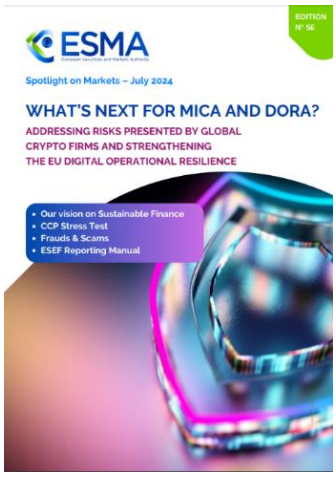
Серійний номер: ДСФМУ-ДК-2024-021
Серпень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Що далі для MiCA та DORA? Управління ризиками, представленими глобальними криптофірмами, та підсилення стійкості цифрових операцій ЄС



Цей документ містить огляд останніх досягнень і оновлень у сфері фінансових ринків, зокрема з боку Європейського управління з цінних паперів та ринків (ESMA). **В ньому висвітлюються основні питання, що стосуються нормативних вимог, цифрової операційної стійкості, а також захисту інвесторів від шахрайства. У фокусі уваги також питання глобальних криптовалютних компаній, які намагаються використовувати свої майданчики для торгівлі активами за межами ЄС, та заходи ESMA щодо посилення нагляду і регулювання для захисту споживачів і забезпечення прозорості ринків**.

Серед ключових тем, порушених у документі, можна виділити **результати стрес-тестування центральних контрагентів, які показали загальну стійкість європейської системи клірингу до основних фінансових ризиків**. Однак були виявлені області, які потребують посилення управління ризиками.

Документ також розглядає ініціативи щодо підвищення цифрової операційної стійкості фінансового сектора ЄС в рамках Акту про цифрову операційну стійкість (DORA). Важливою темою є створення в ЄС системної координаційної структури кіберінцидентів, що мають системне значення, яка дозволить ефективніше реагувати на кіберзагрози, що можуть впливати на фінансову стабільність.

Ще однією важливою темою є консультації щодо оновлень в рамках Регламенту про центральні депозитарії цінних паперів (CSDR), спрямованих на вдосконалення нормативної бази та підвищення прозорості фінансових ринків.

Ключові висновки:

1. **Стійкість європейської системи клірингу:**

У результаті п'ятого стрес-тесту центральних контрагентів (CCPs), проведеного (ESMA, було підтверджено загальну стійкість європейської системи клірингу до суворих фінансових ризиків. Стрес-тест також виявив, що CCPs здатні витримати значні ринкові шоки навіть у випадку дефолту двох найбільших учасників клірингу. Однак були ідентифіковані певні недоліки, особливо щодо концентраційного ризику у різних класах активів, зокрема товарних деривативів. Важливою

новацією цього стрес-тесту стало включення аналізу кліматичних ризиків, що показало різний ступінь готовності CCPs до інтеграції цих ризиків у свої стрес-тестові моделі. Зокрема, ризики переходу до стійкої енергетики мають прямий вплив на ринки, що пов'язані з комунальними послугами і енергетикою.

2. **Ризики, пов'язані з глобальними криптовалютними компаніями:**

ESMA висловлює занепокоєння щодо діяльності глобальних криптовалютних компаній, які прагнуть отримати дозвіл на діяльність у ЄС згідно з регламентом про ринки криптоактивів (MiCA), але при цьому значна частина їхньої діяльності залишається за межами регуляторного нагляду ЄС, зокрема через використання внутрішньогрупових торгових майданчиків за межами ЄС. Така структура бізнесу може створювати нерівні умови конкуренції для компаній, що діють відповідно до європейського законодавства, а також може знизити рівень захисту споживачів. ESMA рекомендує національним компетентним органам уважно оцінювати бізнес-структури таких компаній під час процесу авторизації, щоб уникнути обходу регуляторних вимог MiCA, забезпечуючи тим самим прозорість та порядок функціонування ринків криптоактивів.

3. **Посилення цифрової операційної стійкості фінансового сектора ЄС (DORA):**

В рамках реалізації Закону про цифрову операційну стійкість (DORA) Європейські наглядові органи (ESAs) опублікували другий пакет нормативних продуктів, які включають технічні стандарти, що визначають вимоги до звітності про інциденти, пов'язані з інформаційно-комунікаційними технологіями (ICT), і до тестування на проникнення, що базується на моделюванні загроз. Ці заходи спрямовані на підвищення цифрової операційної стійкості фінансових установ у ЄС, що зрештою має забезпечити безперервне надання фінансових послуг клієнтам та безпеку їхніх даних. Важливим кроком стало запровадження Європейської системної координаційної структури кіберінцидентів (EU-SCICF), яка сприятиме ефективному реагуванню на кіберзагрози, що можуть впливати на фінансову стабільність у межах ЄС.

4. **Підвищення прозорості та ефективності ринків фінансових послуг через консультації щодо перегляду нормативних актів (CSDR, MiFIR):**

ESMA продовжує роботу над вдосконаленням нормативної бази для фінансових ринків ЄС, зокрема через консультації щодо перегляду Регламенту про центральні депозитарії цінних паперів (CSDR) і Регламенту про ринки фінансових інструментів (MiFIR). Ці ініціативи спрямовані на гармонізацію підходів до регулювання, зменшення регуляторного навантаження та підвищення прозорості на ринках. Наприклад, перегляд CSDR спрямований на уточнення та доопрацювання вимог щодо дисципліни розрахунків, зокрема причин невиконання розрахунків, які не можна віднести до вини учасників угоди. Щодо MiFIR, основна увага приділяється підвищенню прозорості ринкових операцій, зменшенню звітного навантаження та підвищенню стійкості систем до можливих ринкових стресів.

Ці висновки підкреслюють важливість продовження зусиль щодо підвищення стійкості, прозорості та ефективності фінансових ринків у ЄС, особливо у світлі зростаючих технологічних викликів і ризиків, пов'язаних з глобальними фінансовими інноваціями, такими як криптоактиви.

https://www.esma.europa.eu/sites/default/files/2024-08/Newsletter_July_2024.pdf

Російські компанії відмивають гроші через платіжні системи Великобританії та ЄС

Transparency International-Russia виявила масштабні порушення в роботі електронних платіжних систем, виявивши, як російські організації відмивають кошти та згодом переказують їх до Великобританії та країн Європейського Союзу. У звіті аналітик Dirty Money Крістін Багдасарян викриває тривожну тенденцію використання фейкових рахунків для незаконних грошових переказів, замаскованих під законні транзакції.

🔍 **Продаж бізнес-рахунків у Darknet:** рахунки, зареєстровані за фальшивими ідентифікаційними даними, продаються в Darknet, що дозволяє користувачам обходити ліміти транзакцій і здійснювати великі перекази, не привертаючи уваги регуляторів.

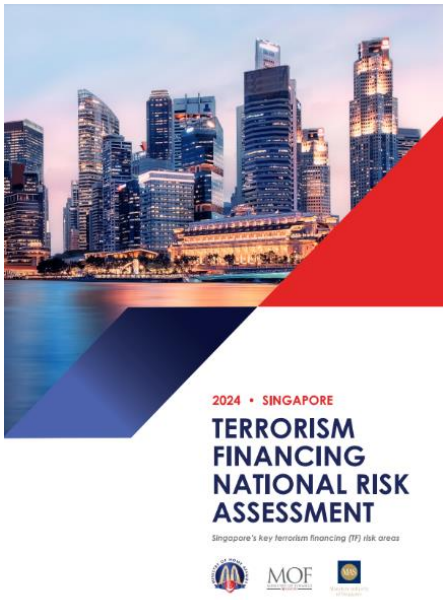
🔸 **Уразливі платформи:** експерти Transparency International проаналізували діяльність Payrow, Paysend, ANNA Business і Gemba Finance. Ці служби особливо сприйнятливі до відмивання коштів через їх складну корпоративну структуру та зв'язки з політично значущими особами (PEP).

🔸 **Використання підроблених документів:** у звіті висвітлюються випадки, коли бізнес-рахунки реєструються за допомогою підроблених документів, що дозволяє зловмисникам приховувати свої справжні особи та легко переміщувати гроші через кордон.

!Незважаючи на регулятивні зусилля, ці схеми продовжують процвітати, що підкреслює необхідність суворішого нагляду та міжнародної співпраці для боротьби з фінансовими злочинами.

https://ti-russia.org/wp-content/uploads/2024/07/unraveling-the-web.pdf

Національна оцінка ризиків фінансування тероризму у Сингапурі за 2024 рік



Документ "Національна оцінка ризиків фінансування тероризму (TF) за 2024 рік" від Сінгапуру аналізує актуальні загрози та вразливості в контексті фінансування тероризму. Звіт оновлює попередню оцінку 2020 року, враховуючи нові глобальні події, включаючи конфлікт між Ізраїлем та ХАМАС, та розвиток цифрової економіки. **Документ висвітлює ключові ризики у фінансових, банківських та інших секторах, які можуть бути використані для фінансування тероризму, та містить рекомендації для посилення контролю та співпраці з міжнародними організаціями**.

Ключові висновки:

1. **Терористичні загрози:** Сінгапур ідентифікує ISIS, Аль-Каїду та Джемаа Ісламія як основні загрози фінансування тероризму. Особливу увагу привертає зростання впливу цих груп через соціальні медіа та можливі наслідки глобальних конфліктів, таких як війна між Ізраїлем і ХАМАС.
2. **Ризики в фінансових і банківських секторах:** Банківський сектор Сінгапуру залишається вразливим через його міжнародний статус і значні потоки капіталу. Хоча прямих доказів використання банків для фінансування тероризму не виявлено, є занепокоєння щодо можливості використання невеликих сум, що важко відрізнити від легальних транзакцій. Зростання цифрових платіжних токенів (DPT) також викликає занепокоєння через анонімність та швидкість транзакцій, що робить їх привабливими для ФТ.

3. **Краудфандинг та онлайн-фінансування:** Документ відзначає зростаючу роль онлайн-краудфандингу як можливого інструменту фінансування тероризму. Після пандемії COVID-19 значно зросла кількість онлайн-фінансових операцій, що відкриває нові можливості для зловживань. Особливу увагу приділено тому, як терористичні організації можуть використовувати онлайн-платформи для збору коштів під виглядом благодійних заходів.
4. **Міжнародне співробітництво та адаптація:** Сінгапур активно співпрацює з міжнародними партнерами, включаючи FATF, для оновлення своїх стратегій боротьби з фінансуванням тероризму. Прийнята стратегія передбачає використання найкращих міжнародних практик і постійне оновлення ризиків на основі новітніх глобальних трендів.
5. **Необхідність підвищення обізнаності:** У документі підкреслюється важливість посилення навчання та підвищення обізнаності серед фінансових установ, неприбуткових організацій та інших зацікавлених сторін для захисту від ризиків фінансування тероризму. Регулятори проводять постійні сесії навчання та надають керівні вказівки для кращого розуміння і управління ризиками.

Ці детальні висновки демонструють необхідність постійного вдосконалення національної стратегії протидії фінансуванню тероризму у відповідь на еволюцію глобальних загроз і розвиток нових технологій.

http://surl.li/vmryzt

Gen-AI: Штучний інтелект і майбутнє роботи

Документ "Gen-AI: Artificial Intelligence and the Future of Work," підготовлений групою дослідників МВФ, аналізує вплив генеративного штучного інтелекту (Gen-AI) на глобальну економіку, особливо на ринки праці. Згідно з документом, ШІ може суттєво змінити трудові ринки, впливаючи на зайнятість у різних країнах по-різному. **В розвинених економіках близько 60% робочих місць піддаються впливу ШІ, з яких половина може отримати вигоду від інтеграції технологій, тоді як інша половина ризикує бути витісненою. У країнах з ринками, що розвиваються, ця частка нижча, що потенційно може збільшити нерівність у доходах між країнами. Важливу роль у адаптації до ШІ відіграватиме рівень підготовленості економік: інфраструктура, навички працівників та наявність регуляторних рамок.** Документ також прогнозує, що ШІ може збільшити нерівність у доходах, особливо в країнах з високим рівнем підготовленості, де високозабезпечені працівники можуть отримати більші вигоди від використання технологій. Для максимізації позитивного впливу AI країнам потрібно адаптувати політики та інвестувати в інфраструктуру, освіту та регуляторні зміни.

Ключові висновки:

1. **Різниця у впливі ШІ на ринки праці:** Розвинені країни мають вищу частку робочих місць, що піддаються впливу ШІ, порівняно з країнами, що розвиваються, що може призвести до поляризованого ефекту — з одного боку, скорочення робочих місць, а з іншого — підвищення продуктивності праці.
2. **Ризик зростання нерівності в доходах:** ШІ може збільшити нерівність у доходах, оскільки високозабезпечені працівники в розвинених економіках отримають більше вигод від ШІ. Однак загальний рівень доходів може зрости для більшості працівників, якщо продуктивність суттєво покращиться.

3. **Підготовленість країн до впровадження ШІ:** Рівень підготовленості економік є ключовим фактором у визначенні впливу ШІ на ринок праці та економіку в цілому. Країни з розвиненою цифровою інфраструктурою та навичками робочої сили мають кращі шанси на успішну інтеграцію ШІ.
4. **Адаптація працівників до ШІ:** Молоді та освічені працівники краще адаптуються до змін, викликаних ШІ, тоді як старші працівники можуть стикатися з великими труднощами при перекваліфікації та працевлаштуванні після втрати роботи через впровадження ШІ.
5. **Необхідність реформ для максимізації вигод:** Для повної реалізації потенціалу ШІ країнам потрібно інвестувати в інфраструктуру, освіту та створювати відповідні регуляторні рамки, які враховуватимуть етичні питання та забезпечуватимуть захист працівників, що зазнають негативного впливу ШІ.

https://www.imf.org/-/media/Files/Publications/SDN/2024/English/SDNEA2024001.ashx

Заява ЄБРР про схильність до ризику

Документ "Risk Appetite Statement 2024" від Європейського банку реконструкції та розвитку (ЄБРР) представляє комплексний підхід банку до управління ризиками. Він містить параметри ризик-апетиту, що визначають рівень ризику, який банк готовий прийняти в різних аспектах своєї діяльності, включаючи фінансові, ринкові, операційні та репутаційні ризики. Заява покликана забезпечити відповідність стратегії банку ринковим умовам, підвищити якість прийняття рішень та зміцнити культуру управління ризиками в організації.

Ключові висновки:

1. **Баланс між ризиком і прибутковістю:**

ЄБРР визначає свій ризик-апетит з метою досягнення балансу між прибутковістю та стійкістю. Це означає, що банк готовий брати на себе певні ризики, але в межах, що дозволяють підтримувати стабільність навіть у стресових умовах. Високий рівень капіталу та ліквідності забезпечує захист від потенційних фінансових шоків і підтримує AAA-кредитний рейтинг банку.

2. **Управління кредитними та ринковими ризиками:**

ЄБРР застосовує ретельні підходи до управління кредитними ризиками, включаючи прискіпливий аналіз позичальників і використання захисних механізмів для мінімізації потенційних втрат. Для ринкових ризиків, зокрема інвестицій у капітал, банк встановлює чіткі межі допустимих втрат, що дозволяє знизити вплив волатильності ринку на фінансовий стан банку.

3. **Фокус на кліматичні ризики:**

ЄБРР приділяє особливу увагу управлінню кліматичними ризиками, враховуючи як фізичні ризики (наприклад, стихійні лиха), так і ризики переходу до низьковуглецевої економіки. Банк активно інвестує в проєкти, спрямовані на пом'якшення впливу змін клімату та сприяння переходу до стійких джерел енергії.

4. **Операційні та репутаційні ризики:**

Операційні ризики, такі як загрози кібербезпеці, шахрайство та управління змінами, є важливими для стабільної роботи банку. ЄБРР також приділяє особливу увагу репутаційним ризикам, розуміючи, що довіра зацікавлених сторін є критично важливою для довгострокового успіху.

Управління репутацією включає підтримку етичних стандартів та прозорості в усіх аспектах діяльності.

5. **Управління модельними ризиками:**

ЄБРР активно використовує математичні моделі для оцінки ризиків, але визнає потенційні небезпеки, пов'язані з неправильними припущеннями або похибками в моделях. Тому банк запроваджує строгі процедури валідації та контролю за моделями, щоб мінімізувати вплив можливих помилок на прийняття рішень. Це підкреслює важливість постійного моніторингу та оновлення моделей для забезпечення їхньої точності та актуальності.

https://www.ebrd.com/corporate-strategy/ebrd-risk-appetite-statement.pdf

Програмованість в оплаті та розрахунках

Документ, підготовлений Міжнародним валютним фондом (МВФ), досліджує концепцію програмованості у системах платежів та розрахунків, а також її потенційні наслідки для фінансових установ та регуляторів. **Програмованість в контексті цих систем описується як здатність виконувати фінансові операції за допомогою комп'ютерних програм, що можуть отримувати доступ до даних системи та виконувати певні функції**. **Автори пропонують структуру, що базується на двох ключових вимірах: зовнішньому програмному доступі (можливості зовнішніх учасників отримувати доступ до системи через код) та внутрішніх програмних можливостях (ступінь, до якого система підтримує та гарантує виконання програм).** Ця структура дозволяє більш детально зрозуміти, як можуть бути розроблені гібридні системи, що поєднують переваги блокчейнів із регуляторними вимогами та більш широким спектром технологій. Документ аналізує ці аспекти, пропонуючи рекомендації для фінансових установ та регуляторів щодо оптимального балансу між інноваціями та управлінням ризиками.

Ключові висновки:

1. **Нереалізований потенціал програмованості:**

Програмованість у системах платежів та розрахунків має потенціал для підтримки ключових політичних цілей, таких як підвищення ефективності, безпеки, інновацій та зниження фрагментації фінансових систем. Незважаючи на активні експерименти з цифровими валютами центральних банків (CBDC) та токенізацією активів, програмованість ще не реалізована повною мірою. Це обумовлено як технічними, так і регуляторними викликами, що потребують подальшого вивчення та вирішення для досягнення оптимального балансу між інноваціями та керуванням ризиками.

2. **Два ключові виміри програмованості:**

Для того щоб повноцінно зрозуміти і оцінити можливості програмованості в контексті платіжних та розрахункових систем, автори пропонують розглядати її через два ключові виміри:

- *Зовнішній програмний доступ*: Це можливість зовнішніх учасників отримувати доступ до даних і функцій системи через програмний код. Відкритість таких систем може

сприяти автоматизації, інтероперабельності та інноваціям, але також створює виклики з точки зору безпеки та управління доступом.

- *Внутрішні програмні можливості*: Це рівень підтримки та гарантованого виконання програм всередині системи. Такі можливості дозволяють автоматизувати фінансові операції на основі певних умов, забезпечуючи більшу гнучкість та ефективність роботи системи.

3. **Гібридні системи як шлях до збалансованої програмованості:**

Більшість сучасних систем платежів та розрахунків знаходяться між крайнощами повністю закритих та повністю відкритих систем. Гібридні системи поєднують в собі елементи як закритих, так і відкритих систем, дозволяючи зовнішнім користувачам отримувати доступ до системи та розширюючи внутрішні можливості в контрольованому середовищі. Такі системи використовують стандартизовані інтерфейси та прозорий доступ, пропонують розширені функціональні можливості та мають спільне управління, що дозволяє краще відповідати потребам фінансового сектору та забезпечувати відповідність регуляторним вимогам.

4. **Роль регуляторів та необхідність координації:**

Впровадження програмованих фінансових платформ потребує тісної координації між фінансовими установами, регуляторами, центральними банками та приватним сектором. Регулятори відіграють ключову роль у розробці стандартів і підходів, які будуть сприяти впровадженню програмованості, забезпечуючи при цьому належне управління ризиками. Координація між різними юрисдикціями та зацікавленими сторонами є важливою для створення гармонізованих підходів до впровадження нових технологій у фінансову систему.

5. **Ризики, пов'язані з програмованістю:**

Програмованість несе в собі ряд технічних ризиків, таких як помилки в програмному забезпеченні, людські помилки, зловмисні дії та навіть потенційні системні збої, що можуть мати серйозні наслідки для фінансових систем. Наприклад, технічні помилки можуть призвести до каскадних збоїв, які можуть поширитися на інші транзакції та системи. У зв'язку з цим необхідно розробити надійні механізми для тестування, аудиту, моніторингу та управління ризиками на етапі проєктування системи.

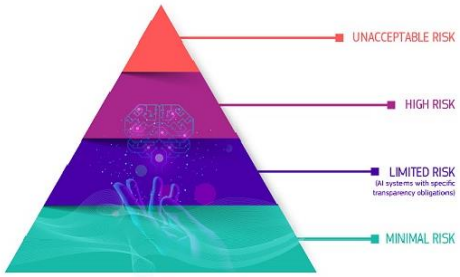
6. **Необхідність міжнародної координації та стандартів:**

Щоб успішно реалізувати потенціал програмованості в глобальних фінансових системах, необхідні міжнародні зусилля щодо розробки загальних концепцій, стандартів та рамок. Спільні зусилля різних країн, фінансових установ та міжнародних організацій дозволять забезпечити кращу координацію, обмін досвідом і оптимізацію впровадження програмованих рішень. Це, в свою чергу, сприятиме розвитку інноваційних екосистем, які відповідатимуть специфічним умовам різних країн та забезпечуватимуть стійкість і безпеку глобальної фінансової системи.

https://www.imf.org/-/media/Files/Publications/WP/2024/English/wpiea2024177-print-pdf.ashx

РЕГУЛЮВАННЯ

Новий Закон про ШІ - Що це означає для відповідності в контексті фінансових злочинів



1 серпня 2024 року офіційно набув чинності Закон ЄС про штучний інтелект (AI Act). AI Act має суттєво вплинути на стратегії боротьби з відмиванням коштів та шахрайством у фінансових установах.

Ключові моменти:

- **Класифікація AI-систем:** AI Act класифікує системи штучного інтелекту як неприйнятно ризикові, високо ризикові, обмеженого ризику і мінімального ризику. Системи протидії відмиванню коштів та шахрайству, ймовірно, належать до категорії високого ризику через їхній вплив на права людей. Ця класифікація означає, що ці системи підлягатимуть суворій регулятивній перевірці.
- **Управління даними та прозорість:** AI Act підкреслює важливість високоякісних, неупереджених і репрезентативних наборів даних, щоб уникнути дискримінації та забезпечити справедливість. Щоб відповідати цим вимогам, фінансовим установам потрібно буде запровадити жорсткі рамки управління даними.
- **Посилений нагляд та аудит:** AI Act вводить вимоги щодо постійного моніторингу, документації та звітування про продуктивність AI-систем. Фінансовим установам необхідно буде створити надійні механізми нагляду для забезпечення комплаєнсу.
- **Етичні практики ШІ:** фінансові установи повинні переконатися, що їхні системи протидії відмиванню коштів та шахрайству, керовані ШІ, випадково не сприяють дискримінаційним практикам.
- **Ризик невідповідності:** невиконання AI Act може призвести до значних штрафів і шкоди репутації. Фінансовим установам потрібно буде включити комплаєнс штучного інтелекту в свої ширші системи управління ризиками, щоб ефективно пом'якшити ці ризики.

Наступні кроки

AI Act являє собою зміну парадигми для фінансових установ, які використовують штучний інтелект у боротьбі з відмиванням коштів та шахрайством. Фінансові установи повинні бути активними в адаптації до цих правил.

AI Act буде повністю застосовуватися через два роки, за деякими винятками: заборони почнуть діяти через шість місяців, правила управління та зобов'язання для моделей ШІ загального призначення – через 12 місяців, а правила для AI-систем в регульованих продуктах – через 36 місяців.

Щоб полегшити перехід до нової нормативно-правової бази, Комісія ЄС запустила Пакт про штучний інтелект, добровільну ініціативу, спрямовану на підтримку майбутнього впровадження ключових зобов'язань AI Act завчасно.

https://digital-strategy.ec.europa.eu/en/policies/ai-pact

Імплементація MiCA в країнах Європи

У світі криптовалют та цифрових активів дотримання регулятивних вимог стає ключовим фактором успіху для бізнесів, що прагнуть легально працювати на ринку. Команда Manimama завершила детальне дослідження впровадження регуляції Markets in Crypto-assets Regulation (MiCA) у різних країнах ЄС. Ці дослідження висвітлюють особливості отримання ліцензії на діяльність з

криптовалютами, нові вимоги для провайдерів криптоактивів, а також процедури та ресурси, необхідні для відповідності новим правилам.

Законодавчі зміни **в Люксембурзі**, пов'язані з регулюванням послуг віртуальних активів, передбачають обов'язкову реєстрацію компаній, що надають такі послуги, в національному органі фінансового нагляду CSSF. Відповідно до змін, внесених до Закону від 12 листопада 2004 року щодо протидії відмиванню коштів та фінансуванням тероризму, будь-яка компанія, що надає послуги з віртуальних активів, повинна зареєструватися як VASP (постачальник послуг з віртуальних активів) та виконувати професійні зобов'язання, описані в законі.

Законопроект №8387 PL MICA TFR, що впроваджує регулювання MiCA, передбачає, що всі компанії, які надають послуги криптоактивів, повинні відповідати новим вимогам до 1 липня 2026 року. До 30 грудня 2024 року компанії можуть зареєструватися за чинними правилами, однак вони повинні будуть перейти на нове регулювання MiCA у встановлені строки. Під час перехідного періоду зареєстровані компанії залишаються під наглядом CSSF, зобов'язані виконувати професійні зобов'язання та дотримуватися вимог закону 2004 року.

Також передбачена відповідальність для компаній, що порушують нові правила: попередження, штрафи до 5 мільйонів євро або 5% річного обороту, наказ про припинення діяльності, що порушує законодавство, та інші санкції. Ці заходи покликані забезпечити суворе дотримання нових регуляцій та підтримання фінансової стабільності в країні.

http://surl.li/upujup

Зміни у законодавстві Іспанії в контексті впровадження регуляції MiCA значно впливають на правила для постачальників послуг криптовалют (CASP). Перед впровадженням MiCA компанії повинні були виконати кілька обов'язкових кроків, таких як реєстрація у Центральному банку Іспанії (SCB), створення юридичної особи, оренда офісу та дотримання вимог щодо боротьби з відмиванням грошей. Ці вимоги включають реєстрацію у реєстрі SCB та подачу спеціальних форм для оцінки придатності компанії та її директорів.

Закон 6/2023 про ринки цінних паперів та інвестиційні послуги ("новий LMV") є головним нормативним актом, який впроваджує вимоги MiCA на національному рівні. Регулюючими органами, які забезпечують виконання нових правил, є Національна комісія з ринків цінних паперів та SCB. CASP мають дотримуватися вимог MiCA, таких як реєстрація та подання відповідних форм, включаючи CRIPTO01 для постачальників послуг з обміну фіатних грошей на криптовалюту та CRIPTO03 для постачальників послуг зі зберігання криптовалютних гаманців.

Важливою особливістю є перехідний період тривалістю 12 місяців, який дозволяє одночасну діяльність фірм, авторизованих і неавторизованих за MiCA, до завершення цього періоду. Це означає, що з 1 січня 2025 року CASP, які працюють в юрисдикціях з перехідним періодом, матимуть можливість діяти в рамках нових вимог MiCA. Проте порушення цих вимог може призвести до серйозних санкцій, включаючи штрафи до 5 мільйонів євро або до 12,5% від загального обороту компанії за попередній рік. Важливо зазначити, що ці санкції можуть бути зменшені, якщо послуги надавалися випадково або ізольовано.

Таким чином, впровадження MiCA в Іспанії забезпечує значне посилення регулювання ринку криптовалют, що вимагає від компаній суворого дотримання нових вимог для уникнення серйозних юридичних наслідків.

https://www.linkedin.com/pulse/mica-implementation-spain-manimama-hfxne/

У Словаччині імплементація регуляції MiCA створює нові вимоги для постачальників послуг криптовалют (CASP), які хочуть легально працювати в країні. До впровадження MiCA компанії повинні були зареєструвати місцеву компанію з мінімальним статутним капіталом 5,000 євро, мати місцеву адресу та забезпечити відповідність AML-вимогам. Після введення MiCA, Національний банк Словаччини (NBS) буде головним регулятором, контролюючи CASP з 30 грудня 2024 року.

Компанії, які прагнуть отримати ліцензію на надання послуг криптоактивів, повинні відповідати вимогам MiCA та зареєструватися у відповідних юридично-правових формах, наприклад, для зберігання криптоактивів, операцій обміну та інших послуг. Процес ліцензування передбачає оцінку відповідності заявок, яка триватиме до 40 робочих днів після повного подання документів. Серед ключових вимог є забезпечення відповідності ПВК/ФТ, а також дотримання вимог MiCA та DORA.

Національний банк Словаччини пропонує попередні консультації з потенційними заявниками, щоб підвищити якість заявок та скоротити час на отримання ліцензії. З 2025 року на вебсайті NBS буде опубліковано список зареєстрованих постачальників послуг криптоактивів, які мають право надавати послуги в Словаччині.

Варто зазначити, що порушення нових вимог можуть призвести до серйозних санкцій, однак конкретні положення щодо відповідальності наразі остаточно не врегульовані. Це свідчить про прагнення Словаччини створити жорстку, але водночас прозору і передбачувану регуляторну систему для ринку криптоактивів, яка забезпечить баланс між інноваціями і безпекою.

https://www.linkedin.com/pulse/mica-implementation-slovakia-manimama-0emee/

САНКЦІЇ

Бізнесмен з інтересами в Німеччині в обхід санкцій експортував до росії американські літографічні машини для виробництва мікрочіпів

Стаття на "The Insider" розповідає про те, як компанія з Гонконгу, що належить бізнесмену із Сінгапуру, обійшла санкції США і експортувала в Росію високотехнологічні машини для виробництва мікрочипів. Попри заборони на експорт обладнання, створеного на основі американських технологій, ця компанія змогла імпортувати машини **на суму понад 4 мільйони доларів через посередників у Китаї та Тайвані**.

Ключові моменти:

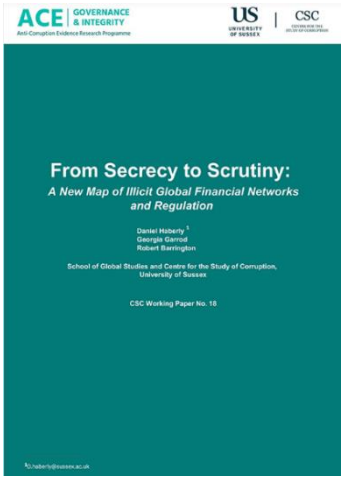
1. **Обхід санкцій США:** Гонконгська компанія, що належить бізнесмену із Сінгапуру, зуміла обійти санкції США, які забороняють експорт високотехнологічного обладнання до Росії. Це обладнання використовувалося для виробництва мікрочипів, що є стратегічно важливим для Росії.
2. **Експорт літографічних машин:** Мова йде про машини для літографії, які є ключовими у виробництві мікросхем. Вартість імпортованих машин склала понад 4 мільйони доларів. Такі машини є критичними для високотехнологічних галузей і використовуються для створення мікрочипів, необхідних у військовій та цивільній промисловості.
3. **Міжнародний маршрут:** Машини були доставлені через посередників у Китаї та Тайвані, що ускладнює відстеження та контроль за виконанням санкцій. Цей ланцюг постачання включав кілька країн, що значно ускладнило виявлення порушення санкцій.
4. **Інтереси в Німеччині:** Бізнесмен, який керує цією схемою, має інтереси в Німеччині, що підкреслює міжнародний характер цієї справи і потенційні наслідки для європейських країн.
5. **Складнощі з виконанням санкцій:** Цей випадок демонструє, наскільки складно забезпечити ефективне виконання санкцій, особливо коли мова йде про високотехнологічні товари, які можуть переміщатися через кілька юрисдикцій.

Стаття підкреслює важливість міжнародної співпраці та посилення контролю за експортом, щоб уникнути подібних порушень санкцій у майбутньому.

https://theins.ru/en/news/274045

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Від секретності до перевірки: нова карта незаконних глобальних фінансових мереж і регулювання



Документ «From Secrecy to Scrutiny: A New Map of Illicit Global Financial Networks and Regulation» є брифінгом, що **аналізує структуру глобальних нелегальних фінансових мереж, які змінюються відповідно до змін у регуляторному середовищі**. Дослідження базується на великих наборах даних: розташування підсанкційних суб'єктів, визначених Законом про Корупцію за Кордоном (FCPA), і змін у регуляції глобальних нелегальних фінансових потоків (RIFF). Зокрема, аналізується географічний розподіл підсанкційних суб'єктів, використання банківських рахунків і фіктивних компаній у корупційних схемах, а також трансформації у фінансових мережах через санкції. Документ відображає, як зміни в регуляторних режимах, зокрема після 9/11 та введення списку FATF, вплинули на ці нелегальні фінансові мережі, зміщуючи їхні центри ваги з Західних фінансових центрів до регіонів на кшталт Дубаю та Гонконгу. Крім того, документ підкреслює розбіжність між регуляторними вимогами у сфері боротьби з відмиванням коштів та фінансовою прозорістю, зокрема в США та Китаї.

Ключові висновки:

1. **Зсув глобальних центрів нелегальних фінансових мереж:**

Глобальний центр ваги нелегальних фінансових мереж переміщується від традиційних західних фінансових центрів, таких як Лондон, до нових осередків — осі Дубай-Гонконг. Ці два міста стають дедалі важливішими хабами завдяки своїм зв’язкам із західними фінансовими інститутами та доступу до англійського загального права, водночас уникаючи безпосереднього політичного впливу Заходу. Такий зсув свідчить про адаптацію нелегальних мереж до нових умов регулювання та санкційного тиску, що стає важливим викликом для глобальних антикорупційних ініціатив.

2. **Регуляторні прогалини у США та Китаї:**

Незважаючи на загальну увагу до офшорних юрисдикцій як основних центрів приховування фінансових потоків, найбільші регуляторні прогалини в ПВК та фінансовій прозорості насправді спостерігаються в найбільших економіках світу — США та Китаї. США, наприклад, поступово замінює Швейцарію як центр для корупційних банківських операцій, що підкреслює потребу в перегляді регуляторних стандартів навіть у країнах, які є світовими лідерами. Відсутність ефективних механізмів контролю у цих країнах підриває глобальні зусилля щодо боротьби з фінансовими злочинами і ставить під сумнів ефективність міжнародних ініціатив у цій сфері.

3. **Вплив міжнародного тиску на офшорні юрисдикції:**

З початку 2000-х років міжнародні ініціативи, такі як OECD та FATF, призвели до значного покращення регуляторних стандартів у багатьох офшорних юрисдикціях і країнах, що розвиваються. Ці ініціативи змусили уряди запровадити нові правила та посилити нагляд, що призвело до того, що деякі офшорні центри почали навіть перевершувати за суворістю регуляційних стандартів окремі країни OECD. Проте, незважаючи на це, залишаються проблеми з прозорістю та конфіденційністю, які продовжують використовуватися для приховування фінансових злочинів.

4. **Розбіжність між ПВК/ФТ та фінансовою прозорістю:**

Незважаючи на значний прогрес у ПВК/ФТ, зокрема в офшорних юрисдикціях, цей прогрес не супроводжується відповідним рівнем фінансової прозорості. Багато з цих юрисдикцій все ще зберігають високий рівень фінансової секретності, використовуючи складні юридичні механізми для приховування реальних власників компаній. Це створює можливості для регуляторного

арбітражу, коли компанії можуть вибирати юрисдикції з найменш прозорими вимогами, що ускладнює боротьбу з фінансовими злочинами на глобальному рівні.

5. **Мобільність і стійкість нелегальних фінансових мереж:**

Хоча нелегальні фінансові мережі демонструють певну географічну мобільність у відповідь на посилення регуляторного тиску, ця мобільність є нерівномірною і значною мірою обмежена природою мереж, які часто залежать від тривалих історичних зв'язків та довіри між учасниками. Незважаючи на переміщення деяких аспектів фінансової діяльності до нових юрисдикцій, таких як Дубай і Гонконг, ці мережі залишаються прив'язаними до кількох ключових центрів, які забезпечують стабільність і доступ до міжнародних фінансових послуг.

6. **Зростання ролі постколоніальних мереж Великобританії:**

Незважаючи на зниження ролі Лондона як центру нелегальних фінансових мереж, мережі колишніх колоній Великобританії, таких як ОАЕ та Гонконг, відіграють дедалі важливішу роль. Ці юрисдикції стають головними хабами для незаконних фінансових мереж, забезпечуючи доступ до глобальних ринків і послуг, залишаючись при цьому за межами західної політичної юрисдикції. Зростання цих мереж підкреслює важливість історичних зв'язків та інституційних структур, які залишаються актуальними в сучасних умовах.

http://surl.li/sjxmvu

Третій симпозіум із боротьби з незаконними фінансовими потоками для захисту демократії, належного врядування та миру

Документ «Global Forum Symposium Report 2024» підсумовує третій симпозіум, що відбувся в червні 2024 року і був присвячений темі боротьби з нелегальними фінансовими потоками (IFFs) для захисту демократії, належного врядування та миру. Захід зібрав понад 500 учасників із різних секторів та країн для обговорення викликів і пошуку рішень у сфері IFFs. **Учасники досліджували субверсивний вплив IFFs на демократичні інституції та мир, а також підкреслювали важливість міжнародної співпраці, прозорості та технологій у боротьбі з цими потоками**.

На симпозіумі обговорювалися основні виклики, пов'язані з фінансуванням тероризму, що є значною загрозою для глобальної безпеки. Учасники зазначали необхідність підвищення ефективності національних та міжнародних зусиль, включаючи адаптацію стратегій під нові ризики та технології. Також були представлені результати конкурсу "Call for Ideas 2023", де наголошувалося на важливості технологій і співпраці для підвищення ефективності заходів протидії відмиванню коштів і фінансуванню тероризму.

Важливою темою були і наслідки внесення країн у "сірий список" FATF, зокрема вплив на економічну стабільність і розвиток. Учасники підкреслювали необхідність стратегічного підходу та політичної волі для ефективного виходу з цього списку. Заключні промови акцентували на необхідності продовження міжнародної співпраці та інноваційних підходів для боротьби з нелегальними фінансовими потоками, що підривають демократію та мир.

Ключові висновки:

1. **Підрив демократії та глобальної стабільності через нелегальні фінансові потоки (IFFs):**

Нелегальні фінансові потоки стають інструментом для підтримки автократій та клептократій, що підривають демократичні інститути. Вони сприяють концентрації влади в руках корумпованих режимів, що використовують ці ресурси для зміцнення своєї влади, впливу на політичні процеси та

придушення опозиції. Це не лише загрожує внутрішній стабільності держав, але й створює передумови для міжнародної нестабільності та конфліктів.

2. **Необхідність глобальної співпраці в боротьбі з IFFs:**

Ефективна боротьба з нелегальними фінансовими потоками потребує всебічної міжнародної співпраці, оскільки IFFs не визнають національних кордонів і часто використовують складні транскордонні структури для приховування фінансових злочинів. Держави повинні покращити координацію своїх зусиль, обмінюватися даними та впроваджувати спільні заходи для протидії цим потокам. Співпраця між різними рівнями влади, приватним сектором, громадянським суспільством і ЗМІ має вирішальне значення для досягнення успіху.

3. **Проблема фінансування тероризму:**

Фінансування тероризму залишається однією з найсерйозніших загроз для глобальної безпеки. Незважаючи на досягнення в боротьбі з цим явищем, ефективність заходів залишається низькою через швидкий розвиток нових технологій, таких як криптовалюти, і складність у відстеженні фінансових потоків. Різні регіони світу стикаються з унікальними викликами, що потребують адаптованих підходів до боротьби з фінансуванням тероризму. Підтримка ефективної системи виявлення та попередження фінансування тероризму має бути пріоритетом як на національному, так і на міжнародному рівнях.

4. **Еволюція підходу до "сірого списку" FATF:**

Підхід FATF до включення країн у "сірий список" змінився від карального до конструктивного. Замість "засудження" держави отримують підтримку для покращення своїх систем боротьби з відмиванням грошей та фінансуванням тероризму (AML/CFT). Однак це може мати серйозні економічні наслідки, такі як зниження кредитних рейтингів та економічної активності. Для країн, що потрапили в "сірий список", важливо швидко і ефективно виправляти недоліки, щоб уникнути тривалого перебування у цьому статусі.

5. **Використання технологій для підвищення ефективності заходів з ПВК/ФТ:**

Технологічні інновації відіграють ключову роль у покращенні ефективності заходів з протидії нелегальним фінансовим потокам. Впровадження передових технологій, таких як аналітичні інструменти для обробки великих масивів даних, може значно підвищити точність і швидкість виявлення підозрілих транзакцій. Застосування наглядових технологій (SupTech) дозволяє фінансовим регуляторам краще відстежувати фінансові потоки та виявляти потенційні ризики. Це особливо важливо в умовах швидкої цифровізації фінансових систем.

https://www.globalforumiff.org/fileadmin/Publications/Global_Forum_Symposium_Report_2024.pdf

ПЛАТЕЖІ З ТОЧКИ ЗОРУ ПРОДАВЦЯ

Звіт "Payments from a Merchant's Perspective" надає всебічний аналіз європейської платіжної індустрії з точки зору торговців. Основна увага приділяється викликам, з якими вони стикаються в умовах економічної нестабільності, зокрема впливу інфляції на купівельну спроможність споживачів та зміну переваг у платіжних методах. Звіт також підкреслює важливість адаптації до змін в ринку, таких як зростання безготівкових транзакцій та використання мобільних гаманців, та вказує на ключові інновації, які торговці очікують від платіжних провайдерів.

Ключові висновки:

1. **Економічні виклики та їхній вплив на торгівлю:**

Європейські торговці стикаються з серйозними викликами через вплив інфляції та зниження споживчої впевненості. Зростання доходів більшості торговців пов'язане переважно з підвищенням

цін, а не зі збільшенням обсягів продажів. Це свідчить про те, що споживачі стають більш обережними у своїх витратах, намагаючись зберегти свій рівень життя в умовах зниження купівельної спроможності.

2. **Зміни в платіжних методах:**

Спостерігається помітний зсув від використання готівки до електронних платіжних засобів, особливо мобільних гаманців та інших цифрових рішень. Це явище, підсилене пандемією COVID-19, стає основною тенденцією в Європі. Наприклад, в Нідерландах зростає популярність локальної платіжної системи iDeal, що відображає зміну переваг споживачів на користь більш зручних та безпечних методів платежів.

3. **Роль відкритого банкінгу:**

Відкритий банкінг, зокрема стандартизовані та низькобар'єрні рішення, стає все більш важливим для торговців. Це дозволяє не лише забезпечити більш ефективне управління фінансами, але й надає клієнтам більшу гнучкість у виборі платіжних методів. Така трансформація платіжної індустрії сприяє появі нових можливостей для інтеграції фінансових послуг безпосередньо у процес покупки.

4. **Проблеми з шахрайством та безпекою:**

Шахрайство залишається головною проблемою як для онлайн, так і для офлайн торговців. Особливо це стосується онлайн-транзакцій, де питання безпеки і аутентифікації клієнтів стають критично важливими для запобігання шахрайству. Водночас, навіть у фізичних магазинах існує значний ризик, пов'язаний із шахрайством, особливо в країнах, де готівка все ще відіграє важливу роль у транзакціях.

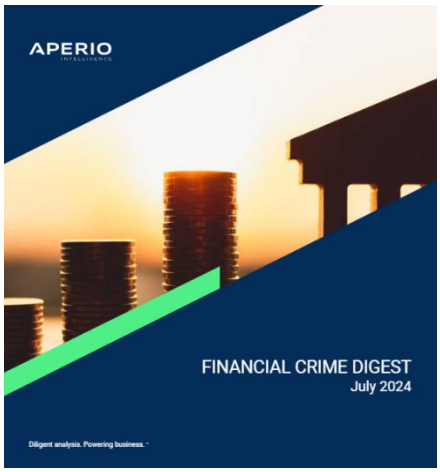
5. **Інновації, які очікують торговці:**

Торговці висловлюють зростаючий інтерес до впровадження нових технологій, які можуть покращити процеси прийняття платежів. Особливо високо цінується впровадження рішень, що забезпечують стандартизацію та зменшення бар'єрів у відкритому банкінгу, а також інтеграція штучного інтелекту для підвищення ефективності виявлення шахрайства. Крім того, очікується розвиток рішень для управління платежами, які поєднують зручність, швидкість і безпеку.

Цей звіт підкреслює важливість тісної взаємодії між платіжною індустрією та торговцями для задоволення зростаючих потреб ринку, що перебуває у стані швидкої трансформації.

http://surl.li/isyibv

ДАЙДЖЕСТ ФІНАНСОВИХ ЗЛОЧИНІВ



Документ "Aperio Financial Crime Digest" за липень 2024 року є оглядом актуальних подій та тенденцій у сфері боротьби з фінансовими злочинами. Він охоплює широкий спектр питань, включаючи останні нормативні зміни, судові процеси, нові схеми шахрайства, а також аналіз ключових трендів, що впливають на фінансовий сектор. У звіті також висвітлюються результати досліджень та рекомендації для організацій щодо вдосконалення практик комплаєнсу та протидії фінансовим злочинам.

Ключові теми:

1. **Нормативні зміни та судові процеси:**

Документ детально розглядає останні зміни в законодавстві, що впливають на боротьбу з фінансовими злочинами, а також аналізує важливі судові рішення, які

можуть мати значний вплив на практику комплаєнсу. Це включає нові вимоги до фінансових установ щодо звітності та посилення контролю за дотриманням антикорупційних та AML правил.

2. **Нові схеми шахрайства:**

У звіті представлені нові методи шахрайства, що набирають популярності, включаючи кібершахрайства, фішингові атаки та інші види фінансових злочинів, які використовують сучасні технології. Особлива увага приділяється новим загрозам, пов’язаним із криптовалютами та децентралізованими фінансовими платформами.

3. **Аналітичний огляд ключових трендів:**

Звіт аналізує основні тренди у сфері фінансових злочинів, включаючи зростання кількості випадків шахрайства, пов'язаних із пандемією COVID-19, та зміни у поведінці фінансових злочинців, що використовують нові інструменти для відмивання грошей. Особлива увага приділяється трендам у сфері регуляції криптоактивів.

4. **Рекомендації з покращення комплаєнсу:**

Документ надає рекомендації для фінансових установ щодо підвищення ефективності заходів протидії фінансовим злочинам. Це включає впровадження нових технологій, таких як штучний інтелект для виявлення підозрілих транзакцій, а також покращення внутрішніх процедур та навчання персоналу.

Ці теми є важливими для розуміння сучасних викликів у сфері боротьби з фінансовими злочинами та надають інструменти для ефективного управління ризиками у фінансовому секторі.

https://www.aperio-fcd.com/fcd-monthly?report_id=92

Глобальний звіт про фінансування тероризму

Документ під назвою "Global Terrorism Financing Report" досліджує глобальні аспекти фінансування тероризму, включаючи основні методи, якими терористичні групи отримують фінансування, та стратегії, які використовуються для протидії цьому процесу. Звіт охоплює різноманітні джерела фінансування, від традиційних механізмів, таких як пожертви, до сучасних методів, включаючи криптовалюти та інші цифрові активи. Окрему увагу приділено ролі, яку відіграють небанківські фінансові установи та нові технології у фінансуванні тероризму. Документ також надає аналіз ефективності існуючих міжнародних та національних правових рамок для боротьби з фінансуванням тероризму, акцентуючи на потребі їх подальшого вдосконалення та адаптації до нових викликів.

Ключові висновки, які можна зробити з цього документу:

1. **Еволюція методів фінансування тероризму:** Терористичні організації постійно адаптуються до нових фінансових інструментів та технологій, що вимагає від урядів та регуляторів постійного оновлення своїх підходів до протидії фінансуванню тероризму.
2. **Зростаюча роль цифрових активів:** Використання криптовалют та інших цифрових фінансових інструментів значно ускладнює відстеження та припинення фінансових потоків, пов'язаних з терористичними групами. Необхідно розробляти нові механізми контролю та регулювання цих активів.

3. **Важливість міжнародного співробітництва:** Ефективна боротьба з фінансуванням тероризму можлива лише за умови тісного міжнародного співробітництва, обміну інформацією та координації дій між країнами.
4. **Проблеми з правовими рамками:** Існуючі правові рамки часто не встигають за розвитком нових технологій та методів фінансування тероризму. Потрібно вдосконалювати законодавство, щоб враховувати сучасні виклики та загрози.
5. **Роль небанківських фінансових установ:** Небанківські фінансові установи часто використовуються для обходу традиційних методів моніторингу та контролю фінансових потоків, що вимагає особливої уваги з боку регуляторів.

http://surl.li/gvaljw

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

Повний гайд із CDD для запобігання фінансовим злочинам

🌟 У цьому всеохоплюючому відео ви можете зануритися в ключові аспекти належної перевірки клієнта (CDD), фундаментальної основи боротьби з фінансовими злочинами. Незалежно від того, чи ви новачок у галузі чи бажаєте оновити знання, цей гайд допоможе вам! 🌐💼

💼 Що в цьому епізоді?

❖ Розуміння CDD та його важливості для запобігання фінансовим злочинам 🕵️‍♂️🔍

- ❖ Детальний процес CDD: ідентифікація клієнта, KYC та оцінка ризиків 📊🛡️
- ❖ Важливість постійного моніторингу та постійного KYC 🔄🕵️‍♂️
- ❖ Роль технологій у вдосконаленні процесів CDD: ШІ, машинне навчання та автоматизовані системи 💻🔒
- ❖ Подолання поширених проблем CDD: конфіденційність даних, клієнти, які не співпрацюють, і застарілі системи 📜🔐

🔍 Чому варто дивитися?

- ❖ Отримайте уявлення про складність CDD та її критичну роль у фінансовій безпеці
- ❖ Дізнайтеся про ефективні стратегії впровадження та вдосконалення процесів CDD
- ❖ Дізнайтеся, як використовувати технології для покращення належної перевірки та комплаєнсу

https://www.youtube.com/watch?app=desktop&v=FOVt9AOsBDc&feature=youtu.be

ІНШІ НОВИНИ

Посилення законів ОАЕ з ПВК є ключем до боротьби зі зростаючою загрозою

Стаття аналізує зусилля ОАЕ щодо посилення законодавства у сфері боротьби з відмиванням грошей (AML) у відповідь на зростаючі загрози фінансових злочинів. ОАЕ активно вдосконалює свою нормативно-правову базу, співпрацюючи з міжнародними організаціями для підвищення ефективності боротьби з відмиванням грошей. Важливим аспектом є постійне оновлення законодавства для протидії складним схемам відмивання грошей. Стаття також підкреслює значущість фінансових установ та правоохоронних органів у забезпеченні дотримання норм та підтримці стабільності фінансової системи.

http://surl.li/bpglfu

Шахрайство проти людей похилого віку набуло масштабів епідемії

Зростаюча проблема шахрайства проти людей похилого віку є тривожною тенденцією, яка має руйнівний вплив. Ця стаття підкреслює сплеск шахрайства, націленого на людей похилого віку, включаючи оманливий маркетинг, фальшиві тоталізатори та фінансову експлуатацію, часто тими, кому вони найбільше довіряють. Сьогодні вкрай важливо обговорити, як боротися з цією неетичною практикою та захистити вразливі верстви населення. 🛡️😷

Ключові моменти зі статті:

❗ Шахрайство проти людей похилого віку передбачає різноманітні види шахрайства, від телемаркетингу до онлайн-фішингу.

❗ Люди похилого віку часто стають цілями через вразливість, таку як ізоляція та потенціал накопичення багатства.

❗ Профілактику можна підсилити кращою освітою, покращеними мережами підтримки та суворими фінансовими гарантіями.

Стратегії для розгляду:

✓ Просвіта та обізнаність: регулярне інформування людей похилого віку про нові тактики шахрайства та профілактичні заходи.

✓ Посилення нормативних актів: пропаганда посилення законів і покарань проти винних у шахрайстві з літніми людьми.

✓ Мережі підтримки спільноти: створення надійних систем для людей похилого віку, щоб звертатися за допомогою та повідомляти про шахрайство.

https://www.fastcompany.com/91144654/elder-fraud-epidemic-how-to-can-combat-scams

Круглий стіл: Презентація результатів аналізу ризиків корупції

У Пріштіні відбувся круглий стіл, організований Радою Європи та ЄС, де представили результати першої в Косово мапи корупційних ризиків. Процес, здійснений за підтримки PECK III, допоміг

ідентифікувати сектори з високим ризиком корупції на основі реальних даних. Захід підкреслив важливість співпраці між державними установами, громадянським суспільством та міжнародними організаціями в боротьбі з корупцією. Отримані висновки допоможуть Косову покращити свої антикорупційні зусилля та зосередитися на пріоритетних напрямках.

http://surl.li/cvyarc

FCA оштрафувало PwC

Документ, підготовлений Управлінням з фінансового регулювання та нагляду Великобританії (FCA), містить остаточне повідомлення для компанії PricewaterhouseCoopers LLP (PwC) про накладення штрафу в розмірі £15 мільйонів. Це пов'язано з невиконанням PwC своїх обов'язків як аудитора компанії London Capital & Finance plc (LCF) у період з 2016 по 2017 рік. PwC не повідомила регулятора про підозри у шахрайській діяльності з боку LCF, що спричинило значні втрати для інвесторів. Попри те, що PwC не брала участь у злочинній діяльності LCF, її обов'язком було інформувати регулятора про можливі порушення, чого не було зроблено.

Деякі цікаві червоні прапорці для аудиторів.

1. Відсутність прозорості та відмова LCF співпрацювати
2. Агресивні відповіді на запити
3. Надання неточної та/або оманливої інформації

https://www.fca.org.uk/publication/final-notices/pricewaterhousecoopers-llp-2024.pdf

KYC та ризик, що змінюється — критична роль KYC в адаптації та сучасному комплаєнсі

Стаття детально розглядає необхідність переходу від традиційних підходів процесу "Знай свого клієнта" (KYC) до сучасного підходу "перманентного KYC" (pKYC). Традиційні KYC-процеси часто не встигають за динамікою сучасного бізнесу, що може призвести до невиявлених ризиків. Особлива увага приділяється складності процесу "Знай свій бізнес" (KYB) при встановленні ділових відносин із корпоративними клієнтами, де зміни у структурі власності або операційній діяльності компанії можуть відбуватися швидко. pKYC дозволяє здійснювати безперервний моніторинг, знижуючи ризики і забезпечуючи відповідність сучасним регуляторним вимогам.

Ключові висновки:

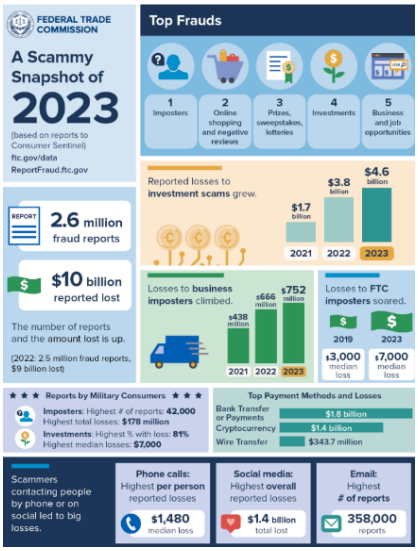
1. Традиційний KYC підхід часто неефективний через періодичний характер перевірок, що може призводити до упущення важливих змін у ризик-профілі клієнта.
2. pKYC пропонує більш ефективний підхід завдяки безперервному моніторингу клієнтів, що дозволяє своєчасно виявляти ризики та реагувати на них.

3. Процес KYB для корпоративних клієнтів значно складніший, ніж для окремих осіб, і pKYC забезпечує ефективне управління цими складнощами.
4. Автоматизація процесів зменшує ручну роботу, підвищує ефективність та зменшує ризик людських помилок.
5. pKYC сприяє покращенню клієнтського досвіду, знижуючи кількість повторних запитів інформації та збільшуючи довіру клієнтів.

Ця стратегія є важливою для фінансових установ, що прагнуть залишатися відповідними та ефективно управляти ризиками у сучасному динамічному бізнес-середовищі.

http://surl.li/lnzhsp

Загальнонаціональні збитки в США від шахрайства перевищили 10 мільярдів доларів у 2023 році



У 2023 році в США збитки від шахрайства перевищили 10 мільярдів доларів, що на 14% більше, ніж у 2022 році. Найбільші втрати були зафіксовані внаслідок інвестиційних шахрайств, які становили 4,6 мільярда доларів, а також шахрайств, пов'язаних з імітацією особи, збитки від яких склали 2,7 мільярда доларів. Федеральна торгова комісія (FTC) активізує зусилля з протидії цим загрозам, посилюючи заходи проти незаконного телемаркетингу, пропонуючи нові правила проти шахрайства, пов'язаного з імітацією, та підсилюючи захист споживачів від новітніх методів шахрайства, таких як шахрайство з використанням штучного інтелекту.

FTC також уважно стежить за тенденціями шахрайства та розширює інформаційно-просвітницькі заходи, щоб краще захищати громадськість. Комісія продовжує працювати над підвищенням обізнаності населення щодо потенційних загроз та пропонує інструменти для самозахисту споживачів. Додатково, агенція проводить спостереження за новими типами шахрайств та адаптує свої методи боротьби у відповідь на еволюцію шахрайських схем.

http://surl.li/lnyeka

Відмивання коштів у криптовалюті зростає в Бразилії

Стаття на Insight Crime описує стрімке зростання використання криптовалют для відмивання коштів у Бразилії. Криптовалюти стали привабливим інструментом для злочинних груп через анонімність і складність відстеження транзакцій. Зокрема, бразильські наркокартелі активно використовують цифрові валюти для легалізації своїх прибутків, що створює серйозні виклики для правоохоронних органів. Влада Бразилії намагається адаптувати своє законодавство і посилити міжнародне співробітництво, щоб ефективніше боротися з цим явищем.

https://insightcrime.org/news/cryptocurrency-money-laundering-is-on-the-rise-in-brazil/

Верховний суд Китаю переглядає закон про протидію відмиванню коштів, щоб включити туди «віртуальні активи»

У статті на Cointelegraph йдеться про оновлення Китаєм законодавства щодо протидії відмиванню коштів, яке тепер включає криптовалюти. Китайський уряд додав цифрові валюти до переліку фінансових інструментів, що підлягають регулюванню, підкреслюючи необхідність підвищеного контролю за транзакціями з криптовалютами. Це оновлення відображає зростаючі глобальні зусилля щодо запобігання використанню криптовалют для фінансових злочинів, таких як відмивання грошей, і посилює відповідальність фінансових установ за моніторинг і звітність про підозрілі операції.

Зміни, оголошені 19 серпня, класифікують цифрові транзакції як визнаний метод для відмивання коштів. Тим, хто бере участь у такій діяльності, тепер загрожує штраф від 10 000 до 200 000 юанів (від 1400 до 28 000 доларів США) і потенційне ув'язнення від п'яти до десяти років. Зміни відбулися на тлі зростання кількості судових переслідувань за відмивання коштів, причому з 2019 року кількість випадків зросла в 20 разів.

https://cointelegraph.com/news/china-revises-anti-money-laundering-law-include-crypto

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Заниження вартості

Заниження вартості – це звичайна техніка відмивання коштів у торгівлі (TBML), коли вартість транзакції навмисно занижується в рахунку-фактурі. Ця практика часто використовується для ухилення від сплати податків, зборів або переміщення незаконних коштів через кордон.

Ось як це працює простою мовою:

- Крок 1 - Дві сторони (експортер (продавець) та імпортер (покупець)) погоджуються торгувати товарами чи послугами. Однак вони таємно погоджуються повідомити в рахунку нижчу вартість, ніж фактична вартість товарів або послуг.
- Крок 2 - Експортер виставляє рахунок-фактуру на товари чи послуги за вартістю, нижчою за справжню ринкову вартість. Наприклад, якщо фактична вартість товару становить 100 000 доларів США, у рахунку-фактурі може бути зазначено 60 000 доларів США.
- Крок 3 - Імпортер (покупець) представляє документ із заниженою фактурою митним органам своєї країни. Митні органи нараховують мита та податки на основі заявленої вартості 60 000 доларів, а не фактичної вартості.
- Крок 4 - Імпортер сплачує заявлену суму (60 000 доларів США) через офіційні банківські канали, тоді як решта 40 000 доларів США можна розрахувати через неофіційні канали, такі як гавала, або зберігати на офшорних рахунках. В іншому випадку товари в країні-одержувачі продаватимуться на вторинному (сірому) ринку.
- Крок 5 - Товар відправляється та доставляється згідно домовленості. Менша сума в рахунку-фактурі реєструється офіційно, а справжній баланс залишається прихованим.

Переваги для експортера та імпортера:

🔺 Імпортер сплачує менше мит і податків через занижену вартість.

🔺 Експортер або імпортер може використати різницю для переміщення незаконних коштів через кордон без виявлення.

🔺 Незареєстровані кошти можуть бути використані для незаконних цілей, таких як хабарництво, корупція чи інша незаконна діяльність.

🔺 Товари можна продавати на вторинному (сірому) ринку без виставлення рахунку за меншу ціну та отримувати більше неоподатковуваного доходу

Надмірне та недостатнє відвантаження

У відмиванні коштів на основі торгівлі (TBML) надлишкове або недостатнє відвантаження стосується методу, коли товари відвантажуються в надлишку або в менших кількостях, ніж те, що задокументовано в торговій накладній.

Ця техніка використовується для незаконного переміщення цінностей через кордон.

📌 **Надлишкове відвантаження:** відправляється більше товарів, ніж зазначено в накладній. 🔔

🛑Мета: додаткові товари можна продати в країні призначення, а виручка залишиться незадекларованою або незаконно відмитою.

▶Приклад: якщо в накладній зазначено, що відправлено 100 одиниць, але фактично відправлено 150 одиниць, додаткові 50 одиниць надають кошти, які неможливо відстежити в країні-одержувачі.

📌 **Недостатнє відвантаження:** відправляється менше товарів, ніж зазначено в накладній. 🔔

🟠Мета: відправник може завищити вартість відправлення, дозволяючи переказати зайві кошти за кордон під виглядом оплати товару.

▶Приклад: у накладній зазначено, що було відправлено 200 одиниць, але фактично було надіслано лише 100 одиниць. Плата за повні 200 одиниць здійснюється, але кошти за відсутні 100 одиниць зберігаються в іноземній юрисдикції.

🔴 Червоні прапорці для виявлення:

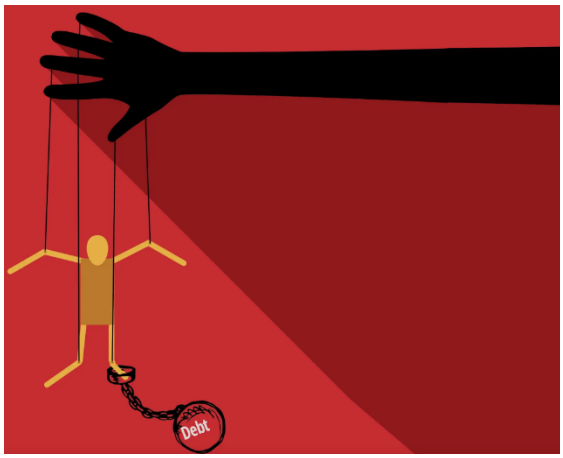
🔥 Розбіжності між товаросупровідними документами та накладними.

🔥 Незвичайні моделі торгівлі, такі як повторювані надлишкові або недостатні відвантаження.

🔥 Невиправдані аномалії ціноутворення, які не відповідають кількості відвантаженого товару.

🔥 Такі схеми використовують складність міжнародної торгівлі, що робить виявлення без ефективного моніторингу та механізмів перевірки важкою задачею.

Паттерни торгівлі людьми



Торгівля людьми (НТ) є серйозною проблемою, і фінансові установи (ФУ) відіграють вирішальну роль у виявленні потенційних червоних прапорців. 🚩

Зазвичай, моменти, коли справа стосується заробітньої плати, яку сильно вираховують у працівника або працівникам вона не надходить вчасно, не розглядаються як НТ. Ось деякі закономірності, за якими фінансові установи мають спостерігати

⛔Якщо існує непояснене велике відрахування із заробітної плати або спостерігається закономірність значних нез'ясованих відрахувань із заробітної плати або депозитів працівника, це може свідчити про те, що працівника експлуатують або примушують.

⛔Коли заробітна плата кількох осіб перераховується на той самий рахунок, особливо якщо вони не пов'язані між собою, це може означати контроль над фінансами жертв.

⛔Якщо спостерігається часте зняття великої кількості готівки одразу після внесення зарплати або багаторазове/послідовне зняття коштів у банкоматах, зроблене однією особою, це може свідчити про те, що жертва не контролює свої власні фінанси

⛔Деякі підприємства, які в основному виплачують заробітну плату за допомогою передплачених карток, особливо в галузях, відомих низькооплачуваними працівниками, можуть бути ознакою уникнення традиційних банківських методів і перевірки.

⛔Якщо третя сторона регулярно здійснює платежі від імені кількох непов'язаних осіб, це може означати контроль над кількома жертвами.

⛔Незвичайна або непостійна банківська поведінка, наприклад часті перекази між кількома рахунками, може свідчити про спробу уникнути виявлення або відмивання доходів.

⛔Якщо посадова інструкція та заробітна плата не відповідають профілю працівника (наприклад, працівник отримує мінімальну заробітну плату зі значними операціями), це може свідчити про експлуатацію.

Червоні прапорці при укладанні клієнтських відносин із установою

Деякі з червоних прапорців 🚩, які спадають на думку під час укладання клієнтських відносин із компанією:

☞ Тривалий період бездіяльності після реєстрації.

☞ Немає онлайн-присутності.

☞ Зареєстрована назва не вказує на діяльність компанії або назва передбачає послугу, яку компанія не надає.

☞ Зареєстровано за адресою, яка не збігається з профілем компанії, або де юридична адреса використовується багатьма іншими компаніями.

☞ Директори чи акціонери, яких неможливо знайти, зв’язатися з ними або які, здається, не беруть активної участі в діяльності компанії.

☞ Професійні номінальні директори/акціонери.

☞ Директори та акціонери власники контрольних пакетів мають різне географічне розташування без логічної причини.

☞ Велика кількість дрібних виправлень даних.