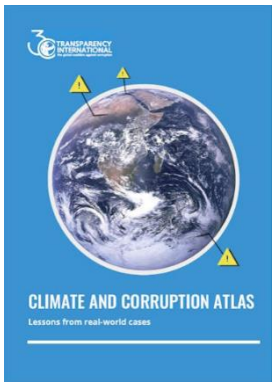
Серійний номер: ДСФМУ-ДК-2024-007
Травень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Атлас клімату і корупції: Уроки реальних кейсів



Нещодавнє дослідження під назвою «Атлас клімату та корупції: уроки реальних випадків» підкреслює, як корупція може перешкоджати ефективності ініціатив із пом'якшення кліматичних змін та адаптації до них.

Опублікований звіт Transparency International висвітлює випадки корупції за допомогою першого цифрового інструменту такого роду, Атласу справ про клімат і корупцію.

Аналізуючи корупційну поведінку, сприятливі фактори та негативні наслідки, у звіті пропонуються рекомендації щодо покращення контролю доброчесності в агентствах, які керують кліматичними фондами. Реалізація цих рекомендацій забезпечить більшу послідовність у контролі цілісності, покращуючи управління фінансуванням боротьби з кліматом у всьому світі.

https://www.transparency.org/en/publications/climate-and-corruption-atlas-lessons-from-real-cases

FinCEN попереджає банки про посилення підтримки Іраном терористичних угруповань

Мережа боротьби з фінансовими злочинами (FinCEN) 7 травня 2024 року опублікувала рекомендацію, в якій закликала фінансові установи США посилити пильність щодо транзакцій, які потенційно пов'язані з терористичними організаціями, підтримуваними Іраном.

Ці дії відбуваються на тлі занепокоєння зростанням терористичної активності на Близькому Сході.

Методи фінансування, які використовує Іран

У рекомендаціях висвітлюються різні методи, що використовуються цими організаціями для отримання доступу та переміщення коштів через фінансову систему. Це включає в себе

- пряму фінансову підтримку від іранського уряду
- використання благодійних організацій та
- на перший погляд законну бізнес-діяльність
- Експорт нафти і газу
- Ненафтовий експорт
- Нелегальний продаж нафти та ухилення від санкцій
- Збільшення збору податків

Як Іран переміщує кошти

З використанням:

- Підставних компаній (торгові компанії та обмінні пункти), які діють як глобальний «тіньовий банкінг».
- Обмінних пунктів та підставних компаній, які фальсифікують ідентифікаційні дані грошових переказів у банках, які мають кореспондентські рахунки у фінансових установах США.

Червоні прапорці для виявлення підозрілої діяльності

FinCEN наголошує на важливості виявлення та повідомлення про підозрілу діяльність.

Червоні прапорці:

- Клієнти, які здійснюють операції з фізичними та юридичними особами, щодо яких застосовано санкції.
- Використання ключових термінів, пов'язаних з терористичними організаціями, в переказах peer-to-peer
- Транзакції з компаніями, що надають грошові послуги, та постачальниками послуг з управління віртуальними активами, які працюють в юрисдикціях зі слабкими процесами ідентифікації та верифікації клієнтів, що мають високий ризик терористичної діяльності.
- Транзакції за участю компаній з непрозорою структурою власності, незрозумілими назвами або бізнес-адресами в житлових районах.
- Транзакції за участю організацій, пов'язаних з Іраном або терористичними угрупованнями, що підтримуються Іраном
- Благодійні організації або неприбуткові організації, які отримують великі пожертви з невідомих джерел.
- Операції з відомими або підозрюваними адресами віртуальних валют, пов'язаними з тероризмом.

https://bit.ly/3yk7vLW

Роль ATM віртуальних валют у відмиванні доходів, отриманих злочинним шляхом

FINTRAC, канадське агентство з протидії відмиванню коштів та фінансуванню тероризму, опублікувало новий звіт, в якому висвітлюються ризики, пов’язаний із криптовалютними АТМ для відмивання коштів і фінансування тероризму, у травні 2024 року.

Аналіз FINTRAC показує, що криптовалютні АТМ стали ключовими інструментами циклу відмивання коштів, особливо в таких мегаполісах, як Торонто, Монреаль і Ванкувер, а також в

інших містах Канади, включаючи Едмонтон, Калгарі та Оттаву. Підозрілі операції часто включають схеми шахрайства, торгівлю людьми та кіберзлочини.

У звіті підкреслюється важливість для компаній і операторів криптовалютних АТМ впровадження суворої політики комплаєнсу, включаючи ідентифікацію клієнтів і постійний моніторинг транзакцій з високим ризиком. FINTRAC закликає громадськість залишатися пильною проти шахрайства, пов'язаного з криптовалютою, і повідомляти про підозрілу діяльність до відповідних органів.

https://fintrac-canafe.canada.ca/intel/advisories-avis/atm-ga-eng

ЗА СТІНОЮ: РОЗСЛІДУВАННЯ ВЛАСНОСТІ НА КОМПАНІЇ ТА НЕРУХОМІСТЬ У ФРАНЦІЇ

Дослідження "Behind a Wall: Investigating Company and Real Estate Ownership in France" від Transparency International розглядає питання володіння нерухомістю у Франції через непрозорі корпоративні структури. Особливу увагу приділено тому, як злочинці та корумповані особи використовують ці структури для приховування своїх активів. Незважаючи на доступність даних про власників з 2021 року, розслідування відмивання грошей стикаються з серйозними труднощами через складність виявлення справжніх власників нерухомості.

https://www.transparency.org/en/publications/behind-a-wall-company-real-estate-ownership-in-france

Смертоносна контрабанда людей через Мексику процвітає в «ідеальному циклі безкарності»

Дослідження ICIJ висвітлює нові деталі щодо маршрутів контрабанди мігрантів у Мексиці. Спільне розслідування різних медіа-організацій показало зростання використання вантажівок для нелегального перевезення людей, що призводить до численних нещасних випадків та смертей. Репортери зібрали свідчення мігрантів, експертів та колишніх чиновників, а також проаналізували тисячі сторінок офіційних документів. Розслідування також виявило вплив мексиканських картелів та участь корумпованих правоохоронців у цьому процесі.

https://bit.ly/4bBFej3

Керівні настанови щодо фінансових санкцій за використання програм-вимагачів

Рекомендації підрозділу Міністерства фінансів Великої Британії по контролю за впровадженням та дотриманням фінансових санкцій, щодо боротьби з програмами-вимагачами надають вказівки з управління ризиками та відповідальністю, пов'язаними з виплатою викупів. У звіті йдеться про важливість дотримання санкційного законодавства та запобігання фінансуванню злочинних груп, що займаються кіберзлочинами. Виплата викупу може підпадати під санкції, що загрожує серйозними правовими наслідками. В керівних настановах також описані кроки для покращення кіберстійкості та процедури звітності для жертв атак.

https://bit.ly/3wB3Xoh

РЕГУЛЮВАННЯ

Закон про санкції 2024 року

У квітні у Великобританії набув чинності Закон про санкції 2024 року («Закон»). Закон і Положення про санкції забезпечують законодавчу основу для того, як санкції Організації Об'єднаних Націй і Сполученого Королівства набувають юридичної сили на острові Мен.

Підрозділ фінансової розвідки острова Мен опублікував вебінар, у якому детально пояснюється нові законодавчі зміни та те, як вони можуть вплинути на фізичних та юридичних осіб.

https://www.youtube.com/watch?v=2I9x7beGFfo

Гайд в сфері регулювання криптоактивів у Європі

🚀 Вийшов останній випуск «MICA to RegRally: The Crypto Guide»! Ознайомтеся з оновленням європейських нормативних документів цього місяця, щоб отримати всю необхідну інформацію. Ось короткий огляд того, що всередині:

🔒 AMF вносить BITGET до чорного списку: AMF попереджає громадськість про BITGET, неавторизовану платформу для торгівлі цифровими активами у Франції.

⚠ Сповіщення AMF і ACPR: спільне попередження AMF і ACPR щодо неавторизованих організацій, які пропонують Forex і похідні криптовалютні активи у Франції.

📜 Пісочниця цифрових цінних паперів: FCA та Банк Англії пропонують запровадити та керувати пісочницею цифрових цінних паперів.

▶ Зловживання ринком, позначене ESMA: ESMA підкреслює максимальну вилучену вартість (MEV) як потенційне зловживання ринком.

💶 Нові закони ЄС про боротьбу з відмиванням коштів: Європейський парламент ухвалив більш суворі закони щодо боротьби з відмиванням коштів і фінансуванням тероризму, які впливають на різні сектори, включно з футбольними клубами вищого рівня.

🌐 Оцінка метавсесвіту для дітей: EPRS оцінює переваги та ризики метавсесвіту для здоров'я та навчання дітей, наголошуючи на необхідності суворих правил.

🌿 Регулювання центрів обробки даних у Норвегії: Норвегія лідирує в Європі з комплексними правилами центрів обробки даних. Через екологічні проблеми операції з криптовалютою виключені.

https://bit.ly/4akJrpz

Пропозиції щодо нового НПА про криптоактиви у Туреччині

Документ представлений Blockchain Institute Ireland є пропозицією щодо внесення змін до Закону про ринки капіталу Туреччини з метою регулювання криптовалют та криптовалютних сервісів. Враховуючи швидкий розвиток технологій та зростання популярності криптовалют у Туреччині, де вже близько 10 мільйонів осіб залучені до торгівлі криптовалютами, законопроект передбачає

впровадження правових рамок для забезпечення прозорості, захисту споживачів та відповідності фінансовим регламентам.

Основні положення законопроекту включають:

- Визначення нових термінів: Введення таких термінів, як "криптоактив", "гаманець", "постачальник послуг криптоактивів" (CASP), "сервіс зберігання криптоактивів" та "платформа".
- Регулювання діяльності CASP: Встановлення вимог до отримання дозволів від Ради ринків капіталу (CMB) на діяльність CASP, включаючи правила для внутрішнього контролю та забезпечення безпеки систем.
- Захист прав споживачів: Забезпечення підписання чітких угод між клієнтами та CASP, створення механізмів вирішення спорів та захист клієнтів від недійсних умов договорів.
- Прозорість та звітність: Вимоги до реєстрації та прозорості транзакцій, відповідність міжнародним стандартам для переказу криптоактивів.
- Зберігання криптоактивів: Основні принципи зберігання криптоактивів клієнтів, включаючи їх розділення від активів CASP для забезпечення захисту від конфіскації.
- Інвестиційні консультації та управління портфелем: CMB встановлює процедури та принципи для надання інвестиційних консультацій та послуг з управління портфелем, пов'язаних з криптоактивами.
- Рекламна діяльність: Регулювання реклами та комерційної комунікації CASP.
- Відповідальність та санкції: Встановлення санкцій за порушення законодавства, включаючи діяльність без дозволу CMB та елементи кримінальної відповідальності за привласнення криптоактивів.

Документ також передбачає внесення змін до існуючих статей Закону, таких як визначення фінансових інструментів, відстеження грошових коштів клієнтів та заходи щодо запобігання несанкціонованій діяльності. Закон набуде чинності після його публікації та буде виконуватися під керівництвом Президента.

https://bit.ly/3WNuIjU

Впровадження міжнародних криптостандартів для банків буде відкладено до 2026 року

У понеділок Група керівників центральних банків і глав нагляду (GHOS) погодилася відкласти впровадження пруденційного стандарту Базельського комітету з банківського нагляду (BCBS) для криптоактивів на один рік до 1 січня 2026 року.

Стандарти, які вперше були прийняті GHOS у грудні 2022 року, використовують багаторівневий підхід до криптоактивів. Активам групи 1, таким як токенізовані традиційні активи та «криптоактиви з ефективним механізмом стабілізації», надається більш сприятливий режим, тоді як активам групи 2, таким як «незабезпечені криптоактиви та стейблкоїни з неефективними механізмами стабілізації», підлягатиме «консервативний пруденційний режим». Зокрема, вразливість банку до таких активів не повинна перевищувати 2% і, як правило, має бути нижчою за 1%.

У грудні 2023 року BCBS уточнив під час консультації, що всі криптоактиви, включно зі стейблкоїнами, які використовують загальнодоступні блокчейни, не будуть кваліфікуватися як активи групи 1 через «унікальні ризики», які становлять загальнодоступні блокчейни, і деякі з яких неможливо наразі достатньо пом'якшити.

Ця пропозиція отримала значну реакцію в галузі. У спільній відповіді п’яти галузевих органів стверджувалося, що «галузь має весь необхідний досвід і надійні рамки відповідності для повного виявлення, управління та пом’якшення цих ризиків», і було рекомендовано дозволити банкам використовувати Групу 1 для загальнодоступних блокчейнів.

Пояснюючи відстрочку, GHOS зазначила, що «переглянута дата впровадження допоможе гарантувати, що всі учасники зможуть запровадити стандарт у повному обсязі, своєчасно та послідовно».

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

2030 рік і далі. Нетрадиційний погляд на майбутнє фінансових технологій

Даний звіт представляє глибоке дослідження майбутнього фінансових технологій. Автори аналізують фінансовий ландшафт, намагаючись передбачити, які зміни очікують індустрію в найближчі роки, а також що залишиться незмінним.

У світі фінансових послуг, де зручність завжди виграє, важливо розуміти, що споживачі завжди обиратимуть найбільш зручні та прості рішення. Це підкреслює, наскільки важливо для стартапів і нових гравців на ринку створювати продукти, які полегшують життя користувачам. Регулювання завжди буде впливати на фінансові послуги, оскільки воно спрямоване на забезпечення довіри до системи. Макроекономічні цикли продовжуватимуть визначати ринок, а фінансові послуги залишаться локальними, враховуючи культурні та економічні відмінності між країнами. Великі фінансові установи, завдяки своїм масштабам та довірі споживачів, збережуть свої позиції, попри конкуренцію з боку нових гравців. Шахрайство буде постійною загрозою, що вимагає нових рішень для захисту.

Звіт також підкреслює тенденції, які ймовірно зміняться в найближчому майбутньому. Технологічні оновлення банків через партнерства з фінтехами, розширення вбудованих фінансових послуг у не фінансових додатках, ребандлінг та інтеграція різних фінансових продуктів стануть звичайним явищем. Потреба в глобальній фінансовій інфраструктурі зростатиме, відкриваючи нові можливості для швидких платежів та стейблкоїнів. Інновації з B2C фінтех поступово проникатимуть у B2B сектор, що сприятиме створенню нових рішень для бізнесу. Споживачі отримають більше влади завдяки відкритим фінансовим даним, що дозволить створювати нові продукти, орієнтовані на їх потреби. Великі технологічні компанії все більше впливатимуть на фінансовий ринок, а відповідність вимогам регуляторів стане конкурентною перевагою.

Зрештою, звіт висвітлює можливі кардинальні зміни, які можуть вплинути на фінансову індустрію. Питання зміни клімату може змінити стимули для бізнесу та фінансових провайдерів, а великі мовні моделі та інші ШІ технології здатні значно знизити витрати банків та страхових компаній. Фінансові послуги можуть стати інтерактивними завдяки віртуальній та доповненій реальності, а цифрові ідентифікаційні дані дозволить споживачам, бізнесам та урядам легше та безпечніше управляти своїми даними. Якщо споживачі оберуть самостійне зберігання своїх даних та грошей, це може значно змінити роль банків у фінансовій екосистемі.

Таким чином, попри зниження загальних інвестицій у фінтех, зараз є відмінний час для запуску нових фінтех-компаній. Технологічні, регуляторні та поведінкові зміни створюють численні можливості для інновацій, а компанії, які зрозуміють ці зміни, матимуть перевагу у майбутньому фінансових послуг.

https://team8.vc/rethink/fintech/2030-and-beyond/

Що таке Dubai Unlocked

Що таке «Dubai Unlocked»?

Dubai Unlocked — це міжнародне розслідування, яке виявляє прихованих власників нерухомості у Дубаї, включно з імовірними злочинцями, втікачами та підсанкційними особами. Цей новий проєкт,

у якому беруть участь понад 70 засобів масової інформації, показує, як м'які закони міста приваблюють світову еліту, яка прагне сховати незаконні кошти.

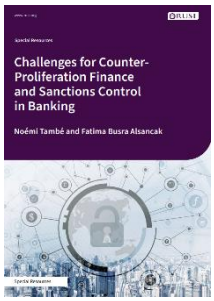
Розслідування є унікальним за своїм глобальним масштабом і спирається на витік даних про нерухомість за 2020 і 2022 роки, що дає безпрецедентний погляд на ринок нерухомості Дубаї. Журналісти ідентифікували численних власників майна, що становить суспільний інтерес, у тому числі обвинувачених у відмиванні коштів, наркобаронів та корумпованих політичних діячів.

Привабливість Дубаї як центру відмивання коштів пояснюється відсутністю договорів про екстрадицію, мінімальною перевіркою покупців майна та бурхливим ринком нерухомості. Дані, підтверджені широким дослідженням, висвітлюють право власності приблизно 200 осіб на понад 1000 об'єктів.

Незважаючи на зусилля щодо посилення правил і розширення співпраці з іноземними правоохоронними органами, заходи ОАЕ залишаються недостатніми, оскільки багато підозрілих операцій залишаються неповідомленими.

https://www.occrp.org/en/dubai-unlocked/

Проблеми протидії фінансуванню розповсюдження та контролю санкцій у банківській сфері

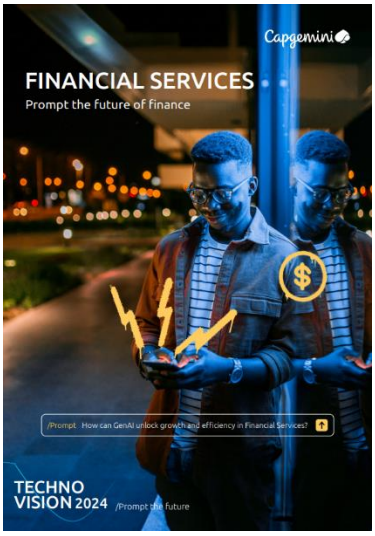


Даний звіт присвячений проблемам, з якими стикаються фінансові установи у сфері протидії фінансуванню розповсюдження (ФР) і контролю за санкціями. У ньому пропонуються тематичні дослідження, стратегії пом'якшення наслідків та рекомендації щодо мінімізації ризиків, пов'язаних із порушенням ФР та санкцій. Виявляючи вразливі місця та зміцнюючи рамки, фінансові установи можуть захистити не лише себе, але й національну економіку та суспільство в цілому. Зрештою, звіт є важливим інструментом для посилення протидії фінансування розповсюдження і систем запобігання санкціям у банківському секторі.

https://static.rusi.org/challenges-to-pr-sanctions-final.pdf

Погляд у майбутнє фінансових послуг

Документ "TechnoVision 2024: Financial Services" представляє собою звіт, підготовлений компанією Capgemini, який досліджує, як новітні технології можуть стимулювати зростання та підвищувати ефективність у фінансових послугах. Основна тема звіту — це вплив генеративного штучного інтелекту (генеративного ШІ) на різні аспекти бізнесу у фінансовому секторі.



Звіт поділений на кілька розділів, кожен з яких висвітлює різні технологічні тренди та їх застосування у фінансових послугах. Основні розділи включають:

1. You Experience: Розглядається інтеграція фінансових послуг у повсякденне життя клієнтів через цифровий досвід, персоналізацію та вбудовані фінансові рішення.
2. We Collaborate: Висвітлюється важливість співпраці між людьми та машинами, а також нові інструменти для ефективної спільної роботи.

3. Thriving on Data: Аналізується роль даних як стратегічного активу, що дозволяє розробляти розумні продукти та послуги, підвищувати задоволеність клієнтів та забезпечувати операційну ефективність.
4. Process on the Fly: Обговорюється оптимізація процесів у режимі реального часу, автоматизація та підвищення гнучкості фінансових інституцій.
5. Applications Unleashed: Вивчається впровадження нових додатків та інструментів для покращення фінансових операцій.
6. Invisible Infostructure: Описуються технологічні інфраструктури, що підтримують безперервність бізнесу та інновації.
7. Balance by Design: Представлені принципи дизайну для забезпечення збалансованого підходу до інновацій та стабільності.

Кожен розділ включає приклади використання новітніх технологій у провідних банках та страхових компаніях, таких як Mastercard, AXA, Visa, Allianz, Bank of America та інших. Звіт також включає аналіз екосистеми фінансових послуг та надає рекомендації щодо впровадження технологій для покращення бізнес-процесів і досягнення стратегічних цілей.

Загалом, "TechnoVision 2024: Financial Services" є цінним ресурсом для керівників і фахівців, які прагнуть зрозуміти, як новітні технології можуть сприяти зростанню та ефективності у фінансовому секторі, надаючи інсайти, рішення та стратегії для впровадження інновацій.

https://www.capgemini.com/insights/research-library/technovision-2024-prompt-the-future/

Що означають щорічні 9,4 трильйона доларів США в контексті можливостей токенізованої готівки?

Стаття на сайті Crypto Adoption Curve аналізує щорічний оборот у 9,4 трильйона доларів, пов'язаний із використанням токенізованої готівки, особливо стейблкоїнів. Вона підкреслює значний вплив стейблкоїнів на фінансові ринки, особливо в контексті спотової та деривативної торгівлі, а також у міжнародних платіжних переказах. Стейблкоїни, такі як USDT (Tether) і USDC (USD Coin), набули широкого використання через їхню стабільність та надійність, що робить їх привабливими для різних фінансових операцій. Токенізовані готівкові активи сприяють збільшенню ліквідності на ринках, покращують ефективність фінансових операцій і зменшують транзакційні витрати завдяки швидким та дешевим блокчейн-транзакціям. Блокчейни, такі як Solana та BSC (Binance Smart Chain), підтримують цей ріст завдяки своїй здатності обробляти велику кількість транзакцій швидко і з низькими витратами. Поточні досягнення у сфері токенізації відкривають нові можливості для розвитку платіжних сервісів, маркет-мейкінгу та інших фінансових послуг, адаптованих до потреб сучасного цифрового ринку.

https://bit.ly/44Oqpag

НАВЧАННЯ

Протидія фінансуванню тероризму

🕵♀ Курс ECOFEL «Протидія фінансуванню тероризму» надасть вам навички виявлення, переривання та запобігання потокам коштів на підтримку терористичної діяльності.

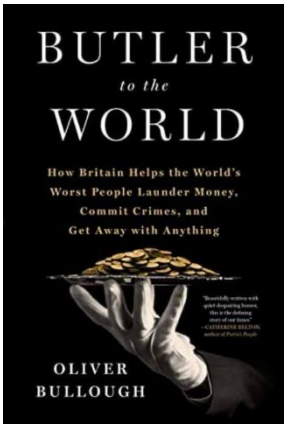
 Курс підкреслює важливість міжнародних стандартів, міжвідомчої координації та державно-приватного партнерства в ефективній боротьбі з фінансуванням тероризму.

➕ Для отримання додаткової інформації:

https://ecofel.org/countering-terrorist-financing/

РЕКОМЕНДОВАНІ КНИГИ

Butler to the World



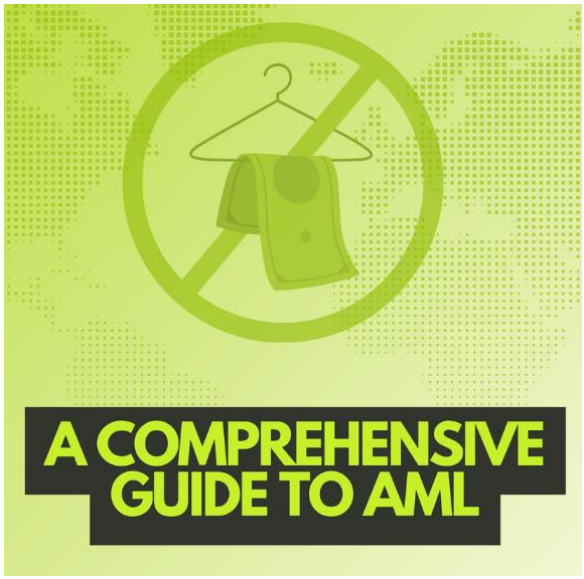
Книгу з рейтингу Forbes готують до друку українською мовою

Це «Butler to the World» Олівера Булло, яка розповідає про темний бік британської економіки – корупцію та олігархат із чітким російським слідом.

Це дослідження розкриває роль Великобританії у світовій фінансовій системі та її зв'язки з відмиванням грошей. Буллоу описує, як британські юристи, банкіри та інші професіонали допомагають заможним клієнтам з інших країн приховувати свої статки від податкових органів і уникати відповідальності за незаконні дії. Книга підкреслює, як Великобританія стала своєрідним «дворецьким» для багатих і впливових осіб з усього світу, надаючи їм фінансові послуги і зберігаючи їхні таємниці.

ІНШІ НОВИНИ

Гайд до розуміння ПВК



Інтерпол, FATF та UNODC спільно закликали країни посилити заходи протидії відмиванню коштів для ефективної боротьби з транснаціональною злочинністю.

🌐 Заклик пролунав на 33-му заході Комісії ООН із запобігання злочинності та кримінального правосуддя у Відні.

💰 Вони наголосили на необхідності боротися з великими незаконними прибутками, які фінансують конфлікти та тероризм.

✅ Пропозиції включали жорсткіші заходи ПВК, зміни до міжнародних стандартів FATF та прискорення прогресу в реформах політики.

🔑 Враховуючи цей заклик до дії, організаціям вкрай важливо зрозуміти основи принципи і практики боротьби з відмиванням коштів.

▨ Гайд з протидії відмиванню коштів охоплює етапи процедур з ПВК, загальні проблеми, останні тенденції та багато іншого.

Європейські країни прагнуть запровадити санкції проти банків, які допомагають Росії

Європейські країни планують посилити санкції проти банків, які допомагають Росії обходити міжнародні обмеження, накладені через її агресію проти України. Згідно з новим пакетом санкцій, до списку потраплять нові компанії та особи, залучені до військових зусиль Росії, включаючи постачальників технологій для виробництва дронів та інших військових систем. Ці заходи спрямовані на обмеження доступу Росії до критичних технологій та ресурсів, необхідних для продовження війни. Також буде запроваджено додаткові торговельні обмеження щодо компаній, які сприяють розвитку російського військово-промислового комплексу, зокрема в Китаї та інших країнах

https://bit.ly/3yr4f1x

Як Мексика втрачає слід хімічних грошей-прекурсорів

Стаття на Insight Crime досліджує слід грошей, пов'язаних з прекурсорами для синтетичних наркотиків. У матеріалі йдеться про використання мексиканськими картелями складних фінансових схем для приховування незаконних прибутків від виробництва метамфетаміну та фентанілу. Розслідування виявляє, що попри великі зусилля з боку американських та мексиканських правоохоронних органів, дуже мало справ про відмивання грошей пов'язаних із синтетичними наркотиками було

розслідувано чи завершено. Ці прогалини у боротьбі з фінансовими злочинами викликають серйозне занепокоєння.

https://insightcrime.org/investigations/mexico-loses-precursor-chemical-money-trade/

Все, що вам потрібно знати про цифровий арешт: нова тенденція кіберзлочинності

Стаття описує нову методику кіберзлочинності під назвою "цифровий арешт", де шахраї видають себе за правоохоронців, щоб вимагати гроші. Злочинці використовують психологічні маніпуляції, створюють фальшиві поліцейські станції та проводять "віртуальні допити", щоб залякати жертв та змусити їх переводити значні суми грошей. Жертвам радять перевіряти особи тих хто телефонує і ніколи не переказувати гроші без підтвердження. Стаття підкреслює важливість інформованості та пильності для запобігання таким шахрайствам.

https://www.the420.in/all-you-need-to-know-about-digital-arrest-a-novel-cybercrime-trend/

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Як навіть звичайне морозиво може бути використано для відмивання коштів

У Німеччині судові органи висвітлили тривожний випадок того, як організована злочинність, зокрема калабрійська "Ndrangheta", використовує комерційну діяльність для відмивання брудних коштів. Розслідувалась діяльність трьох осіб калабрійського походження через використання кафе-морозива, відомого як «Eiscafe Al Teatro» в Зігені, для незаконної діяльності, яка заходила далеко за межі продажу морозива.

Це кафе-морозиво було не лише популярним місцем для любителів морозива, а й критичним центром для відмивання коштів, отриманих від продажу наркотиків. Крім того, воно слугувало оперативною базою для молодих членів Ндрангети, які переїхали до Німеччини, щоб вивчити мову та інтегруватися в місцеві злочинні мережі.

Операція була складною: понад 400 000 євро було інвестовано в кафе-морозиво видатним членом «Ндрангети» з Сан-Луки, перетворивши заклад на інструмент для отримання користі для клану через відмивання коштів. Цей випадок підкреслює необхідність постійної пильності та ефективної міжнародної співпраці для боротьби з цими незаконними практиками, які можуть проникнути в законну економіку та корумпувати соціальну структуру громад.

Для підприємств і фінансових установ важливо посилити внутрішній контроль і суворо дотримуватися правил з ПВК, щоб запобігти зловживанню комерційними структурами в злочинних цілях. Лише спільними зусиллями та ретельним наглядом ми можемо ефективно протистояти цим явищам і захистити цілісність нашої економічної системи.

Що таке джанкет оператори?

Джанкет оператор – це особа чи організація, яка працює з казино, щоб залучити заможних людей до азартних ігор у казино. ♠

Ці посередники організовують спеціальні тури для VIP-гравців і надають їм бонуси та стимули для азартних ігор.

💰 Як джанкет оператори сприяють відмиванню коштів 💰

Альвін Чау з **Suncity** та Лево Чан з **Tak Tak**, двох найбільших світових джанкет операторів, були засуджені до 18 років та 14 років ув'язнення за сотнями звинувачень, що стосуються організованої злочинності, незаконних ставок та відмивання коштів.

Згідно з розслідуваннями, Suncity і Tak Chun не обмежували свої послуги лише джанкет операціями.

Вони були частиною більшої мережі, яка надавала підпільні банківські послуги різним злочинним компаніям, які потребували послуг відмивання коштів або переказу грошей.

Прибутки, отримані від цієї діяльності, використовувалися для фінансування злочинних підприємств і, здавалося б, законних інвестицій.

Як?

Зловживаючи діяльністю джанкет оператора через:

☞ VIP програми та тури

☞ Підпільні банківські послуги

☞ Внесення чи виведення готівки

☞ Сприяючи змові між гравцями в казино

☞ Офсетні операції

☞ Використання ігрових рахунків для незаконних транзакцій

Чому це варто уваги:

Розуміючи тактику відмивання коштів через джанкет операторів, працівники сфери ПВК можуть створити сильніший захист від цієї загрози.

Ці знання дозволяють їм визначати «червоні прапорці» в поведінці клієнтів, транзакціях і відносинах з джанкет операторами.

Тому що боротися з відмивачами коштів можна тільки якщо знати їхню тактику!

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

Тайвань пропонує більш жорсткі заходи протидії відмиванню коштів для постачальників крипто-послуг

Міністерство юстиції Тайваню пропонує жорсткі поправки до правил боротьби з відмиванням коштів, спрямованих на криптокомпанії, з метою боротьби з шахрайством і відмиванням коштів у просторі віртуальних активів. Покарання можуть включати до двох років тюремного ув'язнення та штраф у розмірі 1,5 мільйона доларів за недотримання. Поправки, які отримали назву «Чотири нові закони про боротьбу з шахрайством», спрямовані на запобігання шахрайству, відмиванню коштів, технологічну безпеку та нагляд за комунікаціями. Помітні зміни включають суворіші покарання для VASP і суворіші вимоги до реєстрації. Заступник міністра юстиції Хуань Моушінь наголошує на переході до криміналізації невідповідної поведінки. Іноземні криптоплатформи можуть зіткнутися з покараннями, якщо вони не створять місцеві організації та не будуть дотримуватися правил з ПВК.

https://cointelegraph.com/news/taiwan-aml-regulations-crypto-fraud?es_id=31ac8093e4

Піраміда Понці

Схема Понці — це шахрайська інвестиційна схема, що обіцяє високі прибутки інвесторам, але фактично виплачує їх за рахунок внесків нових інвесторів, а не за рахунок реальної прибуткової діяльності.

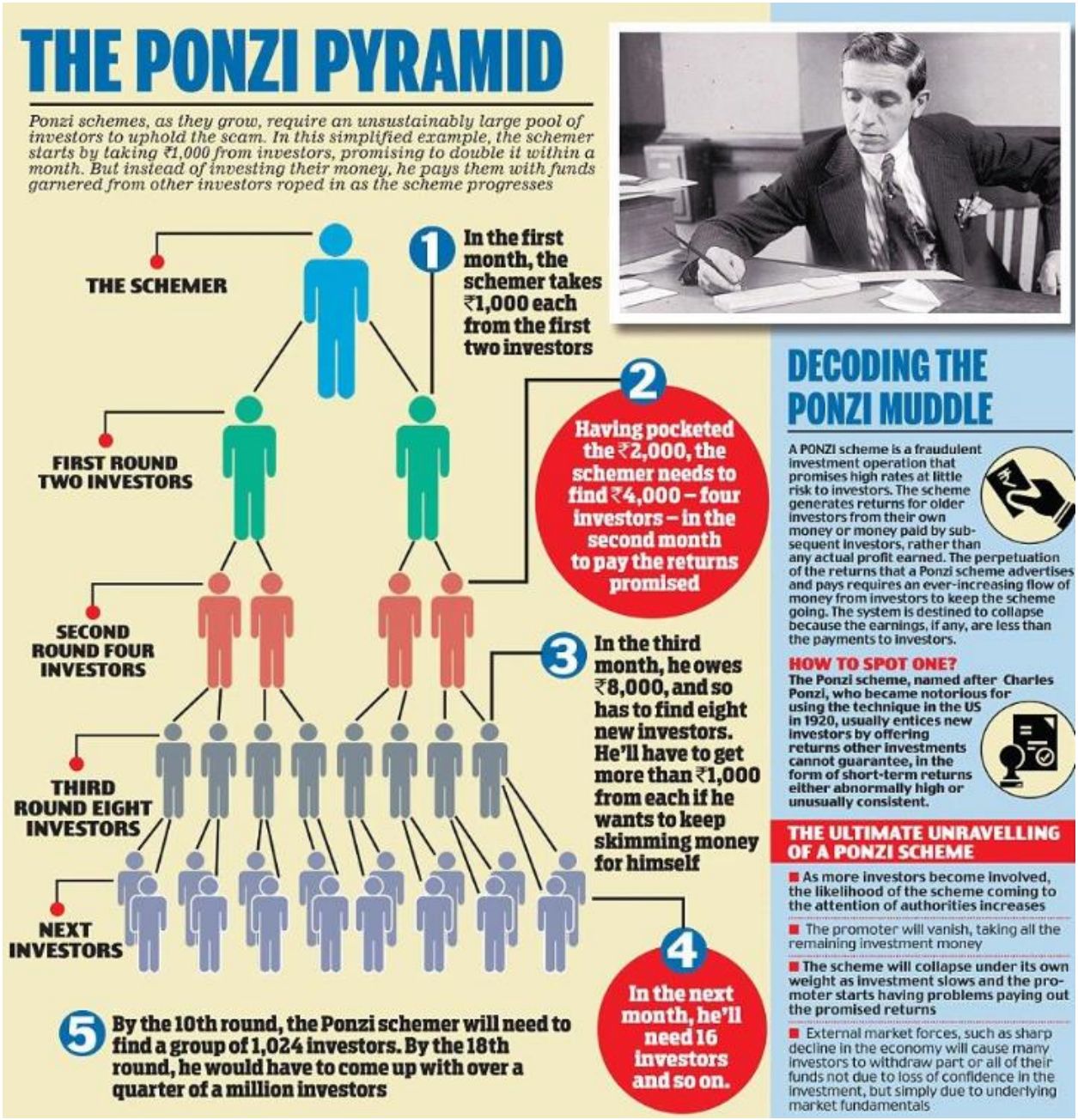
На малюнку зображено, як працює схема Понці:

1. На першому етапі шахрай (організатор схеми) бере по 1,000 від перших двох інвесторів.
2. У другому місяці, щоб виплатити обіцяні прибутки (подвоїти вкладені кошти), йому потрібно залучити нових чотирьох інвесторів, з кожного з яких він також бере по 1,000.
3. На третьому етапі він повинен знайти вже вісім нових інвесторів, щоб виконати свої зобов'язання перед попередніми інвесторами.
4. З кожним наступним місяцем кількість нових інвесторів зростає в геометричній прогресії, щоб схема могла продовжувати функціонувати.
5. До десятого місяця йому потрібно залучити понад тисячу нових інвесторів, а до вісімнадцятого — понад чверть мільйона.

З часом схема Понці неминуче руйнується, оскільки знайти таку велику кількість нових інвесторів стає неможливо. Це призводить до втрат для більшості учасників, крім організатора, який зазвичай встигає забрати значну частину грошей.

Важливо знати про схему Понці та її механізм, щоб розпізнавати подібні шахрайські інвестиційні пропозиції та уникати їх. Основні ознаки таких схем включають обіцянки надзвичайно високих і швидких прибутків з невеликим ризиком, залежність виплат від залучення нових інвесторів і відсутність реальних прибуткових інвестицій чи бізнес-діяльності.

Обізнаність щодо таких схем допомагає уникати фінансових втрат і сприяє поширенню інформації про відповідальні та законні способи інвестування.



Різниця між KYC та KYB

Розуміння відмінностей між KYC (Знай свого клієнта) і KYB (Знай свій бізнес) має вирішальне значення для регульованих організацій, які знаходяться в системі комплаєнсу.

Розуміння відмінностей має вирішальне значення для впровадження ефективних механізмів комплаєнсу, адаптованих до різноманітних клієнтських баз, захисту від фінансових ризиків і зміцнення довіри в нормативному середовищі. ⛵

https://bit.ly/3WLLGix

Що таке оцінка ризику клієнта в контексті ПВК

У цьому відео розглянуто основні визначення оцінки ризику клієнта в контексті ПВК, різні рівні ризику клієнта та те, як визначається ризик клієнта на основі різних атрибутів ризику.

Оцінка ризику клієнта є одним із найважливіших кроків у створенні якісної програми з комплаєнсу для протидії відмиванню коштів. Оскільки ризики відмивання коштів зростають, необхідний посилений контроль. Однак усі категорії ризику — низького, середнього чи високого — мають бути виявлені та пом'якшені за допомогою засобів контролю, таких як перевірка ідентифікаційних даних клієнта, політика CDD, моніторинг підозрілої діяльності та скринінг клієнтів на приналежність до PEP, санкційних списків, наявності негативних згадок у ЗМІ, тощо.

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

Різниця між ФінТех та цифровим банкінгом

Fintech	Digital Banking
Fintech — це економічна індустрія, яка включає компанії, що надають фінансові послуги за допомогою новітніх технологій.	Цифровий банкінг є однією з ключових функціональних сфер Fintech і визначає майбутнє банківської сфери.
Використовуються різні технології, продукти та бізнес-моделі для конкуренції з традиційними фінансовими методами.	Це цифровізація банківських продуктів і послуг через веб-інтерфейс або мобільні додатки.
Мета Fintech — запропонувати довіру, прозорість та технології через покращені та ефективні бізнес-моделі.	Мета цифрового банкінгу — прискорити і покращити процес взаємодії клієнтів з банками через цифрові канали.
Продукти та послуги Fintech включають платіжні системи, грошові перекази, особисті фінанси, страхування, управління капіталом, блокчейн, краудфандинг тощо.	Продукти цифрового банкінгу включають онлайн-банкінг, особисте фінансове планування, цифрові гаманці, цифрові купони, оплату рахунків, мобільні перекази тощо.

Що таке рівень клієнтського ризику

Рівень ризику клієнта – це систематичний процес, який використовується в практиках комплаєнсу та боротьби з відмиванням коштів для оцінки рівня ризику, пов'язаного з окремими клієнтами або організаціями. Він надає фінансовим установам структуровану основу для виявлення та управління потенційним відмиванням коштів та іншою незаконною фінансовою діяльністю. Організації можуть ефективно розподіляти ресурси, призначаючи клієнтам рівні ризику, пріоритезуючи підприємства

із вищим ризиком для посиленої належної перевірки та забезпечуючи дотримання нормативних зобов'язань.

Неможливо переоцінити важливість рівнів ризику клієнтів. Фінансові установи стикаються зі значними ризиками щодо відмивання коштів, оскільки злочинці постійно шукають інноваційні способи використання вразливостей у системі. Рівень ризику клієнта дозволяє організаціям визначати та усувати ці ризики, захищаючи свою репутацію, захищаючись від фінансових втрат і виконуючи нормативні зобов'язання.

Під час визначення рівня ризику клієнта враховується кілька факторів. Ось кілька ключових міркувань:

1: Паттерни транзакцій

Моніторинг паттернів транзакцій клієнтів і аномалій має вирішальне значення для виявлення підозрілої діяльності. Незвичайні обсяги транзакцій, часті великі депозити або зняття готівки, складні структури транзакцій або раптові зміни поведінки транзакцій можуть свідчити про потенційне відмивання коштів або незаконну діяльність.

2: Географічні фактори

Розуміння географічних ризиків, пов'язаних з певними юрисдикціями, має вирішальне значення. Деякі регіони відомі своїм вищим ризиком відмивання коштів і фінансових злочинів через слабкий регуляторний нагляд, політичну нестабільність або історію незаконної фінансової діяльності. Рівень ризику клієнта враховує географічні фактори, пов'язані з операціями чи транзакціями клієнта.

3: Тип бізнесу

Різні галузі та сектори представляють різний рівень ризику через їх сприйнятливість до діяльності з відмивання коштів. Такі галузі, як казино, грошові послуги та некомерційні організації, вважаються більш ризикованими через можливість анонімності, великі грошові потоки або використання благодійних фондів.

4: Джерело багатства

Перевірка легітимності багатства клієнта та його походження має вирішальне значення для зменшення ризиків відмивання коштів. Розуміння джерела коштів і впевненість у тому, що вони отримані в результаті законної діяльності допомагає виявити потенційні червоні прапорці та зменшити ризик сприяння незаконним фінансовим потокам.

5: Політично значущі особи (PEP)

PEP – це особи, які займають визначні державні посади або ті, хто тісно пов'язані з такими особами. Їхній підвищений ризик пов'язаний з можливим зловживанням своїм становищем для отримання особистої вигоди або з метою відмивання коштів. Рівень ризику клієнта враховує залученість політично значущих осіб та їх оточення.