27. NOVEMBRA 2025

CEZHRANIČNÉ OHLASOVANIE

STRATEGICKÁ ANALÝZA

FINANČNÁ SPRAVODAJSKÁ JEDNOTKA

Úvod

V súčasnej mimoriadne dynamickej dobe plnej fintech inovácií, zmenšovania prekážok vstupu na trh, globalizácií finančných a bankových produktov a taktiež zjednodušovania procesu začatia podnikania, napríklad v podobe nákupu ready-made spoločnosti a v neposlednom rade presun procesu tzv. on-boardingu klientov do online priestoru, čelia finančné spravodajské jednotky po celom svete stále novým trendom a výzvam v boji proti praniu špinavých peňazí, či financovania terorizmu.

Právny základ

Aktuálne zákon č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov špecificky neupravuje problematiku cezhraničného ohlasovania (tzv. cross-border reporting, ďalej len „XBR“), nakoľko aj legislatíva EÚ (najmä čl. 33 (2) a čl. 53(1) tretí odsek konsolidovaného znenia Smernice Európskeho parlamentu a Rady (EÚ) 2015/849 z 20. mája 2015 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu, ktorou sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 a zrušuje smernica Európskeho parlamentu a Rady 2005/60/ES a smernica Komisie 2006/70/ES (Text s významom pre EHP)) túto oblasť nedostatočne pokrývala.

Do budúcna je však v tomto kontexte dôležité vyzdvihnúť čl. 33 Smernice Európskeho parlamentu a Rady (EÚ) 2024/1640 z 31. mája 2024 mechanizmoch, ktoré majú členské štáty zaviesť na predchádzanie využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu, ktorou sa mení smernica (EÚ) 2019/1937 a mení a zrušuje smernica (EÚ) 2015/849 (Text s významom pre EHP)) a čl. 69(1) Nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1624 z 31. mája 2024 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu (Text s významom pre EHP)).

Účel strategickej analýzy

Všeobecným cieľom tejto strategickej analýzy je poskytnúť ucelený a komplexný pohľad na XBR prijaté v rámci vyššie popísaného cezhraničného režimu ohlasovania od piatich zahraničných partnerov v období od 15.03.2024 do 31.12.2024.

V tomto kontexte je však nevyhnutné uviesť, že za časové obdobie, ktoré táto strategická analýza pokrýva, FSJ prijala XBR len od niekoľkých desiatok zahraničných poskytovateľov platobných a e-money služieb resp. služieb v oblasti kryptoaktív a to prostredníctvom piatich zahraničných finančných spravodajských jednotiek. Avšak na slovenskom trhu pôsobí na základe voľného pohybu služieb niekoľko stoviek zahraničných subjektov, a to nasledovne[1]:

- voľné cezhraničné pôsobenie zahraničných poskytovateľov služieb kryptoaktív v SR – 32 subjektov,
- voľné cezhraničné pôsobenie zahraničných bánk a iných úverových inštitúcií v SR – 406 subjektov,
- voľné cezhraničné pôsobenie zahraničných platobných inštitúcií v SR – 328 subjektov,
- voľné cezhraničné pôsobenie zahraničných inštitúcií elektronických peňazí v SR - 247 subjektov.

Je teda zrejmé, že subjekty, ktoré v sledovanom období roku 2024 podávali cestou svojej domovskej FIU hlásenia XBR smerované FSJ sú len nepatrnou časťou z celkového objemu, ktorý by mal byť prostredníctvom mechanizmu cezhraničného ohlasovania získaný a spracovaný na FSJ.

Zistenia strategickej analýzy

Prostredníctvom analýzy XBR hlásení boli posúdené všetky dostupné dáta, ktoré presne reflektujú silné a slabé stránky moderného globálneho finančného systému a s ním spojené ohlasovacie povinnosti povinných osôb, a na základe ktorých boli identifikované nasledovné zistenia:

1) Prietokové (tranzitné) účty – zo zistení strategickej analýzy jednoznačne vyplýva veľmi aktívne využívanie účtov, ktoré si otvorili reportované subjekty, ako prietokových účtov. Prietokovými účtami rozumieme účty, ktoré sú využívane na zakrytie pôvodu finančných prostriedkov prostredníctvom série transakcií, najčastejšie v nižších sumách a vo veľmi krátkom časovom slede. Je dôležité spomenúť, že viackrát bolo z hľadiska povinnej osoby indikované, že pravdepodobne ide o účet, ktorý je ovládaný inou osobou (či už dobrovoľne odovzdané prihlasovacie údaje alebo o ukradnutie prístupových údajov) a ďalej o účty, ktoré boli otvorené za pomoci ukradnutých respektíve

[1] https://subjekty.nbs.sk/sk/

sfalšovaných dokumentov alebo podkladov, ktoré boli počas onboardingu klienta prezentované s cieľom uviesť do omylu software / proces, pričom najčastejším spôsobom bolo predkladanie vytlačenej fotografie pri procese overenia skutočnej / fyzickej identity klienta pri otváraní účtu.

2) Predpokladaná latentnosť ohlasovania – vďaka dostupnosti MSB (Money Service Businesses) / Neo Bánk / E-money / poskytovateľov služieb kryptoaktív služieb pre celosvetovú klientelu je na mieste poukázať na nízku mieru ohlasovania neobvyklých / podozrivých transakcií zo strany rôznych, často globálnych, poskytovateľov služieb. Tento bod je v priamej súvislosti aj s nasledujúcim bodom venujúcim sa chybám pri starostlivosti o klientov, ale aj s prvým bodom, ktorý poukazuje na zneužívanie klientskych účtov na prietokové účely. Problémom ohlasovania nie je častokrát len jeho absencia, ale aj neaktuálnosť, kedy zahraničná povinná osoba pristúpi k ohláseniu UTR / STR až s pomerne veľkým časovým odstupom

3) Nedostatky pri vykonávaní starostlivosti vo vzťahu ku klientovi (CDD a KYC) – v tomto kontexte bolo okrem iného zistené, že inštitúcie pristúpia k procesu otvorenia účtu a realizovaniu transakcií (často v nemalom objeme) i keď majú podozrenie alebo vyslovene istotu, že ide o žiadosť o otvorenie účtu s dokumentami, ktoré boli pozmeňované / falšované alebo proces verifikácie klienta prostredníctvom snímania tváre neprebehol správne, pretože namiesto reálnej fyzickej osoby bola pred telefón / zariadenie predložená len fotografia, často nie v dobrej kvalite.

4) Nízka miera opatrnosti / benevolencia zo strany zahraničných povinných osôb – počas analýzy dát bolo viackrát v reportoch objavené - najmä v spojitosti s otváraním účtov pre právnické osoby, že existovali indikátory, ktoré výrazne poukazovali na fakt, že môže ísť o spoločnosť / spoločnosti, ktoré budú využívané na nelegálne aktivity. Napríklad faktory ako: virtuálne sídlo, novozaložená spoločnosť, nesúlad medzi deklarovaným účelom využívania účtu a reálnym transakčným tokom, konateľ spoločnosti je vo vysokom seniorskom veku, negatívne OSINtové informácie, online prístup na účet prebieha z IP adries lokalizovaných v iných krajinách, prepojenie spoločnosti na subjekty alebo osoby, ktoré boli v minulosti reportované finančným spravodajským jednotkám v spojitosti s podozrením na pranie špinavých peňazí alebo financovanie terorizmu. Práve tieto faktory by mali viesť nielen k zvýšenej starostlivosti

zo strany zahraničných povinných osôb, ale i k reštriktívnejšej politike pri zmrazení alebo zatvorení účtu.

5) vIBAN – vďaka zmenám na technologickom poli a v regulácií je umožnené fintechovým spoločnostiam prichádzať na trh s novými riešeniami, ktoré majú za účel zjednodušiť a zefektívniť transfery finančných prostriedkov. Odvrátenou stránkou týchto technologických zmien sú problémy spojené so zneužívaním týchto fintech služieb na legalizáciu výnosov z trestnej činnosti alebo pranie špinavých peňazí. Práve vIBAN-y (Virtuálne IBAN-y), ktoré fungujú prostredníctvom vytvorenia sub-účtu len vo virtuálnej podobe sú jedným z veľkých hrozieb práve kvôli ľahkej zneužiteľnosti a veľmi náročného identifikovania hlavného účtu na ktorý bola vykonaná starostlivosť. V súčasnej dobe neexistuje univerzálny a absolútne spoľahlivý proces na možnosť stotožnenia a úspešného priradenia vIBAN-u k hlavnému (tzv. master) účtu. Práve preto vIBAN-y predstavujú jednu z veľkých hrozieb využiteľných na vrstvenie finančných prostriedkov za účelom legalizácie výnosov z trestnej činnosti alebo prania špinavých peňazí.

Strategická analýza ukazuje, že moderný finančný ekosystém prináša nielen nové príležitosti, ale aj rastúce riziká, ktorým je nevyhnutné porozumieť a aktívne ich znižovať. Identifikované problémy potvrdzujú potrebu posilnenia dohľadu, zlepšenia kvality ohlasovania a dôslednejšieho výkonu starostlivosti o klienta. Implementáciou odporúčaných krokov môže FSJ výrazne zvýšiť svoju schopnosť odhaľovať, predchádzať a potláčať formy legalizácie výnosov z trestnej činnosti v čoraz komplexnejšom globálnom prostredí.

Identifikácia trendov a vzorcov v rámci cezhraničného ohlasovania, ktoré predstavujú zvýšené riziko ML

Strategickou analýzou cezhraničného ohlasovania bolo za sledované obdobie identifikovaných niekoľko nasledovných trendov a vzorcov, ktoré so sebou nesú zvýšené riziko ML/TF, ktoré za účelom lepšej prehľadnosti sú združené nižšie:

- povinné osoby ohlasujúce XBR sú predovšetkým fintech spoločnosti prevádzkujúce on-line platformy, na ktorých je proces registrácie pomerne jednoduchý a od klienta – fyzickej osoby sa vyžaduje len mobilný telefón s operačným systém Android alebo iOS, platný doklad totožnosti, telefónne číslo, emailová adresu a vykonanie procesu spojeného s video/fotografiou tváre potrebného na verifikáciu osoby. Celý proces je veľmi užívateľsky prívetivý, mimoriadne rýchly a neviazaný na bežné pracovné dni/bankové hodiny. Rýchlosť tohto procesu však so sebou nesie aj nižšiu kvalitu identifikačných údajov a dát, a teda v rámci vykonania starostlivosti o klienta pri vstupovaní do obchodného vzťahu najmä pri identifikácii a overovaní identifikácie klienta. Tieto nedostatky **vedú k možnosti zneužitia klientskych účtov a to napr. prevzatím kontroly nad účtom/zriadenie účtu pod falošnou identitou alebo v spojitosti s tranzitnými účtami (klient v pozícii tzv. „money mule“)**.

- rast **kryptoadopcie** v rámci regiónu Európskej únie - využívanie tejto formy prevodu aktív a prostriedkov do určitej miery **sťažuje identifikáciu participujúcich osôb a subjektov na trestnej činnosti vrátane prania špinavých peňazí, ako aj sťažuje identifikáciu ďalších tokov finančných prostriedkov alebo konečnú destináciu týchto tokov**. V tejto súvislosti sa predpokladá sledovanie vývoja využívania krypto-platforiem na prevody a to najmä po implementácii Nariadenia Európskeho parlamentu a Rady (EÚ) 2023/1114 z 31. mája 2023 o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937 (Text s významom pre EHP).

- XBR adresované FSJ sú len nepatrnou časťou z celkového objemu, ktorý by mal byť získaný prostredníctvom mechanizmu cezhraničného ohlasovania. Podľa aktuálnych údajov z web-stránky NBS na slovenskom trhu pôsobí na základe voľného pohybu služieb viac ako 1000 zahraničných subjektov, pričom každý z nich má vo vzťahu k FSJ

ohlasovaciu povinnosť cestou svojej domovskej FIU. **Preto existuje signifikantná časť neobvyklej/podozrivej obchodnej aktivity a operácií, ktorá je latentná a zostáva mimo pozornosti príslušných orgánov, z dôvodu nedostatočného ohlasovania týmto typom povinných osôb**.

- **vzrast využívania virtuálnych IBAN účtov (tzv. vIBAN)**, pričom identifikácia konečného klienta, pre ktorého je vIBAN vedený ako aj účel (iný ako **spôsobiť neprehľadonsť tokov finančných prostriedkov**), pre ktorý takýto účet využíva, sú značne sťažené,

- **signifikantná časť XBR sa týka subjektov, ktoré sa FSJ nedostali do pozornosti v rámci tuzemského systému ohlasovania neobvyklých obchodných operácií**, napriek tomu, že FSJ vo viacerých prípadoch prijala hlásenia o neobvyklých obchodných operáciách, avšak tie po obsahovej stránke neboli relevantné na odstúpenie príslušným orgánom. V rámci analyzovania dát získaných z prijatých XBR hlásení bolo zistené/možno konštatovať, že boli zaznamenané prípady, kedy sa slovenské subjekty pokúšali o páchanie trestnej činnosti a pranie špinavých peňazí, ktoré vykazovalo opakujúci sa vzorec správania. **Prvotné pokusy o páchanie trestnej činnosti prebiehali na území SR s využitím slovenských bankových účtov. Následne páchatelia začali využívať služby zahraničných platobných inštitúcií a posledný stupeň predstavovali transakcie zahŕňajúce kryptomeny**

- dve tretiny ohlásených prípadov sa týkajú **tranzitného vzorca, resp. využívania účtov ako prietokových účtov**. Problematickým elementom v spojitosti s tranzitnými účtami je predovšetkým identifikácia účelu prevodov a prepojenie prípadov s konkrétnou trestnou činnosťou. Ide teda len o indikátor prania špinavých peňazí, avšak ďalšie rozkrytie pravého účelu takto využívaných účtov sa často zistí až neskôr, pri komplexnej analytickej činnosti viacerých informácií prijatých z viacerých zdrojov alebo v rôznom časovom odstupe.

Záver

Strategická analýza k cezhraničnému ohlasovaniu v podmienkach Slovenskej republiky za vybrané obdobie roka 2024, jednoznačne poukazuje na významnú dôležitosť rastu fintech sektora a jeho využitia zo strany klientov aj zo Slovenskej republiky. Predikovať zmeny v tejto oblasti je náročné z dôvodu zmien v regulácii, z dôvodu vstupu novej generácie fintech subjektov na trh a taktiež z dôvodu geopolitických vplyvov. Množstvo prijatých cezhraničných hlásení má výraznú rastovú tendenciu, a preto bolo zo strany FSJ pristúpené k vytvoreniu strategickej analýzy cezhraničného ohlasovania s cieľom efektívne mapovať a následne reagovať na nové trendy a hrozby v oblasti boja proti praniu špinavých peňazí a financovaniu terorizmu.

V rámci záverov strategickej analýzy navrhla FSJ niekoľko krokov a opatrení, pričom jedným z nich je aj komunikácia relevantných zistení povinným osobám prostredníctvom informačného bulletinu.