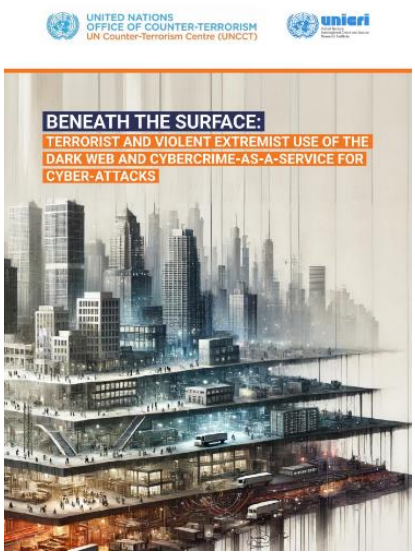
Серійний номер: ДСФМУ-ДК-2024-014
Липень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Під поверхнею: терористи та екстремісти використовують Dark Web і кіберзлочинність як послугу



Оскільки загрози продовжують розвиватися протягом цифрової ери, перетин тероризму, екстремізму і кіберзлочинності представляє все більш грізний виклик глобальній безпеці. Про це йдеться у звіті «Під поверхнею», опублікованому Контртерористичним управлінням ООН.

Цей звіт проливає світло на феномен кіберзлочинності як послуги, досліджуючи, як терористи та кіберзлочинці використовують Дарк Веб для отримання інструментів і послуг для своїх цілей.

📌 Ринки Дарк Веб

Численні джерела підкреслюють зв'язок між суб'єктами, що несуть загрозу, та ринками Дарк Веб. Наприклад, зброя, використана під час терактів у Парижі, Франція, у 2015 році та в Мюнхені, Німеччина, у 2016 році, нібито була придбана у постачальників, які працюють у Дарк Веб. Також широко повідомляється, що засоби шахрайства, такі як викрадені кредитні картки та викрадені паспорти, були придбані терористичними групами на ринках Дарк Веб.

📌 Незалежні домени Дарк Веб (.onion)

Помічено, що зловмисники створюють власні приховані сервіси в Дарк Веб, використовуючи незалежні домени. Помічено, що терористи використовують їх для новин і пропаганди, прикладами є офіційні видання Ісламської держави, що базується в Афганістані в провінції Хорасан, і неонацистський веб-сайт «The Daily Stormer».

📌 Форуми кіберзлочинності

Форуми про кіберзлочинність широко використовуються зловмисниками, які керуються як фінансовими, так і іншими мотивами. Ці форуми, які публічно надають особисту інформацію, уможливлюють обмін приватними повідомленнями та більш обмежені канали зв'язку, де можуть відбуватися детальні обговорення та конфіденційне планування атак.

📌 Шифрування та можливості, орієнтовані на конфіденційність

Зловмисники стають все більш обізнаними з технікою безпеки в Інтернеті. Однак зазначається, що терористичні групи, здається, готові відкрито спілкуватися в публічних каналах Telegram. Хоча ця відкритість допомагає викликати інтерес до їхньої справи та спонукати до подальшої активності, вона також демонструє меншу стурбованість щодо виявлення та необхідності темних мереж маскувати свою діяльність.

📌 Криптовалюти

Криптовалюти стали фундаментальним елементом кіберзлочинності та служать фінансовою опорою для кіберзлочинності як послуги. Вони сприяють низці видів діяльності, від купівлі та продажу продуктів і послуг для кібератак до сприяння іншим формам фінансування тероризму та відмивання грошей.

📌 Кіберзлочинність як послуга

Модель «Кіберзлочинність як послуга» є складною та обширною, охоплюючи широкий спектр послуг, включаючи DDoS, викрадення даних та програми-вимагачі. Незважаючи на те, що дослідження підтверджує, що суб'єкти, які становлять загрозу, мають інші мотиви для взаємодії з цими службами, ніж фінансові міркування, високому ступеню цієї взаємодії перешкоджають викликуи доступу до даних і атрибуції.

http://surl.li/lmmemt

Заява Вольфсберзької групи щодо ефективного моніторингу підозрілої діяльності

Вольфсберзька Група опублікувала Заяву щодо моніторингу підозрілої діяльності відповідно до Вольфсберзьких факторів від 2019 року.

Група не вважає, що цінність, яка отримується від (постійно зростаючого) обсягу SAR/STR, пропорційно сприяє досягненню ефективних результатів у боротьбі з фінансовими злочинами. Хоча концепція ефективності вже багато років обговорюється законодавцями, регуляторами, наглядовими органами, розробниками стандартів, а також приватним сектором, Група вважає, що вона ще не повністю інтегрована в загальну структуру управління ризиками фінансових злочинів (FCRM), що вимагатиме її прийняття та узгодження в державному та приватному секторах.

Цей документ має на меті описати, як врахування Вольфсберзьких факторів може перетворитися на більш ефективний підхід до моніторингу підозрілої діяльності (MSA). Вольфсберзька Група свідомо вирішила охарактеризувати це як MSA, щоб створити ширшу мережу, ніж просто моніторинг транзакцій, оскільки поведінка та атрибути клієнтів у поєднанні з розглядом транзакцій можуть надати ширше уявлення про потенційно підозрілу діяльність. Таким чином, моніторинг транзакцій є частиною MSA, яка також може включати такі поняття, як постійна перевірка клієнтів (CDD).

Цей документ заохочує всі сторони до активної участі в розробці інноваційних методів і допоміжних технологій, які, на думку Вольфсберзької Групи, забезпечать більш ефективні можливості виявлення ризиків на всіх етапах.

http://surl.li/xrwghl

Керівні настанови Вольфсберзької Групи щодо програми протидії хабарництву і корупції

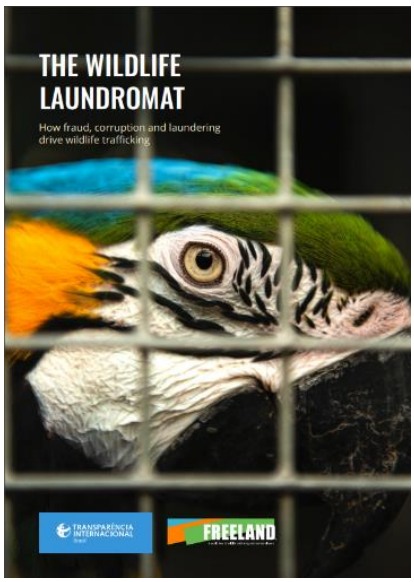
Вольфсберзька Група опублікувала оновлене керівництво щодо програми відповідності вимогам боротьби з хабарництвом та корупцією (ABC). Це оновлення версії 2017 року спрямоване на сприяння етичним бізнес-практикам та відповідності законодавчим вимогам ABC. Керівництво пропонує ризик-орієнтований підхід до розробки та впровадження програм відповідності, включаючи періодичні оцінки ризиків, навчання та моніторинг. Воно враховує досвід з 2017 року, розширює розділи про ризики корупції серед клієнтів та транзакцій та пропонує нові рекомендації для виявлення та пом'якшення нових ризиків хабарництва та корупції.

Важливою частиною керівництва є акцент на адаптації програм відповідності до специфічних ризиків компанії, включаючи аналіз ризиків у різних секторах та географічних регіонах. Керівництво також підкреслює важливість корпоративної культури, що підтримує етичні стандарти, та ролі вищого керівництва у забезпеченні ефективної програми відповідності.

Крім того, керівництво включає практичні поради щодо впровадження систем внутрішнього контролю, регулярного моніторингу та аудиту програм відповідності, а також необхідності забезпечення прозорості та звітності у всіх аспектах діяльності компанії.

http://surl.li/wonans

Як шахрайство, корупція та відмивання коштів стимулюють торгівлю дикими тваринами



Дослідження "The Wildlife Laundromat" від Transparency International Brazil аналізує, як шахрайство, корупція і відмивання грошей сприяють незаконній торгівлі дикими тваринами в Бразилії. Звіт, підготовлений за підтримки Freeland Brazil, аналізує 18 випадків і операцій, спрямованих на боротьбу з торгівлею дикими тваринами в різних регіонах країни. Виявлено 24 практики шахрайства, корупції і відмивання грошей.

Звіт рекомендує створити національну стратегію для боротьби з торгівлею дикими тваринами, мобілізувати механізми протидії корупції та відмиванню грошей, зміцнити систему контролю за дикою природою, сприяти прозорості та цифровій трансформації, а також підвищити відповідальність за контрабанду.

Це дослідження є частиною проекту "Протидія торгівлі дикими тваринами в Центральній і Південній Америці", координованого Freeland за підтримки Міжнародного бюро наркотиків і правоохоронних справ США (INL) та у партнерстві з Transparency International Brazil, WWF Brazil і IFAW. Проект спрямований на підвищення ефективності боротьби з торгівлею дикими тваринами на регіональному рівні, включаючи посилення розслідувань, міжнародну співпрацю, покращення кримінального переслідування та зміцнення прозорості.

https://transparenciainternacional.org.br/publicacoes/the-wildlife-laundromat/

Корупція вбиває: світові докази від природних катаклізмів

Дослідження "Corruption Kills: Global Evidence from Natural Disasters" від МВФ аналізує вплив корупції на втрати людських життів під час природних катастроф, використовуючи дані зі 135 країн за період з 1980 по 2020 рік. Результати дослідження показують, що корупція значно збільшує кількість смертей під час катастроф, особливо в країнах, що розвиваються. Високий рівень корупції підриває якість громадської інфраструктури, ефективність реагування на надзвичайні ситуації та дотримання будівельних норм, що призводить до більшої кількості жертв.

Дослідження використовує економетричний аналіз, який враховує різні чинники, такі як рівень доходів, щільність населення, медичну інфраструктуру та політичну стабільність. Використовуючи регресійний аналіз, дослідники виявили нелінійні ефекти корупції, які збільшують вразливість країн до природних катастроф.

Дослідження наголошує, що природні катастрофи самі по собі є неминучими, але масштаби гуманітарних та економічних втрат значною мірою залежать від політичних і інституційних факторів, які формують якість громадської інфраструктури та забезпечують виконання будівельних норм. Виявлено, що вищий рівень корупції в країні призводить до більшого числа смертей, викликаних природними катастрофами, після врахування економічних, демографічних, медичних та інституційних чинників.

У дослідженні рекомендується посилення антикорупційних заходів для покращення якості будівельних стандартів та інфраструктури. Підтримка міжнародних зусиль для боротьби з корупцією та покращення ефективності реагування на катастрофи є також важливою. Реформи у сфері державного управління повинні забезпечити прозорість та підзвітність у використанні ресурсів на відновлення після катастроф.

http://surl.li/zhtnxv

Звіт про торгівлю людьми за 2024 рік

Звіт "2024 Trafficking in Persons Report" від Державного департаменту США є найвичерпнішим ресурсом з питань боротьби з торгівлею людьми у всьому світі. Цей щорічний звіт охоплює 188 країн і територій, включаючи США, і надає об'єктивну оцінку зусиль урядів у протидії торгівлі людьми.

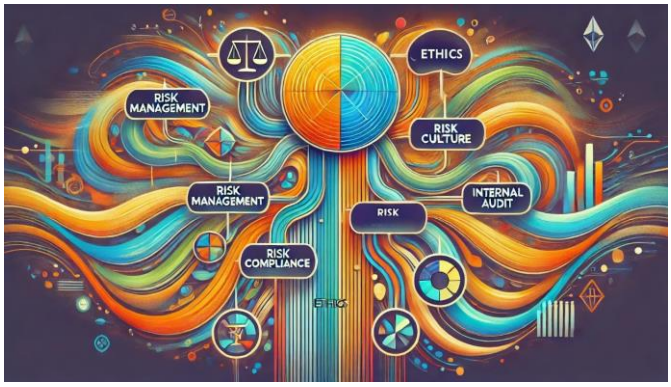
Звіт 2024 року висвітлює низку ключових питань та тенденцій у сфері боротьби з торгівлею людьми, зокрема використання цифрових технологій для виявлення та боротьби з цими злочинами. Він підкреслює, як цифрові технології можуть бути ефективно використані правоохоронною спільнотою для виявлення випадків торгівлі людьми, збору доказів та підтримки жертв.

Звіт базується на широкому спектрі джерел, включаючи дані урядів, міжнародних організацій, громадянського суспільства та самих жертв торгівлі людьми. Він оцінює урядові зусилля у трьох основних напрямках: переслідування, захист і запобігання. Оцінка кожної країни відображає її здатність ефективно боротися з торгівлею людьми та дотримуватися мінімальних стандартів, встановлених Законом про захист жертв торгівлі людьми (TVPA).

Звіт підкреслює, що боротьба з торгівлею людьми вимагає комплексного підходу, який включає співпрацю урядів, приватного сектора та громадянського суспільства. Він також закликає до посилення міжнародної співпраці та обміну інформацією для ефективнішого реагування на глобальні виклики, пов'язані з торгівлею людьми.

http://surl.li/cedckc

Рекомендації EBA щодо мінімального змісту механізмів управління для емітентів токенів, прив’язаних до активів (ART)



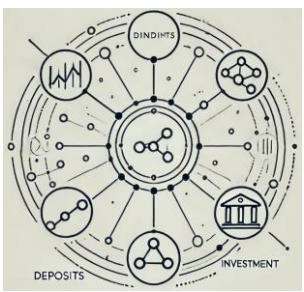
Ці керівні принципи EBA регулюють обов'язки та функціонування органів управління, структуру організаційної рамки, механізми внутрішнього контролю, управління ризиками та бізнес-стійкість. Документ враховує принцип пропорційності, що дозволяє адаптувати вимоги до масштабу та специфіки діяльності емітентів ART. Принципи підкреслюють необхідність ефективного управління усіма ризиками, включаючи операційні, шахрайство, кіберризики та ризики відповідності, для забезпечення належного захисту споживачів та інвесторів.

Також розглядаються аспекти екологічної, соціальної та управлінської (ESG) відповідальності емітентів, особливо щодо впливу на клімат через споживання енергії. Встановлюються чіткі вимоги щодо незалежних функцій внутрішнього контролю, таких як управління ризиками та внутрішній аудит, з метою забезпечення надійного контролю та ефективності управлінських систем.

Звіт також охоплює положення щодо безперервності бізнесу, що включають політики та плани для збереження основних даних та функцій у випадку переривання роботи систем інформаційно-комунікаційних технологій. У документі наголошується на важливості прозорості в управлінських структурах та необхідності регулярного перегляду і оновлення управлінських процесів для адаптації до змін у бізнес-середовищі.

http://surl.li/lspyhp

Огляд літератури з фінансових технологій та конкуренції банківських послуг



Фінансові технології (fintech) значно впливають на банківські послуги, створюючи нові можливості та конкурентні переваги. Документ розглядає різні аспекти цього впливу, включаючи платежі, кредитування, депозити та інвестиційні послуги. Використання фінансових технологій призвело до зростання доступу до фінансових послуг, зниження вартості та підвищення конкуренції серед традиційних банків та нових гравців. Дослідження вказує на значні переваги для споживачів, але також на деякі виклики, пов'язані з регулюванням та впровадженням нових технологій. Подальші дослідження необхідні для кращого розуміння довгострокових наслідків цих змін для банківського сектору.

https://www.bis.org/bcbs/publ/wp43.htm

Проекти технічних стандартів, що визначають певні вимоги Регламенту ринків криптовалютних активів (MiCA) - 1 та 2 пакет

Фінальні звіти ESMA "Draft technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA)" стосуються регулювання ринку криптоактивів відповідно до регуляції MiCA (Markets in Crypto Assets). Ці документи описують технічні стандарти та вимоги для постачальників послуг з криптоактивами (CASPs) і розробників криптоактивів. Звіти включають процедури подання заявок на авторизацію, вимоги до внутрішнього контролю, обробки скарг клієнтів, управління конфліктами інтересів і інформації, яка повинна бути надана при придбанні кваліфікаційної частки у CASPs. Звіти також враховують зворотній зв'язок від учасників ринку та пропонують остаточні версії стандартів для подання до Європейської Комісії. Документи спрямовані на забезпечення гармонізованого підходу до регулювання криптоактивів у всіх країнах ЄС, підвищення прозорості, захисту інвесторів та зниження ризиків на ринку криптоактивів.

http://surl.li/ufntdj

http://surl.li/fgkgwx

РЕГУЛЮВАННЯ

Нове правило FinCEN не дозволить банкам США передавати програми з ПВК на аутсорс за кордон

FinCen, відділ боротьби з фінансовими злочинами Міністерства фінансів США, запропонував нове правило, спрямоване на посилення стандартів з ПВК в американських фінансових установах.

Ця зміна вимагатиме від компаній більш ретельної оцінки ризиків, а також заборонятиме фінансовим установам передавати нагляд за програмами з ПВК/ФТ на аутсорс за кордон.

«Запропоноване правило відображає вимогу що створення, підтримка та застосування програми з ПВК/ФТ фінансової установи має залишатися відповідальністю осіб у Сполучених Штатах», — йдеться в повідомленні FinCEN.

http://surl.li/idmklx

Рекомендації щодо вимог до інформації, пов'язаної із переказом коштів і певних криптоактивів відповідно до Регламенту (ЄС) 2023/1113

Документ "Travel Rule Guidelines" містить керівні настанови щодо інформаційних вимог, які супроводжують перекази коштів та певних криптоактивів відповідно до Регламенту (ЄС) 2023/1113. Цей регламент було прийнято для ускладнення зловживань коштами та криптоактивами з метою фінансування тероризму та інших фінансових злочинів, а також для забезпечення можливості відстеження таких переказів з метою запобігання, виявлення або розслідування відмивання грошей та фінансування тероризму.

Керівні настанови розроблені для постачальників платіжних послуг (PSPs), посередників PSP (IPSPs), постачальників послуг з криптоактивами (CASPs) та посередників CASP (ICASPs), з метою допомогти їм виявляти відсутню або неповну інформацію, яка супроводжує переказ коштів або криптоактивів, а також впроваджувати процедури управління такими переказами.

Регламент зобов'язує EBA видавати керівні вказівки щодо необхідних дій для забезпечення відповідності PSPs, IPSPs, CASPs та ICASPs вимогам регламенту. Це включає виявлення відсутньої або неповної інформації та управління такими переказами. У нових керівних настановах зберігається ризик-орієнтований підхід, який був впроваджений ESA раніше, але додано нові положення для CASPs та ICASPs з огляду на перекази криптоактивів.

Важливо, що ці керівні настанови є обов'язковими для виконання з 30 грудня 2024 року, і компетентні органи повинні будуть прозвітувати щодо своєї відповідності цим керівним настановам протягом двох місяців після їх публікації.

Документ також містить аналіз витрат та вигод, оцінку впливу, а також зворотний зв'язок за результатами публічних консультацій, проведених EBA, які були враховані при підготовці остаточної версії керівних настанов.

Ці керівні настанови мають важливе значення для забезпечення єдиного підходу до виявлення та управління переказами, що супроводжуються відсутньою або неповною інформацією, у всьому Європейському Союзі, що сприятиме посиленню режиму протидії відмиванню грошей та фінансуванню тероризму в ЄС.

http://surl.li/pscxkt

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Розвиток різноманітності – результати опитування BIS 2023 року щодо цифрових валют центрального банку і криптовалют

Документ представляє результати опитування BIS 2023 року, в якому взяли участь 86 центральних банків. У ньому зазначено, що 94% опитаних центральних банків досліджують можливості запровадження цифрових валют центральних банків (CBDC), причому спостерігається значне збільшення експериментів та пілотних проектів. Опитування підкреслює різноманітність підходів до розробки CBDC, з різним залученням розвинених економік та країн, що розвиваються.

Ймовірність випуску оптового CBDC[1] протягом наступних шести років тепер вища, ніж роздрібного CBDC[2]. Для роздрібних CBDC понад половина центральних банків розглядають такі особливості, як обмеження на зберігання, інтероперабельність, офлайн-опції та відсутність винагороди. Основна увага щодо оптових CBDC приділяється інтероперабельності та програмованості. Мотивами центральних банків є підвищення фінансової інклюзивності, забезпечення стабільності фінансової системи та покращення ефективності транскордонних платежів.

У документі також наведено інформацію про використання стейблкоїнів, які рідко використовуються для платежів поза криптоекосистемою. Однак центральні банки все частіше розробляють нормативні бази для вирішення ризиків, пов'язаних зі стейблкоїнами та іншими криптоактивами, при цьому понад 60% юрисдикцій вже мають або розробляють такі рамки.

Документ наголошує на необхідності глобальної співпраці для забезпечення безпечних та ефективних платіжних систем на тлі цифрової трансформації та появи приватно випущених грошей. Він завершується закликом до прийняття різноманітності та спільного прогресу, щоб впоратися з можливостями та ризиками, які виникають у результаті інновацій у платіжній сфері.

https://www.bis.org/publ/bppdf/bispap147.htm

Перетворення законно отриманих ресурсів на незаконні виплати: схема забруднення коштів

Це дослідження зосереджено на русі грошей у фінансовій інфраструктурі, побудованій для приховування їх походження та призначення. Вже існує багато досліджень у сфері відмивання грошей щодо перетворення незаконних грошей у законне джерело, але менше відомо про зворотний процес, приховування та передачу законно отриманих ресурсів для виплати «відкатів» чиновникам. Автори прагнуть проаналізувати, як працюють ці схеми із забруднення грошей, і дослідити їхні приховані механізми. У статті досліджується, що відбувається з грошима в невидимому фінансовому кластері, і визначаються основні дійові особи та інфраструктури, необхідні для управління таким процесом. Використовуючи якісний аналіз різних документів, у статті розглядається корупційна схема, розроблена групою Odebrecht для отримання ресурсів для підкупу політиків і бюрократів у країнах Латинської Америки та на південь від Сахари.

---

[1] Оптові CBDC призначені для використання фінансовими установами, такими як банки та інші фінансові організації, а не широкою громадськістю.

[2] Роздрібні CBDC призначені для широкої громадськості, включаючи домогосподарства та бізнеси, для щоденних транзакцій.

Він наближає увагу до одного з ключових компонентів цієї системи, групи навколо двох перуанських підприємців, де гроші ховаються від очей правоохоронних органів і слідчих. Основний внесок полягає в концептуальному розрізненні між схемами відмивання грошей і забруднення грошей, а також у можливості викриття та тлумачення невидимих критичних процесів такого незаконного руху ресурсів.

http://surl.li/ostdho

Формування майбутнього: дорожня карта відбудови України за допомогою віртуальних активів

Що спільного між віртуальними активами та відбудовою України? Щоб дізнатися про це, прочитайте новий аналітичний запис Оксани Ігнатенко «Формування майбутнього: дорожня карта відновлення України за допомогою віртуальних активів».

Віртуальні активи неочікувано стали ознакою війни та джерелом підтримки проукраїнських зусиль. Але в їх використанні також є ризики.

У цій аналітичній записці описано кроки, які в першу чергу повинен зробити український уряд, щоб мати можливість безпечно використовувати пожертвування віртуальних активів для конкретних проектів реконструкції. Це включає забезпечення регульованого середовища, гарантії щодо кібербезпеки та додаткові рівні перевірки для підтвердження того, як використовуються кошти.

http://surl.li/nimcbw

«Ваші дані викрадено та зашифровано»: досвід жертви програм-вимагачів

🕸Новий звіт RUSI «Ваші дані викрадено та зашифровано»: досвід жертви програм-вимагачів»

🕵💻Хоча все більше людей і організацій стають жертвами атак програм-вимагачів, мало що відомо про досвід жертв. Для тих, хто залучений, це означає низьку точку в їхньому професійному та, можливо, навіть приватному житті з наслідками, які відчуваються далеко за межі часу негайної реакції.

🔍 У новому звіті RUSI, який ґрунтується на інтерв'ю з жертвами програм-вимагачів та зацікавленими сторонами, досліджуються деякі фактори, які можуть або покращити, або погіршити вплив програм-вимагачів на людей, зокрема:

- Час, масштаб і контекст інциденту.
- Рівень підготовки у формі сильних заходів кібербезпеки та планів на випадок надзвичайних ситуацій.
- Людські фактори, такі як середовище на робочому місці та існуюча динаміка, яка часто посилюється під час нещасного випадку.
- Взаємодія зі сторонніми постачальниками послуг, такими як ті, що надають технічне реагування на інциденти або юридичні послуги.
- Успішна комунікаційна кампанія, яка сильно залежить від контексту та жертви.

🕵️⚖️Звіт надає фахівцям з кібербезпеки краще розуміння впливу програм-вимагачів для розробки ефективних планів реагування, заходів політики та реагування на інциденти, а також пропонує 12 рекомендацій для підтримки жертв.

http://surl.li/sxpklz

Підпільний Китай

Розслідування показує, як мільярди євро незаконно переводять з Італії до Китаю через складні системи відмивання грошей. З початку десятиліття десять мільярдів євро офіційних переказів від китайської громади в Італії зникли, зменшившись з майже 2 мільярдів євро в 2012 році до кількох мільйонів минулого року. Китайські посередники сприяють незаконному переказу грошей, часто пов'язаному з податковим шахрайством і діяльністю мафії.

Розслідування Guardia di Finanza та італійської прокуратури виявили величезну мережу відмивання грошей, відому як "Chinese Underground Bank", яка працює через низку брокерів. Ця мережа дозволяє безслідно переказувати великі суми грошей, часто використовуючи шахрайські механізми з ПДВ та контрабанду товарів. Система також включає платежі за незаконну діяльність, таку як наркотрафік і проституція.

Італія є ключовим вузлом у цій системі, а порти та торгові центри діють як хаби для грошових переказів. Розслідування показало, як китайські компанії за допомогою ухилення від оподаткування і використання нелегальної робочої сили створюють великі суми брудних грошей, які потім переводять до Китаю.

Відсутність співпраці з китайськими банками та абсолютна секретність китайської банківської системи ще більше ускладнюють розслідування. Незважаючи на прохання про допомогу з боку італійської влади, Пекін не надав суттєвих відповідей, залишаючи багато питань щодо того, наскільки китайська держава обізнана про ці операції.

Тривають розслідування, у різних італійських містах розслідуються численні випадки, і міжнародний інтерес до цього питання зростає.

http://surl.li/tfodtt

Euro SIFMANet: Звіт круглого столу про санкції в сфері віртуальних активів

Чи використовує російський уряд індустрію віртуальних активів для обходу санкцій?

Минулого тижня Європейська рада встановила заборону на транзакції для постачальників послуг з криптоактивами в ЄС, якщо вони сприяють транзакціям, які підтримують оборонно-промисловий комплекс Росії.

У травні 2024 року CFS скликав круглий стіл за участю експертів і практиків державного та приватного секторів у Брюсселі, щоб дослідити загрозу використання віртуальних активів для обходу санкцій, а також те, як зменшити ризики для галузі.

https://static.rusi.org/digital-assets-sanctions-report-SIFMANET-web-final.pdf

Звіт про зберігання цифрових активів 2024

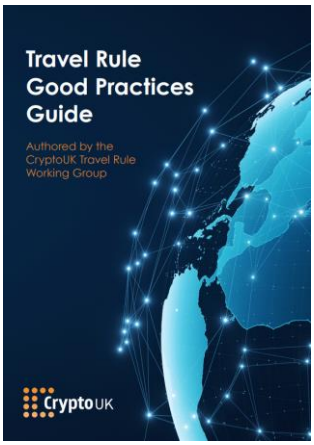
Швейцарський звіт про зберігання цифрових активів на 2024 рік описує розвиток екосистеми зберігання цифрових активів у Швейцарії, включаючи інтеграцію цифрових активів у традиційну фінансову систему. Звіт підкреслює важливість стейблкойнів, різних інвестиційних продуктів і доступу до криптоторгових майданчиків. Він також розглядає виклики зберігання цифрових активів, такі як управління криптографічними ключами та забезпечення безпеки активів. Крім того, документ охоплює регуляторні аспекти, ліцензування, страхування депозитів та значення MiCA (Markets in Crypto Assets Regulation) для швейцарських постачальників послуг зберігання.

Звіт показує зростання числа банків та інших установ, що надають послуги зберігання цифрових активів, а також збільшення різноманіття підтримуваних активів, включаючи токени безпеки та NFT. Важливим аспектом є доступ до нових європейських ринків відповідно до регуляторних вимог MiCA, що створює нові можливості для швейцарських компаній. Документ наголошує на важливості інновацій та ролі регуляторів у сприянні розвитку цифрових фінансових послуг.

Цей звіт є важливим ресурсом для розуміння поточного стану та перспектив розвитку зберігання цифрових активів у Швейцарії, підкреслюючи ключові тенденції та виклики, з якими стикається галузь.

https://www.homeofblockchain.swiss/reports

Посібник із належної практики щодо Travel Rule



Документ "Travel Rule Good Practices Guide", створений робочою групою CryptoUK, спрямований на надання рекомендацій для постачальників послуг віртуальних активів (VASPs) щодо дотримання Travel Rule у Великобританії. Мета документа полягає в забезпеченні зрозумілого керівництва для VASPs та учасників ринку цифрових активів, допомагаючи їм ефективно виконувати вимоги Travel Rule та розв'язувати пов'язані з цим проблеми.

Travel Rule вимагає, щоб VASPs збирали, зберігали та передавали інформацію про відправника і одержувача віртуальних активів для запобігання незаконній діяльності. Документ описує регуляторну базу Великобританії, ключових учасників, включаючи Управління фінансового нагляду (FCA), Joint Money Laundering Steering Group (JMLSG) і Казначейство Її Величності (HMT), а також розглядає специфічні вимоги до виконання Travel Rule.

Звіт містить розділи про належну перевірку контрагентів (Counterparty VASP Due Diligence, CVDD), процеси зняття та депонування коштів, а також управління ризиками, пов'язаними з неконтрольованими гаманцями. Робоча група пропонує принципи і підходи для розробки ефективної системи CVDD, включаючи використання технологічних рішень і третіх сторін для збору і верифікації інформації.

Документ також підкреслює важливість автоматизації процесів для підвищення ефективності і точності перевірок відповідності, а також необхідність встановлення чітких процедур у випадку неповної або відсутньої інформації. Наголошується на важливості співпраці між VASPs для стандартизації підходів до виконання Travel Rule і забезпечення взаємодії між різними постачальниками послуг.

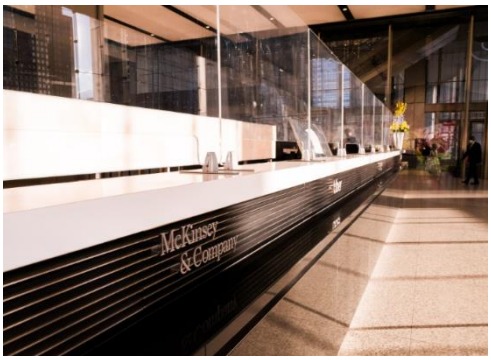
Рекомендації в документі спрямовані на підвищення обізнаності учасників ринку про регуляторні вимоги, покращення процесів дотримання правил та сприяння прозорості та безпеці віртуальних

активів. CryptoUK закликає VASPs дотримуватися рекомендацій і активно співпрацювати з регуляторами для забезпечення відповідності Travel Rule та захисту інтересів усіх учасників ринку.

https://bit.ly/461sgck

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

When McKinsey Comes to Town: прихований вплив найпотужнішої консалтингової фірми світу



Книга «When McKinsey Comes to Town: The Hidden Influence of the World's Most Powerful Consulting Firm» Уолта Богдановича та Майкла Форсайта є проникливим дослідженням ролі та впливу консалтингової фірми McKinsey & Company на глобальну економіку і політику. Автори ретельно досліджують, як ця впливова фірма допомагала урядам і корпораціям ухвалювати стратегічні рішення, часто зі значними наслідками для суспільства.

Однією з центральних тем книги є співпраця McKinsey з клієнтами, які були замішані у відмиванні коштів і фінансуванні тероризму. Богданович і Форсайт наводять конкретні приклади того, як McKinsey надавала консультації компаніям і урядам, які брали участь у незаконних фінансових операціях. Книга піднімає питання про етичність рішень McKinsey щодо вибору клієнтів і характеру наданих послуг, зокрема коли йдеться про клієнтів з репутацією, яка викликає сумніви.

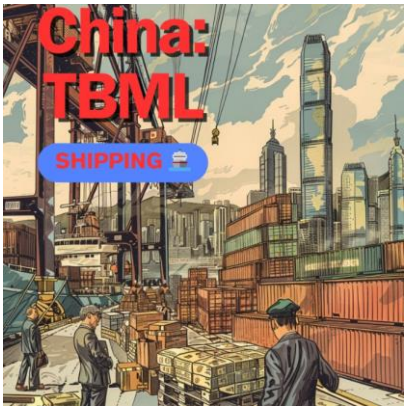
Автори показують, як рекомендації McKinsey іноді сприяли посиленню корупційних практик і підривали зусилля з боротьби з відмиванням коштів та фінансуванням тероризму. Книга розглядає випадки, коли консалтингова фірма впливала на політичні та економічні реформи, що мали суперечливі наслідки для фінансової прозорості.

«When McKinsey Comes to Town» також досліджує внутрішні механізми McKinsey & Company, які дозволяють їм утримувати значний вплив на глобальному рівні. Автори розповідають історію створення і розвитку фірми, надаючи контекст для розуміння її сучасної ролі у світі.

Ця книга є важливим джерелом для розуміння складних питань етики в консалтинговій сфері, особливо у випадках, коли діяльність таких фірм може мати серйозні наслідки для боротьби з фінансовими злочинами. Богданович і Форсайт закликають до більшої прозорості та відповідальності в діяльності великих консалтингових компаній, підкреслюючи необхідність жорсткішого регулювання їхньої роботи.

https://www.amazon.com/When-McKinsey-Comes-Town-Consulting/dp/0593663322

Flags of Convenience



Перетин морської торгівлі та незаконного фінансування викликає дедалі більше занепокоєння, особливо коли досліджується потенційна експлуатація Китаєм судноплавної галузі.

Зручні прапори (FOC) дозволяють власникам суден реєструвати судна в інших країнах, часто з мінімальним наглядом. Майже 75% світового флоту плаває під цими прапорами, створюючи завісу непрозорості, яку можна використовувати для підлих цілей.

Протиправна діяльність Китаю:

З нової книги «Зручні прапори» Марка Піта та Кетрін Бетц ми бачимо тривожну картину:

1. Відмивання грошей у комерційних цілях (TBML): складні структури власності та FOC можуть приховувати справжню природу транзакцій.

2. Ухилення від санкцій: «тіньовий флот» і непрозора власність допомагають обійти міжнародні санкції.

3. Підробка: вразливі місця в контейнерних перевезеннях сприяють глобальному розповсюдженню підроблених товарів.

4. Торгівля наркотиками та дикими тваринами: проблеми з моніторингом великої кількості контейнерів сприяють контрабанді.

5. Кіберексплуатація: потенційний злом морських систем для маніпулювання даними про вантаж.

6. Компанії-оболонки: шари корпоративних структур приховують справжню власність і участь держави.

7. Експлуатація зон вільної торгівлі: поєднання зон вільної торгівлі з вразливостями судноплавства ще більше приховує незаконну торгівлю.

Книга «Зручні прапори» розкриває непрозорий світ глобального судноплавства, деталізуючи, як відсутність прозорості в галузі та слабке правозастосування створюють можливості для зловживань. Автори стверджують, що ця система дозволяє недобросовісним особам уникнути відповідальності та потенційно брати участь у незаконній діяльності. Конвергенція цих факторів створює ідеальне середовище для фінансових злочинів.

https://files.web.host.ch/88/21/8821710a-119a-4e90-a960-82178175e31b.pdf

ІНШІ НОВИНИ

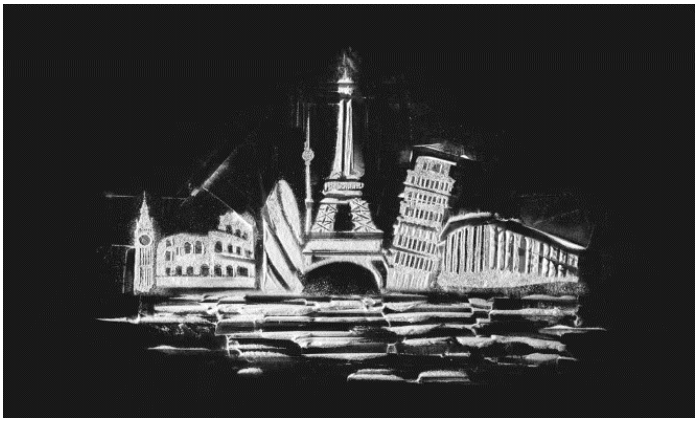
Підбірка новин Dirty Money

У даній публікації розглядається роль криптовалют у відмиванні коштів та пов'язані з цим ризики. Основні моменти даної публікації:

1. У 2023 році через глобальну фінансову систему пройшло $3,1 трлн нелегальних коштів, але лише $24,2 млрд (0,08%) через криптовалюти.
2. Міжнародні фінансові організації (МВФ, FATF, ФРС, ЄЦБ) підкреслюють потенційні ризики криптовалют для відмивання коштів.
3. Основні проблеми: анонімність транзакцій, глобальне охоплення, децентралізована природа криптовалют.
4. Важливість регулювання постачальників послуг віртуальних активів (VASP) та впровадження заходів протидії відмиванню коштів.
5. Ризики пов'язані з використанням криптовалют на Dark Web для нелегальних операцій.
6. Роль крипто-міксерів у підвищенні анонімності транзакцій.
7. Здебільшого відмивання кошів все ще відбувається через традиційну банківську систему.
8. Нові ризики: крипто-банкомати та майнінг криптовалют.
9. Необхідність кращого регулювання та міжнародного співробітництва для боротьби з відмиванням коштів через криптовалюти.
10. Заклик до розробки технологій, які б допомогли запобігати відмиванню кошіт у децентралізованому криптофінансовому світі.

http://surl.li/xrkmsb

Наскільки велика проблема кокаїну в Європі – і яка ціна для людини?



За останні 10 років Європа зіткнулася з серйозною проблемою, пов'язаною з кокаїном. Цей наркотик, що походить із джунглів Південної Америки, транспортується, продається і вживається по всьому європейському континенту у рекордних кількостях. Зростання попиту серед користувачів і величезні прибутки, які можна отримати на цьому ринку, змінюють міжнародну торгівлю наркотиками по обидва боки Атлантики.

За останнє десятиліття торгівля кокаїном у Європі значно зросла. Найсвіжіший звіт UNODC показує, що Велика Британія має другий найвищий рівень вживання кокаїну у світі, де кожен сороковий дорослий (2,7% населення) вживає цю наркотичну речовину. Національне агентство з боротьби зі злочинністю Великої Британії (NCA) оцінює, що щорічно у Великій Британії споживається близько 117 тон кокаїну. У Європейському Союзі майже 2,5 мільйона людей віком від 15 до 34 років (2,5% цієї вікової групи) вживали кокаїн протягом останнього року. Аналіз ООН свідчить про вирішальний момент у розширенні ринків кокаїну в Західній і Центральній Європі, де збільшилася пропозиція та споживання цього наркотику. Згідно з Європейським звітом про наркотики за 2024 рік, залишки кокаїну у стічних водах зросли у двох третинах європейських міст за останні два роки.

Europol і EMCDDA зазначають, що наркоторгівля призводить до небувалих рівнів експлуатації дітей, злочинів із застосуванням зброї та насильства. Наприклад, мер Амстердама попереджає, що торгівля кокаїном може перетворити Нідерланди на "наркодержаву", поглинуту кримінальними грошима, насильством та експлуатацією. Кокаїн, який часто вважають рекреаційним наркотиком, є високоадиктивним. Його зростаюча чистота та поширеність, спричинені продажами через соціальні медіа та зашифровані месенджери, мають катастрофічні наслідки для користувачів, їхніх сімей та громад.

http://surl.li/uhmotv

Тижневий огляд від TRM Labs

TRM Labs — це компанія, що займається питаннями пошуку інформації у блокчейнах, яка допомагає фінансовим установам, криптобізнесу та державним установам виявляти та розслідувати пов'язані з криптовалютою фінансові злочини та шахрайство. Щодня вони вирішують завдання в галузі обробки даних, data science та аналізу загроз.

Цього тижня вони більш детально розглянули наступні питання:

- IRS випускає довгоочікувані правила звітності про податок на криптовалюту
- FinCEN оголошує правила для модернізації програм з ПВК
- Верховний суд США скасовує регулятивні відхилення
- 5-й звіт FATF про віртуальні активи
- Правила MiCA для стейблкоїнів
- Наступні кроки для криптосистеми Гонконгу

https://www.linkedin.com/pulse/trm-weekly-roundup-july-4-2024-trmlabs-nonse/

Ключові новини з пленарного засідання FATF

Завершилося шосте і останнє пленарне засідання FATF під головуванням Сінгапуру. Ось основні результати:

↳ Оновлення сірого списку: додалися Монако та Венесуела, а Ямайка та Туреччина були видалені.

↳ Чорний список: Без змін

↳ FATF встановила нові критерії, щоб визначити, які країни зі слабким контролем ПВК/ФТ будуть перевірені в рамках ICRG.

↳ Членів FATF оцінюватимуть за їхніми зусиллями щодо надання пріоритету поверненню, відстеженню викрадених активів, примусовій конфіскації та міжнародній співпраці на основі нового методу оцінки.

↳ Звіт про взаємну оцінку Індії демонструє високий рівень технічної відповідності, проте необхідні вдосконалення нагляду за нефінансовим сектором.

↳ У Звіті про взаємну оцінку Кувейту зроблено висновок, що країна має належну правову базу, але є серйозні недоліки в досягненні ефективних результатів.

↳ FATF опублікує свої висновки перевірки заходів своїх членів щодо запобігання використанню бухгалтерів, юристів, агентів з нерухомості та TCSP для відмивання грошей і фінансування тероризму

↳ 75% юрисдикцій частково не відповідають стандартам FATF у сфері віртуальних активів. FATF публікуватиме п’яте щорічне оновлення щодо прогресу країн у сфері ВА.

↳ FATF оновлює свої стандарти з ПВК, щоб адаптувати їх до сучасних платіжних систем (наприклад, ISO20022). Вони прагнуть зробити транскордонні платежі швидшими, дешевшими та зрозумілішими для всіх, водночас запобігаючи фінансовим злочинам.

↳ Відсторонення РФ продовжує діяти.

https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-june-2024.html

Міністерство фінансів США публікує режим оподаткування криптовалют на 2025 рік, відкладаючи правила для не зберігачів

Стаття на CoinDesk детально описує новий податковий режим для криптовалют, запроваджений Міністерством фінансів США для 2025 року, та відтермінування правил для учасників, які не надають послуги зі зберігання. Згідно з новими правилами, криптовалютні брокери будуть зобов'язані подавати форми 1099, подібно до традиційних інвестиційних компаній. Однак, правила для децентралізованих фінансових операцій (DeFi) та гаманців, що не надають послуги зі зберігання, були відкладені для подальшого вивчення.

Ці правила мають на меті покращити виявлення податкових порушень у сфері цифрових активів і забезпечити більшу прозорість. Основна частина критики стосується можливих надмірних вимог до майнерів, розробників програмного забезпечення та інших учасників, які не є брокерами і не мають необхідної інформації або інфраструктури для дотримання цих вимог.

Також правила передбачають деякі винятки для користувачів стейблкоїнів, якщо вони не заробляють більше $10,000 на рік від цих активів. Для продажу стейблкоїнів будуть застосовуватись об'єднані звіти замість індивідуальних транзакцій. Продажі NFT, що приносять більше $600 на рік, також підлягатимуть звітності.

Нові регуляції спрямовані на те, щоб запобігти використанню цифрових активів для приховування оподаткованого доходу, водночас спрощуючи процес звітності для платників податків. Якщо Конгрес ухвалить законопроекти щодо регулювання емітентів стейблкоїнів, податкові правила можуть бути переглянуті.

http://surl.li/yvdcjj

Судовий процес у справі «Panama Papers» завершився виправданням усіх обвинувачених у відмиванні грошей

У знаковому рішенні суди Панами виправдали всіх 28 обвинувачених у судовому процесі щодо PanamaPapers, включаючи Юргена Моссака, співзасновника нині неіснуючої юридичної фірми Mossack Fonseca. Суд завершився 28 червня 2024 року після більш ніж двох місяців розгляду. Підсудних звинувачували у створенні компаній-оболонок, залучених у корупційні скандали в Бразилії та Німеччині. Суд, який у квітні тривав 85 годин, включав свідчення 27 свідків і понад 50 доказів. Незважаючи на прохання про максимальне покарання для ключових фігур, суддя Балоїза Маркінес зняла всі звинувачення. Справа була частиною ширшого розслідування Panama Papers, важливого журналістського заходу, спрямованого на розкриття офшорних фінансових таємниць світових лідерів.

http://surl.li/arisad

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Процес перевірки клієнта

Перевірка та моніторинг клієнтів діють як захист від фінансових злочинів, таких як відмивання коштів, фінансування тероризму та шахрайство, захищаючи як фінансові установи, так і їхніх клієнтів. Розуміючи цей процес, установи можуть бути більш пильними щодо процесу комплаєнсу.

✓ Збір даних

Перший крок передбачає збір необхідної інформації про клієнта за допомогою процедур "Знай свого клієнта" (KYC).

Сюди входять:

- Особисті дані, такі як ім'я, дата народження та адреса.
- Контактна інформація, включаючи номер телефону та адресу електронної пошти.
- Видані державою документи, що посвідчують особу (паспорт, водійські права тощо).
- Інформація про бенефіціарних власників (для компаній).

✓ Методи верифікації

Нижче наведено кілька поширених методів верифікації:

- Перевірка документів: Фізичні документи перевіряються на справжність і порівнюються з державними базами даних.
- Перевірка баз даних: Інформація про клієнта перевіряється за різними базами даних, включаючи:
- Списки санкцій: Фізичні або юридичні особи, яким заборонено займатися бізнесом через урядові санкції.
- Списки політично значущих осіб (PEP): Особи, які займають важливі державні посади або мають тісні зв'язки з такими особами.
- Негативні відгуки ЗМІ: Публічні записи та джерела новин скануються на наявність негативної інформації про клієнта.
- Послуги сторонніх перевірок: Для проведення більш поглиблених перевірок можуть залучатися спеціалізовані фірми.

✓ Оцінка ризиків

Ця оцінка враховує такі фактори, як

- Джерело доходу: Оцінюється законність і прозорість джерела доходу клієнта.
- Структура транзакцій: Обсяг, частота та характер транзакцій клієнта аналізуються на предмет підозрілої діяльності.
- Географічне розташування: Країни з високим ризиком відмивання коштів можуть вимагати посиленої перевірки.
- Статус PEP: Тісні зв'язки з публічними діячами можуть підвищити профіль ризику клієнта.
- Негативні повідомлення в засобах масової інформації: Негативні новини про клієнта або пов'язаних з ним осіб можуть викликати тривогу.

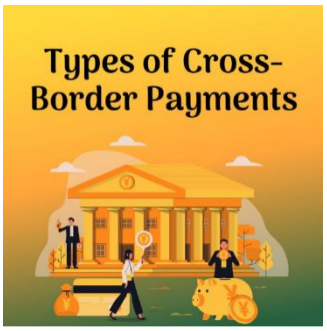
✓ Прийняття рішень

Використовуючи оцінку ризиків як орієнтир, установи приймають обґрунтовані рішення щодо встановлення ділових відносин:

- Затвердження: Якщо профіль ризику вважається прийнятним, процес встановлення відносин з клієнтом можна продовжувати.

- Запит додаткової інформації: У деяких випадках перед прийняттям рішення може знадобитися додаткова інформація або перевірка.
- Відмова: Для клієнтів з високим рівнем ризику може знадобитися відмова від ділових відносин, щоб зменшити потенційні ризики.

Типи транскордонних переказів



✓ Грошові перекази: Переказ коштів від однієї особи в іншу країну, як правило, родині або друзям.

✓ Перекази між підприємствами (B2B): Транзакції, що передбачають обмін платежами між компаніями через кордони, часто на значні суми.

✓ Перекази в рамках відносин B2C: Продаж товарів або послуг підприємствами клієнтам у різних країнах.Операції, в яких клієнт платить компанії в іншій країні, зазвичай за послуги або покупки в Інтернеті.

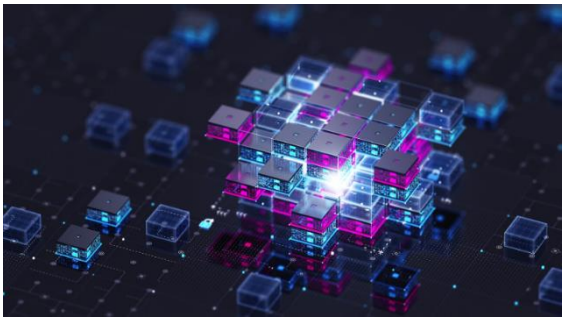
✓ Державні платежі: Фінансова взаємодія між урядами різних країн, що охоплює допомогу, торгові тарифи та інші види платежів.

✓ Транскордонні транзакції на великі суми: Транзакції, пов'язані з придбанням цінних активів, таких як нерухомість, предмети мистецтва, ювелірні вироби або розкішні транспортні засоби.

✓ Транзакції з використанням карток: Платежі, здійснені за кордоном з використанням фізичних кредитних або дебетових карток, як правило, туристами, експатріантами та відрядженими особами.

✓ Транзакції за відсутності картки (CNP): До цієї категорії відносяться міжнародні покупки в Інтернеті та комерційні платежі на користь іноземних компаній.

Як визначити 4 основних джерела фінансових злочинів, які ховаються у вашому банку



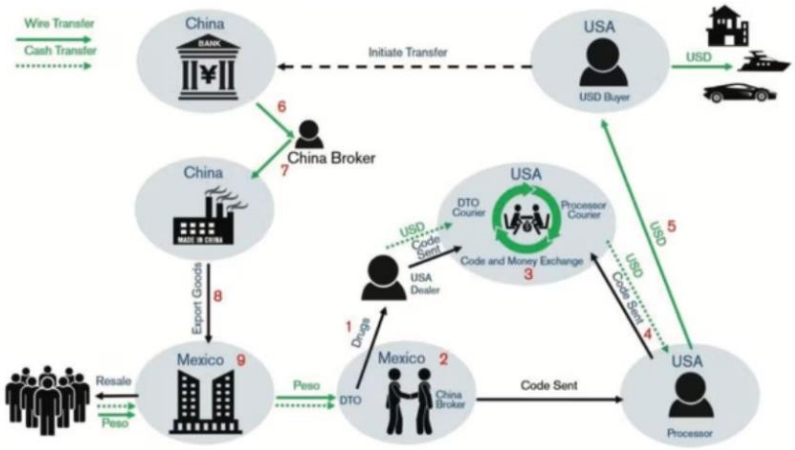
Стаття на блозі Quanteха обговорює чотири основні чинники, що сприяють фінансовим злочинам: підставні компанії, фенікування, контролюючий розум і грошові мули. Підставні компанії використовуються для приховування справжніх власників і ускладнення відстеження грошових потоків. Фенікування полягає у створенні нових компаній після ліквідації старих, часто з тими ж керівниками. Контролюючий розум - це особа, яка керує всією злочинною схемою. Грошові мули передають гроші між рахунками для маскування їх походження. Quanteха пропонує використовувати платформу Decision Intelligence для ефективного виявлення цих схем.

https://www.quantexa.com/blog/4-key-enablers-of-financial-crimes/

Мережа грошових брокерів

Нещодавня стаття Financial Times пролила світло на заплутані операції з відмивання грошей, в яких брали участь мексиканські наркокартелі та китайські посередники. Використовуючи підпільну

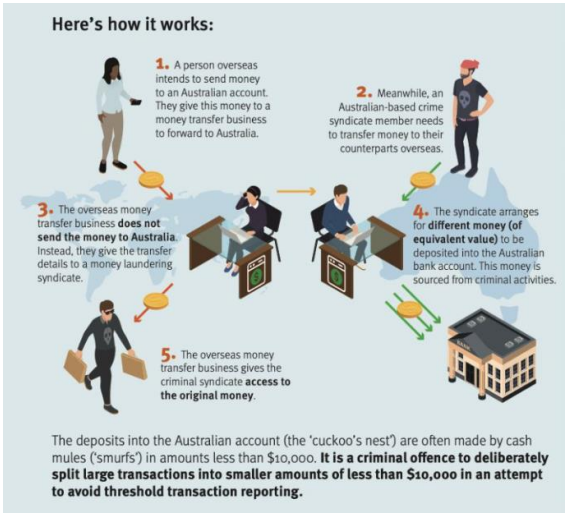
банківську систему, картелі відмивають мільярди доларів від продажу фентанілу у Сполучених Штатах, фактично обходячи суворі обмеження Китаю на грошові перекази.



Ключем до цієї схеми є китайські студенти за кордоном, які отримують готівку від місцевих контактів через такі платформи, як WeChat, в обмін на банківські перекази, зроблені їхніми батьками в Китаї. Ці гроші врешті-решт потрапляють до китайських виробників хімікатів. Ця складна система відмивання, що нагадує традиційний метод гавала, підкреслює глибокий зв'язок між наркотрафіком, валютними обмеженнями та міжнародними грошовими переказами.

Попит на долари серед китайців, які живуть за кордоном, настільки високий, що мексиканські картелі можуть відмивати свої гроші практично безкоштовно. У деяких випадках великі готівкові операції для витрат на освіту в США лише злегка перевіряються, тоді як неофіційні дані свідчать про те, що подібна практика може мати місце у Великій Британії, незважаючи на офіційну політику, яка забороняє приймати готівку. Торгівля фентанілом є прикладом цього методу, показуючи, як поєднуються сучасні та традиційні методи відмивання грошей.

Cuckoo smurfing



Чинні банківські правила вимагають від банків та інших фінансових установ направляти повідомлення про підозрілу діяльність при операціях з готівкою, що перевищують 10 000 євро, іноді навіть менше. Щоб уникнути цього, злочинці використовують смурфінг, техніку відмивання грошей, яка передбачає структурування великих сум готівки на ряд дрібних транзакцій.

«Смурфи» часто поширюють ці невеликі транзакції на багато різних рахунків, щоб утримувати їх у межах нормативних обмежень звітності та уникнути виявлення. Термін «смурф», запозичений від нелегальних виробників наркотиків, які використовують численних спільників, щоб уникнути законодавчих обмежень на закупівлю компонентів наркотиків.

Австралійська служба боротьби з фінансовими злочинами нещодавно попередила фінансовий сектор про певну місцеву типологію під назвою «cuckoo smurfing». Відмивачі грошей використовують її для переміщення незаконних коштів до та з Австралії, використовуючи законні транзакції, здійснені між непомітними особами та підприємствами. У більшості випадків вони співпрацюють із посередником, щоб без відома власника вкладати брудні гроші на законний рахунок. Назва навіяна пташкою зозулею, яка, як відомо, відкладає яйця в гнізда інших птахів.

Процес зазвичай відбувається так:

1. Люди за кордоном, які бажають переказати кошти до Австралії, звертаються до фінансової установи, не знаючи про її причетність до австралійської злочинної організації

2. Фінансова установа передає деталі транзакції (суму, назву та номер рахунку) зловмисникам

3. Потім вони використовують «смурфів», щоб зробити невеликі готівкові депозити на рахунок призначення, фактично переказуючи очікувану суму

4. Водночас корумпована фінансова установа перенаправляє законні кошти на рахунок злочинців, який часто знаходиться в офшорах

5. Найгірше те, що якщо хтось виявляє готівкові депозити, створюється враження, що одержувач коштів є спільником, що може призвести до заморожування рахунку.

Щоб уникнути цього, є кілька хороших практик:

- ✓ Ретельно відстежуйте послідовні готівкові депозити на той самий рахунок протягом короткого періоду часу
- ✓ Беріть до уваги ситуацію власника рахунку (іноземні студенти частіше отримують гроші з-за кордону)
- ✓ (Для фізичних осіб) Слідкуйте за можливими структурованими платежами, коли очікуєте переказ з-за кордону