду, закінчилася в жовтні 2023 року, а Росія наклала вето на продовження діяльності Панелі експертів ООН щодо Північної Кореї у 2024 році.

- Майбутнє ФАТФ

Пріоритети нового президента зосереджуються на підвищенні прозорості, інклюзивності та єдності в роботі Глобальної Мережі. Якщо ФАТФ зможе правильно налаштувати ці аспекти, це значно зміцнить її легітимність. Проте список завдань залишається довгим, включаючи вирішення питання фінансування розповсюдження та взаємодії з FSRBs. Проект оновлення Рекомендації 16 також вимагає ретельного розгляду, оскільки зміни вплинуть на мільйони фінансових транзакцій щодня.

Попри критику, більш інклюзивна та орієнтована на результати ФАТФ принесе користь усім. Роботи багато, і Еліза де Анда Мадразо це добре усвідомлює. Однак, здається, ФАТФ зосереджується на всіх важливих аспектах.

- Висновок

ФАТФ стоїть перед новими викликами, зокрема в умовах геополітичної нестабільності та швидкого розвитку технологій. Новий президент ФАТФ, Еліза де Анда Мадразо, має амбіційний план дій, спрямований на підвищення ефективності роботи організації, підтримку фінансової інклюзії та зміцнення глобальної кооперації. Попри численні виклики, ФАТФ прагне залишатися ключовим гравцем у боротьбі з відмиванням грошей, фінансуванням тероризму та фінансуванням розповсюдження.

Історичне падіння вирубки лісів у Колумбії може бути пов’язане зі злочинними групами.

Стаття від Insight Crime детально розглядає значне зниження рівня вирубки лісів у Колумбії, яке досягло найнижчого рівня за останні 23 роки.

Міністр навколишнього середовища Сусана Мухаммад оголосила про зниження на 36% у 2023 році, порівняно з попереднім роком. Основною причиною цього зниження названо зміни в діяльності

кримінальних груп, таких як колишні бойовики FARC, які взяли під контроль незаконну вирубку лісів та інші нелегальні економічні діяльності.

Згідно з дослідженнями, уряд Колумбії вживає різноманітні заходи для захисту довкілля, включаючи програми відновлення екосистем та збереження природних ресурсів. Проте, діяльність кримінальних груп залишається суттєвим викликом. Колишні бойовики FARC, які раніше активно брали участь в незаконній вирубці лісів, могли змінити свою стратегію, щоб уникнути переслідувань та використовувати зменшення вирубки як інструмент для переговорів з урядом. Це створює нестабільну ситуацію, оскільки ці групи можуть швидко адаптуватися до нових умов і знайти способи обходу законодавчих обмежень.

Також у статті зазначається, що кримінальні угруповання, які раніше були залучені до нелегальної вирубки, могли переорієнтуватися на інші форми нелегальної діяльності, такі як незаконний видобуток золота або виробництво наркотиків. Це підкреслює необхідність комплексного підходу до вирішення проблеми, який включатиме як екологічні, так і соціальні та економічні заходи.

http://surl.li/mcsfec

Чому і бізнес, і шахраї полюбили нову платіжну систему Індії

Стаття описує вплив впровадження системи Unified Payments Interface (UPI) в Індії на повсякденне життя звичайних громадян. UPI, запущена в 2016 році, дозволяє користувачам надсилати та отримувати гроші, оплачувати рахунки та здійснювати інші фінансові операції швидко та безпечно, просто скануючи код. Це значно полегшило життя малого бізнесу, особливо під час пандемії COVID-19, коли безготівкові розрахунки стали необхідністю. Завдяки UPI Індія стала найбільшим ринком реальних платежів у світі, зареєструвавши 14 мільярдів транзакцій у травні 2023 року.

Однак, зі збільшенням популярності UPI зросли й випадки шахрайства. Шахраї використовують різні методи для обману людей, зокрема переконують їх поділитися своїм UPI PIN або створюють фальшиві додатки. У фінансовому році, що закінчився у квітні 2023 року, було зафіксовано понад 95,000 випадків шахрайства, що перевищує показники попереднього року.

Історія Шівкалі, молодої жінки з Бігара, показує, як легко можна стати жертвою шахрайства. Вона була обманута при покупці скутера через Facebook, що призвело до втрати грошей. Незважаючи на освітній рівень і обізнаність, вона стала жертвою добре організованих шахраїв.

Держава та центральний банк працюють над захистом користувачів UPI, але наразі відшкодування збитків можливе лише через банки, що створює додаткові труднощі для постраждалих. Експерти, наголошують на необхідності балансу між безпекою та доступністю фінансових послуг.

Незважаючи на проблеми, UPI активно просувається в сільських районах, де люди навчаються користуватися цифровими банківськими послугами.

https://www.bbc.com/news/articles/c288m1km01po

Питання регулювання криптовалюти

У минулотижневому випуску про оновлення криптополітик та нормативних питань, Elliptic розглянув деякі основних новин з усього світу.

- Гонконг публікує хвідповідь на консультації по стейблкоїнам та оголошує учасників пісочниці
- SEC вирішує не вживати примусових заходів проти Paxos за стейблкоїн
- 🌐 FATF випускає цільове оновлення щодо віртуальних активів
- Сейшельські острови приймають нормативну базу про VASP
- Спроба подолати вето Байдена щодо відхилення SAB 121 не вдається, але SEC дозволяє певним фірмам виключення
- Співзасновник і колишній виконавчий директор Paxful визнає себе винним у недотриманні вимог з ПВК/ФТ
- Трамп обирає сенатора, який підтримує криптовалюту, як напарника

http://surl.li/rycirc

Як чотири президенти США розв'язали економічну війну по всьому світу

Стаття Washington Post досліджує широке використання санкцій Сполученими Штатами як інструменту зовнішньої політики. Ось ключові моменти:

Поширеність санкцій США: Сполучені Штати запроваджують більше санкцій, ніж будь-яка інша країна або міжнародний орган, охоплюючи значну частину світового населення. За останні роки США потроїли кількість санкцій порівняно з іншими країнами або організаціями.

Вплив на країни з низьким рівнем доходу: Санкції США непропорційно впливають на країни з низьким рівнем доходу, причому 60% найбідніших країн світу стикаються з певною формою санкцій США. Ці санкції часто призводять до серйозних гуманітарних наслідків, таких як обмежений доступ до продовольства та ліків.

Ефективність та наслідки: Хоча санкції спрямовані на те, щоб змусити уряди змінити свою поведінку, їх ефективність є спірною. Багато режимів, таких як Куба, Іран, Сирія та Північна Корея, залишаються при владі, незважаючи на ескалацію санкцій. Замість того, щоб послабити ці режими, санкції часто завдають шкоди цивільному населенню і можуть мимоволі зміцнити автократичних правителів, консолідуючи їхню владу та контроль над економікою.

Корупція та лобізм: Санкційний режим породив прибуткову індустрію у Вашингтоні, яка включає лобістські групи, юридичні фірми та колишніх урядовців, які використовують свої знання системи для впливу на політику санкцій для різних клієнтів, що викликає питання щодо цілісності та цілей санкцій.

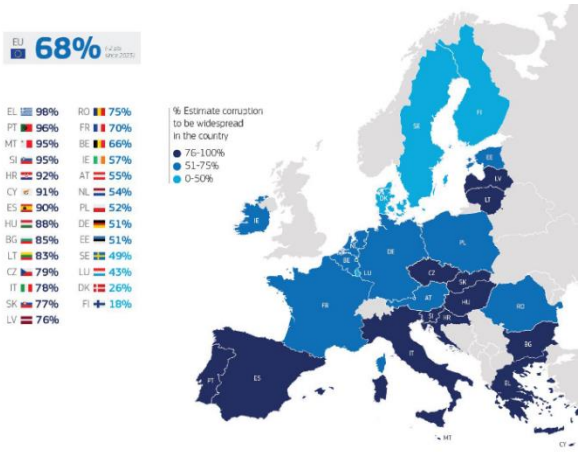
Заклики до альтернатив: Триває дискусія щодо необхідності альтернативних стратегій санкцій. Дехто пропонує збільшити дипломатичні зусилля або переоцінити роль Америки у світі, що може бути більш ефективним у досягненні зовнішньополітичних цілей без негативних побічних ефектів, пов'язаних із санкціями.

http://surl.li/dzacqm

Найпопулярніші новини KYC/AML/CFT за 22-26 липня 2024 року

1. ЄС опублікував спеціальне та флеш опитування щодо ставлення громадян і бізнесу до корупції. 65% громадян вважають, що корупція на високому рівні недостатньо

переслідується, а 51% компаній, що базуються в ЄС, вважають, що людей або компанії, причетні до корупційних дій, спіймають або про них повідомлять владі. На рівні ЄС 68% громадян і 64% компаній ЄС вважають, що корупція широко поширена в їхній державі-члені.



2. [Державний департамент США пропонує винагороду до 10 мільйонів доларів США](#) за інформацію, яка допоможе ідентифікувати або визначити місцезнаходження громадянина КНДР (який пов'язаний зі зловмисною кібергрупою, відомою як Andariel), залученої до зловмисної кібердіяльності проти критичної інфраструктури США .

3. FCA Великобританії вжило перших правозастосовних заходів проти фірми, яка підтримує торгівлю криптоактивами, і [оштрафувала CB Payments Limited (частина Coinbase Group) на 3,5 млн фунтів стерлінгів](#) за неодноразове порушення вимоги, яка перешкоджає фірмам пропонувати послуги клієнтам із високим ризиком.

4. State Street Bank and Trust Company виплатить OFAC 7,5 млн доларів США за [38 очевидних порушень санкцій OFAC пов'язаних із Росією](#) в період з 2016 по 2020 рік.

5. Національне агентство Великобританії з боротьби зі злочинністю та 7 банків Великобританії запустили [великий проект з виявлення та боротьби з організованою злочинністю](#). [Банки-учасники](#) (Barclays, NatWest, Lloyds, Santander, TSB, Metro Bank і Starling Bank) надають NCA дані про рахунки, що вказують на потенційну злочинність, і їх аналізуватиме об'єднана команда експертів, що складатиметься із працівників банків та слідчих із NCA.

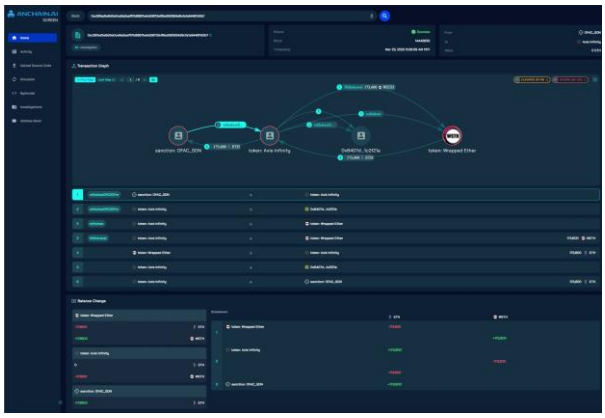
6. Турецька влада розкрила масштабну операцію з відмивання коштів за участю злочинних організацій з використанням банківських рахунків студентів. Сотні студентів [обманом змусили віддати в оренду свої банківські рахунки та отримати значні тюремні терміни](#).

7. Громадянин Ірану був екстрадований з Великої Британії до США, щоб йому пред'явили [звинувачення в обході обмежень США щодо експорту технологій до Ірану](#) через треті країни (ОАЕ та Вірменію), де відповідач контролював компанії-оболонки.

8. [Латвія оскаржила рішення Суду Європейського Союзу, який скасував санкції](#), накладені на російського мільярдера Михайла Фрідмана та його бізнес-партнера Петра Авена

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Чому командам з ПВК і правоохоронним органам потрібно зайнятися смарт-контрактами та DeFi зараз



Смарт контракти та DeFi революціонізують фінанси та створюють нові виклики для розслідувачів фінансових злочинів. Такі шахрайства, як Rug Pulls, Honeypots, шкідливий код, експлойт, Pumps and Dumps і фейкові еірдропи, поширені. І зловмисники використовують це для відмивання коштів і шахрайства.

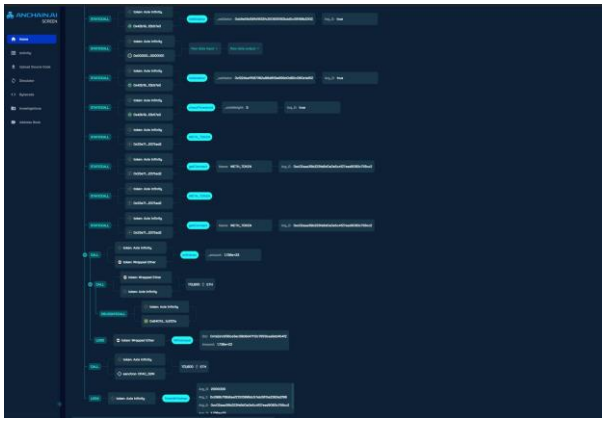
Ось чому потрібно діяти зараз, щоб не залишитися позаду:

🔍 **Запобігання регуляторному арбітражу**: впровадження стандартів ПВК на ранній стадії розробки DeFi та смарт-контрактів допомагає уникнути регуляторного арбітражу, коли зловмисники використовують нормативні прогалини. Ранні стандарти гарантують, що інновації узгоджуються з комплаєнсом із самого початку.

🔍 **Розвиток фінансових злочинів**: злочинці все частіше використовують складні методи для експлойту смарт-контрактів і DeFi для відмивання коштів і шахрайства. Випереджати ці загрози важливо, щоб запобігти значним фінансовим втратам і кримінальній діяльності

🔍 **Швидке впровадження**: швидке зростання DeFi означає, що вікно для впровадження ефективних заходів з ПВК закривається. Необхідно вжити негайних заходів, щоб випередити злочинців, які використовують ці нові технології

🔍 **Технологічна інтеграція**: розвиток досвіду в технології блокчейн і смарт-контрактах тепер готує правоохоронні органи до майбутніх викликів, забезпечуючи більш плавну інтеграцію засобів з ПВК у ці технології



🔍 **Глобальна координація**: раннє залучення, що відповідає міжнародним стандартам, має вирішальне значення для управління транскордонним характером DeFi.

Безпосередньо вирішуючи ці проблеми, ми можемо захистити наші фінансові системи та запобігти експлуатації з боку злочинців.

Елементи звіту спеціалістів з питань протидії відмиванню коштів

Не можна не помітити внесок і участь керівництва в боротьбі з фінансовими злочинами. У цьому контексті регулювання з питань ПВК зобов'язує відповідального працівника готувати та подавати періодичні звіти вищому керівництву про наступне:

- Регуляторні зміни, що впливають на бізнес
- Розвиток програми з ПВК
- Ключові цифри, пов'язані з ПВК у бізнесі (розподіл ризику клієнта, запроваджені заходи CDD тощо).
- Ключові транзакційні паттерни (спосіб оплати, залежно від типу послуг або продуктів тощо)

- Деталі звітності, поданих до ПФР (звіти про підозрілі або інші транзакції)
- Загальний статус відповідності ПВК (помічені недоліки, вжиті заходи з усунення, необхідні додаткові ресурси тощо)

Що такий звіт має в себе включати:

1. Короткий огляд змін у регулюванні з ПВК протягом звітного періоду, які впливають на діяльність компанії
2. Статистична інформація про процес належної перевірки клієнтів (Customer Due Diligence), застосований протягом звітного періоду, така як:
    - Кількість зареєстрованих клієнтів та їх профіль ризику
    - Кількість започаткованих відносин із клієнтами-PEP
    - Клієнти з країн з високим рівнем ризику
    - Відмова від встановлення ділових відносин із потенційними клієнтами або зняті з обслуговування існуючі клієнти
3. Статистична інформація про транзакції з точки зору ПВК, така як:
    - Транзакції з країнами з високим рівнем ризику (обсяг і вартість)
    - Транзакції, здійснені готівкою або віртуальними активами
    - Транзакції, позначені як такі, що несуть ризик відмивання коштів/фінансування тероризму (ВК/ФТ)
4. Резюме звітів про підозрілі транзакції (STR/SAR) та інших звітів з ПВК, поданих протягом звітного періоду
5. Журнал періодичних тренінгів з ПВК
6. Виявлені прогалини в заходах з ПВК, здійснених протягом звітного періоду, та дії, вжиті відповідальним працівником
7. Виконавче резюме щодо стану дотримання правил з ПВК у компанії (потребує покращення або є задовільним)
8. Додаткові вимоги щодо ресурсів для ПВК

Точний та всеосяжний звіт з ПВК від відповідального працівника допомагає вищому керівництву ефективно виконувати свою функцію нагляду за ПВК.

Що таке шахрайство з таймшером?

16 липня FinCEN, OFAC і ФБР опублікували спільне повідомлення про схеми шахрайства з використанням таймшеру. Схеми, реалізовані транснаціональними злочинними організаціями з Мексики, такими як Картель нового покоління Халіско (CJNG).

Що таке таймшер ?

Таймшер — це спосіб спільного володіння нерухомістю, коли покупці отримують право користування нерухомістю протягом певного періоду щороку.

Як працюють таймшери ?

- Шахрайство з таймшером зазвичай націлено на людей похилого віку, які володіють таймшером, обіцяючи купити, орендувати або інвестувати в це майно.
- Шахраї часто видають себе за законних брокерів, адвокатів або торгових представників, щоб зміцнити довіру.
- Вони використовують тактику сильного тиску та підроблену документацію, щоб переконати жертв сплатити авансові збори та податки, які ніколи не повертаються.

Типи шахрайства:

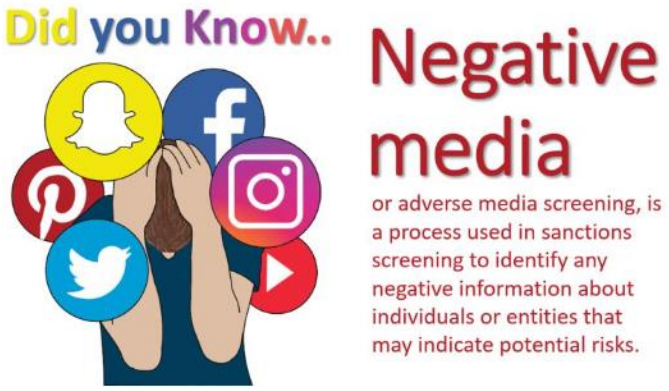
- Шахрайство з виходом із таймшеру: шахраї пропонують купити таймшер жертвам за ринковими ставками або вище.
- Шахрайство з суборендою таймшеру: шахраї обіцяють здавати таймшер жертв в оренду нібито готовим орендарям.
- Шахрайство з інвестиціями в таймшери: жертвам повідомляють, що вони мають право на акції, пов'язані з їхніми таймшерами, і пропонують виступити посередником у продажу акцій.

Шахраї в основному націлені на людей похилого віку, особливо на пенсіонерів, які володіють висококласними таймшерами, якими рідко користуються.

Фінансові установи закликають бути пильними, виявляючи та повідомляючи про підозрілу діяльність, пов'язану з шахрайством із таймшером. Це включає моніторинг попереджень, подання звітів про підозрілу діяльність (SAR) і допомогу жертвам.

http://surl.li/zsmybm

Перевірка на негативні або несприятливі згадки у ЗМІ



Перевірка на негативні або несприятливі згадки у ЗМІ — це процес, який використовується для виявлення будь-якої негативної інформації про осіб або організації, яка може вказувати на потенційні ризики. Цей тип перевірки необхідний для відповідності різноманітним регуляторним вимогам, у тому числі щодо ПВК/ФТ.

Перевірка на негативні згадки у ЗМІ передбачає пошук у різних джерелах інформації, таких як новинні статті, звіти, блоги та інші загальнодоступні дані, щоб знайти будь-яку несприятливу інформацію про особу чи організацію.

📌 Чому перевірка важлива?

- Відповідність нормативним вимогам: забезпечує дотримання вимогам з ПВК/ФТ та інших нормативних вимог.
- Управління ризиками: Визначає потенційні ризики перед започаткуванням ділових відносин.
- Захист репутації: захищає репутацію організації, уникаючи зв'язків із високоризиковими особами чи організаціями.
- Належна перевірка: є частиною процесів належної перевірки клієнта (CDD) і посиленої належної перевірки (EDD).

📌 Негативні згадки можуть включати:

- Кримінальна діяльність
- Причетність до шахрайства або корупції
- Зв'язки з терористичними організаціями
- Порушення санкцій та ембарго
- Регулятивні штрафи
- Інші репутаційні ризики

📌 Джерела негативної інформації

- Сайти основних новинних організацій та газети.
- Відповідні галузеві або регіональні блоги та дискусійні форуми.
- Офіційні сайти, що публікують санкційні списки, штрафи та рекомендації.
- Платформи, де діляться новинами та думками.
- Постачальники, що пропонують комплексні рішення для скринінгу несприятливих медіа.

📌 Інструменти та техніка

- Автоматизовані рішення для перевірки: використовуйте машинне навчання та штучний інтелект для швидкого й ефективного сканування величезних обсягів даних.
- Пошук за ключовими словами: використовуйте конкретні ключові слова, пов'язані з ризиками (наприклад, шахрайство, корупція), щоб визначити відповідні статті.
- Регулярний моніторинг: безперервний або періодичний моніторинг для забезпечення постійної відповідності та управління ризиками.

📌 Виклики

- Помилково позитивні результати: виявлення нерелевантної інформації, яка відповідає ключовим словам ризику, але насправді не є несприятливою.
- Перевантаження даними: керування та аналіз великих обсягів даних із різних джерел.
- Якість даних: забезпечення точності та надійності зібраної інформації.

Розуміння різниці між повідомленнями про підозрілу діяльність (SAR) і повідомленнями про підозрілі операції (STR)

У фінансовій сфері моніторинг та повідомлення про підозрілу діяльність є критично важливими для підтримання цілісності фінансових систем та боротьби з фінансовими злочинами. Проте терміни «повідомлення про підозрілу діяльність» (Suspicious Activity Report, SAR) та «повідомлення про підозрілу операцію» (Suspicious Transaction Report, STR) часто використовуються як синоніми, що може спричиняти плутанину.

Що таке Повідомлення про підозрілу діяльність (SAR)?

Повідомлення про підозрілу діяльність використовуються для повідомлення про будь-яку діяльність, яку фінансова установа вважає підозрілою і такою, що потенційно може свідчити про злочинну поведінку. SAR – це ширша категорія повідомлень, призначена для відображення широкого спектру діяльності, що може свідчити про незаконну або неетичну поведінку, включаючи, але не обмежуючись ними:

- Відмивання коштів
- Шахрайство
- Фінансування тероризму
- Інсайдерська торгівля
- Крадіжка персональних даних

SAR подаються до FinCEN у Сполучених Штатах або до інших відповідних регуляторних органів у різних країнах.

Що таке Повідомлення про підозрілу операцію (STR)?

Повідомлення про підозрілі операції, з іншого боку, зосереджуються на конкретних операціях, які викликають підозру. STR подаються, коли певна операція або серія операцій виглядають незвично або підозріло на основі моделей та поведінки, які зазвичай асоціюються з фінансовими злочинами. STR є підкатегорією SAR і в основному стосується:

- Незвичних операцій, що не відповідають відомому профілю клієнта
- Великих або складних операцій без очевидної законної мети
- Операцій, що включають юрисдикції або суб'єктів з високим рівнем ризику

STR – це детальні звіти, які зосереджуються на конкретних операціях, які можуть свідчити про підозрілу поведінку, допомагаючи органам влади відстежувати та розслідувати конкретну фінансову діяльність.

Ключові відмінності між SAR і STR

1. **Обсяг та фокус:**
    - SAR: Широкий обсяг, охоплює різні типи підозрілої діяльності, не лише транзакції.
    - STR: Спеціалізуються на незвичних або підозрілих операціях.
2. **За змістом:**
    - SAR: Містить опис підозрілої діяльності, причини підозри та відповідні деталі про залучені сторони.
    - STR: Надає детальну інформацію про підозрілу операцію, включаючи суми, дати та характер операції.
3. **Нормативно-правова база:**
    - SAR: Подаються відповідно до нормативних вимог, які зобов’язують звітувати про будь-яку підозрілу діяльність, незалежно від деталей транзакції.
    - STR: Специфічний вид SAR, що зосереджується виключно на транзакціях, які виглядають незвичайними.
4. **Використання:**
    - SAR: Використовуються для виявлення та розслідування ширших схем підозрілої поведінки.
    - STR: Використовуються для розслідування конкретних транзакцій, які можуть свідчити про більш масштабну злочинну схему.