Podezřelé obchody a zajišťování finančních prostředků Finančním analytickým útvarem Ministerstva financí ČR[1]

ADRIANA VAVRUŠKOVÁ

Boj proti legalizaci výnosů z trestné činnosti čelí stále novým výzvám. Ti, kdo dnes perou peníze, již většinou nejsou jednotlivci, ale jedná se o velmi dobře organizované skupiny, které působí mezinárodně. V České republice se bojem proti praní špinavých peněz zabývá **Finanční analytický útvar**, jeden z odborů Ministerstva financí ČR (dále jen „FAÚ"). Jeho analytické oddělení ročně prošetří až 3 192 oznámení podezřelých obchodů[2], které pochází z privátního sektoru.

Boj proti praní špinavých peněz leží v rukách orgánů činných v trestním řízení při uplatňování trestního zákoníku[3]. Zejména preventivní rovina boje proti praní peněz však leží právě v rukách Finančního analytického útvaru – ten má totiž za úkol nastavit v rámci **zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu** (dále jen „AML zákon"), taková opatření, která pachatelům legalizaci výnosů znemožní, resp. co nejvíce ztíží, a neumožní zneužít finanční systém k praní peněz a financování terorismu. Dalším důležitým úkolem boje proti praní špinavých peněz je uchovat stopy po přesunech finančních prostředků a dále zejména odčerpat nelegální výnosy z rukou pachatelů této závažné trestné činnosti, a to za účelem naplnění zásady, že „trestná činnost se nesmí pachatelům vyplácet".

Tento článek si klade za cíl seznámit čtenáře s problematikou podezřelých obchodů a se zajišťováním finančních prostředků na účtu klienta nástroji, které má Finanční analytický útvar k dispozici podle AML zákona. Zároveň uvádí základní rizikové faktory obchodů a klientů.

OBSAH:

KLÍČOVÁ SLOVA:

Finanční analytický útvar, AML zákon, FATF, povinná osoba, podezřelý obchod, identifikace klienta, kontrola klienta, AML/CFT[4], oznámení o podezřelém obchodu, šetření, rizikové faktory, odklad splnění příkazu klienta, trestní oznámení.

1. ČINNOST A PŮSOBENÍ FAÚ MINISTERSTVA FINANCÍ ČR

Finanční analytický útvar Ministerstva financí vznikl již v roce 1996. Je součástí sítě tzv. finančních zpravodajských jednotek, působící v cca 140 státech světa. Jako taková jednotka v České republice zajišťuje především tyto úkoly:

a) šetření podezřelých obchodů primárně hlášených tzv. povinnými osobami,
b) příprava právních předpisů v relevantní oblasti boje proti legalizaci výnosů z trestné činnosti a financování terorismu a koordinace uplatňování mezinárodních sankcí,
c) kontrolní činnost, vedení řízení o přestupcích a správních deliktech,
d) spolupráce se zahraničními jednotkami a vybranými mezinárodními institucemi.

FAÚ je administrativním typem jednotky[5], je tedy zařazen mimo orgány činné v trestním řízení jako jeden z odborů Ministerstva financí ČR. Z toho vyplývá i nastavení specifické komunikace s privátním sektorem a policejními orgány. Výměna informací se zahraničím probíhá mj. na základě Úmluvy o praní, vyhledávání, zadržování a konfiskaci výnosů ze zločinu[6], a to mezi partnerskými finančními zpravodajskými jednotkami zemí, které k této úmluvě také přistoupily. Česká republika je také signatářem Mezinárodní úmluvy o potlačování financování terorismu z roku 1999, čímž se zavazuje postihovat jako trestný čin všechny formy financování terorismu a přijmout opatření k identifikaci, odhalování a zmrazení nebo zabavení jakýchkoliv finančních prostředků určených k financování terorismu.

Činnost FAÚ upravuje zejména AML zákon, který ve svém § 30 říká, že FAÚ může požadovat informace nezbytné pro plnění povinností podle AML zákona od Policie ČR, zpravodajských služeb a dalších orgánů veřejné moci, včetně orgánů věcně příslušných ke správě daní. FAÚ je oprávněn soustřeďovat a analyzovat získané údaje ve svých informačních systémech. Vzhledem k citlivosti některých informací je technicky oddělen od jiných pracovišť Ministerstva financí a jsou v něm uplatňována taková organizační, personální a jiná opatření, která zajišťují, že s informacemi získanými při provádění AML zákona nepřijde do styku nepovolaná osoba.[7] Základním stavebním kamenem pro šetření prováděná FAÚ jsou však informace poskytované privátním sektorem, tedy povinnými osobami.

2. ZÁKLADNÍ POVINNOSTI POVINNÝCH OSOB

Povinné osoby definuje § 2 AML zákona. Jak uvádí FAÚ ve své Výroční zprávě 2014[8], bankovní sektor se podílí ze 70 % na objemu přijatých oznámení podezřelých obchodů. Je důležité uvést, že mezi povinné osoby patří především úvěrové instituce, tedy banky a spořitelní a úvěrní družstva, a finanční instituce, kterými jsou například osoby s povolením k poskytováním investičních služeb, investiční společnosti, samosprávné investiční fondy, penzijní společnosti a fondy, platební instituce, poskytovatelé platebních služeb malého rozsahu, instituce elektronických peněz a vydavatelé elektronických peněz malého rozsahu, osoby oprávněné ke zprostředkování spoření, leasingu, záruk, úvěrů nebo peněžních půjček nebo k obchodování s nimi, pojišťovny, zajišťovny, pojišťovací zprostředkovatelé, osoby, které vyku-

pují dluhy a pohledávky a obchodují s nimi, osoby oprávněné ke směnárenské činnosti podle devizového zákona, osoby poskytující služby peněžního makléřství apod.[9]

Povinné osoby mají v AML zákoně přesně vymezené povinnosti, které musí plnit. Při jejich nesplnění jim hrozí pokuty až do výše 10 mil. Kč. Mezi základní povinnosti, a z hlediska prevence stěžejní, patří identifikace a kontrola klienta.

Povinné osoby musí provést identifikaci klienta, která zahrnuje zaznamenání a ověření identifikační údajů[10] z průkazu totožnosti klienta, resp. z dokladu o existenci právnické osoby, vždy před uskutečněním obchodu v hodnotě převyšující částku 1 000 EUR. Bez ohledu na tento limit povinná osoba vždy identifikuje klienta, mj. při vzniku obchodního vztahu, zejména tedy při uzavření smlouvy o účtu, vkladu, při uzavření smlouvy o nájmu bezpečnostní schránky nebo smlouvy o úschově, při uzavření smlouvy o životním pojištění a v dalších situacích uvedených v § 7 odst. 2 AML zákona. V případě, kdy povinná osoba považuje obchod za podezřelý (viz dále), identifikaci zúčastněných osob provádí bez ohledu na jeho aktuální hodnotu. Identifikace klienta musí vždy proběhnout za jeho fyzické přítomnosti, v případě právnické osoby se pak provádí také identifikace osoby jednající za právnickou osobu. Toto pravidlo se nazývá „tváří v tvář". Platí zde obecný mezinárodně uznávaný princip - „Know Your Customer", tedy poznej svého klienta.

„Kontrola klienta" je prováděna před uskutečněním jednotlivého obchodu v hodnotě 15 000 EUR nebo vyšší a dále mj. v případech podezřelého obchodu, při vzniku obchodního vztahu, při uzavření smlouvy o účtu, při uzavření smlouvy o nájmu bezpečnostní schránky nebo smlouvy o úschově, a dále v situacích obchodu s politicky exponovanou osobou[11] a v době trvání obchodního vztahu. Při kontrole klienta získává povinná osoba informace o účelu a zamýšlené povaze obchodu nebo obchodního vztahu, zjišťuje skutečného majitele[12], pokud je klientem právnická osoba, získává informace potřebné pro provádění průběžného sledování obchodního vztahu včetně přezkoumávání obchodů prováděných v průběhu daného vztahu za účelem zjištění, zda jsou uskutečňované obchody v souladu s tím, co povinná osoba o klientovi ví a co ví o jeho podnikatelském a rizikovém profilu. Dále může podle AML zákona povinná osoba přezkoumávat zdroje peněžních prostředků klienta.

Finanční akční výbor boje proti praní špinavých peněz (dále jen „FATF")[13] klade významný důraz na přístup založený na posouzení rizik (tzv. RBA z anglického „risk-based approach") praní peněz a financování terorismu a ve své Vysvětlivce k doporučení č. 10 (Identifikace a kontrola klienta) mj. uvádí, že existují-li okolnosti, za nichž je riziko praní peněz nebo financování terorismu vyšší, musí být provedena opatření zesílené kontroly klienta. Při hodnocení rizika praní peněz a financování terorismu ve vztahu ke kategoriím klientů, států nebo zeměpisných oblastí a určitým produktům, službám, obchodům nebo distribučním kanálům patří mezi příklady s potenciálně vyšším rizikem[14] tyto situace:

a) rizikové faktory ve vztahu ke klientovi:
- obchodní vztah probíhá za neobvyklých okolností (např. významná nevysvětlená geografická vzdálenost mezi finanční institucí a klientem),
- klient není v daném státě rezidentem,
- právnická osoba nebo jiný subjekt[15] slouží k držení osobního majetku,
- společnost má potřebné akcionáře nebo akcie na doručitele,
- podnikatelská činnost vyžaduje velké množství hotovosti,
- vlastnická struktura společnosti se jeví neobvykle nebo nadměrně složitou vzhledem k povaze její podnikatelské činnosti;

b) rizikové faktory ve vztahu ke státu nebo zeměpisné oblasti:
- státy označené důvěryhodnými zdroji, jako je vzájemné hodnocení nebo podrobné hodnotící zprávy nebo zveřejněné navazující zprávy, za státy bez odpovídajícího systému AML/CFT,
- státy, na něž se vztahují sankce, embarga nebo podobná opatření přijatá například Organizací spojených národů,
- státy označené důvěryhodnými zdroji za státy s významnou mírou korupce nebo jiné trestné činnosti,
- státy nebo zeměpisné oblasti označené důvěryhodnými zdroji za státy poskytující finanční prostředky nebo podporu teroristickým činnostem nebo státy, na jejichž území operují teroristické organizace označené jako mezinárodní autoritou (např. Radou bezpečnosti OSN nebo orgány EU);
- rizikové faktory se vztahem k produktu, službě, obchodu nebo distribučnímu kanálu:
- privátní bankovnictví,
- anonymní obchody (včetně hotovostních),
- nepřímé obchodní vztahy nebo obchody,
- platba přijatá od neznámých nebo nepřidružených třetích osob.

PODEZŘELÝ OBCHOD

Každý rok FAÚ ve své výroční zprávě uvádí příklady nejvýznamnějších nebo nejčetnějších typů podezřelých obchodů, které šetřil. Za rok 2014 uvádí zejména časté případy spojené s daňovými úniky a nadměrnými odpočty DPH.

V roce 2014 byl na základě oznámení podezřelého obchodu prověřován řetězec transakcí mezi účty několika společností, kdy byly fakturovány podezřelé platby za reklamní a marketingové služby. Finanční transakce se uskutečňovaly v řádech statisíců CZK. Na konci řetězce byly peněžní prostředky vybírány v hotovosti, a to zpravidla v částkách cca CZK 100 000 několikrát denně na různých pobočkách bankovních domů. Během šetření bylo zjištěno, že společnosti, z jejichž účtů jsou peněžní prostředky vybírány v hotovosti, jsou zpravidla nově založené společnosti, které mají sídlo zapsáno v kancelářích typu „office house". Jako statutární orgány v nich opakovaně figurují stále stejné osoby, které mají většinou hlášen pobyt na obecních úřadech. Společnosti byly registrovány jako plátci DPH a z veřejně dostupné evidence plátců DPH vyplynulo, že plátce neurčil žádný bankovní účet užívaný k ekonomické činnosti pro daňové účely. Vzhledem k sídlům společností v tzv. „virtuálních kancelářích" a statutárním zástupcům bez trvalého bydliště, byly společnosti pro daňovou správu nekontaktní. Celkem bylo možné vyčíslit, že nebyla přiznána daňová povinnost na DPH v částce přesahující 9 mil. CZK. FAÚ tak byly zajištěny peněžní prostředky na bankovních účtech v celkové výši více než 4 mil. CZK, kdy následným vydáním exekučních příkazů na zajištěné účty byly alespoň zčásti uspokojeny pohledávky správce daně.[17]

Podezřelý obchod je obecně definován v § 6 AML zákona jako obchod uskutečněný za okolností vyvolávajících podezření ze snahy o legalizaci výnosů z trestné činnosti nebo podezření, že v obchodu užité prostředky jsou určeny k financování terorismu, anebo jiná skutečnost, která by mohla takovému podezření nasvědčovat, a to pokud například:

a) klient provádí výběry nebo převody na jiné účty bezprostředně po hotovostních vkladech,
b) během jednoho dne nebo ve dnech bezprostředně následujících uskuteční klient, případně více peněžních operací, než je pro jeho činnost obvyklé,
c) počet účtů zřizovaných klientem je ve zjevném nepoměru k předmětu jeho podnikatelské činnosti nebo jeho majetkovým poměrům,
d) klient provádí převody majetku, které zjevně nemají ekonomický důvod,
e) prostředky, s nimiž klient nakládá, zjevně neodpovídají povaze nebo rozsahu jeho podnikatelské činnosti nebo jeho majetkovým poměrům,
f) účet je využíván v rozporu s účelem, pro který byl zřízen,
g) klient vykonává činnosti, které mohou napomáhat zastírání jeho totožnosti nebo zastření totožnosti skutečného majitele,
h) klientem nebo skutečným majitelem je osoba ze státu, který nedostatečně nebo vůbec neuplatňuje opatření proti legalizaci výnosů z trestné činnosti a financování terorismu, nebo

f) povinná osoba má pochybnosti o pravdivosti získaných identifikačních údajů o klientovi.

Uvedené příklady se samozřejmě mohou lišit průřezem širokého spektra povinných osob, stejně tak mohou být významné rozdíly i v rámci jednoho typu povinné osoby, například banky, kdy je třeba rozlišovat velikost instituce dle počtu klientů, zaměření na privátní nebo korporátní klientelu, druhy nabízených produktů a služeb. Jedná se však vždy obecně o určité anomálie vůči běžnému chování klienta, případně srovnatelného typu klienta. Tyto excesy je tak možné identifikovat jednotlivě, na základě subjektivního posouzení pracovníka front office či skrze automatizované vyhodnocovací systémy povinných osob.

Například karuselové podvody na DPH[18] mohou mít následující indikátory:

a) rizikové komodity – patří mezi ně např. pohonné hmoty, kovy, elektronika, zlato, zemědělské komodity,

b) nově založené účty nebo spící účty zemou vykazovat významné zvýšení obratů, případně se vyskytují vysoké obraty na nově založeném účtu,

c) na účtech neprobíhají běžné provozní výdaje společností, jako jsou například platby za nájem, mzdy, daňové platby, povinné odvody za zaměstnance apod., na účtech neprobíhají ani jiné transakce svědčící o obchodní činnosti společnosti (např. absentují příchozí zahraniční transakce dokládající vývoz či dodání zboží do jiného členského státu),

d) jednatelem (z vůči povinné osobě) je tzv. „bílý kůň", který navíc figuruje u více obdobných společností; sídlo společnosti je často na virtuální adrese (Praha 1, Praha 4 apod.),

e) u subjektu typu Missing trader dochází k hotovostním výběrům, které jsou realizovány bezprostředně po připsání finančních prostředků v plné výši.

Povinné osoby by měly pracovat s informacemi získanými od klientů, ať již v rámci identifikace či kontroly klienta. AML zákon (§ 8 odst. 8 a § 9 odst. 1) klientovi ukládá povinnost součinnosti a současně dává povinné osobě oprávnění ke zpracování osobních údajů za účelem plnění povinností dle AML zákona.[20]

Ve vztahu k zahraničním společnostem je třeba, aby povinné osoby sledovaly také informace o rizikových teritoriích. FAÚ na svých internetových stránkách[21] pravidelně uvádí informace týkající se rizikových jurisdikcí. Jedná se o reakci na veřejné prohlášení („Public Statement") FATF, v němž vyzývá své členy a další jurisdikce k přijetí opatření vůči rizikovým státům, s cílem ochránit mezinárodní finanční systém před přetrvávajícími závažnými riziky praní peněz a financování terorismu, které tyto země pro světový finanční systém znamenají. Poslední prohlášení z června 2015 se týkalo Íránu a KLDR. Írán představuje riziko zejména z hlediska financování terorismu. V KLDR podle FATF stále přetrvávají zásadní nedostatky v celém systému boje proti praní špinavých peněz a financování terorismu.[22] Obdobně jako u Íránu FATF varuje před navazováním korespondenčních vztahů s finančními institucemi a nabádá ke zvýšené ostražitosti v obchodních vztazích a transakcích s touto zemí.

V uvedeném prohlášení FATF dále vyjmenovává země, jejichž systém boje proti praní špinavých peněz a financování terorismu vykazuje strategické nedostatky a které v tomto směru neučinily dostatečný pokrok nebo neplní akční plán zpracovaný společně s FATF k odstranění nedostatků – jde o Alžírsko a Barmu/Myanmar. FAÚ doporučuje věnovat maximální obezřetnost při vstupu do obchodních vztahů a při platebním styku s osobami a finančními institucemi z těchto jurisdikcí (minimálně je vždy třeba vyžadovat dostatečné informace o klientovi, zdroji jeho finančních prostředků a povaze a účelu obchodu).

Dále FATF upozorňuje na země, jejichž AML/CFT systém vykazuje rovněž nedostatky, ale tyto země se zavázaly k akčnímu plánu zpracovanému FATF k odstranění nedostatků a tento plán v uspokojivé míře plní[23] – Afganistán, Angola, Bosna a Hercegovina, Ekvádor, Guayana, Jemen, Laos, Panama, Papua Nová Guinea, Súdán, Sýrie, Uganda. FAÚ doporučuje u těchto zemí přihlédnout při vstupu do obchodních vztahů a při platebním styku s osobami a finančními institucemi z těchto jurisdikcí k rizikům spjatým s identifikovanými nedostatky. Jurisdikce, která podle FATF neučinila žádný významný pokrok je Irák.

Z výroční zprávy FAÚ za rok 2014 také vyplývá, že přibývají případy trestné činnosti realizované v souvislosti s komunikací na sociálních sítích:

Postup pachatele spočívá v tom, že pod identitou známé osoby („přítele") kontaktuje na této síti vytipovanou osobu a snaží se ji přesvědčit, že je zcela bez finančních prostředků a nutně potřebuje zaslat alespoň malou částku, např. 10 Kč. Oslovená důvěřivá osoba v dobré víře, za pomoci bankovních či kontaktů v mobilu a ještě k tomu jen malou finanční částkou, se pouští do delší konverzace s podvodníkem na sociální síti. Během tohoto kontaktu, vylákal podvodník např. s odvoláním na „různé technické problémy" od důvěřivce údaje k jeho bankovnímu účtu (včetně hesel k internetovému bankovnictví). Poté si údajný „kamarád" na základě podvodně získaného, a v podstatě zcela volného přístupu k celému zůstatku na napadeném bankovním účtu, převede libovolnou částku na jiný bankovní účet nebo z napadeného účtu uhradí zboží, např. elektroniku, které si předtím objednal pod smyšlenou identitou v internetovém obchodě.[24]

Výroční zpráva FAÚ za rok 2014 také mj. uveřejnila, že nezanedbatelnou část predikativní trestné činnosti[25] v posledních letech stabilně tvoří internetové podvody, jako podvodné inzeráty, falešné e-shopy či phisingové útoky. Dále přibyly podvody spočívající v doručení velmi věrohodných podvodných notifikací o změně účtu obchodního partnera.

Phising je podvodná internetová technika používaná k získání citlivých údajů při elektronické komunikaci. Pachatelé se snaží vylákat například PINy, hesla k účtům, čísla platebních/kreditních karet. Často dochází k rozesílání emailových zpráv, které vyzývají své adresáty k přihlášení se svými přístupovými údaji a hesly na falešnou internetovou stránku, která je však téměř identická s oficiálními stránkami například internetového bankovnictví úvěrové společnosti. Pachatelé tímto získají přístup k bankovnímu účtu napadeného uživatele.

Novinkou jsou také podezřelé obchody, kdy jsou výnosy z trestné činnosti investovány do virtuální měny[26]. V souvislosti s tím FAÚ vydal svůj Metodický pokyn č. 2 ze září 2013 „o přístupu povinných osob k digitálním měnám". V tomto pokynu FAÚ mj. uvádí, že nově používané nezávislé internetové digitální („open-source") měny, jako je například Bitcoin, představují prvek, s jehož využitím lze přerušit stopu převáděných prostředků. Byť z hlediska zachování elektronické stopy mohou být takové platby dosledovatelné, s ohledem na anonymitu uživatelů a další podmínky těchto „služeb" je používání měny tohoto typu z hlediska opatření proti praní peněz a financování terorismu třeba považovat za velmi rizikové. FAÚ proto v tomto pokynu vyzývá všechny povinné osoby, aby v souvislosti s nákupem/prodejem jakékoliv digitální měny, jako je například Bitcoin, byla jako velmi riziková k posouzení a k rozhodnutí o dalších opatřeních podle okolností označena každá platba nad hodnotu 1 000 EUR a vždy jako podezřelý obchod postupem podle § 18 AML zákona oznámena transakce nad hodnotu 15 000 EUR.

V lednu 2015 bylo FAÚ prověřováno následující oznámení podezřelého obchodu, jehož scénář je častý. FAÚ přijal od banky oznámení týkající se transakcí na CZK účet klienta společnosti AB s.r.o. se sídlem v Praze, s tím, že banka byla kontaktována jednatelem této společnosti se žádostí o prověření obdržené platby na částku 20 000 CZK. K této platbě došlo dne 15. 1. 2015. Dle vyjádření jednatele společnosti AB s.r.o. se klient odmítl podrobit identifikaci a přestal komunikovat. Společnost AB s.r.o. tedy pojala podezření, že došlo k prolomení přístupu klienta, pana XY, do internetového bankovnictví

a zcizené prostředky byly použity k nákupu bitcoinů. Jednatel společnosti AB s.r.o. zároveň bance potvrdil, že obdrženou částku 20 000 CZK je společnost ochotna vrátit zpět odesílateli. Po kontaktování klienta pana XY bankou tento klient potvrdil, že uvedenou transakci dne 15. 1. 2015 na částku 20 000 CZK nezadal. Klient byl dotázán, zda nebyl vyzván v poslední době při přihlašování do banky k vyplnění telefonního čísla a stažení aplikace. Klient potvrdil, že tyto informace při přihlášení viděl a že vše vyplnil a stáhl aplikaci. Dne 20. 1. 2015 obdržela banka další reklamaci od jiného klienta, kterému byla dne 2. 1. 2015 z účtu také neoprávněně odeslána platba na účet společnosti AB s.r.o. Jednalo se o platbu na částku 25 000 CZK z účtu klienta, pana Z. Klient podal v této souvislosti trestní oznámení na Policii ČR. Dle vyjádření jednatele společnosti AB s.r.o. tuto částku již nebylo možné ze strany jejich společnosti vrátit zpět odesílateli, protože za tuto transakci již byly nakoupené bitcoiny zaslány.

FATF uvádí ve svých 40 Doporučeních z února 2012, že pokud má finanční instituce podezření nebo se důvodně domnívá, že finanční prostředky jsou výnosem z trestné činnosti nebo se týkají financování terorismu, měla by být ze zákona povinna tuto skutečnost ihned oznámit finanční zpravodajské jednotce. AML zákon se ve svém § 18 a násl. věnuje právě problematice oznámení podezřelého obchodu. Pokud tedy povinná osoba zjistí v souvislosti se svou činností podezřelý obchod, oznámí tuto skutečnost FAÚ, a to bez zbytečného odkladu, nejpozději však do 5 kalendářních dnů ode dne zjištění podezřelého obchodu. Časové hledisko je zde velmi důležité, a to zejména v době dnešních nových technologií. Hrozí-li nebezpečí z prodlení, oznámí povinná osoba podezřelý obchod neprodleně po jeho zjištění.

FAÚ ve svém Metodickém pokynu pro podání oznámení o podezřelém obchodu dále specifikuje jaké informace má oznámení podezřelého obchodu obsahovat. Kromě identifikace oznamovatele a údajů o tom, koho se oznámení týká, je třeba do oznámení popsat předmět a podstatné okolnosti podezřelého obchodu. Jak tento metodický pokyn mj. uvádí, je třeba podrobně uvést zejména:

- čí/od transakci, který účastník obchodu uvádí,
- popis použité hotovosti či jiných platebních prostředků a další okolnosti hotovostní platby,
- časové údaje,
- čísla účtů, na nichž jsou soustředěny peněžní prostředky, ohledně kterých se oznámení podává a všech účtů, na které nebo z nichž byly či mají být převáděny, včetně identifikace jejich majitelů a disponentů, měl-li k těmto informacím oznamovatel přístup,
- měnu,
- zda je obchod podezřelý,
- případně i zjištěná telefonní a faxová čísla,
- popis chování účastníka obchodu i jeho společníků a další informace, které by mohly mít informační význam k zúčastněným osobám či předmětné transakci.

K oznámení podezřelého obchodu je třeba přiložit kopie všech v oznámení uváděných a s předmětem oznámení souvisejících dokladů, které má oznamovatel k dispozici (například je shromáždil v souvislosti s kontrolou klienta). V oznámení se z bezpečnostních důvodů neuvádí údaje o zaměstnanci povinné osoby nebo osobě v obdobném pracovněprávním vztahu, která podezřelý obchod zjistila.

Pro podání oznámení podezřelého obchodu jsou v AML zákoně přesně vymezeny způsoby, z nichž vyplývá, že pro takové oznámení nelze využít e-mail ani datovou schránku FAÚ[27]. Lze jej podat pouze písemně doporučeným dopisem nebo ústně do protokolu v místě určeném po předchozí domluvě s pracovníky FAÚ. Za písemné oznámení se považuje též oznámení podané elektronicky technickými prostředky zajišťujícími zvláštní ochranu přenášených údajů.[28] FAÚ vytvořil pro pracovníky povinných osob vlastní softwarovou aplikaci MoneyWeb, resp. MoneyWeb Lite, jejímž účelem je poskytnout možnost snadného a úplného podání oznámení podezřelého obchodu povinnou osobou. Tento systém umožňuje také oboustrannou chráněnou komunikaci mezi FAÚ a povinnými osobami.[29]

Na tomto místě je třeba upozornit, že ani komunikace uvnitř povinné osoby ohledně oznámení podezřelého obchodu nemá probíhat cestou nezabezpečené komunikace (např. e-mailem).

4. ŠETŘENÍ PODEZŘELÉHO OBCHODU, POSTUP PODLE § 20 AML ZÁKONA A PODÁNÍ TRESTNÍHO OZNÁMENÍ

Pokud povinná osoba zjistí podezřelý obchod, je povinna jej oznámit ve stanovené lhůtě FAÚ[30]. Každá povinná osoba má povinnost určit tzv. kontaktní osobu, což je konkrétní zaměstnanec, který plní oznamovací povinnost vůči FAÚ. O určení této osoby a o případných následných změnách musí povinná osoba informovat neprodleně FAÚ a tyto osoby musí být kdykoliv možné kontaktovat ze strany FAÚ.

Je zřejmé, že vzhledem k typu a velikosti některých povinných osob bude samotná povinná osoba ještě informaci o podezřelém obchodu dále sama vyhodnocovat[31]. Využívá k tomu nejen otevřených zdrojů, ale také informace, které získala v souvislosti se svou činností. Podle § 16 je totiž povinná osoba povinna mj. uchovávat všechny identifikační údaje, kopie dokladů předložených k identifikaci klienta, údaje o tom, kdo a kdy provedl první identifikaci klienta, a to po dobu 10 let od ukončení obchodního vztahu s klientem. Údaje o obchodech spojených s povinností identifikace uchovává povinná osoba nejméně 10 let po uskutečnění obchodu nebo ukončení obchodního vztahu s klientem. Po svém vnitřním vyhodnocení a doplnění informací teprve povinná osoba podává oznámení o podezřelém obchodu na FAÚ.

Povinná osoba sdělí FAÚ také informaci o tom, zda použila dočasné zajišťovací opatření tzv. odklad splnění příkazu klienta podle § 20 AML zákona. Toto opatření použije povinná osoba v případě, že hrozí nebezpečí, že by bezodkladným splněním příkazu klienta mohlo být zmařeno nebo podstatně ztíženo zajištění výnosu z trestné činnosti nebo prostředků určených k financování terorismu. Odklad spočívá v tom, že povinná osoba zajistí vhodným způsobem majetek klienta, jehož se odklad týká, proti manipulaci, a to maximálně na 24 hodin. Typickým příkladem je nevydání peněžní hotovosti na přepážce do rukou klienta či neuskutečnění jeho příkazu k úhradě, zejména pokud by se hodnoty na účtu dostaly mimo dosah českých státních orgánů a tím by bylo znemožněno nebo podstatně ztíženo sledování či jejich zajištění v případném trestním či daňovém řízení.[32]

Lhůta se počítá od času doručení oznámení podezřelého obchodu na FAÚ. Jedná se o lhůtu v hodinách, počítá se tedy od „momentu k momentu". Jakmile lhůta bez dalšího vyprší, smí povinná osoba transakci provést, bez ohledu na to, zda skončila v pracovní či jiný den.[33]

Lhůtu 24 hodin je možné prodloužit, a to pouze v případě, že si šetření podezřelého obchodu pro svou složitost vyžaduje delší dobu. O prodloužení této lhůty rozhoduje vždy FAÚ. Doba, na kterou se odkládá splnění příkazu klienta, může být prodloužena nejdéle na dobu 72 hodin od přijetí oznámení podezřelého obchodu FAÚ. Na stejnou dobu může být maximálně odloženo splnění příkazu klienta nebo zajištění majetku, které má být předmětem podezřelého obchodu u povinné osoby, u níž se majetek nachází. Rozhodnutí o prodloužení doby nebo o odložení splnění příkazu klienta nabývá právní moci jeho vyhlášením, které může být provedeno ústně, telefonicky, telefaxem nebo elektronicky (vždy se však následně doručuje stejnopis písemného vyhotovení). Účastníkem řízení je vždy pouze povinná osoba a proti tomuto rozhodnutí není přípustný rozklad.

Na zajištění podle § 20 AML zákona se vztahuje povinnost mlčenlivosti, zejména vůči klientovi. Vyzrazením informace o odkladu splnění příkazu klienta, resp. o oznámení podezřelého obchodu, by totiž mohlo dojít ke zmaření zajištění nelegálních výnosů. V zájmu maximální ochrany vlastnických práv končí povinnost mlčenlivosti uplynutím nebo ukončením lhůty – po uplynutí 3 kalendářních dnů od dne podání trestního oznámení FAÚ orgánům činným v trest-

ním řízení, v případě, že bylo trestní oznámení podáno FAÚ ve lhůtě 24, resp. 72 hodin, od obdržení oznámení podezřelého obchodu na FAÚ; dříve může tato lhůta skončit pouze v případě, že orgán činný v trestním řízení rozhodne o odnětí nebo zajištění předmětu podezřelého obchodu (např. zajištění peněžních prostředků na účtu u banky dle § 79a trestního řádu).

FAÚ zajistil na účtech úvěrových a finančních institucí jen mezi roky 2012–2014 více než 6,1 miliardy korun, vše na základě podnětů, tedy oznámení podezřelých obchodů.

Po přijetí oznámení podezřelého obchodu probíhá na FAÚ analýza, resp. šetření podezřelého obchodu. FAÚ v jeho rámci vyžaduje informace od Policie ČR, zpravodajských služeb a orgánů veřejné moci, a také od orgánů věcně příslušných ke správě daní; tyto údaje FAÚ soustřeďuje a analyzuje a může je vést ve svých informačních systémech. FAÚ uchovává údaje a doklady o přijatých oznámeních a o vlastních šetřeních po dobu 10 let od konce roku, v němž bylo šetření ukončeno. Výše uvedená spolupráce je pro FAÚ stěžejní. FAÚ si dále může ke svému šetření vyžádat informace od povinné osoby, která zaslala oznámení podezřelého obchodu, nebo na základě tzv. informační povinnosti podle § 24 AML zákona mu na žádost sdělí jiná povinná osoba údaje o obchodech souvisejících s povinností identifikace nebo ohledně nichž FAÚ provádí šetření, a to včetně dokladů o těchto obchodech nebo k nim umožní pověřeným zaměstnancům FAÚ přístup při prověřování oznámení a poskytne informace o osobách, které se jakýmkoliv způsobem účastnily takových obchodů.

FAÚ dále spolupracuje se zahraničními orgány a mezinárodními organizacemi se stejnou věcnou působností, zejména při předávání a získávání údajů sloužících k dosažení účelu AML zákona.[34] V roce 2014 se FAÚ dotázal k 260 případům do zahraničí a získal 149 spontánních informací ze zahraničí.[35] FAÚ ke svému šetření využívá také otevřené zdroje (např. údaje z obchodního rejstříku, z katastru nemovitostí, informace z internetových stránek, sociálních sítí apod.).

Zjistí-li FAÚ skutečnosti nasvědčující tomu, že byl spáchán trestný čin, podá oznámení podle trestního řádu a současně orgánu činnému v trestním řízení poskytne všechny související informace z výsledků vlastního šetření. V roce 2014 podal FAÚ 680 trestních oznámení.[36] Zároveň FAÚ spolupracuje s orgány Finanční správy České republiky nebo celními orgány a pokud zjistí skutečnosti, které jsou významné pro výkon činnosti těchto orgánů, informuje je o těchto zjištěních. V roce 2014 postoupil FAÚ Generálnímu finančnímu ředitelství 1 491 informací a Generálnímu ředitelství cel 103 informací.

ZÁVĚR

Závěrem je třeba upozornit na vybrané nedostatky v nastavení systému boje proti praní špinavých peněz u povinných osob, zejména s ohledem na podezřelé obchody. Úvěrové nebo finanční instituce mohou mít neadekvátně nastavený automatizovaný systém pro vyhodnocování podezřelých obchodů. Zde je třeba rozlišovat dvě roviny:

A) prvotní vstup informací do systému, tj. zařazení klienta, produktů a služeb do příslušné kategorie rizika;

- může se zde objevit problém při hodnocení kvality samotných vstupních informací o klientovi – s tím souvisí špatně provedená identifikace nebo kontrola klienta a zaměstnancem povinné osoby (relativní místní znalost osob, kterých zaměstnanec povinné osoby by dotazovat se na povinná údaje, zapsání nespolehlivých informací, neznalost AML problematiky u zaměstnanců front office povinných osob, nedostatek času pro provedení adekvátní kontroly klienta, apod.);

B) využívání informací ze systému, vyhodnocení podezřelých obchodů – systém předkládá k ručnímu posouzení kapacitně a kvalitativně nezvladatelné množství podezřelých transakcí; opakem je, kdy systém nedokáže odhalit základní znaky podezřelých transakcí.

Nesprávné a AML zákonem zakázané je také zasahování zaměstnanců obchodního oddělení do činnosti oddělení „Compliance", příp. přímo do systému automatizovaného vyhodnocování transakcí, například úpravou rizikového profilu klienta (např. zásah manažera pobočky úvěrové instituce do systému z důvodu povolení transakce, založení obchodního vztahu rizikového klienta).

Ke snižování bezpečnostních prvků k obchodním cílům dochází také například nadměrným využíváním výjimek z AML zákona (např. § 11 AML zákona – tzv. „převzetí identifikace" je nad běžnou míru využíván internetovými bankami, přičemž původním smyslem této výjimky bylo využití pro spolupracující instituce např. ve finančním konglomerátu). Samotní klienti svým neopatrným zacházením s citlivými informacemi navíc velmi zvýšili rizika internetového bankovnictví.

Po soustavném výkladu a vydání stanoviska FAÚ k tzv. „neuskutečnění obchodu" podle § 15 AML zákona, začaly povinné osoby konečně využívat tento institut. Důvodem pro dřívější absenci uplatňování této „možnosti" byl například strach o ztrátu klienta. Jedná se přitom o kogentní ustanovení AML zákona, které uvádí, že povinná osoba odmítne uskutečnění obchodu nebo uzavření obchodního vztahu v případě, že je dána identifikační povinnost a klient se odmítne podrobit této identifikaci nebo odmítne doložit plnou moc, neposkytne potřebnou součinnost při kontrole klienta, nebo z jiného důvodu nelze provést identifikaci a kontrolu klienta, anebo má-li osoba provádějící identifikaci nebo kontrolu klienta pochybnosti o pravdivosti informací poskytnutých klientem nebo o pravosti předložených dokladů. Za porušení tohoto zákazu přitom povinným osobám hrozí pokuta až do výše 10 mil. Kč.

Je tedy třeba zejména klást důraz na osvětovou činnost, protože preventivní hledisko je v rámci boje proti praní špinavých peněz a financování terorismu nejdůležitější. Zaměstnanci povinných osob (a osob v obdobném zaměstnaneckém vztahu) jsou z AML zákona povinny absolvovat nejméně jedenkrát za 12 kalendářních měsíců školení, jehož obsahem je mj. typologie a znaky podezřelých obchodů a postupy při zjištění podezřelého obchodu. Problém většiny úvěrových a finančních institucí je však způsob, jakým provádí tato školení. Většinou jsou prováděna stále stejným neaktualizovaným e-learningovým kurzem, bez možnosti ověření znalostí z AML oblasti. Často je možné takový kurz, včetně výsledného testování, absolvovat během několika málo vteřin...

...ale o tom někdy příště...

Autorka JUDr. Adriana Vavrušková je absolventkou Právnické fakulty Univerzity Karlovy, titul JUDr. získala v roce 2009 v oboru finančního práva. Je expertkou v oblasti boje proti legalizaci výnosů z trestné činnosti a financování terorismu a koordinace uplatňování mezinárodních sankcí. V letech 2006–2010 působila v oddělení Mezinárodním a právním Finančního analytického útvaru Ministerstva financí. Pravidelně přednáší a účastní se grantových projektů spojených s problematikou praní špinavých peněz a financování terorismu. Je spoluautorkou komentáře k zákonu č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu a souvisejících předpisů.

1] Tento článek je publikován v rámci projektu výzkumu, vývoje a inovací s názvem „Nové postupy a metody finančního šetření, zajišťování majetku a identifikace legalizace výnosů z trestné činnosti" v rámci Programu bezpečnostního výzkumu České republiky v letech 2010-2015, s evidenčním číslem VF20142015038.

2] Údaj z roku 2014

3] § 216 legalizace výnosů z trestné činnosti, resp. § 217 legalizace výnosů z trestné činnosti z nedbalosti, zákona č. 40/2009 Sb., trestní zákoník

4] Systém boje proti praní špinavých peněz a financování terorismu (Anti Money Laundering/Counter Terrorist Financing)

5] Druhým základním typem je policejní jednotka, která působí například na Slovensku, v Německu, v Rakousku, ve Velké Británii.

6] Tzv. Štrasburská úmluva z roku 1990

7] § 31 AML zákona

8] ISBN 978-80-85045-76-5, on-line ISBN 978-80-85045-77-2

9] Úplný výčet povinných osob lze nalézt v § 2 AML zákona. Mezi povinné osoby patří mj. také osoby oprávněné k obchodování s nemovitostmi a ke zprostředkování obchodu s nimi, auditoři, daňový poradci a účetní, soudní exekutoři například při úschově peněz, cenných papírů nebo jiného majetku, notáři při úkonech v rámci notářské úschovy nebo advokáti při úschově peněz, ale také osoby oprávněné k obchodování s kulturními památkami nebo s použitým zbožím.

10] Identifikační údaje jsou podle § 5 AML zákona u fyzické osoby všechna jména a příjmení, rodné číslo (a nebylo-li přiděleno datum narození), místo narození, pohlaví, trvalý nebo jiný pobyt a státní občanství; jde-li o podnikající fyzickou osobu, též její obchodní firma, odlišující dodatek nebo další označení, místo podnikání a identifikační číslo osoby. U právnické osoby se identifikačními údaji rozumí obchodní firma nebo název včetně odlišujícího dodatku nebo dalšího označení, sídlo, identifikační číslo osoby nebo obdobné číslo přidělované v zahraničí; u osob, které jsou statutárním orgánem nebo jeho členem se dále vyžadují údaje jako u fyzické osoby.

11] Definice tzv. PEP je v § 4 odst. 5 AML zákona, obecně jde o zahraniční osobu, které byly svěřeny významné veřejné funkce s celostátní působností.

12] Definice skutečného majitele je v § 4 odst. 4 AML zákona.

13] Financial Action Tasks Force, mezivládní orgán ustavený v roce 1989, jehož úkolem je vytvářet standardy, propagovat účinnou implementaci právních, regulačních a operativních opatření v boji proti praní špinavých peněz, financování terorismu, financování šíření zbraní hromadného ničení a dalším souvisejícím hrozbám vůči integritě mezinárodního finančního systému. FATF 40 Doporučení představují tzv. minimální standard, tím, že stanovují komplexní a konzistentní rámec opatření, které by měly státy v uvedených problematikách přijmout.

14] Vedle situací uvedených v doporučeních č. 12 – 16, tj. politicky exponované osoby, korespondenční bankovnictví, služby převodu peněz nebo hodnoty, nové technologie, bezhotovostní převody.

15] Např. trust

16] Např. hodnocení výborem Moneyval Rady Evropy

17] Finanční analytický útvar: Výroční zpráva 2014, str. 6 – 7

18] Předmětem karuselového (též řetězového) podvodu je vytvoření řetězce daňových subjektů a obchodních transakcí mezi nimi s předem stanoveným cílem, že jeden z těchto subjektů (tzv. Missing trader) nesplní svou daňovou povinnost.

19] Zdroj www.financnisprava.cz: Finanční správa zavedla v říjnu 2014 přísnější podmínky pro aplikaci institutu tzv. „nespolehlivého plátce". Jedná se o další nástroj finanční správy v boji s daňovými úniky a podvody na DPH. Za nespolehlivého plátce je nyní označen i plátce DPH, který je účelově nekontaktní (opakovaně neplní lhůty pro povinná podání, dluží státu na DPH více než půl milionu korun déle než tři měsíce a správce daně mu musel stanovit opakovaně daň podle pomůcek). Od ledna 2015 došlo ke zpřísnění navíc ve vztahu ke společnostem sídlícím na virtuálních adresách. Informace o těchto „nespolehlivých plátcích" lze získat přímo na stránkách www.financnisprava.cz pod odkazem Registr plátců DPH.

20] Tvrdý/Bártová: Komentář Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu a předpisy související, C.H.Beck, ISBN 978-80-7400-099-7, str. 122

21] www.mfcr.cz/fau

22] FATF nepřestává varovat před korespondenčními vztahy využívanými k překonání nebo obcházení opatření proti financování terorismu a praní špinavých peněz. Vyzývá k důslednému vyhodnocování všech rizik při posuzování žádostí íránských finančních institucí o otevírání poboček a zakládání dceřiných společností v jednotlivých jurisdikcích. FATF současně vybízí Írán k urychlenému odstranění svých nedostatků zejména v kriminalizaci financování terorismu a k efektivnímu přijetí požadavků na hlášení podezřelých transakcí. Pokud Írán neprodleně nepřijme příslušná opatření ke zlepšení svého systému boje proti financování terorismu, FATF v říjnu 2015 navrhne svým členům přijetí zesílených protiopatření.

23] Improving Global AML/CFT Compliance: On-going process

24] Finanční analytický útvar: Výroční zpráva 2014, str. 11

25] Tedy primární trestné činnosti, která předchází praní špinavých peněz a která generuje nelegální zisky.

26] Např. Bitcoin, Litecoin, Peercoin, Quark, Megacon, Primecoin, Namecoin, Worldcoin...

27] Stanovisko FAÚ k datovým schránkám uvádí: „Podání oznámení podezřelého obchodu má svoji speciální úpravu v § 19 AML zákona a lze je tedy podat jen v tomto ustanovení popsanými způsoby. Nevztahuje se na ně obecná právní úprava a není tedy přípustné podání tohoto oznámení, včetně jeho případného doplnění, prostřednictvím datové schránky".

28] § 19 AML zákona

29] Postup instalace, technické požadavky a potřebné certifikáty je možné stáhnout přímo z webových stránek www.mfcr.cz/fau nebo na e-mailu: info@moneyweb.cz.

30] Kontaktní osobou nesmí být člen statutární orgánu úvěrové nebo finanční instituce, výjimkou je, pokud je to s ohledem na velikost instituce, způsob jejího řízení nebo počet zaměstnanců nezbytné.

31] Obvykle oddělení „Compliance"

32] Stanovisko FAÚ (zveřejněné na www.mfcr.cz/fau): „Ustanovení nekonkretizuje, zda se jedná o splnění příkazu klienta daného s předstihem (např. i formou „trvalého příkazu"), příkazu souvisejícího se zjištěním podezřelého obchodu, nebo příkazu, který bude přijat až po oznámení podezřelého obchodu. S ohledem na současně používané formy moderního obchodního styku je přitom třeba předejít i manipulaci s tímto majetkem takovými prostředky, kdy např. převod může být uskutečněn automaticky bez nutnosti (ale i možnosti) zásahu ze strany pracovníků povinné osoby (elektronické příkazy, použití platebních karet apod.); majetek je proto skutečně nutno zajistit i proti těmto možnostem nakládání".

33] Tvrdý/Bártová: Komentář Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu a předpisy související, C.H.Beck, ISBN 978-80-7400-099-7, str. 158

34] § 33 AML zákona

35] Do zahraničí FAÚ zaslal v roce 2014 154 spontánních informací. Ze zahraničních partnerských jednotek přišlo na FAÚ za rok 2014 200 dotazů.

36] V roce 2012 podal FAÚ 429 trestních oznámení, v roce 2013 547 trestních oznámení.