Nowe horyzonty przestępczości finansowej

Pranie pieniędzy, finansowanie terroryzmu i inne zagrożenia w ekosystemach gier Web2 i Web3

Global Coalition To Fight Financial Crime | Digital Asset Task Force | Financial Crimes in Gaming Work Group

Ekosystemy gier: Jedne z największych środowisk transferu wartości

189 mld USD

Globalne przychody z gier w 2025 r. (PwC Global Entertainment & Media Outlook 2025-2029)

300+ mld USD

Prognozowane przychody sektora do 2029 r. — jeden z najwyższych wskaźników wzrostu w gospodarce cyfrowej

3,6 miliarda

Aktywnych graczy na świecie — około 62% światowej populacji użytkowników internetu

1,6 miliarda

Graczy wydających pieniądze na platformach gamingowych w ciągu każdych sześciu miesięcy

Platformy gamingowe pełnią funkcje ekonomicznie analogiczne do licencjonowanych instytucji płatniczych i transferu wartości:

(1) Emisja własnych jednostek rozrachunkowych (np. V-Bucks, Robux, Linden Dollars) · **(2) Przechowywanie** sald użytkowników w rejestrach kontrolowanych przez platformę · **(3) Transfer** wartości między użytkownikami, w tym transgranicznie · **(4) Wymiana** przez wtórne rynki aktywów · **(5) Realizacja** wirtualnych sald na waluty fiducjarne

Gdy licencjonowana instytucja finansowa wykonuje chociaż jedną z tych funkcji, podlega obowiązkom AML/CFT. Gdy platforma gamingowa wykonuje wszystkie pięć, może nie podlegać.

Nierówności oraz braki - co widać obecnie?

Problem

- Platformy gamingowe są prawnie klasyfikowane jako usługa rozrywkowa lub cyfrowa, mimo że ich architektura pełni funkcje ekonomicznie analogiczne do sieci płatniczych i transferu wartości.
- Nadzór jest rozproszony między regulatora ds. usług cyfrowych, organy ochrony konsumentów, organy hazardowe i agencje ochrony danych. Organy finansowe angażują się jedynie pośrednio.
- Żadne pojedyncze organy nie są upoważnione do oceny ekosystemów gamingowych jako składników krajowej infrastruktury wartości z punktu widzenia ryzyka przestępczości finansowej.
- Ekosystemy gamingowe są rzadko ujmowane w Krajowych Ocenach Ryzyka (NRA), a gry oparte na blockchainie niemal nigdy.

Konsekwencje

Przesunięcie ryzyka: platformy gamingowe projektują i kontrolują wewnętrzną architekturę wartości, natomiast regulowane instytucje finansowe przejmują odpowiedzialność compliance, monitoringu i reputacyjną w punktach konwersji.

Brak transgranicznego pola widzenia: gdy przepływ wartości następuje między jurysdykcjami w ramach jednej platformy, krajowe organy nie mają pełnego obrazu całego systemu.

Spójność regulacyjna jest naruszona: porównywalne funkcjonalnie transfery transgraniczne mogą podlegać zasadniczo różnym ramom nadzorczym, w zależności od tego, czy dotyczą banku, instytucji płatniczej, czy ekosystemu gamingowego.

MiCA obejmuje gry z kryptoaktywami; platformy nieposiadające produktów opartych na kryptoaktywach pozostają poza zakresem tej regulacji i mogą nadal działać bez jakichkolwiek ram regulacyjnych.

Gaming Web3: Krajobraz zagrożeń

Studium Przypadku: Axie Infinity / Włamanie do Sieci Ronin

- Atak hakerski na sieć Ronin (marzec 2022 r.) został przypisany przez FBI państwowej grupie hakerskiej Lazarus Group z Korei Północnej.
- Napastnicy użyli inżynierii społecznej, by przejąć większość węzłów walidatora Ronin, kradnąc około 173 600 ETH i 25,5 mln USDC - ówcześnie około 620 mln USD - największa na tamten czas kradzież kryptoaktywów w historii.
- Skradzione aktywa zostały nastepnie zmiksowane przez Blender.io i Tornado Cash, co przyczyniło się do nałożenia przez US Treasury sankcji na oba mixery.

Rynki Podmiotów Zewnętrznych i Sieci Mules

› Nieuregulowane rynki podmiotów zewnętrznych (G2G, PlayerAuctions, DMarket, SkinBaron) tworzą równoległą infrastrukturę finansową, działającą poza jakimikolwiek ramami AML/CFT. Rynki te zazwyczaj wymagają minimalnej weryfikacji tożsamości i akceptują kryptowaluty, karty przedpłacone i aplikacje płatnicze P2P.

› Grupy przestępcze używają platform gamingowych oraz kanałów Discord i czatu wewnątrzgrupowego do werbowania osób (często nieświadomych) do otrzymywania, transferowania lub wypłacania nielegalnych dochodów.

› Kradzież kont, phishing i inżynieria społeczna są szeroko rozpowszechnione; tak zdobyte konta są następnie używane do transferów aktywów bez wiedzy i zgody ich prawdziwych właścicieli.

Rekomendowane działania i możliwe przyszłe środki regulacyjne

Istotą jest przywrócenie spójności między funkcją ekonomiczną a zarządzaniem przestepczoscia finansowa w sposob proporcjonalny i oparty na ryzyku.

Regulatorzy i Jednostki Wywiadu Finansowego

- Przeprowadzić mapowanie ryzyka głównych platform jako część Krajowych Ocen Ryzyka, identyfikując osadzone systemy wartości, wolumeny transakcji i ekspozycje transgraniczne.
- Ustanowić sformalizowane i bezpieczne kanały wymiany informacji z wiodącymi operatorami platform gamingowych, w tym dobrowolne lub prawnie zdefiniowane mechanizmy automatycznego raportowania.
- Wyznaczyć mechanizmy koordynacji łączące regulatorów finansowych, regulatorów usług cyfrowych i organy ochrony konsumentów.
- Ocenić, czy określone umożliwiane czynności finansowe, w szczególności transfery o wysokiej wartości lub realizowanie wypłat, wymagają nałożenia odpowiednich obowiązków AML/CFT niezależnie od etykiety sektorowej.

Platformy Gamingowe

- Przeprowadzić wewnętrzne oceny ryzyka analizujące sposób emitowania, przechowywania, transferowania, handlowania i wypłaty wartości, ze szczególnym naciskiem na wymianę wartości na blockchainie.
- Wprowadzić identyfikowalność, współpracę z dostawcami analityki blockchainu i możliwość audytu jako elementy projektu od początku, jeżeli dana gra będzie korzystała z powiązanych elementów.
- Ustanowić dedykowane funkcje interfejsu regulacyjnego zdolne do strukturalnego zaangażowania z organami finansowymi i FIU.
- Przyjąć dobre praktyki projektowania: proaktywne przewidywanie, wykrywanie i łagodzenie szkód na etapie tworzenia produktu.

Instytucje Finansowe

- Stosować wzmożone środki bezpieczeństwa w stosunku do platform (merchantów) z działalnością transgraniczną, wewnętrznym handlem lub funkcjami wypłaty aktywów.
- Różnicować klientów gamingowych w oparciu o cechy biznesu oraz oferowanego produktu.
- Opracować wspólne oczekiwania dotyczące ujawniania informacji za pośrednictwem stowarzyszeń bankowych i sieci płatniczych.
- Zaangażować się w dialog z nadzorcami w celu wyjaśnienia i ustrukturyzowania ram dotyczących sposobu podziału odpowiedzialności w punktach konwersji na fiat i kryptoaktywa.

Wnioski Końcowe

Czy istniejące ramy prawne dotyczące przestępczości finansowej i regulacji gier będą ewoluować w sposób wystarczająco skoordynowany i proporcjonalny, aby sprostać rosnącemu znaczeniu złożonych cyfrowych systemów wartości w globalnej gospodarce?

1. Ryzyka przestępczości finansowej w ekosystemach gamingowych będą się prawdopodobnie materializować nie jako nagłe, skokowe wzrosty, lecz przez stopniową ewolucję, migrację i adaptację w ramach sfragmentaryzowanego i nierównego krajobrazu nadzorczego.

2. Niezbędna jest większa przejrzystość i wytyczne regulacyjne w zakresie klasyfikacji i traktowania aktywów wewnątrzgrowych, wzmocniona transgraniczna koordynacja nadzorcza oraz spójniejsza alokacja odpowiedzialności operacyjnej i prawnej wśród uczestników rynku.

3. Reaktywne egzekwowanie prawa może nie wystarczyć. Konieczne jest natomiast opracowanie spójnych, wybiegających w przyszłość ram zarządzania, zdolnych do adresowania zarówno ryzyk związanych z kryptoaktywami, jak i opartych na walucie fiducjarnej.

GLOBAL COALITION TO FIGHT FINANCIAL CRIME

Nowe horyzonty przestępczości finansowej

Pranie pieniędzy, finansowanie terroryzmu i inne zagrożenia w ekosystemach gier Web2 i Web3

GLOBAL COALITION TO FIGHT FINANCIAL CRIME