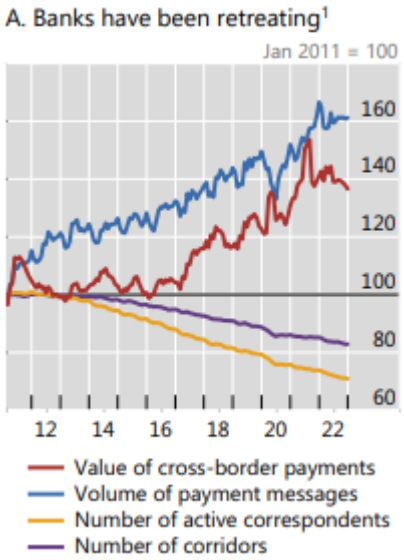
Серійний номер: ДСФМУ-ДК-2024-011
Липень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Кореспондентський банкінг наступного покоління



Бюлетень Банку міжнародних розрахунків №87 під назвою "Наступне покоління кореспондентських банків" досліджує еволюцію та перспективи кореспондентських банківських послуг, акцентуючи увагу на можливостях токенізації для модернізації системи відповідно до сучасних регуляторних і користувацьких вимог.

Документ розглядає зниження кількості активних кореспондентських банків та коридорів як виклик, що вимагає технологічних інновацій. Пропонується використовувати концепцію об'єднаного реєстру BIS для підвищення ефективності та прозорості операцій. Ініціатива Project Agorá, спрямована на дослідження токенізації міжнародних платежів, має на меті спростити процеси і покращити відповідність нормам KYC/AML.

Токенізація дозволяє здійснювати миттєві та синхронізовані оновлення у всіх залучених реєстрах, що знижує ризики помилок і затримок. Вона також інтегрує попередній скринінг і перевірки на відповідність вимогам AML, зменшуючи дублювання зусиль і підвищуючи точність.

Проект Agorá є перспективним кроком до модернізації кореспондентських банківських послуг, що має потенціал відкрити нові економічні можливості, особливо для країн з низьким рівнем доходу.

https://www.bis.org/publ/bisbull87.pdf

Вепонізація стандартів FATF: посібник для глобального громадянського суспільства

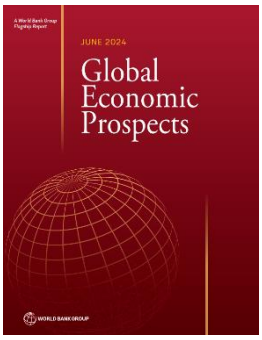
Стандарти Групи розробки фінансових заходів боротьби з відмиванням коштів (FATF) забезпечують скоординовану глобальну відповідь на організовану злочинність, корупцію та загрози тероризму та розповсюдження зброї масового знищення. Тим не менш, нова доповідь асоційованого наукового співробітника CFS Стівена Реймера показує, що уряди в усьому світі систематично зловживають повноваженнями, які випливають із стандартів FATF, щоб заморожувати банківські рахунки опонентів, збирати конфіденційну банківську інформацію про некомерційні організації та тримати активістів у тривалих досудових ув'язненнях через сфабриковані дії та висунуті звинувачення у відмиванні коштів або фінансуванні тероризму.

У новому звіті окреслено атрибути заходів з ПВК/ФТ, які піддають стандарти FATF зловживанню, і він є цінним інструментом для учасників громадянського суспільства, оскільки:

- Висвітлює суб'єктів та організації, які найбільш вразливі до нападів, і вказує на те, де найімовірніше станеться зловживання.
- Підкреслює наслідки такого зловживання для організацій громадянського суспільства, наглядових організацій, журналістів, опозиційних активістів тощо.
- Пропонує стратегії для громадянського суспільства з метою підвищення стійкості та ефективного реагування.

https://static.rusi.org/weaponisation-of-fatf-standards-a-guide.pdf

Глобальні економічні перспективи



Незважаючи на поліпшення найближчих перспектив, глобальні перспективи залишаються підкореними історичним стандартам. У 2024-2025 роках темпи зростання будуть нижчими за середні показники 2010-х років майже в 60 відсотках економік, що становлять понад 80 відсотків населення світу. Переважають ризики зниження, включаючи геополітичну напруженість, фрагментацію торгівлі, вищі відсоткові ставки та катаклізми, пов'язані з кліматом. Глобальна співпраця необхідна для захисту торгівлі, підтримки екологічного та цифрового переходу, полегшення боргів і покращення продовольчої безпеки. У EMDE державні інвестиції можуть підвищити продуктивність і каталізувати приватні інвестиції, сприяючи довгостроковому зростанню. Комплексні фіскальні реформи мають важливе значення для вирішення поточних фіскальних проблем у малих державах, у тому числі викликаних підвищеною вразливістю зовнішніх шоків.

https://bit.ly/3Vkyjnh

Огляд обов'язку моніторингу транзакцій

Документ "A Look Through the Obligation of Transaction Monitoring" виданий Мальтійським управлінням фінансової розвідки (FIAU) і містить керівництво щодо обов'язків з моніторингу транзакцій для запобігання відмиванню коштів і фінансуванню тероризму. Він наголошує на важливості систематичного та безперервного перегляду транзакцій клієнтів для виявлення незвичних, аномальних та підозрілих операцій.

Документ детально описує, що фінансові установи, такі як банки, емітенти електронних грошей, платіжні провайдери та компанії, що займаються обробкою

платежів, повинні впроваджувати ефективні програми моніторингу транзакцій. Ці програми мають включати детальні правила для виявлення ризиків, регулярне тестування та налаштування порогових значень для мінімізації хибно позитивних результатів.

У документі також наведено приклади типових порушень, коли фінансові установи не змогли належним чином перевірити транзакції, що призвело до ризику фінансових злочинів. Розглядаються методи вдосконалення систем моніторингу, включаючи використання автоматизованих систем і впровадження підходів на основі ризиків.

Особливу увагу приділено важливості ресурсів та навчання персоналу, а також необхідності забезпечення належної документації та управління сигналами про підозрілі транзакції. Описуються як попередні (pre-transaction), так і постфактум (post-transaction) методи моніторингу, що дозволяють своєчасно виявляти та запобігати підозрілим транзакціям до або після їх здійснення.

Документ підкреслює, що успішна програма моніторингу транзакцій має бути підтримана належними технологічними рішеннями, такими як машинне навчання та штучний інтелект, які можуть допомогти виявляти складні патерни транзакцій, що важко виявити іншими методами.

Загалом, документ є важливим посібником для фінансових установ щодо впровадження і підтримки ефективних систем моніторингу транзакцій з метою забезпечення відповідності законодавчим вимогам і зниження ризиків фінансових злочинів.

https://bit.ly/3VoU3OH

Річний звіт ПФР ОАЕ

Виконавчий офіс з протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ) опублікував свій перший Річний звіт, що пропонує всебічний огляд потужних ініціатив Об'єднаних Арабських Еміратів у боротьбі з фінансовими злочинами та забезпеченні цілісності і стійкості фінансової системи.

У звіті висвітлено значний прогрес ОАЕ у боротьбі з відмиванням коштів та фінансуванням тероризму, детально описано роль національних органів, зокрема Вищого комітету з нагляду за національною стратегією у сфері ПВК/ФТ та Виконавчого директорату з питань ПВК/ФТ, який є національним координатором. У звіті висвітлено внесок наглядових та правоохоронних органів у підвищення ефективності національної системи ПВК/ФТ.

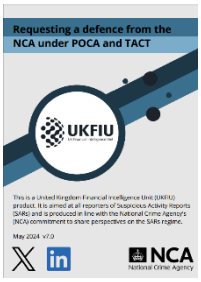
Хамід Альзаабі, Генеральний директор виконавчого офісу у сфері ПВК/ФТ ОАЕ, підкреслив відданість ОАЕ прозорості, міжнародному співробітництву та постійному вдосконаленню боротьби з фінансовими злочинами. Він зазначив, що детальна інформація у звіті демонструє відданість ОАЕ фінансовій доброчесності та глобальній безпеці.

Серед ключових досягнень, описаних у звіті, - цілісна стратегія боротьби з відмиванням коштів та фінансуванням тероризму, співпраця з міжнародними організаціями та активна участь у глобальних форумах. У звіті також висвітлюється прогрес у дотриманні міжнародних стандартів у сфері ПВК/ФТ, успішне виконання Плану дій FATF, а також посилення правових та інституційних заходів.

Крім того, у звіті підкреслюється інтеграція інновацій та технологій у національну стратегію, що покращує спроможність ПВК/ФТ у передбаченні та реагуванні на фінансові злочини. У звіті також підкреслюється гендерна рівність при прийомі на роботу: серед нових співробітників 55% жінок і 45% чоловіків.

https://isuport.org/flipbook/annual-report/mobile/index.html

Запит на захист від NCA відповідно до POCA та TACT



NCA випустило Посібник, у якому пояснюється, як подати звіт про підозрілу діяльність (SAR) і отримати захист (або «згоду») від NCA.

1) Яку інформацію потребує ПФР через новий безпечний портал подання SAR

- Опис підозрюваного злочинного чи терористичного майна, напр. про яку суму грошей чи майна йдеться?
- Як відбуватиметься транзакція, напр. особисто чи онлайн?
- Яка (є) причина (причини) або контекст транзакції?
- Деталі залучених (або ймовірно залучених) організацій
- Коли, ймовірно, відбудеться транзакція або буде укладено угоду?
- Чи була заява про згоду на запити правоохоронних органів? Якщо так, то яке агентство зробило ці запити?
- Якщо про суб'єкта повідомляли раніше, які відповідні значення SAR та результати?
- Чи є діяльність, щодо якої подається звіт, наприклад, гуманітарною допомогою?
- Деталі будь-якої проведеної належної перевірки
- Будь-які інші зобов'язання щодо відповідності та те, як вони були вирішені, наприклад зобов'язання щодо фінансових санкцій

2) Деталі щодо залучених установ

- У відповідних полях вкажіть якомога більше деталей щодо залучених установ (осіб, адрес, компаній, рахунків):
- Повне ім'я суб'єкта, дата народження та адреси (включаючи поштовий індекс).
- Більш детальні дані суб'єкта (наприклад, номери національного страхування, реєстрація транспортного засобу, водійські права, номер паспорта, номери телефонів, адреси електронної пошти тощо).
- Професія суб'єкта.
- Інформація про будь-яких пов'язаних суб'єктів (включаючи, у відповідних випадках, повну інформацію про фахівців, залучених до діяльності).
- Відомості про компанію, включаючи повну юридичну назву, правовий статус (Ltd, LLP, GmbH, SARL), реєстраційний номер і номер платника податків/ПДВ, країну реєстрації та відомості про бенефіціарну власність, де вона є).
- Якщо це стосується вашого бізнесу, фінансові дані суб'єкта (номери рахунків) і відомості про партнерів.
- Чи залучає транзакція/угода визнану – у тому числі заборонену – терористичну організацію чи іншу особу чи організацію, щодо яких поширюються санкції.

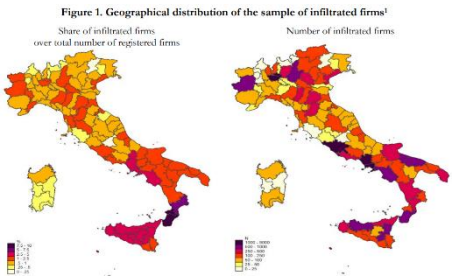
https://bit.ly/4chbIPl

Часті питання щодо інформації про бенефіціарну власність

Мережа боротьби з фінансовими злочинами Міністерства фінансів США (FinCEN) опублікувала оновлений документ щодо поширених запитань (FAQ) про бенефіціарну власність. В оновленому документі містяться роз'яснення щодо підзвітних компаній і винятків, бенефіціарних власників, вимог до звітності та загальні запитання. Він також містить інформацію про те, як Закон про корпоративну прозорість застосовується до індіанських племен.

https://www.fincen.gov/boi-faqs

Підхід машинного навчання для виявлення компаній, пов’язаних з організованою злочинністю в Італії, на основі балансових даних



Інноваційне дослідження Паскуале Каріелло, Марко Де Сімоні та Стефано Ієцці (Banca d'Italia) розробило алгоритм машинного навчання для ідентифікації компаній, потенційно пов’язаних із організованою злочинністю (ОЗ) в Італії. Використовуючи повний набір даних італійських компаній та інтегруючи хфінансову інформацію з різних джерел, насамперед із фінансових звітів, модель була навчена та випробувана на більш ніж 28 000 компаніях.

Результати показують, що алгоритм успішно ідентифікує близько 76% компаній, пов'язаних із ОЗ, і 74% імовірно «чистих» компаній. Основним результатом алгоритму є оцінка ризику, яка може використовуватися антилегалізаційними органами влади і правоохоронними органами як попередній інструмент скринінгу.

Це дослідження є значним прогресом у боротьбі з організованою злочинністю, пропонуючи новий технологічний інструмент для підтримки виявлення та боротьби з незаконною діяльністю в італійській економічній структурі.

https://bit.ly/4cjVmWd

Оцінка загроз серйозної та/або організованої злочинності за 2019-2022 роки

Звіт SOCTA 2019-2022 оцінює загрози серйозної та організованої злочинності в Україні, використовуючи методологію Європолу. Документ висвітлює правові засади та методологію оцінювання загроз, а також спроможності держави в протидії цим загрозам. Основна увага приділена характеристиці загроз у різних сферах злочинної діяльності, таких як корупція, кіберзлочинність, наркоторгівля, нелегальна міграція, торгівля людьми та інші. Звіт підкреслює вплив російського вторгнення на зростання злочинної активності, зокрема щодо державної безпеки та колабораційної діяльності, і надає рекомендації для ефективної протидії.

https://mvs.gov.ua/upload/1/8/5/3/8/2/socta.pdf

РЕГУЛЮВАННЯ

ЕВА проводить консультації щодо нової системи втрат від операційного ризику в рамках впровадження Банківського пакету ЄС

ЕВА запустив консультації щодо трьох наборів проектів регуляторних технічних стандартів (RTS) щодо нового системи для втрат від операційного ризику.

Вони мають на меті зробити наступне:

🎯 Проект RTS щодо створення таксономії операційного ризику:

- надати перелік типів подій операційного ризику, категорій та атрибутів, які установи повинні використовувати під час фіксування подій збитків від операційного ризику.

🎯 Проект RTS щодо умов, за яких для установи було б надмірно обтяжливим розрахувати річний збиток від операційного ризику:

- розпізнає випадки, коли для установи було б непропорційно розраховувати щорічні втрати від операційного ризику.

🎯 Проект RTS щодо коригування набору даних про збитки установи:

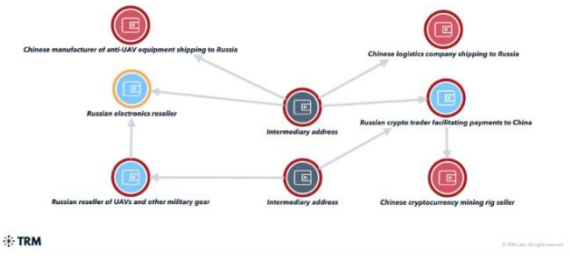
- надати вказівки щодо валюти та таксономії ризику, які будуть використовуватися під час включення набору даних про збитки об'єднаних суб'єктів господарювання чи діяльності.

📨 Надсилайте свої коментарі до 6 вересня 2024 року за цим посиланням 👇

https://bit.ly/3yWEmHc

OFAC запровадило санкції проти 300 осіб та організацій, залучених до війни Росії, включаючи мережі ухилення від санкцій

Дії були спрямовані, серед інших сфер, на мережі, які використовує Росія, щоб «годувати свою військову машину та забезпечити виробничі матеріали для підтримки її військових зусиль». Ці мережі використовуються для спроб уникнути санкцій за допомогою схем переміщення грошей та інших цінних товарів і активів.



До однієї з таких мереж був залучений росіянин Андрій Дмитрович Судаков, співробітник російського державного золотовиробника Публічного акціонерного товариства «Полюс» («Полюс»). За даними Міністерства фінансів США, Судаков брав участь у складній багаторівневій схемі відмивання, за допомогою якої платежі від продажу золота російського походження конвертувалися у фіатну валюту та криптовалюти через численні підставні компанії в ОАЕ та Гонконгу.

Схеми відмивання узгоджуються з тим, що TRM Labs спостерігає протягом деякого часу – тобто китайські виробники електроніки використовуються для військових зусиль Росії, включаючи китайські компанії, що постачають запчастини до Росії, залучення китайських посередників, координацію між російськими та китайськими логістичними компаніями, а також російські трейдери криптовалют, що полегшують платежі компаніям у Китаї. Криптовалюти використовувалися для оплати товарів і послуг, а також для оплати транспортування товарів.

https://bit.ly/3VENWr6

Режим з ПВК/ФТ для криптоактивів: відгуки про хороші та погані заявки

Управління з питань фінансової поведінки (FCA) Великобританії опублікувало відгуки про хороші та неякісні заявки щодо існуючого режиму з ПВК/ФТ для криптоактивів. Ключові моменти:

- Ключові кроки, рекомендовані FCA:

1. переглянути Положення про боротьбу з відмиванням коштів, фінансуванням тероризму та переказом коштів (інформація про платника) 2017 року (MLRs);
2. встановити, чи буде заявник здійснювати діяльність із криптовалютними активами;
3. розглянути можливість отримати незалежну юридичну консультацію/консультацію з питань відповідності;
4. переглянути інформацію на веб-сторінках FCA та реєстраційну форму; і
5. призначити відповідального працівника (положення MLRs, 21(3)).

ПРИ ПІДГОТОВЦІ ЗАЯВКИ

- Під час підготовки заявки сфери, які мають бути описані максимально деталізовано, включають:

1. бізнес-план;
2. вичерпний опис товарів та послуг;
3. оцінка та управління ризиками;
4. політики, системи та засоби контролю (PSC);
5. моніторинг транзакцій та аналіз блокчейнів;
6. структура групи та покладання на групову політику та процедури;
7. аутсорсинг;
8. навчання; і
9. повідомлення про підозрілу діяльність (SAR).

- Інші сфери, які мають бути охоплені, включають правильне розкриття інформації клієнтам, запровадження відповідних заходів контролю, пов'язаних із санкціями, і забезпечення того, щоб веб-сайти та маркетингові матеріали містили точні та чесні представлення продуктів і послуг.

- Йдеться не лише про складність і обсяг сфер, які необхідно охопити, але й про витрати, пов'язані з отриманням спеціалізованого експертного персоналу та запровадження розгалужених систем внутрішнього управління, управління ризиками та PSC.

- Наприклад, бізнес-плани мають охоплювати бізнес-моделі, детальні діаграми (шлях клієнта, потік коштів), джерела ліквідності, а також ролі й обов'язки всіх бізнес-партнерів (наприклад, брокерів, аутсорсингових фірм, суб-кастодіанів).

- Оцінка та управління ризиками повинні охоплювати криптоактиви та проблеми з санкціями, ризики фінансування розповсюдження і фінансування тероризму, а також методології оцінки ризиків (тобто висновок про залишковий ризик, оцінка застосованих засобів контролю, визначення внутрішніх ризиків, зважения ризиків).

- FCA виявило, що багато криптокомпаній не можуть ефективно ідентифікувати й оцінювати притаманні ризики ВК/ФТ/ФР. Вони також робили дуже елементарні помилки, такі як визначення провалів заходів контролю у фірми в якості «ризиків» (наприклад, неадекватна належна перевірка клієнта, помилково визначена як ризик, а не провал).

https://www.fca.org.uk/firms/cryptoassets-aml-ctf-regime/feedback-good-poor-applications

Політично значущі особи. Де ми пів року по тому?

Центр фінансів та безпеки (CFS) при Королівському Об'єднаному інституті оборонних досліджень (RUSI https://www.rusi.org/) та Офіс ефективного регулювання BRDO проводять дискусії у форматі круглого столу «Політично значущі особи. Де ми пів року по тому?».

Пів року тому – жовтні 2023 року – був ухвалений новий закон про політично значущих осіб (PEPs), що викликав активні дискусії у суспільстві щодо можливості довічного моніторингу PEPs. У лютому 2024 року, Національний банк України видав роз'яснення щодо процедури моніторингу та застосування ризик-орієнтованого підходу щодо PEPs. Незважаючи на ці зусилля, на практиці PEPs і далі зіштовхуються з дерискінгом та необґрунтованими відмовами. Це стосується також членів родини та пов'язаних із PEPs осіб.

Круглий стіл збере представників громадянського суспільства, приватного сектору, банки, PEPs та інших.

До обговорення запрошені:

- Ольга Василевська-Смаглюк, заступниця Голови Комітету Верховної Ради України з питань фінансів, податкової та митної політики
- Михайло Кольцов, експерт із комплаєнсу YouControl, зовнішній консультант World Bank Group з аналізу даних та кібербезпеки
- Олена Коробкова, Голова Ради Незалежної асоціації банків України

https://www.facebook.com/brdo.ukraine/videos/318961021256505/

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Використання великих мовних моделей для збагачення даних в контексті фінансових злочинів і комплаєнсу

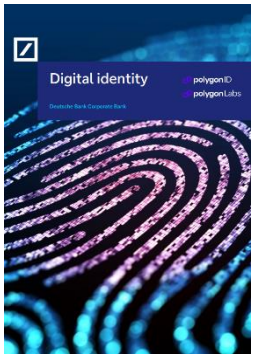
У статті Бенджамін Вуттон досліджує інноваційні можливості великих мовних моделей (LLM) для підвищення ефективності виявлення фінансових злочинів. Вуттон підкреслює, що традиційні системи захисту не справляються з дедалі складнішими методами шахраїв і злочинців.

LLM, такі як GPT-4, можуть автоматично обробляти великі обсяги неструктурованого тексту, виділяючи ключові дані, що дозволяє швидше та точніше інтегрувати їх у системи аналізу ризиків. Ці технології допомагають автоматизувати аналіз документів, знижуючи потребу в ручній обробці та зменшуючи ймовірність помилок.

Стаття також наводить приклади використання LLM для збагачення даних у сфері фінансових злочинів, показуючи, як ці моделі можуть значно підвищити ефективність роботи аналітиків з ризиків та забезпечення відповідності регламентам.

https://www.linkedin.com/pulse/using-large-language-models-data-enrichment-financial-wootton-ampae/

Digital Identity



У даному звіті розповідається, як банки можуть використовувати нові інструменти Web3 для створення та вирішення проблем корпоративної та індивідуальної ідентифікації – доказ концепції за допомогою Polygon ID.

Ідентичність була важливою частиною історії, і хоча цифрова ідентичність є новою сферою, її значення різко зросло. Пандемія призвела до переходу більшості взаємодій в цифрову сферу, але управління ідентичністю не встигало за цим, що призвело до передачі контролю над даними великим технологічним компаніям. Це викликає питання конфіденційності та безпеки.

Самостійна ідентичність (SSI) пропонує вирішення цих проблем, дозволяючи користувачам самостійно керувати своєю ідентичністю. Polygon ID є прикладом такої платформи. SSI може бути корисною як для Web3, так і для банківських процесів, таких як «знай свого клієнта» (KYC). Дослідження концепцій показують, що SSI забезпечує безпеку, покращену конфіденційність та контроль над даними, переосмислюючи підходи до ідентифікації.

Для успішного впровадження SSI необхідні широке прийняття, покращений користувацький досвід і освітня робота. Банки можуть відігравати ключову роль у цьому процесі, керуючи ідентичністю своїх клієнтів.

https://bit.ly/3XoaJbL

Вони знаходять трупи поза колл-центрами шахраїв; настав час бити на сполох щодо шахрайства

Стаття на bobsullivan.net висвітлює критичну ситуацію із зростанням масштабів фінансового шахрайства та відмивання коштів, яке здійснюється через шахрайські кол-центри, керованими організованими злочинними групами, на прикладі Картелю нового покоління Халіско (CJNG) в Мексиці.

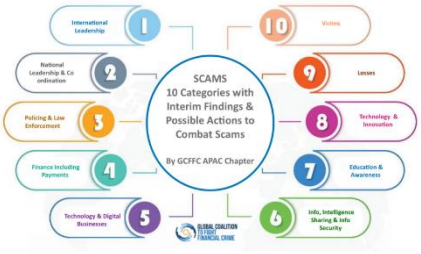
Такі шахрайські центри використовують технології для здійснення фінансових махінацій. Жертви часто стикаються з великими фінансовими втратами. Проблема поглиблюється насильством, яке відбувається всередині цих центрів, зокрема випадками вбивств співробітників, що підкреслюється знайденими тілами біля цих об'єктів. Автор закликає до активізації зусиль з боку міжнародних правоохоронних органів та посилення заходів безпеки для протидії цим небезпечним шахрайським організаціям.

Стаття також зазначає, що шахрайські кол-центри стають дедалі складнішими, використовуючи передові технології та психологічні методи маніпуляції, щоб обманути своїх жертв. Вони часто працюють під виглядом легальних компаній, що робить їх виявлення та ліквідацію складнішим завданням для правоохоронних органів. Крім того, підкреслюється, що працівники цих центрів, багато з яких наймані під обіцянками законної роботи, знаходяться під постійною загрозою насильства та експлуатації з боку своїх роботодавців.

Автор закликає до більш рішучих дій з боку урядів та міжнародних організацій, щоб зупинити діяльність цих шахрайських кол-центрів. Це включає впровадження жорсткіших регуляторних заходів, посилення правоохоронної співпраці між країнами та підвищення обізнаності громадськості про ризики шахрайства. Зрештою, боротьба з цією проблемою вимагає комплексного підходу, який поєднує в собі правові, технічні та освітні заходи.

https://bit.ly/3VCNdqh

Звіт про фінансове шахрайство



Усі країни стикаються з ростом шахрайств, проте багатші країни, такі як члени G7, ЄС та ОЕСР, повідомляють про найбільшу кількість випадків та втрат. Деякі країни, як Австралія, Гонконг і Сінгапур, надають достатньо інформації для розуміння загрози та відповіді на неї. В звіті виявлено понад 20 основних типів шахрайств, деякі з яких є гібридами або включають додаткові форми злочинності, що призводять до фінансових втрат, зміни способу життя та серйозних наслідків, як-от рабство та самогубства через шахрайства. Оціночні втрати від шахрайств у цих країнах, якщо екстраполювати їх на глобальний рівень, становлять від 50 до 177 мільярдів доларів США. Середні втрати на жертву оцінюються в 12 000 доларів, а на громадянина – приблизно в 62 долари. Фактори, що роблять країни привабливими для шахраїв, включають багатство, цифровізацію, швидкий банківський сервіс, використання віртуальних валют, активність в інтернеті та соціальних мережах, а також низьку обізнаність громадян про шахрайства. На основі дослідження Австралії, Гонконгу та Сінгапуру, GCFFC APAC Chapter консультує щодо можливих дій для покращення ефективності боротьби з шахрайствами.

https://www.gcffc.org/wp-content/uploads/2024/06/GCFFC-Scams-Report-6June2024Pbd-3.pdf

Токенізація: Відновлення ефективності та руху капіталу в морській галузі

Документ "Renewed Efficiency and Capital Flow in the Maritime Industry" досліджує впровадження технології блокчейн і токенізації у морську галузь для підвищення ефективності та залучення капіталу. Він описує, як морська галузь, що забезпечує транспортування 92% світових товарів, стикається з викликами модернізації флоту, які потребують значних капіталовкладень. Технологія блокчейн може зменшити адміністративні витрати та покращити процеси верифікації. Токенізація відкриває нові можливості для інвестування, дозволяючи конвертувати вартість активів, таких як кораблі, в цифрові токени, які можуть бути куплені та

продані інвесторами. Документ також розглядає різні види токенів, включаючи прямі активи, утиліти та зелені токени, які можуть сприяти екологічній сталості. Успішні приклади впровадження токенізації, такі як проекти з цифровими активами та ініціативи з використанням смарт-контрактів, підкреслюють потенціал цієї технології для стимулювання інновацій та інвестицій у морську галузь.

https://bit.ly/3VpxoC1

Крім фентанілу: роль криптовалюти на міжнародному ринку прекурсорів синтетичних наркотиків

🌎 Ви можете подумати, що фентаніл є проблемою лише для США, але, як показує цей звіт від TRM Labs, США є лише одним вузлом у величезній мережі, яка охоплює більшу частину світової торгівлі забороненими синтетичними наркотиками, яка значною мірою залежить від криптовалют. 🌍

У документі докладніше розглядаються китайські виробники прекурсорів наркотиків і вивчаються тенденції в тому, як вони використовують криптовалюту:

▲ Китайські виробники прекурсорів отримали понад 26 мільйонів доларів США у криптовалюті у 2023 році

▲ З 2022 по 2023 рік кількість криптовалюти, покладеної в гаманці, пов'язані з китайськими виробниками прекурсорів, зросла більш ніж на 600%.

▲ Близько 60% платежів у криптовалюті китайським виробникам прекурсорів на сьогоднішній день було здійснено через блокчейн біткойн

https://bit.ly/3VmTmWg

Фінансування загроз міжнародній безпеці

Стаття досліджує питання фінансування загроз національній безпеці, підкреслюючи, що незалежно від виду загрози, вона завжди потребує фінансування. Обговорюються різні види загроз, такі як шпигунство, тероризм, іноземний вплив, уникнення санкцій і корупція, кожен з яких має фінансовий компонент.

Фінансування шпигунства, наприклад, може здійснюватися через державні бюджети, криптовалюти або складні мережі компаній і банківських рахунків. Терористичні організації також потребують грошей для своїх операцій, і вони використовують як традиційну банківську систему, так і криптовалюти.

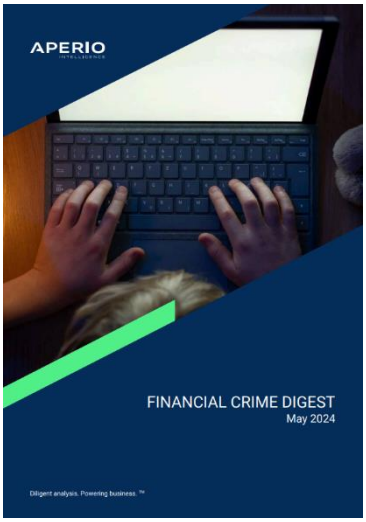
У Канаді існує значна проблема з ефективністю заходів протидії фінансуванню загроз, відсутність реальних результатів і переслідувань порушників, а також слабкі слідчі можливості. Попри наявність рамкової структури для протидії фінансуванню загроз, країна має дуже мало успішних справ про фінансування тероризму.

Важливість фінансового компоненту загроз підкреслюється на міжнародному рівні, але існують значні проблеми з координацією між різними державними установами, такими як фінансові розвідки та правоохоронні органи. Часто ці установи мають обмежені повноваження для розслідування і не є центром виявлення та припинення фінансування загроз.

Стаття підсумовує, що для зміцнення економіки, безпечної фінансової системи та більш безпечної глобальної спільноти, Канада та її союзники повинні модернізувати свій підхід до виявлення, аналізу та припинення фінансування загроз. Це включає більш ефективне виявлення та припинення фінансування загроз на ранніх стадіях, що дозволить попереджати теракти та інші загрози до їхнього виникнення.

https://newsletter.insightthreatintel.com/p/financing-threats-to-the-security

ДАЙДЖЕСТ ФІНАНСОВИХ ЗЛОЧИНІВ



Financial Crime Digest (FCD) за травень 2024 року надає детальний огляд останніх подій у сфері фінансових злочинів, законодавства, правозастосування та регуляторних оновлень.

У цьому випуску висвітлюються ключові моменти, такі як штрафи, накладені на міжнародного брокера Citigroup Global Markets Limited (CGML) за недоліки в системах торгівлі та контролю. Крім того, обговорюється резонансна справа з засудженням колишнього голови адміністрації президента Мадагаскару за хабарництво, що стала прикладом значного корупційного правопорушення.

Однією з основних тем цього випуску є зростаюча проблема онлайн-сексторції неповнолітніх, яка набуває дедалі більшої поширеності та має трагічні наслідки. Цей тип злочину особливо небезпечний, оскільки вразливими стають діти, яких шантажують заради фінансової вигоди. FCD також надає аналіз значущих інцидентів фінансових злочинів та регуляторних заходів у всьому світі.

У розділі інтерв'ю FCD пропонує розмову з Іліасом Хатзісом, керівником відділу боротьби з торгівлею людьми та контрабандою мігрантів ООН. Він обговорює сучасні виклики та зусилля в боротьбі з цими явищами, акцентуючи увагу на необхідності комплексних фінансових розслідувань у справах торгівлі людьми.

У розділі звітів представлені докладні дослідження різних аспектів фінансових злочинів, включаючи аналіз ринку, ланцюжків постачання та оцінку ризиків для країн. Оновлення щодо санкцій ЄС та Великобританії, зокрема нові заходи та рішення, прийняті у травні 2024 року, також займають важливе місце у цьому випуску.

Особливу увагу приділено розвитку стандартів корпоративної сталості та новим регуляціям, спрямованим на сприяння сталому розвитку. Наприклад, у випуску згадується про позов проти TotalEnergies за значний внесок у зміну клімату та його вплив на екстремальні погодні катастрофи.

Крім того, журнал охоплює геополітичні впливи суперництва між США та Китаєм на Близькому Сході та їх наслідки для міжнародного бізнесу. Представлені також оновлення щодо зусиль різних країн у боротьбі з фінансовими злочинами та підвищення прозорості.

Цей випуск Financial Crime Digest є важливим джерелом інформації для професіоналів у сфері фінансової безпеки, допомагаючи їм залишатися в курсі останніх подій, регуляторних змін та передових практик у запобіганні фінансовим злочинам і забезпеченні відповідності.

https://www.aperio-fcd.com/fcd-monthly?report_id=87

Злочинність за допомогою ШІ в екосистемі криптоактивів

Звіт Elliptic аналізує використання штучного інтелекту (ШІ) для вчинення злочинів у сфері криптовалют. Основні типології злочинів включають використання генеративного ШІ для обману,

створення шахрайських токенів і схем маніпулювання ринком, застосування великих мовних моделей для кіберзлочинів, масштабне розгортання дезінформації та розширення нелегальних ринків.

Звіт описує конкретні кейси, як-от фейкові відео з відомими особами для легітимізації шахрайства, шахрайські інвестиційні платформи, автоматизація обманних комунікацій і використання ШІ для кіберзлочинів. Документ також містить рекомендації щодо запобігання таким злочинам, підкреслюючи важливість раннього виявлення нових тенденцій у злочинності з використанням ШІ.

https://www.elliptic.co/resources/ai-enabled-crime-in-the-cryptoasset-ecosystem

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

Dark money[1] та політика: чи продається демократія?

У цьому епізоді подкасту RUSI до директора CFS Тома Кітінга приєднується Пітер Геогеган, репортер-розслідувач у Global Crime and Corruption Reporting Project – глобальній мережі журналістів – і автор книги «Демократія на продаж».

Вони обговорюють роль «Dark money» у політичному фінансуванні, лазівки, відсутність регулятивної підзвітності в соціальних мережах, те, як аналітичні центри можуть впливати на політичні процеси, а також як компанії-оболонки можна використовувати в якості механізму для здійснення великих політичних пожертвувань.

https://bit.ly/4emPWeM

Курси RAW Compliance

Доступ до понад 100 сертифікованих навчальних курсів, пов'язаних із комплаєнсом, понад 26 мовами, частина з яких безкоштовна.

https://www.rawcompliancehub.com/courses

[1] У політиці, Dark money стосуються витрат, спрямованих на вплив на вибори, державну політику та політичний дискурс, де джерело грошей не розкривається громадськості.

ІНШІ НОВИНИ

Останні оновлення щодо санкцій та відмивання коштів від RegTech

Цей бюлетень містить інформацію про

- Законодавці США наполягають на забороні акумуляторних батарей китайських гігантів CATL і Gotion High-Tech через ймовірні зв'язки з примусовою працею уйгурів.
- Санкції проти Росії та Китаю стикаються з проблемами застосування, оскільки такі фірми, як Jatronic, допомагають російський ВПК, а Oracle підтримує TikTok, незважаючи на обмеження.
- Основні справи про відмивання коштів стосуються Білла Гуана з Epoch Times' та Рьохеї Фуджі з Японії.
- Австралійському оператору казино SkyCity загрожує величезний штраф за збої в боротьбі з відмиванням коштів, а сім шведських фірм знаходяться під розслідуванням за порушення санкцій ЄС проти Росії.
- Глобальна боротьба з фінансовими злочинами та питання відповідності продовжує висвітлювати складність міжнародного регулювання.

https://bit.ly/4efClWG

Інформатор звинувачує США в ігноруванні доказів, що Standard Chartered Bank обслуговував підозрілих іранських клієнтів

Стаття описує звинувачення колишнього співробітника Standard Chartered Bank Джуліана Найта, який стверджує, що уряд США приховав докази того, що банк продовжував здійснювати транзакції з підсанкційними іранськими клієнтами і терористичними організаціями після 2007 року. Найт надав інформацію про ці транзакції уряду США, але його претензії були відхилені, а докази ігноровані або приховані. Він знову подав позов, стверджуючи, що уряд обманув суд, заявивши про відсутність додаткових порушень.

https://bit.ly/3XgZfa9

У 2024 році використання програм-вимагачів стало «жорстокішими», ніж будь-коли

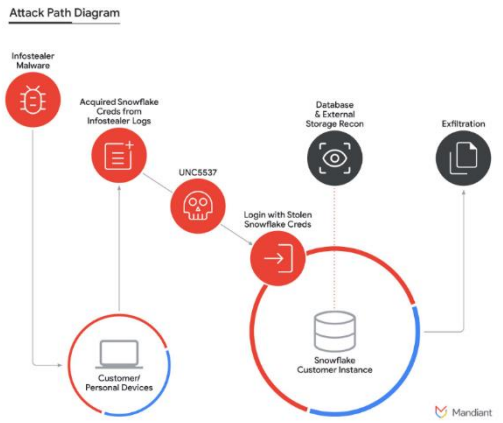
Стаття на сайті Wired аналізує останні тенденції у сфері програм-вимагачів, зокрема зростання кількості атак та зміни в тактиці кіберзлочинців. У 2023 році кількість атак майже подвоїлася порівняно з 2022 роком, що свідчить про еволюцію і зростання загрози. Розслідування показує, що кіберзлочинні групи стають дедалі професійнішими і витонченішими, що призводить до значного збільшення витрат на відновлення після атак. Середня сума викупу зросла в п’ять разів, досягнувши 2 мільйонів доларів, хоча лише 24% жертв платять суму, що вимагають на початку.

Більше половини організацій, що постраждали від атак, вдаються до оплати викупу, і зростає кількість тих, хто використовує кілька підходів до відновлення даних, таких як оплата викупу та використання резервних копій. Значно зросли витрати на відновлення, досягнувши в середньому 2,73 мільйона доларів, що на 50% більше порівняно з попереднім роком.

Значну увагу приділяють також змінам у мотивації кіберзлочинців: збільшується кількість атак з метою витоку даних замість простого шифрування. Крім того, зростає кількість атак на медичні установи, що відображає зміну тактики злочинців. У статті підкреслюється важливість проактивних заходів кібербезпеки для захисту бізнесу та мінімізації ризиків, пов’язаних з атакою на ланцюги поставок.

https://bit.ly/4bT02T4

UNC5537 націлений на клієнтів Snowflake для крадіжки та вимагання даних



Стаття описує серію кібер-атак, здійснених групою UNC5537, яка націлилася на клієнтів Snowflake – хмарної платформи для зберігання даних. Група використовувала викрадені облікові дані клієнтів та спеціальний інструмент під назвою "rapeflake" для несанкціонованого доступу до облікових записів, які не мали двофакторної автентифікації (2FA). Вони зосередилися на викраденні даних з метою подальшого шантажу, погрожуючи продати викрадену інформацію на хакерських форумах, якщо викуп не буде сплачений.

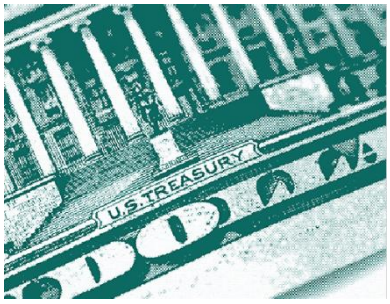
Зловмисники використовували комерційні VPN IP-адреси для збереження анонімності під час атак. Перші ознаки цієї атаки були виявлені в квітні 2024 року, а до травня Snowflake підтвердив випадки несанкціонованого доступу. Незважаючи на це, компанія заявила, що інциденти не пов'язані з вразливостями чи неправильними налаштуваннями в їх продукті, а скоріше були результатом атак, заснованих на викраденні ідентифікаційних даних клієнтів.

Snowflake видав рекомендації щодо посилення безпеки, включаючи впровадження 2FA, регулярний моніторинг журналів доступу та сегментацію мережі для обмеження доступу тільки з довірених IP-адрес. Також були надані індикатори компрометації (IoC) та інструменти для виявлення підозрілої активності.

Цей випадок підкреслює важливість проактивних заходів кібербезпеки для захисту даних у хмарних середовищах, а також необхідність постійного моніторингу та вдосконалення захисних механізмів.

https://bit.ly/3z83jiK

Тенденція посилення перевірки SEC є хорошим передвісником для фахівців з ПВК



У статті Fraud Magazine описується посилення уваги з боку Комісії з цінних паперів і бірж США (SEC) до питань шахрайства, що є позитивним сигналом для професіоналів у сфері боротьби з шахрайством.

Головною темою є зростаюча увага SEC до дотримання законів про цінні папери та фінансові ринки під керівництвом Гері Генслера. Автори статті підкреслюють, що Генслер серйозно налаштований на посилення заходів з протидії шахрайству, що включає збільшення кількості розслідувань та реформування ринків капіталу. Це сприятливо впливає на сферу боротьби з шахрайством, оскільки збільшення контролю та прозорості знижує можливості для зловживань.

Один з прикладів, наведений у статті, - це випадок Арона Говіля, який організував шахрайську схему, завдяки якій обдурив інвесторів на понад $7 мільйонів. Він переконав інвесторів вкладати кошти у фальшиві проекти, використовуючи підроблені документи та неправдиву інформацію. SEC активно розслідувала цю справу, що стало важливим кроком у боротьбі з подібними злочинами.

SEC зосереджена на реформуванні ринків капіталу, що включає зміни в обліку та аудиті. Це передбачає більш жорсткі вимоги до фінансової звітності компаній, а також покращення прозорості та підзвітності. Такі заходи допомагають знизити ризики шахрайства та підвищити довіру інвесторів до ринків.

Стаття також обговорює важливість впровадження анонімних ліній звітності для виявлення внутрішнього шахрайства. Відповідно до звіту ACFE "Occupational Fraud 2024: A Report to the Nations", звіти співробітників є найпоширенішим методом виявлення шахрайства в організаціях. Анонімні лінії звітності сприяють більш швидкому виявленню порушень та втрат.

Загалом, стаття підкреслює важливість активної ролі регуляторів у запобіганні шахрайству та необхідність впровадження ефективних заходів контролю в організаціях.

https://www.fraud-magazine.com/article.aspx?id=4295023425

Відеоігри можуть мати значення для фінансування тероризму

У дослідженні Lawfare досліджується, як терористичні групи можуть використовувати відеоігри для фінансування своєї діяльності. Основна увага приділяється віртуальним валютам та цифровим активам, які використовуються у відеоіграх.

Терористичні групи можуть використовувати кілька схем для фінансування через відеоігри. Одна з них включає покупку віртуальних валют за незаконно отримані гроші, потім передача цих валют між акаунтами та їх продаж на ринках для отримання реальних грошей. Інша схема включає продаж рідкісних ігрових предметів або акаунтів, що мають високу цінність, за реальні гроші. Використання таких схем стає можливим через анонімність та глобальну доступність ігрових платформ.

Хоча наразі мало доказів використання відеоігор саме терористами, автори підкреслюють важливість вивчення цієї загрози та впровадження жорсткіших регуляцій. Віртуальні економіки, такі як ті, що існують у популярних онлайн-іграх, можуть стати зручним інструментом для відмивання коштів через складність відстеження та регулювання таких транзакцій. Ігрові платформи, що використовують віртуальні валюти, можуть стати потенційним середовищем для незаконної діяльності через свою глобальну доступність та анонімність користувачів. Автори закликають до міждисциплінарного підходу, залучаючи регуляторів, розробників ігор та правоохоронні органи для запобігання можливому використанню цих технологій у злочинних цілях.

https://www.lawfaremedia.org/article/video-games-might-matter-for-terrorist-financing

Боротьба з незаконним, незареєстрованим і нерегульованим рибальством через дії США та світу

Стаття висвітлює глобальні зусилля у боротьбі з незаконним, незадекларованим і нерегульованим (IUU) рибальством, яке завдає значних економічних втрат та шкодить морським екосистемам. Щорічно втрачаються мільярди доларів через неоплачені податки, митні та ліцензійні збори, а також через вплив IUU рибальства на біорізноманіття

океанів. Крім того, IUU рибальство негативно впливає на прибережні спільноти, які залежать від стійких рибних запасів для доходів та їжі.

Незаконне, незадекларованe і нерегульованe (IUU) рибальство часто пов'язане з фінансовим шахрайством та відмиванням коштів. Злочинні угруповання використовують примусову працю і займаються торгівлею наркотиками та зброєю, отримуючи незаконні доходи. Ці доходи потім відмиваються через складні фінансові схеми, включаючи фіктивні компанії та підставних осіб. Втрачені мільярди доларів через неоплачені податки, митні та ліцензійні збори є однією з форм фінансового шахрайства. США та міжнародні партнери працюють над посиленням моніторингу, контролю та відповідальності, щоб протидіяти цим незаконним практикам.

Для вирішення цієї проблеми необхідні скоординовані глобальні дії. Співпраця між урядами, міжнародними організаціями, громадянським суспільством та місцевими громадами є ключовою для досягнення успіху. США активно беруть участь у глобальних, регіональних і двосторонніх зусиллях, допомагаючи рибалкам, захищаючи морські екосистеми та зміцнюючи місцеві громади. Закон про безпеку на морі та рибальстві (SAFE Act) передбачає залучення всіх урядових структур США до боротьби з цими проблемами.

Як приклад, США та ООН співпрацюють з Сенегалом для підтримки судової та прокурорської здатності протидіяти злочинцям. Інший приклад - у Філіппінах USAID працює з урядом, академічними колами та риболовними громадами для припинення незаконного вилову риби. Публічно-приватне партнерство "Por la Pesca" в Перу та Еквадорі допомагає формалізувати місцеве рибальство та покращити економічні можливості рибальства.

Ці приклади демонструють, як США ведуть глобальні зусилля з боротьби з IUU рибальством, застосовуючи комплексний підхід до вирішення цієї критичної та багатосторонньої проблеми.

https://bit.ly/45FCxuF

Очікується, що Generative AI збільшить ризик діпфейків та іншого шахрайства в банківській сфері

У статті Deloitte обговорюється, як генеративний штучний інтелект (AI) стає інструментом для шахрайства, дозволяючи злочинцям створювати підроблені відео, голоси та документи для обману фінансових установ і їх клієнтів. На початку 2024 року працівниця гонконгського банку відправила шахраям $25 мільйонів, думаючи, що виконує інструкції фінансового директора по відеозв'язку. Насправді, шахраї використовували діпфейк, щоб переконати її у реальності доручень.

Прогнози Deloitte свідчать, що до 2027 року збитки від шахрайства з використанням генеративного AI в США можуть досягти $40 мільярдів, що втричі більше, ніж у 2023 році. Це зростання пояснюється здатністю AI постійно вдосконалювати свої методи обману, роблячи системи виявлення шахрайства менш ефективними.

Фінансові установи стикаються з дедалі складнішими завданнями щодо виявлення шахрайства. Генеративний AI дозволяє створювати підробки високої якості, які важко відрізнити від справжніх. Злочинці можуть використовувати ці технології для доступу до рахунків, крадіжки особистих даних та проведення несанкціонованих транзакцій. Наприклад, у 2023 році кількість інцидентів з використанням діпфейків зросла на 700%.

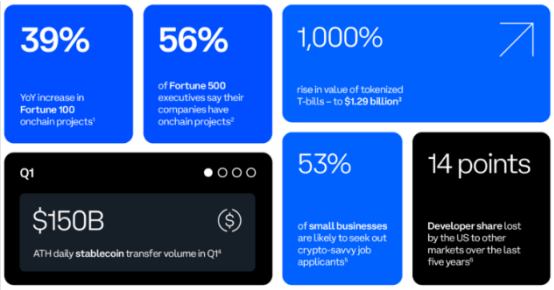
Для боротьби з новими загрозами фінансові установи повинні впроваджувати сучасні технології виявлення шахрайства, такі як великі мовні моделі для виявлення ознак шахрайства в текстових і голосових повідомленнях. Деякі банки вже використовують AI для автоматизації процесів, які

діагностують загрози та відправляють сповіщення відповідним командам. Наприклад, JPMorgan використовує AI для виявлення компрометації електронної пошти, а Mastercard використовує свою платформу Decision Intelligence для прогнозування ймовірності шахрайських транзакцій.

Фінансові установи повинні інвестувати в навчання співробітників для виявлення, зупинки та повідомлення про шахрайство, що базується на AI. Це дозволить банкам підтримувати високу ефективність боротьби з шахрайством та забезпечити безпеку своїх клієнтів.

https://bit.ly/3KKfHbC

Стан крипто: Fortune 500 переміщується в Onchain



Провідні американські публічні компанії ведуть діяльність ончейн як ніколи. Проекти ончейн, анонсовані компаніями зі списку Fortune 100, зросли на 39% порівняно з минулим роком і досягли рекордного рівня в першому кварталі 2024 року.

Опитування керівників зі списку Fortune 500 показало, що 56% говорять, що їхні компанії працюють над проектами onchain. Від найбільших застарілих брендів до малого бізнесу, від стейблкойнів до токенізованих державних векселів, імена та продукти у сфері фінансів, яким довіряєш, використовують технологію блокчейн і крипто, стимулюючи інновації та забезпечуючи широкі можливості для широкого впровадження. Посилення активності підкреслює необхідність встановлення чітких правил для крипто, які допоможуть утримувати крипторозробників та інших талантів у США.

https://www.coinbase.com/blog/the-state-of-crypto-the-fortune-500-moving-onchain

Підсанкційні танкери створюють зростаючий екологічний ризик

Підсанкційні нафтові танкери, які є частиною «тіньового флоту», створюють зростаючий екологічний ризик у Середземному морі, особливо поблизу Греції. Ці нерегульовані кораблі, часто з Ірану, Венесуели та Росії, обходять західні санкції та працюють маючи непрозору власність, відсутність страхування та невідповідність екологічними стандартами. Міністр судноплавства Греції підкреслив загрозу аварій і розливів нафти, що призвело до посилення захисних заходів і обмежень на транспортування нафти з судна на судно біля узбережжя Греції.

https://www.marinelink.com/news/sanctioned-tankers-pose-rising-514229?es_id=b0235ccba2

Фінансування тероризму: забутий предикатний злочин

У статті "Terrorist Financing: The Neglected Predicate Crime" досліджується проблема фінансування тероризму (TF) як недостатньо розуміємої складової у боротьбі з відмиванням грошей (AML). Автор статті, розмовляючи з колегою Ендрю Девісом, з'ясував, що TF часто розглядається окремо від AML, хоча обидва ці явища є тісно пов'язаними.

Основна причина такого розподілу полягає в тому, що фінансування тероризму часто отримує кошти з легальних джерел, таких як краудфандинг та добровільні пожертвування, що, на перший

погляд, не пов'язує його з відмиванням грошей. Однак, як зазначає Девіс, терористи ховають свої кошти так само, як і злочинці, що отримують гроші незаконним шляхом.

У статті наголошується на рекомендаціях FATF, які вимагають криміналізувати фінансування тероризму як підставне правопорушення для відмивання грошей. Проте, попри ці вимоги, багато організацій та регуляторів продовжують розглядати TF, AML та інші фінансові злочини окремо.

Однією з найбільших проблем у протидії TF є ізоляція даних між різними організаціями, що перешкоджає ефективному виявленню та боротьбі з цими злочинами. Ендрю Девіс і його колега Ієн Армстронг, які працюють у ComplyAdvantage, наголошують на необхідності співпраці та обміну даними між публічним та приватним секторами для швидшого та ефективнішого виявлення загроз.

Щоб вирішити проблему, експерти рекомендують зосередитися на спільному використанні даних про тенденції, типології та нелегальні фінансові потоки. Вони підкреслюють, що обмін такою інформацією не порушує приватності даних, але значно покращує ефективність боротьби з фінансуванням тероризму.

У підсумку, стаття закликає до переосмислення парадигми фінансових злочинів, де відмивання грошей слід розглядати як центральний елемент, що поєднує різні форми злочинної діяльності, включаючи фінансування тероризму, шахрайство, торгівлю людьми та політичну корупцію. Співпраця між різними секторами та організаціями є ключовим елементом у цій боротьбі.

https://bit.ly/3z37GvL

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Підробка та піратство продуктів

Торгівля контрафактними та піратськими товарами є серйозною проблемою в глобальній економіці, яка ґрунтується на інноваціях. Організовані злочинні групи відіграють дедалі важливішу роль у цій діяльності та отримують значні вигоди від підробки та піратства. Від годинників до ліків і оливкової олії, Європол підтримує боротьбу з підробками в ЄС.

Цей вид злочинності має більший вплив на наше суспільство, ніж ви думаєте:

Нерегульоване використання ліків і допінгових речовин, особливо підробленої продукції, може спричинити серйозні та незворотні тілесні ушкодження.

Тим часом підробка одягу в ЄС коштує бізнесу 43,3 мільярда євро у вигляді втрачених продажів, урядам – 8,1 мільярда втрачених доходів і 518 281 людині втраченої роботи.

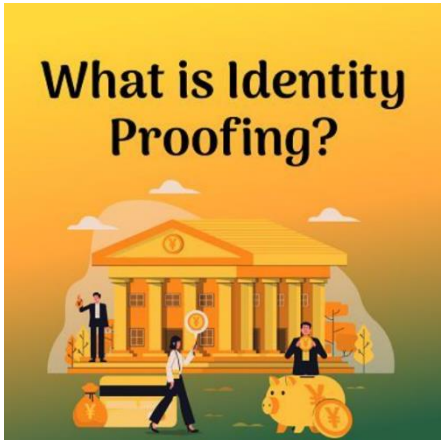
https://www.europol.europa.eu/crime-areas/intellectual-property-crime/counterfeiting-and-product-piracy

Що таке інтеграція у відмиванні коштів?

Інтеграція у відмиванні коштів - це заключний етап процесу, коли незаконно отримані кошти змішуються з легальними, щоб приховати їхнє походження. На цьому етапі злочинці використовують складні транзакції, інвестують у легальні бізнеси, купують нерухомість або інші активи, використовують офшорні рахунки та фірми-пустишки. Мета інтеграції - зробити нелегальні кошти невідрізними від легальних, що дозволяє їм безперешкодно використовувати ці гроші.

https://bit.ly/3xfXuzl

Що таке підтвердження особи?



CSRC описує підтвердження особи як "процес надання достатньої інформації (наприклад, історії особи, облікових даних, документів) для встановлення особи".

Типи підтвердження особи

У сучасному кібер-світі, де наші ідентифікаційні дані постійно циркулюють в Інтернеті, дуже важливо перевіряти ідентичність людей. Саме тоді стає важливою перевірка особи, яка використовує різноманітні методи для підтвердження того, що ви маєте справу з автентичною особою. З такою великою кількістю доступних варіантів, як ви можете визначити оптимальний?

Автентифікація на основі знань (KBA)

Пам'ятаєте ті питання безпеки, які ви встановлювали для своїх онлайн-акаунтів? KBA є натхненником цих методів. Він перевіряє ваші знання особистих даних, таких як ім'я домашнього улюбленця з дитинства або ваш перший автомобіль. Незважаючи на зручність, ефективність KBA залежить від обраних питань. Якщо дані можна легко отримати з соціальних мереж, вони стають менш безпечними.

Перевірка документів

Цей метод є цифровим еквівалентом пред'явлення посвідчення особи. Ви надаєте оцифровані або сфотографовані копії офіційних державних документів, таких як паспорт або водійське посвідчення. Просунуті версії використовують технологічні засоби для перевірки автентичності, такі як голограми або вбудоване програмне забезпечення. Хоча перевірка документів є надійною, вона може бути громіздкою і вразливою до підробки високоякісних підробок.

Біометрична верифікація

Цей високотехнологічний метод використовує унікальні особливості вашого тіла, щоб довести, хто ви є. Подумайте про зчитувачі відбитків пальців, камери, які можуть розпізнавати обличчя, або навіть сканери райдужної оболонки ока. Біометрія забезпечує дуже високий рівень безпеки, але існують побоювання щодо захисту даних і можливих упереджень у цій технології.

Позамережева перевірка

Використовуючи інший канал зв'язку, цей метод додає додатковий рівень безпеки. Скажімо, ви підписуєтесь на новий сервіс, який надсилає код підтвердження на номер телефону, прив'язаний до вашої електронної адреси. Це доводить, що у вас є доступ до обох цих пристроїв, що зменшує ймовірність того, що хтось використає викрадену інформацію, щоб видати себе за вас.

Перевірки кредитного бюро

Для фінансових установ перевірки кредитного бюро можуть бути цінним інструментом. Отримавши доступ до вашого кредитного звіту за вашою згодою, вони можуть перевірити вашу особу на основі вашої фінансової історії та інформації про позики. Цей метод особливо корисний для транзакцій на великі суми або для встановлення фінансової достовірності.

Аналіз даних і машинне навчання

Ці найсучасніші алгоритми оцінюють величезні бази даних, щоб створити повну картину інтернет-активності людини. Вони можуть знайти аномалії, які можуть вказувати на шахрайську діяльність, аналізуючи такі фактори, як IP-адреса, історія пристроїв і навіть звички друку. Незважаючи на їхню силу, будь-які упередження та питання конфіденційності даних повинні бути ретельно розглянуті.

Роль гейткіперів у протидії відмиванню коштів

Хто такі гейткіпери фінансової системи?

Це фахівці, в тому числі юристи, бухгалтери та нотаріуси, які часто виступають посередниками у фінансових операціях. Вони діють як гейткіпери фінансової системи в тому сенсі, що, дотримуючись правил ПВК, вони мають змогу, в першу чергу, запобігти потраплянню брудних грошей у систему.

Як можна зловживати гейткіперами для відмивання коштів

Завдяки своєму надійному становищу та досвіду роботи у фінансовій системі, гейткіпери є привабливою мішенню для злочинців, які прагнуть відмити кошти. Ось як особи, що відмивають кошти, можуть зловживати гейткіперами:

☞ створюють складні структури власності

☞ сприяння переміщенню незаконних коштів через операції з нерухомістю

☞ створення підставних компаній

☞ надавати консультації щодо слабких місць у законодавстві з протидії відмиванню коштів та його прогалин

☞ виступати номінальними власниками для приховування реальних бенефіціарних власників компаній

☞ юристи зобов'язані дотримуватися конфіденційності, щоб захистити своїх клієнтів.

та багато іншого.

Обов’язки гейткіперів

Гейткіпери підпадають під дію суворих правил протидії відмиванню коштів. Вони повинні здійснювати належну перевірку, повідомляти про підозрілу діяльність і вести докладні записи. Вони не повинні сприяти, вільно або мимоволі, відмиванню коштів або іншим фінансовим злочинам.

Приклад з реального життя

Яскравим прикладом зловживань з боку гейткіперів є скандал з "Панамськими документами". Цей масштабний витік показав, як деякі юристи та бухгалтери допомагали створювати підставні компанії для приховування активів і відмивання коштів для заможних клієнтів, включаючи політиків і знаменитостей. Чи означає це, що всі гейткіпери використовуються для відмивання грошей?

Ні.

Більшість гейткіперів старанно виконують свої обов'язки і роблять значний внесок у підтримання фінансової доброчесності. Але вони часто є привабливою мішенню для незаконних цілей.

Обов’язкові процеси для Програм з ПВК

1. Ризик-орієнтований підхід:

↳ Заходи з ПВК мають бути адаптовані до конкретних ризиків, з якими стикається організація.

↳ Регулярно оновлюйте оцінки ризиків, щоб випереджати нові загрози.

2. Політики та процедури:

↳ Розробіть комплексні політику та процедури з ПВК.

↳ Переконайтеся, що вони відповідають нормативним вимогам, пристосовані до конкретних ризиків організації та періодично переглядаються.

3. Відповідальний працівник:

↳ Призначте спеціального відповідального працівника на рівні керівництва.

↳ Здійснюйте нагляд за програмою з ПВК та забезпечуйте дотримання нормативних актів.

4. CDD та KYC:

↳ Проводьте ретельні процеси CDD і KYC.

↳ Перевіряйте інформацію про клієнтів і розумійте природу ділових відносин.

5. Моніторинг операцій:

Ļ Впроваджуйте системи для виявлення підозрілих операцій.

Ļ Адаптуйте системи моніторингу до конкретного профілю ризику установи.

6. Ведення записів:

Ļ Ведіть точні записи про клієнтів і деталі транзакцій.

Ļ Дотримуйтеся нормативних вимог щодо збереження записів.

7. Повідомлення:

Ļ Негайно надсилайте звіти про підозрілу активність (SAR).

Ļ Забезпечте точне та своєчасне звітування до регуляторних органів.

8. Навчання та обізнаність:

Ļ Забезпечте постійне навчання співробітників з питань ПВК.

Ļ Надайте персоналу знання, щоб розпізнавати підозрілу діяльність і повідомляти про неї.

9. Незалежний аудит:

Ļ Регулярно перевіряйте ефективність програми ПВК.

Ļ Негайно усувайте будь-які виявлені недоліки.

10. Управління та нагляд:

Ļ Створіть чіткі структури управління для дотримання вимог з ПВК.

Ļ Забезпечте активну участь вищого керівництва та правління.

Відмивання грошей на основі торгівлі (TBML)

Глобальна торгівля товарами — це величезний ринок, розмір якого оцінюється приблизно в 20 трильйонів доларів США на рік. Група розробки фінансових заходів боротьби з відмиванням грошей (FATF) визначає TBML як процес приховування доходів, отриманих злочинним шляхом, і рухомих цінностей за допомогою торговельних операцій для узаконення їх незаконного походження.

Він використовується злочинними організаціями та тими, хто фінансує терористів для переміщення грошей, приховування їх походження та інтеграції їх назад у легальну економіку. Основною метою будь-якої трансакції TBML є рух грошей, а не рух товарів, якому ці торгові операції сприяють. TBML відбувається як через внутрішні, так і через міжнародні торговельні операції, але вартість транзакцій набагато вища в міжнародних торгових транзакціях.

TBML є одним із кращих шляхів відмивання коштів, і його популярність пояснюється складністю світових торгових операцій. Певні інші причини, які роблять його популярним серед мереж, які

займаються відмиванням коштів, організованими злочинними групами та фінансуванням тероризму, наведені нижче.

1. Складний характер валютних операцій і використання різноманітних механізмів фінансування.
2. Величезний характер торгових потоків, що дозволяє легко приховати окремі транзакції серед складних шарів і мереж транзакцій.
3. Численні пункти перевалки, треті сторони, учасники ланцюга поставок дозволяють злочинцям дистанціюватися від діяльності TBML.
4. Обмежений або відсутній механізм між різними країнами для перевірки транзакцій, що додатково сприяє незаконним торговим операціям.
5. Складнощі фізичної перевірки товарів у пунктах пропуску.
6. Практика змішування незаконних коштів із грошовими потоками законного бізнесу.
7. Слабкий регуляторний фінансовий нагляд у кількох країнах і корупція.

Як правило, товари з подовженими торговельними циклами, тобто ті, які відправляються вздовж кількох юрисдикцій і кордонів, товари з великою ціновою маржею та товари, які важко перевірити, зазвичай торгуються в TBML. Сектори або продукти, які є найбільш вразливими до відмивання грошей у торгівлі, наведені нижче:

Мінерали, золото, дорогоцінне каміння та ювелірні вироби, будівельні матеріали, машинне устаткування, хімічні речовини, паливно-енергетичні продукти, одяг та вживаний текстиль, портативна електроніка, тощо.

Методи відмивання коштів на основі торгівлі:

- Завищення ціни (недостатня доставка)
- Заниження ціни (надмірна доставка)
- Використання кількох рахунків-фактур
- Фіктивне відвантаження
- Карусельне шахрайство тощо.

Методи відмивання коштів на основі торгівлі

Завищення ціни (недостатня доставка)

Спотворення ціни товару чи послуги шляхом її підвищення вище «справедливої ринкової» ціни, за допомогою якої експортер може отримати додаткову вартість від імпортера.

Заниження ціни (надмірна доставки)

Спотворення ціни товару чи послуги шляхом її зниження нижче «справедливої ринкової» ціни, за допомогою якої експортер може передати додаткову вартість імпортеру.

Використання кількох рахунків-фактур

Надсилання кількох платежів на декілька банківських рахунків за допомогою однієї документації.

Фіктивне відвантаження

Створення документа для неіснуючого відправлення, тобто товари ніколи не експортувалися чи імпортувалися

Карусельне шахрайство

Циркулярна транзакція або поїздка в обидві сторони шляхом імпорту товарів із країни без ПДВ, продажу в країні-імпортері шляхом додавання ПДВ і несплати ПДВ уряду.

Трансфертне ціноутворення через торгівлю

Використовується з метою зменшення податкових зобов'язань підприємств через структуровані торговельні операції, особливо в країнах податкового раю, шляхом постійного переміщення ресурсів між пов'язаними сторонами.

Неправильне декларування товарів

Неправильне представлення якості або типу товару, нечіткий або технічний опис товару

Проблеми та механізм запобігання TBML

Відмиванню коштів у сфері торгівлі можна запобігти за допомогою належної перевірки клієнта (CDD) і програми ідентифікації клієнта (CIP). І це саме по собі є найбільшим викликом, і має бути виконано належним чином.

Правильне розуміння профілю та бізнесу клієнта також має велике значення для боротьби з загрозою TBML, оскільки відмивачі грошей зазвичай уникають обізнаних банківських робітників, які добре розуміються на торгівлі.

Розуміння різноманітних торговельних документів, таких як коносамент, авіанакладна та інші Інкотермс, було б корисним.

Філії, які обслуговують транзакції, пов'язані з транскордонною торгівлею, повинні прискіпливо перевіряти торговельні документи, вимагати надання додаткових документів, якщо це необхідно для дотримання інструкцій Банку з дотримання нормативних вимог, або зіткнутися з ризиком величезного штрафу чи навіть санкцій.