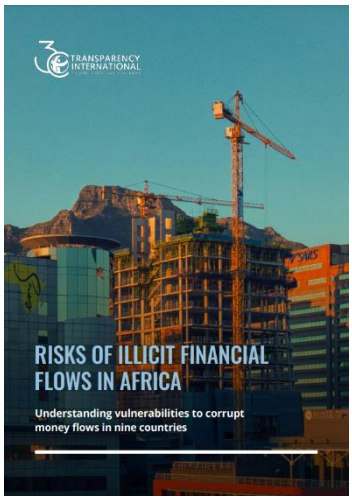
Серійний номер: ДСФМУ-ДК-2024-003
Квітень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Ризики незаконних фінансових потоків в Африці



Нещодавно Transparency International опублікувала звіт, в якому проаналізувала вразливість до корупційних грошових потоків у дев'яти африканських країнах. Документ під назвою «Ризики незаконних фінансових потоків у Африці: розуміння вразливості до корупційних грошових потоків у дев'яти країнах» підкреслює, наскільки незаконні операції становлять серйозну проблему для розвитку, виснажуючи капітал і скорочуючи ресурси, доступні для основних державних послуг, таких як освіта, охорона здоров'я та інфраструктура.

Ці потоки, часто спричинені корупцією, посилюють нерівність і підживлюють велику corruption, що ускладнює їх вимірювання та протидію. Доповідь зосереджена на Республіці Конго, Кот-д'Івуарі, Ефіопії, Кенії, Маврикії, Марокко, Нігерії, Південній Африка та Замбії, досліджуючи типи, джерела та напрямки незаконних потоків, а також визначаючи управлінські та структурні чинники, які підвищують ризики.

Працюючи в більш ніж 100 країнах, Transparency International продовжує мобілізувати зусилля для боротьби з цими потоками за допомогою таких ініціатив, як Ініціатива Африка нерівності, і пропонує щотижневі оновлення через свій інформаційний бюлетень для тих, хто бажає бути в курсі подій і зробити свій внесок у боротьбу з корупцією.

https://www.transparency.org/en/publications/risks-of-illicit-financial-flows-in-africa

Звіт про злочини в інтернеті у 2023 році

Звіт ФБР "Internet Crime Report 2023" вказує на значне зростання кількості скарг і фінансових втрат від кіберзлочинності у США. Він детально розглядає такі злочини як шахрайства з інвестиціями, компрометація ділових електронних листів (BEC), вимагання викупу за допомогою шкідливого програмного забезпечення (ransomware) та шахрайства, пов'язані з технічною підтримкою. Звіт також висвітлює успіхи ФБР у боротьбі з кіберзагрозами, зокрема співпрацю з фінансовими інститутами та правоохоронними органами для покращення звітування про кіберзлочини і відновлення активів.

https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-releases-internet-crime-report

Декларація FATF про фінансові заходи

Документ представляє собою декларацію Групи FATF за 18 квітня 2024 року. Декларація містить кілька ключових пунктів:

1. Підтвердження зобов’язань: Члени FATF підтверджують свою прихильність до боротьби з нелегальним фінансуванням, яке підриває безпеку, спокій та економічний розвиток суспільств.

2. Розширення та привітання: Індонезію вітають як 40-ого члена FATF, що підкреслює важливість різноманітної та єдиної глобальної дії проти нелегального фінансування.

3. Фінансова підтримка та сталість: зобов'язання збільшити базове фінансування, щоб забезпечити сталість FATF і підтримати стратегічні пріоритети ефективного впровадження стандартів FATF.

4. Засудження Росії: FATF засуджує дії Росії в Україні, оскільки вони суперечать принципам FATF, і закликає бути пильними щодо загроз фінансовим системам від цих дій.

5. Прогрес та поліпшення: Протягом останніх двох років, під час президентства Сінгапуру, FATF покращив стандарти з повернення активів і прозорості бенефіціарних власників, а також відповідала на виникаючи ризики в контексті віртуальних активів.

6. Триваючі виклики та майбутній фокус: В декларації визнаються прогалини в ефективному впровадженні стандартів FATF і окреслено зобов'язання вирішувати їх, включаючи покращення нагляду, профілактичних заходів та посилення міжнародної співпраці.

7. Особливі напрямки зосередження: FATF планує продовжити зосередження на протидії фінансуванню тероризму, боротьбі з розповсюдженням зброї масового знищення та підвищенні ефективності фінансових санкцій, пов'язаних з фінансуванням розповсюдження.

8. Підтримка країн з низькими можливостями: Зобов'язання допомагати країнам з нижчими можливостями зміцнити їхні системи з ПВК, особливо тим, які стикаються зі значними ризиками.

9. Управління та інновації: FATF виділяє міцне управління на основі цілісності, відповідальності та прозорості, планує продовжити співпрацю з приватним сектором та іншими зацікавленими сторонами для сприяння інноваціям, забезпечуючи фінансову цілісність.

Загалом, декларація демонструє тривалі зусилля FATF по зміцненню глобальних фінансових систем проти нелегального фінансування та адаптації до нових викликів та технологій, зосереджуючись на міжнародній співпраці, ефективному впровадженні стандартів та постійному покращенні систем боротьби з фінансовими злочинами.

https://bit.ly/3UnMsAP

Фінтернет: фінансова система для майбутнього

Документ описує концепцію "Finternet" — фінансової системи, яка призначена функціонувати аналогічно до інтернету, з'єднуючи різні фінансові екосистеми для підсилення можливостей індивідів та бізнесів. Пропонована модель має на меті спростити взаємодію між різними фінансовими послугами, підвищити доступність і знизити витрати через інтеграцію передових технологій, таких як токенізація активів і єдині реєстри. Ці реєстри є цифровими платформами, що інтегрують численні фінансові ринки та інструменти, що дозволяє оптимізувати транзакції, підвищити безпеку та зменшити витрати.

Система побудована на міцній економічній архітектурі та суворих регуляторних стандартах, що забезпечують її цілісність і функціональність. Особливу увагу приділено орієнтації на користувача, з наданням можливості керувати фінансовими транзакціями та особистими даними. В документі також обговорюється необхідність співпраці між державними органами та приватними секторами для розробки та підтримки необхідної інфраструктури. Це включає створення підтримуючої управлінської рамки та забезпечення відповідності системи юридичним і регуляторним вимогам.

Документ також розглядає потенційні виклики при впровадженні такої системи, включаючи технологічні, регуляторні та операційні перешкоди. Для їх вирішення пропонується поетапний, інклюзивний підхід до розробки та впровадження. Загалом, Finternet має на меті модернізувати глобальну фінансову систему, інтегруючи передові технології та принципи дизайну, орієнтовані на користувача, для створення більш доступного, ефективного і безпечного фінансового середовища, сприяючи ширшій участі на фінансовому ринку і потенційно трансформуючи спосіб надання фінансових послуг у всьому світі.

https://www.bis.org/publ/work1178.pdf

Правила відмови

Метою документа “goAML Rejection Rules”, розробленому FIAU, є огляд правил відхилення у системі goAML. Цей документ надає огляд правил, що використовуються для автоматизованого фільтрування звітів перед їх прийняттям.

Мета цих правил - забезпечити, щоб подані звіти містили достатньо інформації для ефективного оцінювання та пріоритизації отриманих звітів FIAU.

https://fiaumalta.org/app/uploads/2024/04/goAML-Rejection-Rules.pdf

Оцінка ризику ФТ для НПО у Південноафриканській Республіці

У новому звіті Південноафриканської податкової служби оцінено ризики фінансування тероризму серед неприбуткових організацій (НПО). Дослідження має на меті формулювання заходів, що забезпечують зменшення ідентифікованих ризиків. Оцінка базується на опитуванні 301 НПО, дані від правоохоронних та фінансових органів, і виявила основні загрози та вразливості, пов'язані з фінансуванням тероризму. Звіт також наголошує на необхідності підвищення обізнаності серед НПО щодо законодавчих вимог і заходів безпеки для запобігання фінансуванню тероризму. Окреслено рекомендації для поліпшення системи внутрішнього контролю і моніторингу транзакцій, які можуть бути пов'язані з терористичною діяльністю.

https://bit.ly/3JspfXO

РЕГУЛЮВАННЯ

Регламент ЄС 2021/0239 (COD) щодо попередження використання фінансової системи в цілях ВК/ФТ

Не припиняється робота над Пакетом з ПВК у Європейському Союзі, зокрема над фіналізацією тексту нового Регламенту з ПВК/ФТ. Сьогодні у центрі уваги знаходиться тематика обміну інформації в межах ЄС для здійснення кращого аналізу, яка має отримати значний буст і змінити правила гри. Ось, що про це говорять залучені у процес розробки сторони:

«Кілька чудових днів на пленарному засіданні державно-приватного партнерства з питань фінансової розвідки (EFIPPP) Європолу.

Новий Регламент законодавство щодо боротьби з відмиванням коштів (AMLR) кардинально змінює правила обміну інформацією в ЄС для підтримки аналізу ПВК. Ми бачимо значні зміни в усьому світі після «великого вибуху» для співпраці у сфері ПВК, що відбувся влітку 2022 року (коли FFIS (The Future of Financial Intelligence Sharing) організувала виставку співпраці з ПВК у Берліні, а FATF опублікувала посібник «Партнерство у боротьбі з фінансовими злочинами», який рекомендував країнам створити законний шлюз для обміну інформацією між приватними особами).

Ми бачили нещодавні законодавчі зміни або пропозиції щодо підтримки обміну інформацією з ПВК між приватними особами у Великій Британії, Сінгапурі, Канаді та ОАЕ, а також спроби посилити оперативний обмін відповідно до чинних законів у США, Австралії, Мексиці та ПАР. Але Пакет з ПВК у ЄС, мабуть, на іншому рівні. Одразу 27 країн-членів ЄС отримають нове законодавство, яке безпосередньо застосовуватиметься до них (а не просто Директива, яка вимагає багато часу для транспонування та створює так багато відмінностей у ЄС).

Але спочатку перші кроки. Протягом періоду між офіційним схваленням пакету та часом коли положення набудуть чинності, FFIS проведе велику серію семінарів по всьому ЄС (у 2024 та 2025 роках). Ця серія подій щодо стаття 75 AMLR допоможе розібратися в забезпеченні обміну інформацією, розкриє різні ролі приватного сектору та державних установ і окреслить питання, які потребують подальших вказівок. Зрештою, ми сподіваємося сприяти новому поколінню партнерства з обміну інформацією, яке, як ми очікуємо, стане результатом статті 75 AMLR.»

«Тепер, коли Європа визначилася щодо свого майбутнього щодо боротьби з відмиванням коштів, парламент і Рада офіційно приймуть AMLR, Директиву про боротьбу з відмиванням грошей (AMLD) і Регламент про орган влади з ПВК (AMLA) протягом наступних тижнів, робота ще далеко не завершена: перш ніж нове законодавство почне діяти приблизно в середині 2027 року, нам потрібно використати наступні 3 роки, щоб наповнити нову нормативну базу деталями та підготуватися до того, як ми хочемо її застосовувати.

Минулого четверга на симпозіумі з ПВК, організованому Євою-Марією Попчевою в Європейському парламенті в Брюсселі, ми обговорили те, що ми вважаємо головними досягненнями нового законодавчого пакету. На мій погляд, це сліпі плями в поточній системі, які цей пакет дозволить нам усунути. У той час як 27 різних імплементацій попередніх Директив з ПВК створили лазівки, а поле зору національних наглядових органів було обмежене національними кордонами, нова система з однаковими правилами для усього ЄС, з новою наглядовою мережею AMLA та національними компетентними органами на додаток до повноважень AMLA зроблять так, що правила справді застосовуються та виконуються однаково в усіх державах-членах. Але те, що є революційним у новій системі з ПВК у ЄС, коли йдеться про усунення сліпих зон, — це правила, які передбачають

обмін інформацією між приватними особами і у приватно-державних партнерствах, і це охоплює не лише стратегічну інформацію, а й персональні дані!

У штаб-квартирі Європолу в Гаазі нам вдалося дослідити деталі статті 75 AMLR та статті 93 AMLA щодо майбутнього режиму обміну інформацією в ЄС разом із Ніком Максвеллом для обговорення варіантів тлумачення з експертами EFIPPP (uropol's Financial Intelligence Public Private Partnership). У двох словах: нові правила встановлюють баланс між захистом і безпекою даних, з одного боку, та ефективною протидією легалізації коштів через обмін інформацією, з іншого боку. Це усуне поточну правову невизначеність, оскільки правила передбачають, якими даними за яких умов можна обмінюватися в який спосіб. Але все ж є потреба в деталізації. Новий режим встановлює обмеження, оскільки не вся інформація буде доступною для обміну, а лише з певним рівнем ризику. З іншого боку, це дозволить партнерствам обмінюватися персональними даними без необхідності подальшого національного законодавства, лише на основі нових правил ЄС і без офіційного схвалення наглядового органу, але після процесу наглядової перевірки, який може включати органи влади із захисту даних та ПФР.»

Рада Європи дає остаточне схвалення запровадженню кримінальної відповідальності за порушення санкцій ЄС

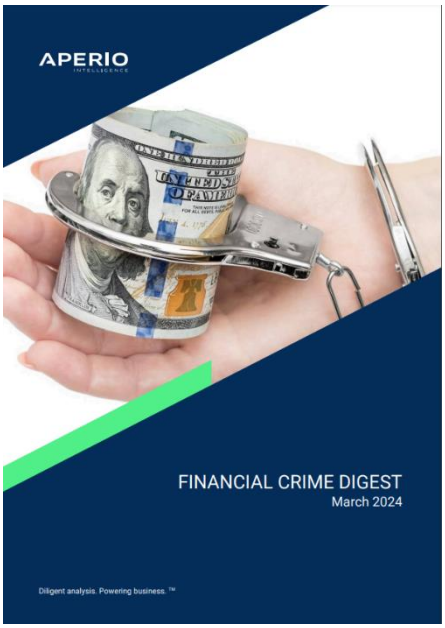
Рада ЄС дала остаточне схвалення на запровадження кримінальних злочинів та покарань за порушення санкцій ЄС. 12 квітня 2024 року Рада ЄС схвалила закон, що встановлює загальноєвропейські кримінальні покарання за порушення або обхід санкцій ЄС у державах-членах. Такі дії, як ухилення від заборони на поїздки або торгівля підсанкційними товарами, тепер є кримінальними злочинами. Покарання включають штрафи та тюремне ув'язнення, особливо за навмисні порушення. Юридичні особи, як і компанії, також можуть бути притягнуті до відповідальності.

Директива набуває чинності з моменту публікації в Офіційному віснику ЄС, при цьому державам-членам надається 12 місяців на інтеграцію її в національне законодавство. Це має на меті посилити боротьбу з обходом санкцій, зокрема у відповідь на російську агресію проти України.

https://bit.ly/3w6wq4T

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Дайджест Фінансових злочинів за березень 2024 року



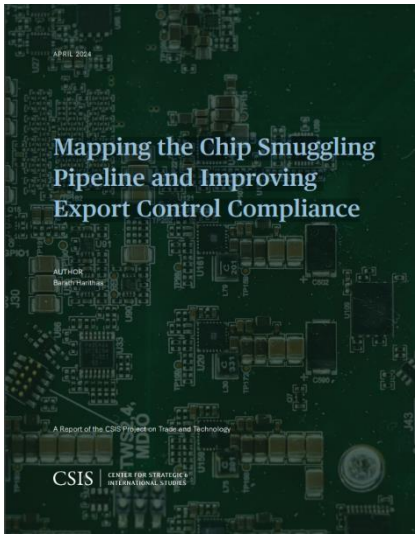
Основні моменти цього видання включають:

- Особливість - Слідування за грошовим слідом: використання фінансових розслідувань для боротьби з #humantrafficking. Для цього Bianca-Ioana Hanganu поговорив з Tarana Baghirova OSCE Програми фінансових розслідувань, RedCompass Labs директором ПФР Silvija Krupena, CFCS, CAMS, координатором La Strada International International Suzanne Hoff, колишнім керівником відділу сучасного рабства Лондонської столичної поліції та радником-спеціалістом у The Human Trafficking Foundation Phil Brewer MA, а також професором Маастрихтського університету та Вільного університету Амстердама Jill E.B. Coster van Voorhout

- Special Feature від Oana Gurbanoaia - Румунія намагається регулювати #deepfakes на тлі зростання кількості випадків захворювання та насиченого виборами року
- ЄС AMLR не забороняє самостійні платежі #crypto гаманця, уточнює European Crypto Initiative
- U.S. Department of the Treasury попереджає фінансові установи про #fraud #AI та ризики кібербезпеки
- Оновлення по країні за Mairi Bocker; проникнення італійських #organisedcrime груп у сектори управління відходами та нерухомості
- Оновлення країни від Andrea Peniche Cobo: Улюблений кандидат Мексики: хто така Клаудія #Sheinbaum?
- Оновлення по країні від Luis L.: Громадський тендерний клімат у Бразилії після скандалу з Korruption Lava Jato

https://www.aperio-fcd.com/

Відображення каналу контрабанди чіпів та покращення дотримання експортного контролю



Як пояснюється в резюме виконавчого директора «Ухилення від експортного контролю контрольованих чіпів є відомою проблемою, але специфіка цієї діяльності непрозора. Крім того, помітно відсутній систематичний аналіз усього конвеєра контрабанди мікросхем, від початкової закупівлі до незаконного розповсюдження. Це дослідження має на меті подолати цю методологічну прогалину Він розбирає контрабандний трубопровід на чотири окремі етапи - (1) початкові закупівлі. (2) ухилення від митного контролю, (3) вихід з порту та (4) перевалка - і визначає 11 потенційних тактик контрабанди».

Пропонуючи ігрову презентацію різних кейсів, документ стене хорошим ресурсом для навчання, підвищення обізнаності про ваші compliance команди.

- Документ підштовхує до подальшої реалізації вже розпочатої політики формування безпечних торговельних коридорів через регулювання експортного контролю Аналіз CSIS поширює цю тенденцію на додаткові контрольні можливості в третіх країнах, а також пропонує новий підхід до торгівлі чутливими товарами:

Техно націоналізм може вимагати, щоб Сполучені Штати знайшли більшу безпеку не через внутрішнє втручання, а через зовнішню взаємодію та розширення підтримки розбудови потенціалу в окремих третіх країнах. В іншому випадку ці країни навряд чи самі будуть самостійно інвестувати в удосконалені заходи експортного контролю

- Використання користувальницької цифрової накладної, індивідуальна цифрова накладна на чіпи. що містить унікальний Ідентифікатор, може мінімізувати ризики, пов'язані з фальсифікацією митних документів. Цифрова автентифікація додатково забезпечує цілісність накладної, що ускладнює контрабандистам підробку документів без виявлення.
- Попереднє схвалення логістичних провайдерів. Покупцям чіпів буде дозволено використовувати лише попередньо перевірені логістичні провайдери та маршрути Покупець повинен визначити обраного ним логістичного провайдера в точці продажу Якщо цього не зробити мас призвести до скасування продажу.

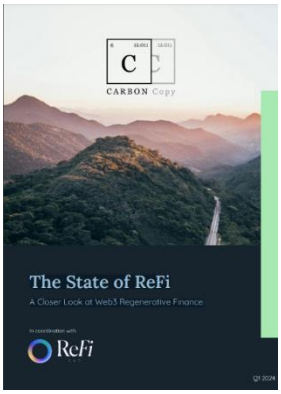
https://bit.ly/49NctxL

Навігація глобальним криптоландшафтом за допомогою PwC: Погляд у 2024

Документ "Crypto regulation worldwide PWC 2024" від PwC надає всебічний огляд глобального регулятивного ландшафту криптовалют на 2024 рік. Звіт визначає ключові напрямки розвитку правових рамок, які покликані стабілізувати ринок цифрових активів та сприяти інноваціям. Він підкреслює різноманітність регулятивних підходів, які приймаються в різних юрисдикціях, і аналізує їхні впливи на гравців індустрії. Особлива увага приділяється концепції юрисдикційної еквівалентності, де стандарти однієї країни визнаються порівнянними іншою, що сприяє транскордонній діяльності криптофірм. Звіт також включає стратегічні розглядання для криптофірм, які обирають юрисдикції для своєї діяльності, з огляду на регулятивну зрілість, вартість операцій та доступність талантів у різних регіонах. Представлено також погляди ключових глобальних регуляторів, таких як Фінансова стабільність рада (FSB) та Міжнародний валютний фонд (IMF), на управління ризиками, пов'язаними з криптоактивами, та забезпечення міцних регулятивних рамок. Окрім цього, звіт детально розглядає специфіку регулятивних рамок у ключових юрисдикціях, таких як Сполучені Штати, Велика Британія та ЄС, забезпечуючи огляд законодавчого та регулятивного статусу станом на січень 2024 року. Звіт PwC призначений для керівництва криптобізнесу у складному та швидко змінюваному глобальному регулятивному середовищі, підкреслюючи як можливості, так і виклики, які постають перед різними регулятивними середовищами.

https://bit.ly/3JlPFum

Стан ReFi. Детальніше про регенеративні фінанси Web3



Документ "The State of ReFi Q1 2024" пропонує детальний огляд стану регенеративних фінансів (ReFi) у контексті веб-технологій третього покоління (Web3). Звіт висвітлює, як ReFi використовує блокчейн, криптовалюти, смарт-контракти та інші сучасні технології для вирішення глобальних проблем, таких як зміна клімату та нерівність доходів. Виділено різні проекти, які використовують ці технології для створення позитивного соціального та екологічного впливу, включно з фінансуванням громадських благ, цифровим моніторингом, звітністю та верифікацією (dMRV) та універсальним базовим доходом.

Звіт також зазначає, що, незважаючи на несприятливі умови ринку, активність у сфері ReFi залишалася високою протягом 2023 року. Основні

аспекти включають зростання кількості екологічних активів, які токенізуються та переносяться на блокчейн, та впровадження альтернативних механізмів фінансування, таких як ретроспективне та квадратичне фінансування.

Тим не менш, ReFi стикається з низкою викликів, зокрема з питаннями репутації через зв'язок з криптовалютами та добровільним вуглецевим ринком, а також з проблемами комерціалізації та регулювання. Незважаючи на це, ReFi продемонстрував свій потенціал як значущий гравець у боротьбі зі зміною клімату та нерівністю доходів, пропонуючи нові підходи до фінансування та інвестування, які зосереджені на регенеративному впливі та стійкості.

https://carboncopy.news/reports/state-of-refi-2024

Секрети Свазіленду

Це транскордонне розслідування, яке розкриває раніше невивчену роль Есватіні, останньої абсолютної монархії в Африці, як потенційного каналу в економіці незаконної торгівлі золотом у Південній Африці. Розслідування підкреслює, як неналежний контроль з ПВК дозволяє особам, близьким до королівської родини, отримувати вигоду від своєї близькості до короля.

Розслідування базується на витоку понад 890 000 внутрішніх документів із підрозділу фінансової розвідки Есватіні, отриманих Distributed Denial of Secrets і наданих Міжнародному консорціуму журналістів-розслідувачів (ICIJ). Команда з 38 журналістів з 11 країн проаналізувала документи, серед яких банківські звіти, звіти про поліцейські розслідування, судові свідчення під присягою та конфіденційні комунікації між урядовими установами.

Документи викривають зв’язки між видатними особами, включно з членами королівської сім’ї, і показують, що мільйони доларів переводилися від компанії з перевезення готівки в Південній Африці до золотопереробної компанії в Есватіні, яка потім відправляла кошти в Дубай. Ця золотопереробна компанія була заснована двома діловими партнерами, один з яких є зятем короля Мсваті III. Підозріла діяльність включає ухилення від сплати податків, незаконне переміщення грошей за кордон і управління незаконними коштами через королівство.

https://www.icij.org/investigations/swazi-secrets/

Незаконна криптоекономіка 2023 року

У 2023 році зловмисники отримали у криптовалюті суму на понад 34 мільярди доларів США.

У останньому звіті TRM Labs «Незаконна криптоекономіка» детально розглядаються основні тенденції, які були помітні та розвивалися в криптопросторі у 2023 році. Цей звіт є безцінним ресурсом для правоохоронних і регуляторних органів, фінансових установ і криптобізнесу, кому потрібно краще розуміти галузь і випереджати зростаючі загрози.

Ця постійна поширеність і складність злочинної діяльності з криптовалютами підкріплює важливість інтелектуальних рішень для

блокчейну. І оскільки такі злочинні категорії, як торгівля наркотиками в даркнеті та фінансування тероризму, стають все більш поширеними в блокчейнах, спеціалісти як у державному, так і в приватному секторах повинні залишатися пильними і бути поінформованими для ефективної боротьби зі злочинністю у криптосвіті.

Висновки звіту The Illicit Crypto Economy 2023 показують, що:

1. Загальні незаконні обсяги скоротилися

2. Обсяги санкцій різко впали

3. Дохід від хакерських атак зменшився вдвічі

4. Загальні обсяги скамів та шахрайства зменшилися

5. Темпи зростання фентанілу впали

6. Незаконний продаж наркотиків залишається високим

7. Майже половина всього обсягу незаконної криптовалюти припадає на мережу TRON

8. Tether домінує у фінансуванні тероризму

https://www.trmlabs.com/post/new-report-the-2023-illicit-crypto-economy

Економічний профіль: ваш важливий інструмент у боротьбі з фінансовими злочинами

Національні регуляції наголошують на важливості дотримання процедур належної перевірки клієнтів (CDD) для боротьби з фінансовими злочинами, акцентуючи на створенні економічного профілю під час початку або продовження ділових відносин. Економічний профіль збирає детальну інформацію про діяльність та транзакційні звички клієнта, що дозволяє оцінити рівень ризику та підтримувати комплаєнс у сфері протидії відмиванню коштів та фінансуванню тероризму.

https://bit.ly/4b572vv

Річний глобальний звіт про оподаткування криптовалют за 2024 рік

Звіт PwC Global Crypto Tax за 2024 рік детально розглядає зміни у сфері оподаткування криптовалют у різних країнах. У документі аналізуються основні тенденції регулювання криптовалют, виклики оподаткування токенізованих активів та особливості стейблкоінів та інших токенізованих фінансових інструментів. Звіт призначений для учасників крипторинку, включаючи інвесторів та регуляторні органи, і пропонує детальний аналіз податкових наслідків та рекомендації щодо дотримання вимог.

https://www.pwc.com/ee/en/press-room/news-and-articles/pwc-global-crypto-tax-report-2024.html

Обмін даними та санкції проти Росії

Опубліковано останній звіт SIFMANet про роль обміну даними для покращення імплементації та дотримання санкцій! Ось кілька ключових висновків:

- Червоних прапорців недостатньо. Правоохоронні органи шукають дієві докази, які можуть бути використані для переслідування суб'єктів з новими обмеженнями та притягнення до відповідальності порушників санкцій.
- Не все так просто. Ключові дані, такі як торгівля третьою стороною з Росією, часто відсутні, ненадійні або недоступні.
- Державний сектор стикається з перешкодами для обміну даними за фрагментарними моделями та захисту даних. Це особливо помітно в країнах з децентралізованими моделями впровадження з безліччю національних компетентних органів.
- Навантаження на приватний сектор продовжує зростати. У той час як великі виробники можуть виділяти ресурси для перевірки своєї діяльності, фінансові установи повинні мати важелі впливу для підтримки малого та середнього бізнесу.

Використання та обмін якісними даними мають важливе значення для ефективної імплементації та забезпечення дотримання санкцій. Щоб дізнатися більше, прочитайте звіт.

Поточний досвід із санкціями проти Росії кардинально змінює ситуацію в багатьох сферах. Нефінансові корпорації просять вийти за рамки традиційної перевірки ділових партнерів на присутність у санкційних списках. Натомість їм доручено контролювати складні ланцюжки постачання та дистриб'юторські мережі – завдання, до якого вони не готові. Крім того, сам міжюрисдикційний характер транзакцій надає значні можливості для приховування незаконної діяльності.

Чи спостерігаємо ми появу свого роду спільного громадського порядку, де завдяки OSINT та іншим інформаційним технікам широкий спектр зацікавлених сторін може сприяти застосуванню санкцій? «Скоріше за все, правоохоронні органи просто шукають корисну інформацію, яка може бути використана для переслідування порушників санкцій та/або цільових організацій із запровадженням нових обмежень. Крім того, вони прагнуть конкретних і детальних оцінок того, як їхні заходи впливають на транзакції та дотримання санкцій». Як зазначено в останніх заявах/деклараціях США, державно-приватне партнерство ніколи не було сильнішим у цій сфері, де торгівля та безпека перетинаються.

Дані проти реальності? «Оскільки фізичні перевезення таких товарів здебільшого відбуваються за межами країн коаліції їхні власні митні дані мало допомагають. І багато країн, через які ведеться основна частина цієї торгівлі, не діляться інформацією, тому що не беруть участі в санкціях».

Цілісність даних, «Поза межами обмежень, які ставлять під загрозу якість інформація, митні дані часто є неповними (наприклад, через контрабанду) та/або підлягають фальсифікації. Насправді коаліційні органи влади часто виявляють суттєві невідповідності під час порівняння даних, що стосуються тієї самої транзакції з різних джерел. Найчастіше коди, що ідентифікують відповідні товари – так звані коди Гармонізованої системи (HS) – відрізняються між експортом до Росії, як зазначено в митних деклараціях коаліції чи третіх країн, та імпортом із цих країн до Росії, як відображено в даних російської торгівлі. "

Безпека проти захисту даних? «У багатьох країнах стандарти захисту даних є високими, що ускладнює доступ ключових установ до інформації. Це може стосуватися, наприклад, інформації про фізичні потоки товарів, що надаються митними службами, і про фінансові операції, що надаються центральними банками і ПФР. Бар'єри як правило, можна подолати у випадку підозри в конкретних незаконних діях, але вони часто перешкоджають зусиллям у більш широкому відстеженні розвитку подій, пов’язаних із санкціями».

Дані є ключовими для того, щоб санкції діяли, але вони є доповненням до розслідувань та перевірок на місцях для завершення циклу.

https://bit.ly/4d1Rydo

Халвінг біткойна: вичерпний посібник для інвесторів

«Халвінг» означає скорочення наполовину винагороди за майнінг біткойнів.

Ця подія, записана в алгоритм видобутку біткойнів, відбувається після видобутку кожних 210 000 блоків біткойнів, що трапляється в середньому раз на 4 роки.

Майбутній халвінг є четвертим з моменту появи біткойна і очікується приблизно 19-20 квітня. Винагорода за кожен видобутий блок буде скорочена до 3,125 BTC. Це означає, що 3,125 нових BTC будуть з'являтися у циркуляції за кожен новий видобутий блок. (Зараз це 6,25 BTC.)

Халвінг призначений для зменшення швидкості, з якою нові біткойни потрапляють в обіг, створюючи дефіцит.

Код також обмежує обіг біткойнів на рівні 21 млн. Очікується, що фінальний халвінг, який приведе нас до цієї цифри, відбудеться у 2140 році.

Отже, що це означає для нас?

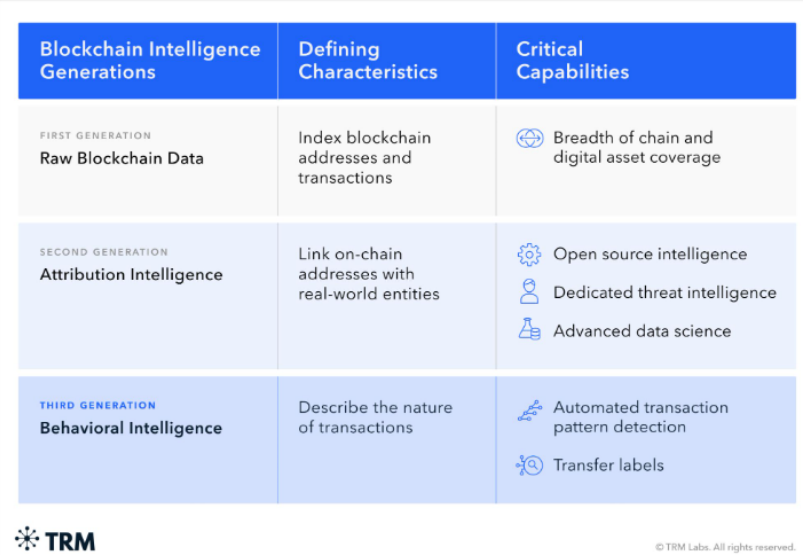
Як ми всі знаємо, дефіцит зазвичай підвищує ціни. Після кожного попереднього халвінгу ціни на біткойни різко зростали.

Як цей халвінг вплине на ціни біткойнів? Деякі аналітики вважають, що це дещо складніше передбачити, оскільки біткойн уже досяг історичного максимуму напередодні халвінгу, безпрецедентна подія, спричинена різними факторами, такими як ейфорія від запуску спотових біткойн-ETF. Тим не менш, деякі спостерігачі залишаються оптимістично налаштованими щодо ще одного зростання після халвінгу.

https://bit.ly/3JqeFAQ

ІНШІ НОВИНИ

Поведінковий інетелект



Минулого тижня TRM Labs представила наступний стрибок вперед у блокчейн-інтелекті - поведінковий інтелект, що ознаменувало початок третього покоління блокчейн-розслідувань.

У 2020 році TRM став піонером основ поведінкового інтелекту, запустивши Signatures®, здатність, яка виявляє закономірності в групах транзакцій у мережі, які вказують на приховану підозрілу поведінку, яка в іншому випадку могла б залишитися непоміченою. Підписи дозволяють слідчим швидко знаходити та планувати складні методи відмивання грошей та інші типології в мережі.

Щоб зробити дані в блокчейні більш зрозумілими та дієвими для слідчих, TRM збагачує поведінковий інтелект впровадженням міток передачі - набору даних, який збагачує контекст того, що означають конкретні транзакції в мережі. В даний час більшість інструментів відображають рух коштів між суб'єктами спрощено, без сигналу про мету транзакції.

Мітки переказу дозволяють досліджувати транзакцію, щоб зрозуміти, що в ній відбувається, наприклад, повідомлення, що зберігаються в блокчейні. створення смарт-контракту, крадіжка коштів у мережі або виплата викупу.

Такий підхід допоможе:

- Правоохоронним органам швидше виявляти складні методи заплутування та реагувати на них
- Фінансовим установам та криптовалютним бізнесам розширювати можливості належної перевірки та покращувати відповідність нормативним вимогам
- Податковим органам ефективніше виявляти ухилення від сплати податків
- TRM Labs робить цю технологію доступною для агентств та організацій, зацікавлених у поглибленні свого розуміння блокчейн-діяльності.

У світі, в якому зловмисники можуть створювати адреси одним натисканням кнопки, слідчим потрібні найсучасніші інструменти, які виходять за рамки розуміння приписуваних адрес до розуміння моделей і поведінки відмивання грошей.

Азартні ігри та корпоративна соціальна відповідальність: найкращі практики для малого та середнього бізнесу

Стаття Business Matters розглядає практики корпоративної соціальної відповідальності (КСВ) у гральному бізнесі, особливо для малих та середніх підприємств. Вона акцентує на важливості впровадження ефективних КСВ практик для збереження позитивного іміджу та уникнення серйозних наслідків, таких як штрафи або втрата ліцензій, через невідповідність регуляторним та анти-відмивальним

нормам. Окрім того, стаття підкреслює важливість налагодження взаємодії з місцевими спільнотами та здійснення позитивного впливу на суспільство.

https://bit.ly/49Iydeg

Міністерство фінансів ПАР просить коментарі до проекту змін до законодавства про відмивання коштів

У статті обговорюються пропозиції змін до регулювання відмивання грошей у Південній Африці. Зміни мають на меті зміцнення системи країни шляхом покращення звітності щодо переміщення готівки та інструментів на пред'явника через кордон, що важливо для ефективності роботи ПФР. Ці поправки також спрямовані на підвищення прозорості фінансових операцій, зокрема, щодо іноземних інвестицій та великих готівкових транзакцій. Вони передбачають вдосконалення координації між різними регуляторними органами та фінансовими установами, що сприятиме більш ефективному запобіганню фінансових злочинів на національному рівні.

https://bit.ly/3JwzmLb

Європейська нерухомість: мішень для брудних грошей?

Європейська нерухомість останніми роками стала пріоритетною ціллю для кримінальних груп, які прагнуть відмити свої незаконні прибутки. Сприятливі умови для інфільтрації незаконних коштів у легальну економіку створюються через ряд обставин: привабливість регіону як інвестиційного напрямку, недостатній регуляторний нагляд, та непрозорість фінансових операцій. У зв’язку з посиленням усвідомлення серйозності цієї проблеми, стаття обговорює необхідність вирішення системних вразливостей та захисту цілісності ринків нерухомості Європи.

https://www.msn.com/en-us/money/realestate/europe-s-real-estate-a-target-for-dirty-money/ar-BB1laBUr

Держави басейну озера Чад можуть перервати життєвий цикл тероризму – його фінансування

Стаття на DefenceWeb обговорює виклики та стратегії боротьби з фінансуванням тероризму в басейні озера Чад. Особлива увага приділяється зусиллям країн регіону щодо перерізання фінансових каналів терористичних груп, таких як Боко Харам та ІДІЛ , через санкції та правові заходи. Стаття також звертає увагу на необхідність створення міцніших інформаційних систем для відстеження та блокування фінансових потоків терористичних організацій. Автори вказують на значення обміну розвідувальною інформацією між країнами, що може підвищити ефективність зусиль у боротьбі з тероризмом.

https://bit.ly/447pukL

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Злиття та поглинання (M&A): потенційні інструменти для відмивання грошей

Злиття та поглинання є важливими для зростання бізнесу та розширення ринку, але вкрай важливо знати про їх потенційне використання в незаконній діяльності, такій як відмивання коштів. Давайте розглянемо деякі способи, якими M&A можна використовувати в незаконних цілях:

1. Приховування походження коштів: через M&A гроші, отримані незаконним шляхом, можна інвестувати в законний бізнес. Придбання компанії може сприяти змішуванню незаконних коштів із законними, ускладнюючи відстеження походження грошей.

2. Переоцінка та передача активів: під час придбання, активи цільової компанії можуть бути навмисно завищені у ціні, щоб виправдати переказ великої суми грошей компанії. Це може служити для «очищення» великих сум брудних грошей під виглядом легальної операції.

3. Складність і відсутність прозорості: M&A можуть бути складними та залучати багато сторін і країн. Цю складність можна використати для створення димової завіси, яка маскує відмивання грошей, особливо якщо в залучених країнах діють менш суворі правила з ПВК.

4. Використання менш регульованих секторів: деякі сектори чи країни можуть мати менш суворий контроль, що дозволяє використовувати організації як засоби відмивання коштів. Придбання або злиття з компаніями в цих секторах або країнах може полегшити процес.

5. Неадекватність програм комплаєнсу: якщо придбана компанія має неадекватну програму комплаєнсу, відмивачі можуть легше використати це. Інтеграція після придбання може не впоратися із виявленням або виправленням цих недоліків, що дозволить безперешкодно продовжувати діяльність з відмивання.

Враховуючи потенціал цих незаконних дій, дуже важливо, щоб компанії впроваджували суворі процеси належної перевірки та підтримували надійні програми комплаєнсу. Інвестори та компанії повинні проявляти активність у розпізнаванні та управлінні ризиками відповідності та доброчесності в угодах злиття та поглинання не тільки для захисту своїх операцій, але й для захисту цілісності глобального фінансового ринку.

FATF Travel Rule and Know Your Corresponding VASPs

У рамках Програми з протидії відмиванню коштів та фінансуванню тероризму постачальники послуг віртуальних активів (VASP) також повинні дотримуватися Travel Rule від FATF, включаючи дотримання процесу Know Your Corresponding VASP (KYV). В цій стаття обговорюється Travel Rule, його основні елементи, KYV і процес його імплементації, а також деякі найкращі практики для сприяння заходам протидії відмиванню коштів та дотриманню Travel Rule.

https://amluae.com/fatf-travel-rule-and-know-your-corresponding-vasps/

Підготовка до моніторингу фінансових операцій

Будьте в курсі регулювання: Ознайомтеся з нормами протидії відмиванню коштів (ПВК). Це важливо для розуміння комплаєнсу.

Майте план, заснований на ризиках: Розробіть стратегію для вашої установи. Сконцентруйтеся на високоризикових клієнтах, продуктах та регіонах.

Встановіть норми моніторингу: Створіть правила спільно з вашою командою комплаєнсу, які виявлять складні операції. Ці правила повинні відповідати вимогам законодавства та вашому рівню ризику.

Налаштуйте свою систему: Налаштуйте систему моніторингу операцій відповідно до ваших правил. Мета - точність та ефективність для уникнення помилкових повідомлень.

Перевіряйте повідомлення: Регулярно перевіряйте повідомлення з вашої системи. Визначте їх важливість та ризик, щоб визначити потребу в подальшому розслідуванні.

Глибоко аналізуйте: Глибоко аналізуйте проблеми, якщо повідомлення вказують на серйозні проблеми. Збирайте більше даних, переглядайте документи та спілкуйтеся з відповідними особами.

Все записуйте: Зберігайте записи своїх розслідувань. Вони важливі для аудитів та регуляторних перевірок, щоб показати вашу відданість прозорості та наполегливу роботу.

Дійте рішуче та ескалуйте, якщо необхідно. Наприклад, подавайте звіти або закривайте ризиковані рахунки.

Забезпечте точну та своєчасну звітність: Швидко та правильно надсилайте необхідні звіти, такі як Звіти про підозрілу діяльність (SAR). Співпрацюйте з вашою командою компаєнсу, щоб виконати всі терміни та стандарти.

Продовжуйте вдосконалюватися: Постійно вдосконалюйте свої Майте план, заснований на ризиках стратегії моніторингу та використовуйте нові технології для підтримки ефективності системи.