Серійний номер: ДСФМУ-ДК-2024-016
Липень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Вольфсберзька група щодо протидії фінансуванню тероризму

Вольфсберзька група випустила оновлений документ про протидію фінансуванню тероризму (ПФТ), в якому відображає актуальний ландшафт і підтверджує свої зобов'язання.

Ключові моменти:

1. Комплексна еволюція заходів ПФТ:

- ✓ Ризикоорієнтована належна перевірка: ширше впровадження практики належної перевірки, спрямованої на зменшення ризиків фінансування тероризму.
- ✓ Підвищена обізнаність: краще розуміння поведінки, ризиків і типології фінансування тероризму.
- ✓ Покращене звітування: оптимізовані вимоги до звітування для швидшого розгляду справи.
- ✓ Передові технології: використання витончених технологій для кращого виявлення діяльності з фінансування тероризму.
- ✓ Державно-приватне партнерство: покращена співпраця та координація між юрисдикціями.

2. Роль фінансових установ:

- ✓ Фінансові установи відіграють вирішальну роль у запобіганні та виявленні фінансування тероризму за допомогою профілактичних заходів і дотримання нормативних вимог.
- ✓ Акцент на збалансованості зменшення ризиків із збереженням доступу до фінансової системи для законних цілей.

3. Система контролю на основі ризику:

- ✓ Відданість ризик-орієнтованому підходу, відповідно до керівних настанов FATF.
- ✓ Застосування посиленої належної перевірки для клієнтів і секторів із високим ризиком.
- ✓ Фокус на підтримці0020ефективних програм ПВК/ФТ для виявлення та повідомлення про підозрілу діяльність.

4. Глобальне співробітництво:

- ✓ Підтримка поглибленої співпраці між індустрією фінансових послуг, правоохоронними органами та державними установами.
- ✓ Заохочення до обміну інформацією та співпраці для ефективної боротьби з фінансуванням тероризму.

5. Поточні зусилля та фокус на майбутнє:

- ✓ Постійний розвиток процесів моніторингу та методів виявлення підозрілих операцій.
- ✓ Постійна підтримка Рекомендацій FATF та глобальних ініціатив щодо протидії фінансуванню тероризму.

https://wolfsberg-group.org/news/63

Передовий досвід прискорення вилучення активів, набутих незаконним шляхом

📣Запуск ключового посібника з належної практики повернення активів!

«Кращий досвід у прискоренні вилучення активів набутих незаконним шляхом» — це важливий посібник, розроблений у рамках Ініціативи сусідства та розширення ЄС, щоб посилити повернення активів у країнах Східного партнерства.

🔎 Цей всеосяжний звіт окреслює – через кілька прикладів – корисність прийняття механізмів, які прискорюють конфіскацію незаконно набутих активів. Такі модальності включають, наприклад, цивільну конфіскацію. Підкреслюючи інтеграцію перевірених практик і дотримання міжнародних стандартів, таких як UNCAC і UNTOC, це важливий документ для фахівців, які займаються правоохоронною діяльністю та розробкою політик.

🌍 Цей посібник, що містить історії успіху, є свідченням потужності сучасних та ефективних методів повернення активів, які дозволяють позбавити злочинців їхніх незаконних доходів.

https://unicri.it/Publication/Good_Practices_Accelerating_Capture_Illicitly-Acquired_Assets

Ставлення до політично значущих осіб – багатопрофільний огляд

Управління з питань фінансової поведінки публікує висновки свого аналізу щодо поводження з клієнтами-PEP компаніями, які регулюються FCA. Керівні настанови FCA радять компаніям використовувати ризикорієнтований та пропорційний підхід до публічних діячів в контексті ризиків відмивання грошей.

Регулятор зв’язався з понад 1000 публічних діячів Великобританії та отримав 65 відповідей, а потім зібрав і проаналізував дані від фірм у 5 секторах, зрештою звузивши коло до 15 фірм для детального огляду.

Ось основні висновки огляду FCA:

- Деякі фірми включили визначення PEP, які не відповідають НПА і Посібникам FCA;
- Деякі фірми не мали ефективних механізмів перегляду PEP, щоб забезпечити відповідність класифікації PEP після того, як PEP залишив державну посаду;
- Невелика кількість фірм не врахувала фактичний ризик клієнта в своїй оцінці та рейтингу;
- Не дивлячись на потребу покращити політику та процедури фірм, перевірка файлів клієнтів не показала, що фірми регулярно застосовують заходи посиленої \належної перевірки (EDD) щодо клієнтів;
- Усі з 15 фірм чітко заявили, що вони не будуть відмовляти в продуктах чи послугах британським публічним діячам або пов'язаним з ними особам лише через статус публічних діячів;
- Фірмам потрібно покращити ясність і деталізацію комунікацій з клієнтами PEP;
- Більшість із 15 фірм потребували вдосконалення навчання персоналу;

- Десять із 15 компаній внесли зміни та вдосконалення після нещодавньої поправки до Положення 35 (яке встановлює зобов'язання з ПВК щодо публічних діячів для компаній), але деяким потрібно було оновити свою політику, щоб відобразити цю зміну законодавства.

https://www.fca.org.uk/publication/multi-firm-reviews/treatment-politically-exposed-persons-2024.pdf

СТВОРЕННЯ ДОРОЖНЬОЇ КАРТИ КРАЇНИ ДЛЯ РЕЖИМУ РОЗКРИТТЯ ІНФОРМАЦІЇ ПРО БЕНЕФІЦІАРНУ ВЛАСНІСТЬ

У цьому стратегічному документі представляється **інноваційний і комплексний підхід до розробки та впровадження режимів розкриття інформації про бенефіціарну власність (БВ)**, заснований на великому досвіді в понад 26 юрисдикціях поза ЄС.

Кілька ключових пунктів цього стратегічного документа:

Цілісний і модульний підхід: метод Глобального фонду ЄС є одночасно гнучким і адаптованим, поважаючи місцевий контекст і чинні структури з ПВК/ФТ. Цей стратегічний документ забезпечує ефективне проектування, впровадження та транскордонне співробітництво, одночасно покращуючи загальне управління.

Етапи впровадження: у документі детально описано чотири важливі етапи розробки та впровадження структури БВ, забезпечуючи структурований та ефективний процес, адаптований до унікальних потреб кожної юрисдикції.

Інтегрована підтримка: наголошуючи на багатосторонньому підході, документ підкреслює важливість співпраці між різними установами, юридичними та фізичними особами для створення надійної екосистеми розкриття БВ.

Максимальний вплив: Вивчається, як використовувати підтримку та інструменти, розроблені Глобальним фондом ЄС, щоб підвищити ефективність режиму БВ, гарантуючи, що він відповідає міжнародним стандартам і найкращим практикам.

Глобальна релевантність: цей стратегічний документ надає модель, застосовну до юрисдикцій у всьому світі, пропонуючи вичерпний посібник із успішного впровадження режиму БВ.

https://www.global-amlcft.eu/wp-content/uploads/2024/05/BO-Country-Roadmap-vfinale.pdf

Звіт ПФР Мальти за 2023 рік

Звіт "Annual Report 2023" від ПФР Мальти (FIAU) надає детальний огляд діяльності, досягнень та стратегічних ініціатив організації протягом року. Основна мета FIAU - захист фінансової системи Мальти від відмивання грошей і фінансування тероризму. Звіт охоплює різні аспекти діяльності FIAU, включаючи аналіз підозрілих транзакцій, нагляд за дотриманням законодавства з ПВК/ФТ/ФР, заходи з забезпечення виконання законів, а також міжнародні та внутрішні взаємодії.

Ключові висновки

Збільшення кількості STR/SAR: У 2023 році FIAU отримала 9,157 STR/SAR, що на 5% більше порівняно з 2022 роком. Це свідчить про зростаючу обізнаність та відповідність вимогам з боку суб'єктів.

Підвищення якості звітів: Спостерігається покращення якості звітів, зокрема збільшення кількості звітів, які включають більше однієї фізичної або юридичної особи. Це вказує на більш детальне та комплексне звітування.

Секторні звіти: Основні підозріли діяльності були пов'язані з електронними грошовими установами, казино та компаніями, що надають фінансові послуги, де спостерігається значне зростання кількості звітів.

Міжнародна співпраця: FIAU активно співпрацювала з міжнародними партнерами, підписавши чотири меморандуми про взаєморозуміння та організувавши 19 ініціатив у рамках публічно-приватного партнерства.

Навчання та розвиток: У 2023 році FIAU провела навчання з питань AML для понад 3,700 осіб та опублікувала дев'ять документів з рекомендаціями, спрямованих на підвищення обізнаності та відповідності вимогам.

Технологічні покращення: FIAU інвестувала у вдосконалення технологічних можливостей, включаючи впровадження системи CASPAR для більш ефективного збору та аналізу даних.

Підтримка прозорості: Було зроблено значні кроки для забезпечення прозорості, включаючи запуск оновленого веб-сайту та публікацію результатів тематичних оглядів для підзвітних суб'єктів.

Ризик-орієнтований підхід: FIAU продовжує застосовувати ризик-орієнтований підхід до нагляду та контролю за дотриманням ПВК/ФТ, що дозволяє ефективніше розподіляти ресурси та швидко реагувати на виникаючі загрози.

Цей звіт демонструє відданість FIAU своїй місії та підкреслює важливість співпраці між національними та міжнародними партнерами для забезпечення фінансової безпеки та запобігання фінансовим злочинам.

https://fiaumalta.org/app/uploads/2024/07/AnnualReport_2023_.pdf

Розкриття інформації про експозицію щодо криптоактивів

Базельський комітет банківського нагляду (BCBS) завершив розробку свого стандарту щодо експозиції до криптоактивів (DIS55) після періоду консультацій у жовтні 2023 року. Використовуючи типову таблицю розкриття інформації та шаблони, цей стандарт запроваджує мінімальні вимоги до розкриття інформації щодо експозиції банків до криптоактивів. Метою забезпечення прозорості для учасників ринку є посилення ринкової дисципліни та зменшення інформаційної асиметрії.

Завершений стандарт зберігає структуру, запропоновану в консультативному документі, з таблицею якісного розкриття інформації та кількісними шаблонами для токенізованих традиційних активів і криптоактивів. На основі відгуків зацікавлених сторін було внесено деякі зміни, зокрема коригування критеріїв класифікації, показників ризику та певних вимог до розкриття інформації. Терміном введення в дію визначено 1 січня 2026 року.

Наслідки для компаній:

Підвищена прозорість: банки повинні надавати більш детальну інформацію про свої криптоактиви, включаючи якісну інформацію про методи управління ризиками та кількісні відомості про типи та обсяги криптоактивів.

Посилений контроль: така підвищена прозорість, швидше за все, призведе до більшого контролю з боку інвесторів, регуляторів і громадськості, що потенційно вплине на репутацію банків і ринкову оцінку. Банки повинні бути готові до такої посиленої перевірки та гарантувати, що їх розкриття інформації є точним і повним.

Операційні коригування: банки повинні адаптувати свої внутрішні процеси та системи, щоб збирати та повідомляти необхідні дані точно та послідовно. Це вимагатиме негайних дій, додаткових ресурсів та інвестицій для забезпечення відповідності стандарту.

Зосередженість на управлінні ризиками: стандарт наголошує на практиці управління ризиками для криптоактивів, спонукаючи банки до подальшого розвитку своїх можливостей у цій сфері, щоб забезпечити дотримання вимог і зменшити потенційні ризики.

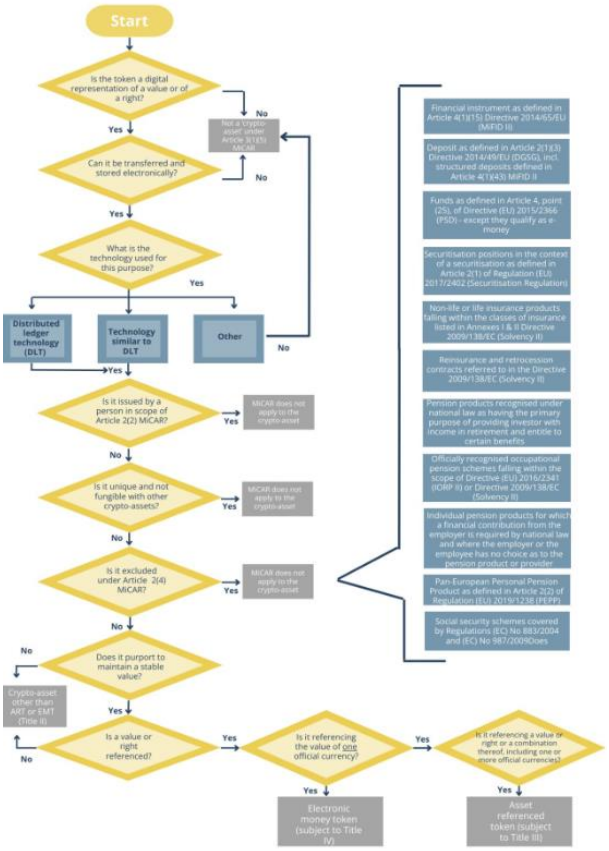
Конкурентний ландшафт: стандартизоване розкриття інформації може вирівняти умови для банків із експозицією до криптоактивів, що полегшить порівняння та потенційно вплине на конкуренцію на ринку.

Загалом впровадження DIS55 означає значний крок до більшого регуляторного нагляду та прозорості у взаємодії банківського сектора з криптоактивами. Банки повинні активно адаптуватися до цих нових вимог щодо розкриття інформації, щоб зберегти довіру та орієнтуватися в нормативному ландшафті, що розвивається.

https://www.bis.org/bcbs/publ/d580.htm

РЕГУЛЮВАННЯ

Класифікація активів відповідно до MiCA



MiCA.

http://surl.li/xivlju

Три європейські наглядові органи (EBA, EIOPA та ESMA – ESA) опублікували консультаційний документ щодо Рекомендацій у рамках регулювання ринків криптоактивів (MiCA), встановлюючи шаблони для

➞пояснення та юридичних висновків щодо класифікації криптоактивів разом із стандартизованим тестом для сприяння спільному підходу до класифікації в таких випадках:

❖ Токени, пов'язані з активами (ARTs): white paper для випуску ART, який містить вичерпну інформацію про криптоактив, має супроводжуватися юридичним висновком, який пояснює класифікацію криптоактиву – зокрема, факт того, що це не токен е-грошей (EMT) і не криптоактив, який можна вважати виключеним зі сфери дії MiCA

❖ Криптоактиви, які не є ART або EMT відповідно до MiCA: white paper для криптоактиву повинен супроводжуватися поясненням класифікації криптоактиву – зокрема, той факт, що він не є EMT, ART або криптоактивом, який виключений зі сфери дії

Глобальний ринок Абу-Дабі (ADGM) вводить в дію нові правила щодо інформаторів, щоб покращити практику фінансового ринку

ADGM, міжнародний фінансовий центр столиці ОАЕ, оголосив про публікацію своєї системи інформаторів, скоординованої ініціативи між органами ADGM для підтримки прозорості, підзвітності та цілісності ринку. Система, яка є частиною прогресивного бізнес-середовища ADGM, доповнює існуючу нормативну базу та охоплює:

- Спеціальні нормативні акти, які визнають і захищають добросовісне «розкриття захищеної інформації».
- Наявність внутрішніх і зовнішніх каналів для повідомлення про обґрунтовані підозри в порушенні законодавства ADGM або скоєнні фінансових злочинів.
- Захист анонімного добросовісного повідомлення про обґрунтовану підозру в неправомірній поведінці.
- Захист від помсти, інтегрований в існуючі правила зайнятості, щоб захистити працівників усіх організацій ADGM від помсти за те, що вони надають інформацію.
- Вимоги до ефективного врядування для підтримки інформаторів з усіх організацій ADGM.
- Письмові правила та процедури для фірм, які мають ліцензію FSRA, ВНУП і великих організацій ADGM.

До 31 травня 2025 року установи центру введуть пропорційні заходи для підтримки ефективного інформування. Ці угоди мають бути оформлені в письмовій формі компаніями, які перевищують певний розмір або несуть додаткові ризики фінансових злочинів.

https://adgmen.thomsonreuters.com/rulebook/11-july-fsra-rules-whistleblowing

https://adgmen.thomsonreuters.com/rulebook/11-july-amendments-legislation-whistleblowing

Законодавча пропозиція щодо впровадження режиму регулювання для емітентів стейблкойнів у Гонконгу

Важливе оновлення у світі стейблкоїнів. Сьогодні Монетарне управління Гонконгу (HKMA) і Бюро фінансових послуг та казначейства (FSTB) опублікували свою відповідь на консультації щодо стейблкоїнів, які почалися ще в грудні. В рамках консультації було отримано відповіді від понад 100 зацікавлених сторін, у тому числі представників крипто- та банківської індустрії, які ляжуть в основу законодавчих змін, щоб створити нормативну базу для стейблкоїнів.

Ось деякі основні моменти документу:

- ✓ Регуляторний режим зосереджуватиметься на представленнях вартості, які базуються на мережах, що діють децентралізовано, тобто на тих, які працюють на основі технології децентралізованої розподіленої мережі або подібної
- ✓ Визначення «стейблкоїна на основі фіатних валют» (FRS) включатиме як стейблкоїни, які базуються на одній валюті, так і ті, що базуються на кількох.
- ✓ Хоча в найближчій перспективі немає планів поширити сферу регулювання на стейблкоїни, які основані не на фіатних валютах - наприклад, ті, що базуються на товарах, - регуляторам буде надано гнучкість, необхідну для введення інших типів стейблкоїнів до режиму регулювання у майбутньому, якщо вони визнають, що це необхідно ✓
- ✓ Режимом ліцензування керуватиме HKMA і застосовуватиме не лише до зареєстрованих у Гонконгу емітентів FRS, але й до будь-кого, хто пропонує стейблкоїн, що буде оснований на HKD, на ринку Гонконгу з-за меж Гонконгу, або будь-кого, хто активно просуває випуск стейблкоїнів для споживачів у Гонконгу.
- ✓ Передумови для отримання ліцензії включатимуть те, що емітент повинен продемонструвати: 1) повне резервне забезпечення; 2) адекватний, ризик-орієнтований склад високоякісних інвестицій, що використовуються як резерви; 3) відокремлення та безпечне зберігання резервних активів; 4) наявність засобів контролю для моніторингу та управління ризиками; 5) вимоги до розкриття інформації та звітності
- ✓ Від емітентів також очікується, що вони принаймні раз на рік будуть проводити оцінку ризиків своєї системи FRS
- ✓ Очікується, що емітенти дотримуватимуться вимог ПВК/ФТ, включаючи здійснення моніторингу транзакцій та забезпечення комплаєнсу Travel Rule. HKMA використовуватиме заплановану пісочницю емітентів стейблкоїнів для отримання відгуків від емітентів щодо проблем, з якими вони можуть зіткнутися під час виконання цих вимог.

Хоча для завершення законодавчих і регуляторних змін знадобиться час, завершення консультацій є критично важливим кроком на шляху Гонконгу до створення надійної основи для регулювання криптоактивів, а разом із розгортанням його пісочниці емітентів стейблкоїнів має потенціал для позиціонування Гонконгу. як лідера у сфері криптоінновацій в регіоні APAC.

https://www.hkma.gov.hk/eng/news-and-media/press-releases/2024/07/20240717-3/

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Стратегія глобальної боротьби з організованою злочинністю: інтеграція та співпраця

Звіт "Intersections: Building Blocks of a Global Strategy Against Organized Crime" від Global Initiative досліджує комплексний підхід до боротьби з організованою злочинністю на глобальному рівні. Дослідження аналізує важливість міжнародної співпраці, інтеграції даних та розробки спільних стратегій для протидії різним формам злочинної діяльності, таким як торгівля наркотиками, контрабанда людей, корупція та екологічні злочини.

Нелегальні ринки:

- Організована злочинність процвітає через попит на нелегальні товари та послуги, експлуатуючи людей, тварин та довкілля.

Управління:

- Корупція перешкоджає ефективній діяльності правоохоронних органів і урядів, дозволяючи злочинним угрупуванням проникати у політичні інституції та використовувати їх.

Геополітика:

- Державні органи використовують свою владу та корупцію для участі у незаконних діях і співпрацюють із злочинними групами для досягнення політичних цілей, дестабілізуючи міжнародні відносини.

Довкілля:

- Злочинність посилює кліматичні та ресурсні проблеми, що негативно впливають на глобальні ресурси та здоров'я людини.

Насильство та нестабільність:

- Насильство є інструментом для встановлення контролю над незаконними ринками, а також для створення атмосфери страху та тиску на громади.

Вразливі групи населення:

- Недорозвиненість міських районів і сільських громад робить їх більш вразливими до злочинної діяльності.

Інфраструктура:

- Незаконні товари та послуги використовують ті ж транспортні мережі, що й законний бізнес, що ускладнює їх виявлення.

Таємні юрисдикції та фінансові злочини:

- Офшорні зони використовуються для відмивання коштів, що позбавляє уряди ресурсів на фінансування громадських послуг і безпеки.

Технології:

- Цифрові технології надають нові можливості як для злочинців, так і для правоохоронних органів, дозволяючи комунікацію, переміщення коштыв і експлуатацію вразливих осіб.

Звіт також наголошує на важливості залучення громадянського суспільства та приватного сектора до боротьби з організованою злочинністю. Він підкреслює необхідність врахування глобальних трендів, таких як цифровізація та глобалізація, що змінюють функціонування злочинних мереж. Для ефективної боротьби необхідний розвиток механізмів обміну інформацією між країнами та міжнародними організаціями, що дозволить швидко реагувати на нові виклики та загрози.

Результати дослідження показують, що інтеграція нових технологій та посилення міжнародної співпраці є ключовими для ефективного протидії організованій злочинності. Рекомендації звіту включають посилення правозастосування, зміцнення судової системи та впровадження технологічних рішень для моніторингу злочинної діяльності. Звіт також акцентує увагу на необхідності створення сприятливих умов для співпраці між державами та залучення приватного сектору для спільної боротьби зі злочинністю.

http://surl.li/wwkody

Регуляторні технології (RegTech) та сучасний банківський сектор: Прогнози на 2024 рік

Дослідження аналізує роль регуляторних технологій (RegTech) у сучасному банківському секторі, підкреслюючи важливість адаптації фінансових установ до змін у регуляторному середовищі та використання новітніх технологій для оптимізації процесів дотримання нормативних вимог.

Основні виклики, з якими стикаються банки, включають зростаючі обсяги шахрайства, фінансових втрат, високі витрати на дотримання вимог і складне регуляторне середовище. RegTech пропонує інноваційні рішення для автоматизації та спрощення процесів дотримання вимог, управління ризиками та звітності. Застосування штучного інтелекту (AI) та машинного навчання (ML) допомагає банкам автоматизувати моніторинг транзакцій, виявлення шахрайства та звітність, що дозволяє зменшити витрати, підвищити ефективність та знизити ризики.

Зокрема, RegTech допомагає банкам швидше адаптуватися до змін у законодавстві, забезпечуючи своєчасне оновлення внутрішніх політик і процедур. Це також включає використання передових аналітичних інструментів для аналізу великих обсягів даних, що дозволяє виявляти підозрілі транзакції та оцінювати ризики в режимі реального часу. Крім того, RegTech рішення дозволяють банкам краще управляти комплаєнсом, знижуючи навантаження на співробітників і мінімізуючи людський фактор у процесах дотримання нормативних вимог.

У дослідженні також обговорюються перспективи подальшого розвитку RegTech у 2024 році, включаючи інтеграцію з іншими фінансовими технологіями (FinTech), розширення використання блокчейну для забезпечення прозорості та безпеки, а також впровадження нових стандартів і протоколів для обміну даними між фінансовими установами та регуляторами. Ці інновації сприятимуть створенню більш гнучкої та стійкої фінансової системи, здатної ефективно реагувати на виклики майбутнього.

https://thl.com/articles/regulatory-technology-and-modern-banking-a-2024-outlook/

Чому Нідерланди залишаються податковою гаванню: аналіз сучасних тенденцій та викликів

Стаття від SOMO досліджує, чому Нідерланди залишаються міжнародним центром для фінансових потоків, незважаючи на заходи уряду щодо боротьби з ухиленням від сплати податків.

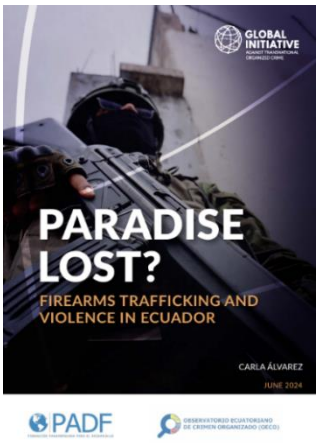
Нідерланди, разом з Люксембургом, складають понад 50% всіх прямих іноземних інвестицій в ЄС, більшість з яких є "фантомними інвестиціями" - інвестиціями без зв'язку з реальною економікою. Ці інвестиції переважно здійснюються через "поштові скриньки" - пусті компанії, які є частиною багатонаціональних корпорацій і служать для перенаправлення прибутків у країни з низькими податковими ставками.

За останні три роки значно зросли доходи від фінансових потоків, що проходять через Нідерланди, незважаючи на спроби уряду скоротити ці потоки. Це призводить до втрати доходів для багатьох країн, особливо країн Глобального Півдня. Стаття підкреслює, що незважаючи на деякі реформи, такі як введення податку на роялті та процентні платежі, заходи уряду все ще недостатні для значного зменшення обсягів "фантомних інвестицій".

Одним із запропонованих рішень є введення стандартних податків на доходи, що може допомогти скоротити ухилення від сплати податків. Крім того, для розуміння причин високих фінансових потоків через "поштові скриньки" необхідно більше даних про їхнє походження та призначення. Автори закликають до більш прозорої та суворої політики, яка могла б значно скоротити можливості для податкових схем.

https://www.somo.nl/the-netherlands-still-a-tax-haven/

Торгівля вогнепальною зброєю та насильство в Еквадорі



Еквадор стикається з безпрецедентним сплеском насильства і злочинності, ставши однією з найбільш кримінальних країн у світі. За останні роки рівень смертей через насильство в країні досяг 47,25 на 100 тисяч населення, що у вісім разів вище, ніж у 2016 році.

Основною причиною цієї кризи є стрімке зростання торгівлі вогнепальною зброєю. Зброя посилює діяльність кримінальних організацій, що займаються наркотрафіком та нелегальним видобутком корисних копалин, і слугує інструментом для встановлення територіального контролю.

З 2020 року рівень вбивств майже щорічно подвоюється, перевищуючи регіональні та глобальні середні показники. Основними жертвами є молоді чоловіки, але також спостерігається зростання кількості жертв серед жінок, зокрема 321 випадок у 2023 році, 37% з яких були скоєні із використанням вогнепальної зброї. Це зростання насильства значною мірою пояснюється послабленням законодавчих регулювань щодо імпорту, виробництва, торгівлі та носіння вогнепальної зброї, що сталося на тлі інституційних слабкостей, корупції у секторах безпеки та громадського тиску.

Звіт досліджує зв'язки між торгівлею зброєю, змінами у регуляторній політиці, зростанням злочинності та насильства в Еквадорі. Він аналізує типи вогнепальної зброї, що використовується у країні, їх походження, вартість та маршрути контрабанди. Звіт завершується терміновими рекомендаціями щодо боротьби з торгівлею зброєю через національні та регіональні стратегії, які спрямовані на розрив поточного циклу насильства та ослаблення кримінальних організацій.

http://surl.li/xmegrl

ДАЙДЖЕСТ ФІНАНСОВИХ ЗЛОЧИНІВ

"Financial Crime Digest" за червень 2024 року виданий компанією Aperio Intelligence, що спеціалізується на корпоративній розвідці та аналізі фінансових злочинів. Випуск зосереджується на аналізі глобальних тенденцій у боротьбі з фінансовими злочинами, нових законодавчих ініціативах та випадках викриття злочинних схем.

Ключові теми:

1. **Санкції Великобританії та ЄС**: Нові санкції проти Росії спрямовані на руйнування військових постачань та фінансових систем, включаючи замороження активів та заборону на постачання зброї.
2. **Торгівля людьми в Румунії**: Інтерв'ю з виконавчим директором eLiberare Лореданою Урзіцею-Міреєю висвітлює труднощі та тенденції у боротьбі з торгівлею людьми, включаючи зростання онлайн-рекрутингу та експлуатації дітей.
3. **Шахрайство з літніми людьми**: Аналіз складних схем шахрайства, спрямованих на літніх людей у США, які призвели до значних фінансових втрат.
4. **Тіньовий банкінг в Ірані**: Санкції США проти мереж, які сприяють фінансовим транзакціям для іранських військових та терористичних організацій, включаючи використання прикритих компаній.
5. **Антикорупційна директива ЄС**: Новий закон ЄС встановлює мінімальні стандарти для визначення та санкціонування корупційних правопорушень у публічному та приватному секторах.
6. **Звіт про торгівлю людьми**: Державний департамент США опублікував звіт за 2024 рік, який висвітлює статистику та тенденції у сфері торгівлі людьми в усьому світі.
7. **Звіт Moneyval про Угорщину**: Покращення заходів Угорщини проти відмивання грошей, особливо щодо віртуальних активів.
8. **Результати EMPACT**: У 2023 році під час операцій EMPACT в ЄС було конфісковано понад 797 мільйонів євро та затримано понад 13,800 осіб, причетних до організованої злочинності.
9. **Звіт OAE про боротьбу з відмиванням грошей**: Перший річний звіт OAE про заходи протидії відмиванню грошей та фінансуванню тероризму, включаючи збільшення кількості підозрілих транзакцій.
10. **Оновлення ESG (екологічні, соціальні та управлінські питання)**: Нові тенденції та ініціативи у сфері ESG, що включають екологічну та соціальну відповідальність компаній.

https://www.aperio-fcd.com/fcd-monthly?report_id=88

Стан справ із платежами в ОАЕ

Звіт "Стан платежів в ОАЕ" досліджує різні аспекти платіжної екосистеми Об'єднаних Арабських Еміратів (ОАЕ), відзначаючи значний економічний розвиток та інновації в фінансовому секторі країни. **Звіт демонструє значний розвиток платіжної екосистеми ОАЕ, що обумовлено регуляторною підтримкою, технологічними інноваціями та зростанням фінансових інституцій**. Відзначено стрімке зростання як роздрібних, так і великих платіжних систем, що підкреслює важливість інвестицій у покращення платіжної інфраструктури для підтримки економічного зростання країни.

Ключові висновки

1. Зростання доходів платіжного сектора:

- Очікується, що до 2027 року загальний дохід платіжного сектора в ОАЕ досягне $19.8 мільярдів з річним середнім темпом зростання (CAGR) у 3.6%.

2. Різноманіття учасників ринку:
   - Платіжний ринок ОАЕ складається з урядових ініціатив, банківських інновацій, міжнародних компаній (Visa, Mastercard, Amazon Payment Services) та місцевих фінтех-стартапів (NymCard, Tabby).
3. Сильна інфраструктура та регуляторна підтримка:
   - Центральний банк ОАЕ відіграє ключову роль у регулюванні та ліцензуванні платіжних систем, що сприяє зростанню кількості ліцензованих платіжних компаній, зокрема, роздрібних платіжних сервісів та систем зберігання вартості.
4. Значне зростання цифрових платежів:
   - Система миттєвих платежів (IPI) зазнала різкого зростання транзакцій з 2.4 мільйона в 2019 році до 64.1 мільйона в 2023 році.
5. Зростання великих платіжних систем (LVPS):
   - Великі платіжні системи (LVPS) домінують за вартістю транзакцій, обробляючи 17.16 трильйона AED в 2023 році, що становить 89.75% від загальної вартості транзакцій.

Глобальний звіт про фінансування тероризму

Звіт "Global Terrorist Financing Report" досліджує глобальні тенденції та методи фінансування тероризму. Звіт аналізує різні аспекти фінансування тероризму, включаючи джерела коштів, фінансові інструменти, що використовуються, та міжнародні зусилля з боротьби з цією проблемою. Основна мета документа — надати всебічний огляд проблематики фінансування тероризму та рекомендації для посилення глобальної безпеки.

Ключові висновки

1. **Джерела фінансування тероризму:**
   - Терористичні групи використовують різноманітні джерела фінансування, включаючи незаконний обіг наркотиків, торгівлю людьми, викрадання з метою викупу, контрабанду товарів та зброї, а також пожертвування від симпатиків.
2. **Фінансові інструменти:**
   - Готівка залишається основним засобом фінансування, але все більшої популярності набувають цифрові валюти, такі як криптовалюти, завдяки їх анонімності та складності відстеження.
3. **Використання небанківських фінансових установ:**
   - Терористичні організації часто використовують небанківські фінансові установи, такі як обмінні пункти та неофіційні системи переказів коштів (наприклад, хавала), для уникнення контролю з боку офіційних фінансових установ.
4. **Технологічні виклики:**

- Розвиток фінансових технологій (FinTech) створює нові виклики для правоохоронних органів, оскільки терористи можуть використовувати нові платформи для анонімних та незареєстрованих фінансових операцій.

5. **Необхідність міжнародної співпраці:**

   - Ефективна боротьба з фінансуванням тероризму вимагає тісної співпраці між країнами, обміну інформацією та координації зусиль на глобальному рівні.

Рекомендації

✓ **Покращення правового регулювання:** Розробка та впровадження чітких нормативно-правових актів для моніторингу та запобігання фінансовим операціям, що пов'язані з терористичною діяльністю.

✓ **Посилення фінансового контролю**: Застосування більш жорстких заходів контролю над небанківськими фінансовими установами та цифровими валютами.

✓ **Міжнародна співпраця:** Підвищення рівня співпраці та обміну інформацією між міжнародними та національними організаціями для ефективного відстеження та припинення фінансових потоків, пов'язаних з тероризмом.

✓ **Впровадження новітніх технологій**: Використання передових технологій для відстеження фінансових операцій та виявлення підозрілих транзакцій.

Цей звіт слугує важливим джерелом інформації для урядів, міжнародних організацій та правоохоронних органів у їх зусиллях з боротьби проти фінансування тероризму.

https://newsletter.insightthreatintel.com/p/global-terrorist-financing-report-86d

Огляд технологічних трендів 2024 від McKinsey

Звіт "Technology Trends Outlook 2024" від McKinsey & Company досліджує основні технологічні тренди, які формують майбутнє індустрій та бізнесу в усьому світі. Цей звіт надає важливі інсайти та рекомендації для бізнес-лідерів, які прагнуть залишатися на передовій технологічних інновацій та забезпечувати стале зростання своїх компаній.

Ключові висновки

1. **Зростання інтересу до генеративного ШІ:**

   - Інтерес до генеративного ШІ зростає, що відобразилося на збільшенні інвестицій у сім разів, зокрема у сфері текстової та візуальної генерації. Моделі генеративного ШІ, такі як OpenAI GPT-4, інтегруються у різні програмні інструменти для підвищення ефективності бізнесу.

2. **Електрифікація та відновлювані джерела енергії:**

   - Цей тренд показав найвищі показники інвестицій та інтересу серед усіх досліджених трендів, підкріплений зростанням глобальної потужності відновлюваної енергії та підвищеною енергетичною безпекою.

3. **Зниження інвестицій в технології:**

   - Незважаючи на загальне зниження інвестицій в технології на 30-40% у 2023 році, довгострокова перспектива залишається позитивною, оскільки підприємства продовжують інвестувати в інновації.

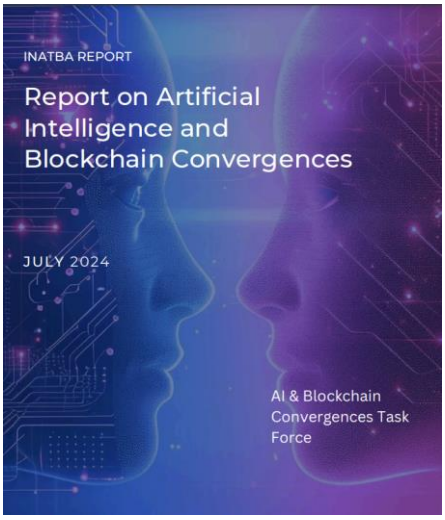
4. **Попит на технічні навички:**

- Незважаючи на значні звільнення у технічному секторі, попит на навички, пов'язані з генеративним ШІ та електрифікацією, залишався високим.

5. **Розвиток індустріалізації машинного навчання (MLOps):**
   - Індустріалізація машинного навчання стає все більш важливою, забезпечуючи ефективне масштабування рішень ШІ в бізнесі.
6. **Прогрес у впровадженні нових технологій:**
   - Технології, такі як квантові обчислення, робототехніка та біоінженерія, продовжують розвиватися, хоча їх впровадження вимагає значних інвестицій та спеціалізованих навичок.

https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech

Доповідь про штучний інтелект і конвергенції блокчейнів



Звіт "Report on Artificial Intelligence and Blockchain Convergences" досліджує **можливості та виклики конвергенції технологій штучного інтелекту (ШІ) та блокчейну.** Звіт охоплює історичний розвиток обох технологій, їхні незалежні досягнення та потенціал синергетичного поєднання. Основна мета документа — вивчити, як ці технології можуть взаємодіяти для створення більш безпечних, прозорих та ефективних рішень у різних галузях, таких як децентралізовані фінанси (DeFi), метавсесвіт, стійкість та автентичність продуктів, а також охорона здоров'я.

Ключові висновки

1. **Синергетичний потенціал ШІ та блокчейну:**
   - Поєднання ШІ та блокчейну дозволяє підвищити прозорість, безпеку та ефективність, що особливо важливо для децентралізованих фінансів, де ШІ може оптимізувати торгові стратегії, а блокчейн забезпечує безпеку та прозорість транзакцій.
2. **Виклики та рішення:**
   - Серед основних викликів — забезпечення конфіденційності даних, управління правами на дані та захист від дезінформації. Блокчейн може допомогти вирішити ці проблеми, забезпечуючи прозорі аудиторські сліди, контроль доступу до даних та механізми підтвердження достовірності інформації.
3. **Етичні, соціальні та управлінські аспекти:**
   - Важливо розглядати питання етики, соціальної відповідальності та управління в контексті впровадження ШІ та блокчейну. Звіт наголошує на необхідності розробки чітких нормативних актів та стандартів для забезпечення відповідального використання цих технологій.
4. **Практичні застосування:**
   - Звіт наводить приклади реальних застосувань, таких як використання ШІ для покращення алгоритмів торгівлі в DeFi, створення цифрових двійників для моніторингу та управління критичними активами, а також впровадження блокчейну для забезпечення автентичності та прозорості у ланцюжках постачання.
5. **Майбутні перспективи:**

- Конвергенція ШІ та блокчейну має значний потенціал для трансформації різних секторів економіки та суспільства. Майбутні дослідження та інновації в цій галузі сприятимуть розвитку нових моделей бізнесу, підвищенню ефективності та стійкості, а також покращенню управління даними.

Звіт підкреслює важливість глобальної співпраці, обміну знаннями та розвитку інноваційних рішень для досягнення сталого та технологічно розвиненого майбутнього.

https://inatba.org/reports/inatbas-latest-report-on-ai-blockchain-convergences/

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

Даркнет: Історії кіберзлочинів (подкаст "Darknet Diaries")

"Darknet Diaries" - це подкаст, який глибоко занурюється у світ кіберзлочинності, кібербезпеки та темних сторін інтернету.

Кожен епізод розповідає захоплюючі та реальні історії про зломи, кіберзлочини, шахрайства і соціальну інженерію. Наприклад, у останньому епізоді 147 "Tornado" розглядається одне із найбільших цифрових пограбувань, пов'язаних із Axie Infinity і Tornado Cash.

Попередный епізод, 146 "ANOM", висвітлює створення фальшивого безпечного телефону, який використовувався злочинцями, що зрештою призвело до масштабних арештів по всьому світу.

Подкаст також досліджує теми соціальної інженерії, шкідливого програмного забезпечення та фінансових шахрайств, надаючи слухачам детальний огляд методів і мотивів кіберзлочинців. Він часто розкриває складні схеми, використовувані хакерами, і розповідає історії жертв, щоб показати реальний вплив кіберзлочинності. Наприклад, у епізоді "Grand Theft PayPal" слухачі дізнаються, як шахраї крадуть і перепродають акаунти PayPal, а в епізоді "The Spy" розповідається історія про шпигунство в кіберпросторі.

Крім того, "Darknet Diaries" аналізує законодавчі аспекти кібербезпеки, обговорюючи з експертами та правоохоронцями їхні підходи до боротьби з кіберзлочинністю. Це робить подкаст цінним джерелом інформації для тих, хто цікавиться кібербезпекою та хоче зрозуміти, як захистити себе від цифрових загроз.

https://darknetdiaries.com/episode/

Ризики відмивання грошей для корпорацій економічного розвитку

🌟 У цьому захоплюючому відео досліджується роль Корпорацій економічного розвитку (EDC) у схемах відмивання грошей, про яку часто забувають. Якщо ви займаєтесь фінансовими злочинами чи дотриманням нормативних вимог, це відео обов’язкове до перегляду! 🌐💼

💼 Що в цьому епізоді?

- ❖ Визначення та мета корпорацій економічного розвитку 🏢🏗️
- ❖ Ситуація з реального життя, що висвітлює вразливі місця в EDC: справа Джеффрі Чарльза Зандера в Юті 🏝️🕵️‍♂️🔥
- ❖ Реакція галузі: посилена належна перевірка, перевірка відповідності та передові системи моніторингу 🛡️🔍
- ❖ Технологічні досягнення та їх роль у захисті EDC від фінансових злочинів 📄📈

🔍 Чому варто дивитися?

- ▪ Отримайте уявлення про складності та ризики, пов’язані з EDC

- Дізнайтеся про ефективні заходи боротьби з відмиванням грошей у цьому секторі
- Будьте в курсі останніх тенденцій у сфері запобігання фінансовим злочинам

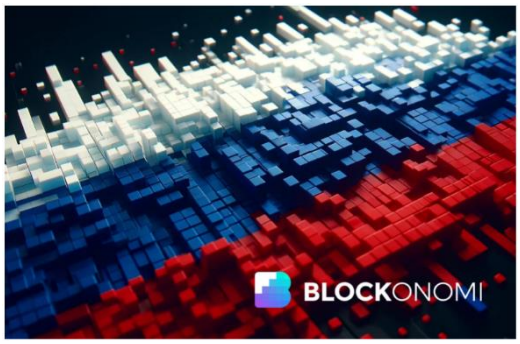
💡 Останні новини галузі:

Технологічний прогрес революціонізує економічний розвиток шляхом підвищення прозорості та прийняття рішень в рамках EDC. Ці зміни мають вирішальне значення для запобігання зловживанням і забезпечення цілісності фінансових систем.

https://www.youtube.com/watch?app=desktop&v=hfDE8ndsgao&feature=youtu.be

ІНШІ НОВИНИ

Росія може легалізувати стейблкоїни для обходу санкцій



Стаття від Blockonomi обговорює можливість легалізації стейблкоїнів (stablecoins) в Росії як засобу обходу міжнародних санкцій та ізоляції від системи SWIFT. Заступник голови Центрального банку Росії Олексій Гузнов заявив, що легалізація стейблкоїнів дозволить громадянам і компаніям проводити міжнародні транзакції, не покладаючись на традиційні фінансові системи. Використання монет, таких як USDT, може забезпечити стабільність і ліквідність для російських користувачів, дозволяючи проводити транзакції з партнерами в інших країнах.

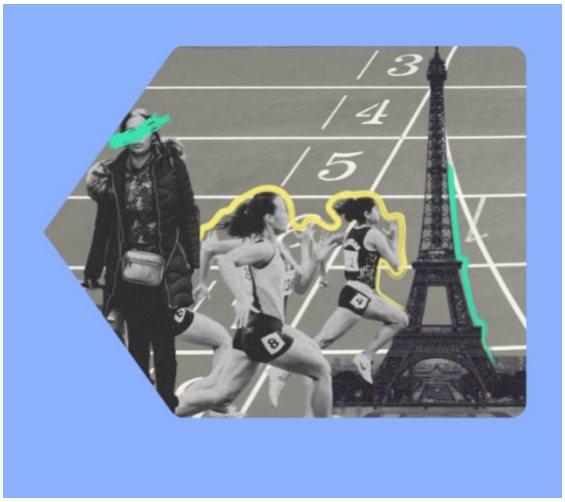
Росія планує використовувати стейблкоїни для проведення міжнародних фінансових операцій без необхідності користуватися традиційними платіжними системами, такими як SWIFT. Легалізація дозволить здійснювати транзакції безпосередньо між російськими підприємствами та їхніми закордонними партнерами, зменшуючи залежність від долара США та інших традиційних валют. Використання стейблкоїнів, прив'язаних до надійних активів, таких як золото, забезпечить стабільність і ліквідність, необхідні для обходу санкційних обмежень.

Президент Володимир Путін підписав закон, який дозволяє використання цифрових фінансових активів (DFAs) для міжнародних платежів. Однак, їх використання залишається обмеженим через низьку ліквідність і побоювання щодо вторинних санкцій. Росія також розглядає можливість використання стабільних монет, прив'язаних до золота, для міжнародних розрахунків, що може допомогти «підірвати домінування долара США у світовій економіці».

У статті також обговорюється ініціатива BRICS Bridge, яку Росія просуває як член організації BRICS. Ця система передбачає використання цифрових валют для транскордонних платежів між країнами-членами BRICS, що може створити альтернативу традиційним фінансовим системам і посилити економічні зв'язки між цими країнами.

https://blockonomi.com/russia-could-legalize-stablecoins-to-break-free-from-sanctions-swift/

Торгівля людьми та Олімпійські ігри в Парижі



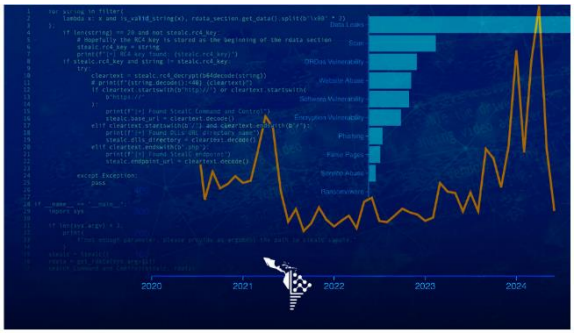
Стаття від STOP THE TRAFFIK висвітлює складну проблему торгівлі людьми у контексті підготовки до Олімпійських ігор у Парижі 2024 року. Великі спортивні події, такі як Олімпіада, часто призводять до зростання попиту на комерційні секс-послуги, що створює сприятливе середовище для експлуатації та торгівлі людьми. Стаття підкреслює важливість підвищення обізнаності серед громадськості, правоохоронних органів і політиків про ризики, пов'язані з торгівлею людьми під час таких подій.

Даркнет відіграє значну роль у сприянні торгівлі людьми, надаючи платформу для вербування та комунікації між злочинцями. Організатори та правоохоронні органи мають посилити моніторинг і контроль, щоб запобігти експлуатації вразливих груп населення. STOP THE TRAFFIK закликає до активних дій, включаючи впровадження превентивних заходів, освітніх кампаній та співпраці з міжнародними партнерами для боротьби з цією глобальною проблемою.

Стаття також наголошує на необхідності розробки ефективних стратегій захисту жертв торгівлі людьми, забезпечення їхньої безпеки та підтримки під час реабілітації. Це включає створення спеціальних центрів допомоги та надання психологічної та юридичної підтримки постраждалим. STOP THE TRAFFIK підкреслює важливість залучення громадських організацій до процесу боротьби з торгівлею людьми, оскільки вони можуть відігравати ключову роль у виявленні та підтримці жертв.

https://stopthetraffik.org/human-trafficking-and-the-paris-olympics/

В Бразилії процвітають випадки викрадення даних з метою отримання викупу



Стаття від Insight Crime досліджує зростання випадків викрадення даних з метою отримання викупу в Бразилії. Кіберзлочинні групи, використовуючи шкідливе програмне забезпечення, як-от троянські програми та програми-вимагачі, атакують фінансові установи та інші організації, викрадаючи дані і вимагаючи викуп за їх повернення. Зокрема, у 2024 році кількість інцидентів з кібербезпеки досягла рекордного рівня, зокрема через групу RansomHub, яка викрадає дані.

Кіберзлочинці використовують різноманітні методи для крадіжки даних, включаючи використання шкідливого програмного забезпечення, що краде логіни і паролі, або програми-вимагачі, які шифрують дані жертви, вимагаючи викуп за їх розшифрування. Унікальність бразильської кіберзлочинної спільноти полягає в тому, що вона активно використовує платформи, такі як Telegram і WhatsApp, для координації своїх дій і вербування нових членів.

Цифрові докази, необхідні для розслідування кіберзлочинів, часто зберігаються у приватного сектору та можуть бути розташовані за межами країни, що ускладнює процес розслідування для правоохоронних органів. Незважаючи на зусилля бразильської влади щодо посилення кібербезпеки, країна все ще залишається уразливою до кібератак.

https://insightcrime.org/news/kidnapping-data-for-ransom-is-a-booming-business-in-brazil/

Фінансовий сектор має складнощі з викликами в контексті ПВК

Нещодавнє опитування PwC показує, що фінансова індустрія Люксембургу насилу встигає за зміною правил з ПВК. Основні висновки підкреслюють труднощі з наймом кваліфікованого персоналу: 44% респондентів із Люксембургу вказали на цю проблему, порівняно з 25% в ЄС.

Крім того, витрати на комплаєнс у Люксембурзі зросли на 18% за останні два роки, що ще більше напружило фінансові установи. Незважаючи на ці виклики, фінансовий сектор Люксембургу повільно впроваджував нові технології: лише 53% розглядають ШІ та лише 13% використовують хмарні рішення, що нижче за середні показники у регіоні EMEA (Європа, Близький Схід та Африка) 81% та 53% відповідно.

Комісія з нагляду за фінансовим сектором (CSSF) підкреслює потребу в сучасних технологіях для посилення заходів з ПВК, зазначаючи, що багато установ все ще покладаються на застарілі системи.

Нещодавні штрафи, включно з 3 мільйонами євро, накладеними на BGL BNP Paribas, підкреслюють прагнення регуляторів до суворішого дотримання вимог.

Щоб вирішити ці проблеми, фінансові установи виступають за універсальні нормативні стандарти для підвищення ефективності ПВК та спрощення процесів відповідності.

http://surl.li/xdbrdp

BaFin закликає страховиків посилити заходи контролю

Федеральне управління фінансового нагляду (BaFin) оголосило про посилення заходів контролю за страховими компаніями для боротьби ВК/ФТ. За словами Карстена Сперла, керівника цього сектору в BaFin, орган посилює виїзні перевірки, особливо для філій іноземних страхових компаній, що працюють у Німеччині.

BaFin також запустив опитувальник для збору інформації про ці філії. Нові виклики включають моніторинг нерегулярних операцій гнучких страхових продуктів і банківських послуг, які пропонують страхові компанії. Сперл рекомендував впровадження передових IT-систем для моніторингу.

Особлива увага приділяється фінансуванню тероризму через виплати бенефіціарам за кордоном та поліси страхування життя. BaFin помітив розбіжності в моніторингу політично значущих осіб і рекомендує щоденні оновлення систем управління портфелем.

Орган продовжує підвищувати обізнаність компаній про ризики та необхідні превентивні заходи, з можливістю застосування санкцій у випадках виявлення недоліків.

http://surl.li/wrdigc

Аргентина прагне приборкати крипторинок, оскільки побоювання щодо відмивання грошей привертають увагу

Уряд Аргентини запровадив новий закон для регулювання ринку криптовалют і зниження ризиків відмивання коштів. З 85,4 мільярдами доларів криптовалютних транзакцій за минулий рік Аргентина стала одним із найбільших у світі крипторинків. Фіскальний пакет, підписаний у середу, включає амністію для осіб, які декларують до $100 000 у криптоактивах, крок, який може послабити тиск з боку FATF. FATF погрожував внести Аргентину в свій сірий список, посилюючи нагляд і потенційно завдаючи шкоди економіці. Аргентина посилила свою боротьбу зі злочинами, пов’язаними з криптовалютою, провівши 64 рейди та 30 арештів. Аргентинські лідери зустрінуться з представниками FATF у Парижі в жовтні для подальших обговорень.

http://surl.li/qortkv

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Швейцарські адвокати та заходи протидії відмиванню коштів

Стаття на платформі Public Eye обговорює важливу проблему, пов'язану з участю швейцарських адвокатів у наданні нетипових консультаційних послуг, які можуть використовуватися для ухилення від податків і відмивання грошей. Наразі у Швейцарії адвокати, які займаються консультаціями щодо створення компаній, фондів і трастів, не зобов'язані дотримуватися вимог Закону про боротьбу з відмиванням грошей (AMLA). Це створює можливості для використання їхніх послуг у незаконних фінансових схемах.

Адвокати часто допомагають у створенні компаній, фондів і трастів, які можуть використовуватися для уникнення податків і відмивання грошей. Стаття підкреслює, що така діяльність адвокатів робить їх ключовими фігурами у фінансових схемах, які можуть приховувати нелегальні кошти.

Під міжнародним тиском Федеральна рада Швейцарії запропонувала зміни до законодавства, що зобов'язали б адвокатів дотримуватися AMLA, включаючи належну перевірку клієнтів і моніторинг підозрілих транзакцій. Однак у 2021 році парламент відхилив цю пропозицію, що викликало занепокоєння серед міжнародної спільноти та організацій, які борються з корупцією.

Існує вагомий заклик до посилення законодавства для зобов'язання адвокатів дотримуватися AMLA, що включає вимоги до належної перевірки клієнтів, моніторингу підозрілих транзакцій та звітності перед відповідними органами. Незважаючи на відхилення пропозиції парламентом, тиск з боку міжнародної спільноти на Швейцарію щодо цього питання продовжується, оскільки існуюча ситуація дозволяє злочинцям користуватися правовими прогалинами.

Стаття підкреслює роль адвокатів як ключових посередників у фінансових схемах, що можуть приховувати незаконні кошти. Вона також наголошує на необхідності реформування швейцарського законодавства для забезпечення більшої прозорості та підзвітності у фінансовому секторі. Це включає запровадження суворіших вимог до адвокатів, що надають консультаційні послуги, для підвищення ефективності боротьби з відмиванням грошей.

http://surl.li/boojtv

Що таке сертифікати відповідності?

Сертифікат відповідності — це документ, який підтверджує виконання певних критеріїв. Це офіційна декларація того, що особа чи організація виконали низку вимог.

Сертифікати відповідності видаються з різних причин, і зазвичай їх готують і підписують офіційні установи. Основною метою запиту на отримання цих сертифікатів є задоволення законної потреби в отриманні дозволу на здійснення діяльності або здійснення господарської операції. Вони досить часті і в інших секторах, наприклад, у сфері нерухомості та комунальних послуг. Коли ріелтор допомагає клієнту у завершенні продажу нерухомості, уряд може вимагати кілька сертифікатів відповідності, щоб забезпечити функціональність і безпеку нерухомості. Вони також можуть бути використані як форма довіри.

Тож, які є найнадійніші сертифікати для працівників у сфері ПВК.

- Сертифікований спеціаліст із боротьби з відмиванням коштів (CAMS)
- Сертифікований спеціаліст із відповідності вимогам банківських установ (CCBCO)

- Сертифікований спеціаліст з безпеки інформаційних систем (CISSP)
- Сертифікат спеціаліста з фінансових злочинів (CFCS).
- Міжнародний диплом ICA з управління, ризиків і відповідності (ICA IDGRC)
- Сертифікований спеціаліст із відповідності та етики (CCEP)

Наявність сертифіката відповідності має кілька переваг, зокрема:

- Демонстрація досвіду: цей сертифікат демонструє, що особа володіє знаннями та навичками, необхідними для запобігання відмиванню коштів і фінансовим злочинам.
- Розширення можливостей кар'єрного зростання: наявність сертифіката відповідності може збільшити можливості працевлаштування особи, зокрема на посадах, пов'язаних із запобіганням відмиванню коштів та фінансовим злочинам.
- Підвищення довіри: сертифікат відповідності підвищує довіру до людини у своїй галузі та може підвищити довіру роботодавців і клієнтів.
- Стимулювання безперервного навчання: процес отримання та збереження сертифіката може спонукати людей постійно вдосконалювати свої знання та навички у своїй галузі.
- Відповідність нормативним вимогам: у деяких галузях, наприклад фінансових послуг, сертифікат відповідності може вимагатися згідно із законом. Володіння сертифікатом відповідності в цих галузях демонструє, що особа відповідає нормативним вимогам і може запобігти штрафам.

4 стовпи AML комплаєнсу

Чотири стовпи комплаєнсу з ПВК є фундаментальними елементами, які фінансові установи та інші підзвітні суб'єкти повинні імплементувати, щоб забезпечити ефективне попередження, виявлення та звітування про діяльність з ВК/ФТ

Ці стовпи формують основу надійної програми з AML комплаєнсу:

📌 ***Внутрішні політики, процедури та контроль :***

- Розробіть та впровадьте комплексну політику та процедури боротьби з відмиванням коштів, які відповідають чинним законам і нормам.
- Встановіть внутрішній контроль для виявлення та запобігання відмиванню коштів.
- Регулярно переглядайте та оновлюйте політики та процедури для усунення нових ризиків і нормативних змін.

📌 ***Визначення відповідального працівника :***

- Призначте кваліфікованого та обізнаного спеціаліста з питань протидії відмиванню коштів, відповідального за нагляд за програмою з ПВК.
- Переконайтеся, що відповідальний працівник має повноваження та ресурси для забезпечення дотримання політик і процедур боротьби з відмиванням коштів.
- Відповідальний працівник має підпорядковуватися безпосередньо вищому керівництву та раді директорів.

📌 ***Постійне навчання працівників :***

- Забезпечуйте регулярні навчальні програми для співробітників щодо законів, нормативних актів і внутрішньої політики з ПВК.
- Переконайтеся, що навчання охоплює виявлення підозрілих дій, процедури звітування та важливість дотримання вимог.
- Пристосовуйте навчальні програми до конкретних ролей і обов'язків співробітників в організації.

📌 ***Незалежний аудит :***

- Проводьте регулярні незалежні перевірки програми з ПВК, щоб оцінити її ефективність і відповідність нормативним вимогам.
- Аудити повинні проводитися кваліфікованими незалежними аудиторами, які не залучені до повсякденної роботи з програмою з ПВК.
- Швидко усувайте будь-які недоліки, виявлені під час перевірок, і вживайте коригувальних заходів.

Дотримуючись чотирьох стовпів, організації можуть створити надійну систему відповідності вимогам ПВК, яка допомагає захистити від ризиків відмивання грошей і фінансування тероризму.

Ключові шлюзи обміну інформацією щодо ПВК/ФТ

Обмін інформацією: за допомогою шлюзу для обміну інформацією для боротьби з ВК/ФТ, про який нещодавно було оголошено відповідно до статті 75 Регламенту ЄС щодо ПВК від 2024 року, відкриваються варіанти та компроміси між розробниками політики щодо боротьби з фінансовими злочинами та лідерами в контексті захисту даних в ЄС.

AML/CTF Information Sharing Key Gateways Compared

	Criteria/Countries - Bloc	European Union	Singapore	United Kingdom	United States
	Privacy / DP Laws & Regs	GDPR 2018	Personal DP Act 2020	UK DP Act/ UK GDPR 2018	Gramm Leach Bliley 1999
1	**Sharing Gateways:**				
1.1	**Legal Gateways:**	Art 75 EU AML Regulation 2024	Part 4 A Section 28 Financial Services & Markets Act 2022	S188/189 Economic Crime Transparency Act 2023	S314(b) Patriot Act 2001
1.2	**Voluntary Sharing:**	✓	✓	✓	✓
2.1	**Purpose:**	✓ AML/CTF (to support Regulatory KYC/CDD Obligations inc SAR Filling)	✓ AML/CTF/CPF (Pilot - Comm Bank, Legal Persons Misuse, TBML, PF)	✓ Economic Crime (Predicate Crimes to ML & TF)	✓ AML/CTF (specified unlawful activities, drugs, human, arms trafficking etc)
3	**Eligible Parties:**				
3.1	Banks & FI's:	✓	✓ Pilot - 6 Banks	✓ (For Indirect only if Large = ECL >£36M p.a. Revenue)	✓
3.2	Other Regulated Entities:	✓	✗	✓ (For Indirect only Large & Law,Account,TCSP,Auction)	✗
4	**Authorisation & Examined:**				
4.1	Registration Only:	✗	✗	✗	✓ (With FinCEN)
4.2	Supervisor/Other Approvals:	✓ (& FIU if SARs shared)	✗ (Approval for COSMIC Pilot Banks by MAS)	✗	✗
4.3	Examination:	✓ Compliance with Reqts	✓ Compliance with Reqts	✓ Compliance with Reqts	✓ Compliance with Reqts
5	**Data Protection Matters:**				
5.1	DP Agency Approval:	✗ (Supervisor consults)	✗	✗	✗
5.2	DP Impact Assessment Reqt:	✓	✗	✓ (Indirect GDPR applies)	✗
5.3	DP Sharing Considerations:	✓ (Sharing for Purpose/Pre Condition/Eligible etc) & security protocols *"incl pseudo anonymisation")*	✓ (Sharing for Purpose/Pre Condition/Eligible/ Confidential etc & "Necessary/Proportionate")	✓ (Sharing for Purpose/Pre Condition/Eligible/ Confidential etc & Indirect GDPR expressly applies)	✓ (Sharing for Purpose/Pre Condition/Eligible/ Confidential/Security, etc)
6.1	**Information to be Shared:** (SAR related, Customer, CDD SOW/SOF & Trnx Data etc)	✓	✓	✓	✓
7	**Pre Condition for Sharing:**				
7.1	Post Suspicion & Action:	✓	✓ (SAR+ e.g. a/c rejected or exit to list on COSMIC)	✓ ("Safeguarding". e.g. exit or a/c limits)	✓
7.2	Post Suspicion e.g. SAR Filed:	✓	✓ (Threshold Criteria/ Higher Risk Factors to (MAS to determine) to request)	✗	✓
7.3	Pre Suspicion but Higher Risk Scenarios/Customers/Trnx's:	✓	✓ (as directly above)	✗	✓
7.4	Pre Suspicion Investigation to Determine Suspicion or not:	✗*	✓ (as directly above)	✗	✓
7.5	No Indications of Concerns:	✗	✗	✗	✗
8	**Partners:**				
8.1	Private Sector (Pv2Pv):	✓ (Direct & Indirect)	✓ (Via COSMIC Only)	✓ (Direct & Indirect)	✓ (Direct & Indirect)
8.2	Public 2 Private & Vice Versa:	✓	✓ (Via COSMIC)	✗**	✗**
9.1	**Domestic/Cross Border:**	✓ (27 EU Members)	✗ (only Singapore)	✗ (only UK)	✗ (only USA)
10.1	**Reliance by Recipient:**	✗ (Independent Decision)	✗ (Independent Decision)	✗ (Independent Decision)	✗ (Independent Decision)

* Potential EU Art 75 Interpretation could enable this type of sharing. ** Alternative Gateways available for public and private information sharing. Copyright Metriqa Ltd/FCN

Цей компроміс має наслідки для TMNL (моніторингу транзакцій у Нідерландах), флагманської ініціативи з обміну інформацією, яка оголосила про підтримку прозорості, але також оголосила, що потрібно буде адаптуватись та згортати операції, які не підтримуються новими правилами та які коштували учасникам значних сум, які на той час підтримував уряд Нідерландів.

Тим не менш, шлюз ЄС потенційно може змінити правила гри, і його можна порівняти з шлюзами в інших країнах: США, Великобританії та Сінгапуру, які зараз мають легальні шлюзи. Кожен по-своєму, хоч і має відмінності, але більшою чи меншою мірою балансує між боротьбою з фінансовими злочинами та конфіденційністю та захистом даних. Те, як ви їх порівнюєте, може більше сказати про те, де ви знаходитесь в контексті боротьбі з фінансовими злочинами та захистом даних, але, яким не було б ваше місце, компроміси для досягнення шлюзів необхідні з обох сторін, що в основному означає повагу до принципу, згідно з яким повинна відбуватися гарна робота з обох сторін.

Порівнюючи ці 4 провідні шлюзи (існує ще декілька шлюзів, наприклад, у Франції, Румунії та Мексиці) і підсумовуючи ключові подібності та відмінності, країни, які обмірковують, як рухатися в цьому напрямку, можуть зосередитися на ключових елементах для визначення можливостей і викликів, а також працювати над досягненням будь-якого можливого консенсусу, щоб дозволити

шлюзам функціонувати з відповідними гарантіями. Це порівняльне резюме містить огляд того, як ЄС, Великобританія, США та Сінгапур підійшли до цього та що наразі працює для них.

Звичайно, настав час для всіх країн мати національні шлюзи з гарантіями конфіденційності/захисту даних для обміну приватною інформацією, і тоді можна буде зосередитися на тому, як об'єднати їх на міжнародному рівні.

Глобальна коаліція для боротьби з фінансовими злочинами підтримує шлюзи з обміну інформацією з моменту свого заснування в 2018 році, і Робоча група експертів працює над завершенням роботи, розпочатої минулого року, яка надасть експертний контекст, думку та рекомендації пізніше цього року щодо пошуку балансу між боротьбою з фінансовими злочинами та надійним захистом даних.

Методи відмивання грошей у ювелірному бізнесі

Ювелірний бізнес надає широкі можливості для відмивання грошей, і злочинці часто використовують комбінацію методів, щоб приховати джерело своїх коштів. Ось кілька поширених методів відмивання грошей, які використовуються в ювелірному бізнесі:

Структурування транзакцій. Злочинці можуть структурувати транзакції, щоб уникнути вимог щодо звітності, як-от внесення кількох невеликих депозитів або покупок, щоб уникнути ініціювання порогових значень для звітності про готівкові операції.

Змішування незаконних коштів із законними: злочинці можуть змішувати незаконні кошти з законними, використовуючи злочинні доходи для придбання законних товарів, наприклад ювелірних виробів, а потім продавати їх за готівку.

Фальшиве виставлення рахунків: злочинці можуть використовувати фальшиві рахунки-фактури, щоб завищити вартість дорогоцінних металів, фактично «відмиваючи» доходи, отримані злочинним шляхом.

Купівля готівкою: злочинці можуть використовувати готівку для придбання цінних предметів, наприклад ювелірних виробів, щоб приховати джерело своїх коштів.

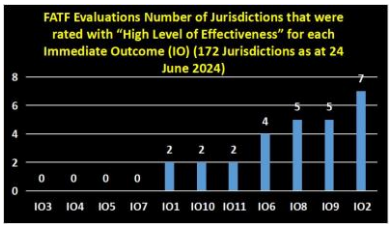
Контрабанда: злочинці можуть незаконно перевозити дорогоцінні метали та камені через кордон для продажу за готівку, фактично «відмиваючи» доходи, отримані злочинним шляхом.

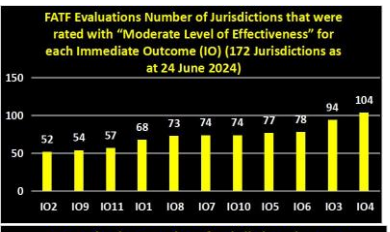
TBML: злочинці можуть використовувати дорогоцінні метали та дорогоцінні камені для торгівлі з іншими у спосіб, який важко відстежити чи виявити.

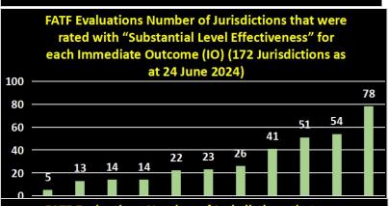
Підприємствам ювелірної промисловості важливо знати про ці поширені методи відмивання грошей і вживати заходів проти відмивання грошей, щоб запобігти їх використанню.

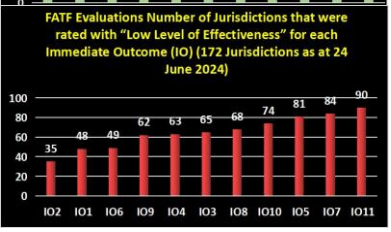
Дані 11 Безпосередніх Результатів

Інфографіка представляє результати оцінки ефективності заходів у боротьбі з відмиванням грошей та фінансуванням тероризму (AML/CFT), проведеної FATF для 172 юрисдикцій станом на 24 червня 2024 року. Дані розподілені за чотирма рівнями ефективності: низький, помірний, суттєвий та високий, по кожному з одинадцяти безпосередніх результатів (Immediate Outcomes, IO).









Висновки

Слабкі місця у системах AML/CFT:

Багато юрисдикцій мають низький рівень ефективності за більшістю показників, особливо за IO11 (забезпечення фінансових санкцій проти фінансування тероризму) та IO7 (відслідковування і стягнення активів злочинців).

Позитивні тенденції:

IO2 (розуміння ризиків та національна політика) має найвищу кількість юрисдикцій з високим та суттєвим рівнем ефективності, що свідчить про добру обізнаність та відповідні національні політики у цих країнах.

Необхідність покращення:

Велику кількість юрисдикцій мають низький або помірний рівень ефективності, що вказує на необхідність значних покращень у системах AML/CFT. Особливу увагу варто звернути на підвищення ефективності у сферах, де показники найнижчі, як-от IO11 та IO7.

Ці дані підкреслюють важливість продовження міжнародних зусиль з покращення заходів боротьби з відмиванням грошей та фінансуванням тероризму, зосереджуючись на слабких місцях та підтримуючи успішні практики.