Pintér Dániel*

Pénzintézeti küzdelem a pénzmosás ellen

„Aki elfogadja a rosszat és nem tesz ellene semmit, az ugyanúgy részt vesz benne, mint az, aki segít elkövetni”
(Martin Luther King) [1]

1. Bevezető gondolatok[2]

A pénzügyi piacok liberalizálódása és az ezt kísérő technológiai forradalom hatására az utóbbi évtizedekben egy olyan nemzetközi gazdasági környezet alakulhatott ki, melyben a többszörösen összetett, határokon átívelő pénzügyi tranzakciókat egyszerűen és szinte azonnal meg lehet valósítani. Ezen feltételek olyannyira kedveznek a büntetendő cselekményből származó vagyonok legalizálásának, hogy a pénzmosás napjaink egyik legsúlyosabb gazdasági eredetű bűncselekményévé nőtte ki magát. Ha a vizsgált tevékenység megjelenik egy régió, vagy intézményrendszer életében, az a kezdeti serkentő hatásokat követően súlyos torzulásokat eredményezhet az adott terület gazdasági, politikai és társadalmi berendezkedésében. Ennek fényében nem meglepő, hogy a pénzmosás elleni küzdelem kapcsán egy olyan globális szabályozási folyamat indult meg, mely addig szinte teljesen elképzelhetetlen volt. Számos szervezet és szakértő foglalkozott a bűncselekmény vizsgálatával, illetve az ellene való fellépés lehetőségeivel. A küzdelem közel négy évtizedes tapasztalatai azt mutatják, hogy bár a hagyományos büntetőjogi eszközök is a pénzmosás elleni fellépés fontos alkotó elemei közé tartoznak, azonban a büntetőjog továbbra is csak végső eszköz lehet. A hangsúlyt ezért inkább a megelőzésre kell helyezni, melynek legjobb módszere egy olyan pénzügyi infrastruktúra kiépítése és működtetése, mely képes sikeresen ellenállni a pénzmosással kapcsolatos törekvéseknek.[3] Ennek szükségességét szakértők már a nemzetközi fellépés korai szakaszában felismerték, hiszen már az 1980-ban született Strasbourgi Konvenció is rámutatott a pénzügyi szolgáltatók jelentős szerepére[4].

Mégis a bankok pénzmosás elleni küzdelmének (továbbiakban: AML[5]) fejlődését vizsgálva megfigyelhetjük, hogy néhány kivételtől eltekintve hazánkban az intézményi fellépés csak az 1994-es szabályozási rendszer kiépítését követően indult meg. Kezdetben a bűncselekmény megelőzésére és megakadályozására fordított erőfeszítések fő motiváló ereje elsősorban a jogszabályi kötelezettségeknek való megfelelés volt. Azonban a szabályozás fokozatos szigorodásával, illetve a bankok kockázati attitűdjének változásával párhuzamban folyamatosan erősödött a fellépés mértéke. Napjainkban a hatályos pénzmosás elleni törvény[6] (továbbiakban: Pmt.) már számos kötelezettséget határoz meg a pénzmosás szempontjából leginkább veszélyeztetett pénzügyi szektor számára. Az ügyféllel közvetlen kapcsolatban lévő személyeknek az ügyintézés során körültekintően kell eljárniuk, az ügyfélről tevékenységének és szokásainak megismerése céljából, a lehető legtöbb adatot be kell gyűjteniük, amelyek alapján az esetleges gyanús tranzakciót észlelni, és jelenteni tudják. Emellett a napjainkat jellemző technológiai megoldásokat kihasználva, a szokatlan ügyleteket sokéves tapasztalatokon alapuló riasztási feltételek, illetve terrorista és egyéb korlátozó listák alapján, fejlett monitoring rendszerekkel is vizsgálják. Az automatizált szoftvermegoldások jelzéseit, az ügyintézői bejelentésekhez hasonlóan a pénzmosás ellen szakterület kollégái dolgozzák fel és a szolgáltató által kijelölt személyen[7] keresztül továbbítják a hatóságok felé.

* *közgazdász*

[1] Peter Lilley (2001): Piszkos ügyletek. A pénzmosás világa. Budapest, Perfekt Gazdasági Tanácsadó, Oktató és Kiadó Rt., 169. oldal

[2] A tanulmány elkészítéséhez szükséges ismeretek jelentős hányadra a területen szerzett szakmai gyakorlatom, valamint a pénzintézeti munkatársakkal készített mélyinterjúim alkalmával tettem szert.

[3] Gál István László (2009): Bejelentés vagy feljelentés? A pénzmosással és a terrorizmus finanszírozása elleni küzdelemmel kapcsolatos feladatok és kötelezettségek. Budapest, Penta Unió Kft.

[4] Tóth Mihály (2002): Gazdasági bűnözés és bűncselekmények. Budapest, KJK-KERSZÖV Jogi és Üzleti Kiadó

[5] Anti Money Laundering

[6] 2007. évi CXXXVI. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról.

[7] A Pmt. értelmében a szolgáltató köteles kijelölni egy, vagy több személyt, aki a legtöbb esetben a pénzmosás megelőzési terület vezetője. Az AML Officer legfontosabb feladata a beérkezett bejelentések és a hozzá kapcsolódó egyéb rendelkezésre álló információk továbbítása a Pénzügyi Információs Osztály felé. Emellett kapcsolattartó személyként jelenik meg a hatóság irányába, elvégzi a pénzmosási szabályzat aktualizálását, évente legalább egyszer pénzmosással kapcsolatos továbbképzést szervez az alkalmazottak részére, valamint szintén éves gyakorisággal végrehajtja az egyszerűsített ügyfél-átvilágításban részesült személyek körének felülvizsgálatát.

Továbbá a csoport dolgozóinak számos olyan egyéb feladatot is el kell látniuk, mellyel egyrészt a törvényi megfelelést biztosítják, másfelől a kockázatokból származó esetleges veszteségek minimalizálásán keresztül értéket is teremtenek a bank számára.

2. A Front Office-ban dolgozó ügyintézők szerepe

A pénzmosási tevékenységre utaló jeleket legkönnyebben az elhelyezés fázisában lehet észlelni, ezért ez tekinthető a műveletsorozat legkényesebb részének. Mivel a pénzmosók célja ebben a periódusban, hogy a szennyezett pénzeket bejuttassák a pénzügyi rendszerbe, ezért a banki alkalmazottaknak fokozott figyelemmel, a belső szabályzat betartása mellett kell munkájukat végezniük. Bár az utóbbi években kialakuló fejlett monitoring technológiák hatékony eszközei a szokatlan ügyletek felismerésének, azonban az ügyfelekkel közvetlen kapcsolatban álló banki alkalmazottakra továbbra is jelentős feladat és felelősség hárul az ilyen típusú tranzakciók kiszűrésében. A KPMG felmérése szerint a szakterület banki képviselőinek 97%-a ért egyet ezzel a megállapítással, ugyanis véleményük szerint a gyanús megbízásokat kísérő szubjektív körülményeket elsősorban a személyes kontaktus alkalmával lehet felismerni[8].

A pénzmosás és terrorizmus finanszírozása elleni törvény két lényeges kötelezettséget ír elő a hitelintézetek munkatársainak. Egyrészt a törvényi előírások, illetve belső eljárási mód szerint végrehajtandó ügyfél-átvilágítási kötelezettséget, másrészt a pénzmosásra, illetve terrorizmus finanszírozására utaló adat, tény, vagy körülmény felmerülése esetén bejelentési kötelezettséget.

2.1. Ügyfél-átvilágítási kötelezettség

Az FATF frissen átdolgozott 40 ajánlásának 10. pontjában felhívja a pénzügyi szolgáltatók figyelmét arra, hogy ne vezessenek névtelen, vagy nyilvánvalóan fiktív nevekre nyitott számlákat. Ennek érdekében vezessék be az ügyfél adatainak kellő ellenőrzését biztosító intézkedéseket[9]. Bár már a 2003-as téglatörvényként elhíresült szabályozás is azonosítási kötelezettséget írt elő a magyar szolgáltatók számára, azonban az új, hatályos Pmt. tovább bővítette az ezzel kapcsolatos teendőket. Az ügyfél-átvilágítási kötelezettség keretén belül az ügyfél azonosításán túlmenően el kell végezni az ügyfél személyazonosságának igazoló ellenőrzését, nyilatkoztatni kell az ügyfelet a tényleges tulajdonos személyéről, illetve hogy közszereplőnek minősül-e, valamint az üzleti kapcsolatra, vagy ügyleti megbízásra vonatkozó adatokat is vizsgálni kell, azokról a lehető legtöbb információt be kell szerezni. Ezek alapján felmerülhet a kérdés, hogy a hivatalos magyar fordítás, vagyis az ügyfél-átvilágítási kötelezettség mennyire adja vissza a szabályozás valódi célját, hiszen a vizsgálatnak nem csak az ügyfél személyére, hanem az üzleti kapcsolat, illetve ügyleti megbízás hátterére is ki kell terjednie[10].

A hatályos törvény szerint az ügyfél-átvilágítását az alábbi esetekben kötelező elvégezni:

1. üzleti kapcsolat létesítésekor,
2. 3 600 000 forintot elérő, vagy azt meghaladó összegű, készpénzben teljesített ügyleti megbízás teljesítésekor,
3. 500 000 forintot elérő, vagy azt meghaladó pénzváltás esetén,[11, 12]
4. összeghatártól függetlenül minden esetben, ha pénzmosásra, vagy terrorizmus finanszírozására utaló adat, tény, vagy körülmény merül fel,
5. ha a korábban rögzített, ügyféltől kapott azonosító adatok valódiságával, illetve megfelelőségével kapcsolatban kétség merül fel.

2.1.1. Ügyfél azonosítása

Az ügyfél azonosítással kapcsolatban sokakban él az a tévhit, hogy mikor a szolgáltató munkatársai azonosítást végeznek, akkor azt azért teszik, mert valamit gyanúsnak találtak, és ezt jelenteni kívánják. A valóságban azonban nem ez a folyamat elsődleges szerepe. Célja, hogy a bank megismerje ügyfeleit és ezáltal csökkentse a velük fennálló üzleti kapcsolatból származó jövőbeli kockázatait. Ennek érdekében az ügyintézőknek a belső szabályzatban meghatározott esetekben azonosítaniuk kell az ügyfelet, az ügyfél nevében vagy megbízása alapján eljáró természetes személyt és a számla felett rendelkezni jogosult személyeket. A folyamat elvégzésére az azonosítási adatlap kitöltésével kerül sor.

Az azonosítást két egymással igen szoros kapcsolatban álló elv alapján kell elvégezni. A pénzmosásból származó kockázatok csökkentésének egyik leghatékonyabb eszköze az „Ismerd meg az ügyfeled" (Know Your Customer – KYC) elv, mely szerint a banknak az ügyfélről és az ügyféltől a lehető legtöbb adatot be

[8] KPMG (2011): Global Anti-Money Laundering Survey. How banks are facing up to the challenge. Letöltve: KPMG hivatalos oldala, http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/anti-money-laundering.pdf, 2012.03.10.

[9] FATF (2012): International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – the FATF Recommendations. Letöltve: FATF hivatalos oldala, http://www.fatf-gafi.org/topics/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html, 2012.05.25.

[10] Jacsó Judit (2000): A pénzmosás elleni nemzetközi fellépés eszközei. Magyar Jog. 47. évf. 9. szám. 545–556. o.

[11] Utóbbi két esetben a kötelezettség kiterjed az egymással ténylegesen összefüggő, több ügyleti megbízásra/pénzváltásra is, ha ezek együttes értéke eléri a megszabott összeghatárt. Ebben az esetben az átvilágítást az összeghatár elérésekor kell elvégezni.

[12] Mind a készpénzes fizetés, mind pedig a pénzváltás esetén, ha az ügyletet külföldi pénznemben bonyolítják le, az értékhatár megállapításához az adott művelethez alapjában is alkalmazott árfolyam az irányadó.

kell gyűjteni annak érdekében, hogy tisztába legyen tevékenységével, üzleti kapcsolatai jellegével, pénzügyi szokásaival. Bár a „Körültekintő Ügyfélkezelés" (Customer Due Diligence –CDD) elve igen szoros kapcsolatot mutat a KYC-cel, azonban egy kicsiben mégis különbözik. A CDD ugyanis az azonosítás módját, a felelős ügyintézői magatartást határozza meg. Eszerint az ügyintézőnek minden esetben az ügyfél kockázati profiljához igazodva kell eljárnia.

Ugyanis az ügyfelekhez társítható, pénzmosással és terrorizmus finanszírozásával kapcsolatos kockázat nem minden esetben ugyanolyan mértékű. A hatékony fellépés érdekében a pénzügyi intézményeknek korlátolt erőforrásaikat a potenciálisan legnagyobb veszélyt jelentő területekre kell koncentrálnia. Ebből, az úgynevezett kockázat alapú megközelítésből kiindulva az új Pmt. bevezette a háromszintű ügyfél-átvilágítási kötelezettséget. Vagyis az ügyfelek vizsgálatát nem azonos mértékben kell elvégezni[13].

Ha a banki ügyintéző megítélése szerint az ügyfél-jelölt beletartozik az alacsony kockázati besorolású ügyfelek közé, akkor esetében az átvilágítás egyszerűsített módozata is alkalmazható. Ilyen esetben az üzleti kapcsolat létesítése előtt meg kell kérni a Kijelölt személy engedélyét, és a számlanyitást csakis az ő pozitív válaszát követően lehet elvégezni. Ilyen esetben az ügyfél-átvilágítás intézkedéseit csakis a pénzmosás és terrorizmus finanszírozására utaló adat, tény vagy körülmény felmerüléskor kell elvégezni, ha pedig ez nem áll fenn, akkor elég csupán az üzleti kapcsolatot figyelemmel kísérni.

A kockázat alapú megközelítés másik végletét a fokozott ügyfél-átvilágítás képezi, melynek kötelező alkalmazását a Pmt. négy esetben várja el:

- Külföldi kiemelt közszereplő (Politically Exposed Person – PEP)
- Harmadik országokkal folytatott határon átnyúló levelező banki kapcsolatok
- Távollévő ügyfél
- 500 000 forintot elérő, vagy azt meghaladó pénzváltás esetén[14]

Véleményem szerint az utolsó két esetben tanúsított nagyobb körültekintés szükségességét – pénzmosás megelőzési és megakadályozási szempontból – nem kell magyarázni. Mivel a külföldi kiemelt közszereplő kérdéskörét az ügyfél nyilatkozattételi kötelezettségénél fogom kifejteni, ezért most csak a levelező banki szolgáltatásokkal járó magasabb kockázatokat indokolom meg. A tevékenység valamely hitelintézet által más hitelintézetnek nyújtott olyan banki szolgáltatást jelenti, melyet a pénzintézetek közvetlen módon ügyfeleiknek nem nyújtanak. Ez alapján a levelező banki kapcsolat szereplőit tekintve megkülönböztethetjük a szolgáltatást nyújtó, vagyis a külföldi pénzintézet számláját vezető levelező bankot, valamint a szolgáltatást igénybe vevő levelezett bankot. Mivel előbbi szolgáltatók a levelezőbanki számlák vezetése során ki vannak téve annak a veszélynek, hogy klíring rendszerüket illegális forrásból származó pénzek tisztára mosására használják fel, ezért a pénzintézeteknek kellő mennyiségű információt kell beszerezniük levelezett bankjaikkal kapcsolatban annak érdekében, hogy megértsék partnerük üzleteinek jellegét, illetve célját. Ezért harmadik országban székhellyel rendelkező szolgáltatóktól levelezőbanki szolgáltatás keretében adott megbízást csakis abban az esetben lehet elfogadni, ha a levelezőbanki kapcsolat létesítését megelőzően az ügyfél-átvilágítási intézkedések megtörténtek, valamint a levelező bank a Pmt.-ben tételesen felsorolt egyéb kapcsolódó kötelezettségeinek is eleget tett. Bár az ezzel kapcsolatos feladatokat az ügyintézők mellett általában a nemzetközi bankműveletekkel foglalkozó csoport munkatársai látják el, azonban a kapcsolat létesítéséhez a magas kockázatok miatt, minden esetben szükséges a Kijelölt személy engedélye. A pénzintézeteknek tevékenységük végzése során kiemelt figyelmet kell szentelniük az olyan országokban, illetve területeken működő szolgáltatókkal fenntartott levelező banki kapcsolatok alkalmával, melyek szerepelnek az FATF által kibocsátott NCCT listán[15], gyenge pénzmosás elleni szabályozással, valamint felügyelettel rendelkeznek. A szabályozás továbbá rendelkezik a fiktív bankokkal, valamint az az EU és az ENSZ szankciós listáin szereplő szolgáltatókkal fenntartott levelezőbanki kapcsolat létesítésének és fenntartásának tilalmáról.

A fent említett négy eset mellett a bankok tevékenységének vizsgálata során azt tapasztaltam, hogy kockázataik csökkentése érdekében belső szabályzatukban további eseteket is megfogalmaznak, mint például:

- devizakülföldi ügyféllel üzleti kapcsolat létesítésekor, ha az ügyfél a közepes, vagy a magas kockázatúnak minősülő országok állampolgára, illetve ott állandó lakhellyel vagy székhellyel rendelkezik,
- üzleti kapcsolat létesítésekor a pénzmosási szempontból kockázatos gazdasági tevékenységek végzése esetén,
- az ügyfél nyilatkozata alapján várhatóan határon átnyúló tranzakciós tevékenységet folytató ügyfél esetén.

Ha ezek a körülmények nem állnak fenn, akkor a banki alkalmazottaknak normál módozat szerint kell az átvilágítást elvégezniük. Azonban ebben az esetben az ügyfélnek csupán a minimum adatkörhöz tartozó információkat[16] kell megadnia, mely a természetes

[13] Steiner Péter (2006): Paradigmaváltás a pénzmosás elleni küzdelemben: Globális rendszer a bűnözés ellen. Pénzügyi Szemle. 51. évf. 3. szám. 320–335. o.

[14] A kötelezettség kiterjed az egymással összefüggő, több ügyleti megbízásra/pénzváltásra is, ha ezek együttes értéke egy héten belül eléri a megszabott összeghatárt.

[15] Az FATF pénzmosási szempontból nem együttműködő országokat és területeket tartalmazó listája.

[16] Minimum adatkör: családi és utónév, lakcím, állampolgárság, azonosító

személyek esetében problémát jelenthet a szolgáltatók számára. Ugyanis ez nem tartalmazza sem az ügyfél születési helyét és idejét, sem pedig az anyja születési nevét. Pedig pont ezen adatok alapján lehet a természetes személyeket egyértelműen azonosítani, hiszen ezek a természetes azonosító jegyek az ember életében nem változtathatóak meg. A bankok ezt úgy próbálják kivédeni, hogy szinte minden esetben a magasabb kockázati kategóriához tartozó maximum adatkört kérik be ügyfeleiktől. Bár az adatvédelmi törvény miatt a két említett adat megadását nem tehetik kötelezővé, azonban az ügyfelek legtöbbször nincsenek tisztába jogaikkal, ezért nem is érdeklődnek ezzel kapcsolatban.[17]

Mivel a 2003-as pénzmosás elleni törvény által megszabott azonosítási kötelezettség során a mostani maximális adatkörnek megfelelő információkat kérték be, ezért feltehetnénk a kérdést, hogy hatékonyság szempontjából visszalépés-e az új törvény? Véleményem szerint ez nem jelenthető ki. A kockázat alapú megközelítés a banki erőforrások koncentrálásának jó módszere lehet. Azonban ennek ki kell forrnia magát. Ugyanis az ideális állapot majd az lehet, hogy a bankok az ügyfelektől felveszik az alap adatokat, majd kockázatérzékenységi alapon, az ügyfél hozzájárulása mellett, ügyfélprofil kérdőív formájában további kérdéseket tesznek fel. Megjegyezném, hogy számos bank gyakorlatában már alkalmazzák, vagy a közeljövőben tervezik ennek a módszernek a bevezetését.

2.1.2. Személyazonosság igazoló ellenőrzése

Az ügyfél-átvilágítás során a szolgáltatónak az ügyfelek személyazonosságának valódiságáról is meg kell bizonyosodniuk. Ennek érdekében az ügyintéző köteles megkövetelni a Pmt. által meghatározott okiratok bemutatását, illetve ellenőriznie kell az átadott okmányok érvényességét. Továbbá ha az ügyfél írásban hozzájárul a bemutatott okiratok másolásához, a bank munkatársának a személyazonosság igazoló ellenőrzésére alkalmas hatósági igazolványokról másolatot kell készítenie. Ellenkező esetben az ügyfélnek nyilatkoznia kell, hogy nem járul hozzá okmányai másolásához, és ezt a dokumentumot aláírásával hitelesíteni kell. Ha a banknak kétsége merülne fel az okiratok eredetiségével kapcsolatban, abban az esetben a jogszabály alapján rendelkezésére álló nyilvántartásban, valamint a nyilvánosan hozzáférhető adatbázisban köteles az adatokat ellenőrizni.

okmányának típusa és száma, illetve külföldi természetes személy esetén a magyarországi tartózkodási helye.

[17] Pénzügyi Szervezetek Állami Felügyelete (2004): 1/2004. évi ajánlás a terrorizmus finanszírozása és a pénzmosás megelőzéséről és megakadályozásáról. Letöltve: PSZÁF, http://www.pszaf.hu/intezmenyeknek/biztositok/szabalyozo_eszkozok/ajanlasok/pszafhu_penzmosastrv_20050729_1.html, 2012.03.10.

2.1.3. Ügyfél nyilatkozattételi kötelezettsége

Kiemelt politikai közszereplő (Politically Exposed Person – PEP)

A Pmt. rendelkezése értelmében üzleti kapcsolat létesítése, illetve ügyleti megbízás esetén külföldi lakóhellyel rendelkező ügyfélnek írásban nyilatkoznia kell arra vonatkozóan, hogy saját országa joga szerint kiemelt politikai közszereplőnek minősül-e, és ha igen, akkor milyen minőségben. Ezzel a szabályozás kettős feladata tovább bővült a korrupció elleni fellépés elősegítésével. Ugyanis a PEP intézményrendszer bevezetésének elsődleges célja, hogy a kiemelt közszereplők a büntetendő cselekményből származó vagyonukat ne tudják külföldön tisztára mosni. Emellett amolyan másodlagos szándéknak a pénzügyi intézményrendszer védelme tekinthető. Mivel ezek a személyek az átlag emberekhez képest sokkal inkább vannak a figyelem középpontjába, így a bankok számára magas reputációs kockázatot jelentenek. Ebből adódóan, ha az ügyfél nyilatkozata alapján kiemelt politikai közszereplőnek minősül, akkor az ügyintézőnek egyrészt a fokozott ügyfél-átvilágítás során megszabott eljárásmód szerint kell intézkedniük, másrészt az üzleti kapcsolat létesítése, illetve az ügyleti megbízás teljesítése előtt engedélyt kell kérnie a bank által kijelölt személytől, mely a legtöbb esetben az AML Officer. Abban az esetben, ha a nyilatkozatban állítottak valódiságát illetően bármilyen kétség merülne is fel, az ügyintézőnek minden műveletet fel kell függesztenie az érintett ügyféllel, és az AML Officer-t tájékoztatnia kell. Ilyenkor a Kijelölt személy, illetve meghatalmazott munkatársának feladata, hogy a jogszabály alapján rendelkezésre álló nyilvántartásban, valamint a nyilvánosan hozzáférhető adatbázisban ellenőrizze a megismert adatok valószínűségét és vizsgálatának eredményéről mielőbb visszajelzést adjon a fiók számára. Ha a pénzmosás elleni osztály szakértője úgy ítéli meg, hogy az ügyfél kiemelt közszereplőnek minősül, a felfüggesztést egészen addig fent kell tartani, amíg az ügyfél megfelelő, valós tartalommal nyilatkozatot nem tesz. Ellenkező esetben, ha erre nem hajlandó, az ügyintézőnek el kell utasítani mindennemű további üzleti kapcsolatot.

A pénzügyi intézmények gyakorlatának vizsgálatát követően a PEP-ek kezelésével kapcsolatban számos kérdés és kritikai észrevétel megfogalmazódott bennem. Az első ilyen, hogy Magyarországon, jelenleg a legtöbb bank az ügyfél PEP státuszát az általa kitöltött nyilatkozat alapján ítéli meg, melynek valós tartalma sok esetben kérdéses lehet. Ezért megfontolandó lenne a jelenlegi nyilatkozati elv mellé a nemzetközi gyakorlatban elterjedt, dokumentum alapú ellenőrzés, illetve automatizált listás szűrés bevezetése is. Ennek során a bank alkalmazottai már az első találkozáskor ellenőrizhetnék a PEP nyilatkozatok tartalmát a rendelkezésükre

álló adatbázisok segítségével. Az ilyen vizsgálat hatékonyságát azonban nehezítené, hogy a kiemelt közszereplőkről legtöbb esetben a nevükön kívül nem áll rendelkezésre egyéb adat, így egyértelmű beazonosításuk rendkívül nehéz. Továbbá véleményem szerint a bankok hírnevének védelme érdekében a hazai pénzintézeteknek a magyar közszereplőkkel folytatott üzleti kapcsolatokat is figyelnie kellene. Bár tény, hogy a PEP definíciója szerint a vizsgálatnak csak a külföldi közszereplőre kell kiterjednie, azonban megítélésem alapján a magyar szolgáltatók számára a hazai közszereplők által hordozott reputációs kockázat még magasabb, mint a legtöbb, kevésbé ismert külföldi társuké. Ugyancsak a hazai közszereplőkkel kapcsolatos, hogy számos ország gyakorlatához hasonlóan érdemes lenne róluk, illetve a kapcsolódó adatkörükről országos szinten listát készíteni. Ezzel egyrészt az előző pontban felvetett, reputációs kockázatok kivédésére irányuló folyamatot lehetne hatékonyabbá tenné, másrészt akár összesített globális PEP-jegyzéket is létre lehetne hozni. Bár az elképzelés nem újszerű, hiszen az Egyesült Államok már régóta szeretné elérni egy ilyen lista összeállítását, azonban számos országban a vele járó nemzetbiztonsági kockázat miatt ellenállásba ütközik az elképzelés. Végül gyakorlati problémaként említeném meg, hogy a pénzügyi intézmények számára a legtöbbször igen nehéz megállapítani a külföldi szereplők esetében a reális pénzáramlás mértékét. Ebből kifolyólag azonban sokkal nehezebb a szokatlan összegű tranzakciók kiszűrése.

Tényleges tulajdonos (Beneficial Owner)

A tényleges tulajdonos azonosítása kiemelt jelentőséggel bír. Számos esetben előfordul ugyanis, hogy a bankfiókban megjelenő személy, valamint a pénzeszköz felett ténylegesen rendelkező természetes személy egymástól különbözik. Ilyen esetekben a transzparens látásmód hiányában a bank nem lenne tisztában, hogy valójában kinek a pénzét is kezeli, az milyen forrásból származik, ezáltal könnyen a pénzmosási folyamat részesévé válhatna. Ennek érdekében az ügyfél-átvilágítás alkalmával az ügyfeleknek kötelező írásban nyilatkozniuk, hogy saját, vagy harmadik személy nevében, illetve érdekében járnak-e el. Első üzleti kapcsolat alkalmával jogi személy, vagy jogi személyiséggel nem rendelkező szervezet esetében az erről szóló nyilatkozatot csakis a képviseletre jogosult személy tehet. Ha az üzleti kapcsolat, vagy ügyleti megbízás körülményei alapján a pénzmosás és terrorizmus finanszírozásának veszélye nem áll fenn, akkor a tényleges tulajdonosról a családi és utónevét, a lakcímét, illetve az állampolgárságát elég bekérni. Ellenkező esetben a Pmt. által meghatározott maximum adatkörhöz tartozó információkat is rögzíteni kell. Véleményem szerint érdekes, hogy mivel a normál esetben felvett adatkör egyáltalán nem tartalmaz természetes azonosító jegyeket, ezért a PEP státuszt a tényleges tulajdonos esetében nem kell megállapítani.

Mivel a kiemelt politikai közszereplőkhöz hasonlóan a tényleges tulajdonos személyének megállapítását is az ügyfél nyilatkozata alapján kell meghatározni, ezért a pénzek valós háttere gyakran bizonytalan. Bár ha a banki alkalmazottban kétség merül fel a nyilatkozat tartalmával kapcsolatban, akkor ismételt írásbeli nyilatkozat megtételére kell felszólítani az ügyfelet, azonban ez továbbra sem jelenthet számukra biztosítékot. Így egységes adatbázis hiányában a pénzintézet szakértői maximum a számukra elérhető információkból következtethetnek a mögöttes személy, vagy szervezet kilétére.

2.1.4. Üzleti kapcsolatra és ügyleti megbízásra vonatkozó adatok rögzítése

Az eddig bemutatott kötelezettségek elsősorban az ügyfél és hátterének megismerését szolgálták. A Pmt. ezek mellett üzleti kapcsolat létesítése, vagy ügyleti megbízás teljesítése esetére adatrögzítési kötelezettséget ír elő a szolgáltató számára. Ennek során a kötelezően rögzítendő adatok üzleti kapcsolat esetén a szerződés típusa, tárgya és időtartama, míg ügyleti megbízás esetén a megbízás tárgya és összege. A kockázatalapú megközelítés elvének szem előtt tartásából adódóan szokatlan tranzakciók esetén ez kiegészülhet a teljesítés körülményeinek leírásával. Megjegyezném, hogy a magyar szabályozás által megkövetelt információmennyiség még így is kevesebb, mint amit az EU III. direktívája megszab, ugyanis ott az adatkör tovább bővül az üzleti kapcsolat céljával és tervezett jellegének leírásával.

2.1.5. A kockázatalapú megközelítés szoftveres támogatása

Az elmúlt másfél évtized folyamatos fejlesztéseinek és technológiai innovációinak köszönhetően a pénzügyi szolgáltatók pénzmosás és terrorizmus finanszírozás elleni küzdelmének hatékonyságát automatizált szoftverek bevezetésével és működtetésével jelentősen meg lehetett növelni. Ezeknek a rendszereknek egyik típusát a kockázatértékelő programok jelentik. Az ilyen informatikai megoldások bevezetése képessé teheti a bankokat, hogy az ügyfél-átvilágítás alkalmával begyűjtött adatok, valamint belső adatbázisok alapján teljes kockázati profilképet alkossanak ügyfeleikről. A program elemzése alkalmával általában három tényezőt vesz figyelembe:

- *Ügyfélkockázat:* A kockázatnak ezt a típusát két részre kell bontanunk. Természetes személyek esetében az ügyfél kora, végzettsége, jövedelme, állampolgársága, családi állapota és egyéb hasonló tényezők számítanak ide, míg szervezetek esetében a tevékenységi kör, társasági forma, tulajdonosi háttér, illetve a készpénz és internet

banki forgalom várható volumene alapján lehet az ügyfélkockázatot számítani.[18]

- *Ország kockázat:* Az ügyféllel kapcsolatban vizsgálják a tartózkodási-, illetve székhelyhez tartozó kockázatot is, melyet számos tényező együttes figyelembevétele mellett állapítanak meg. Leggyakrabban az ország gazdasági kockázatát, esetleges offshore besorolását, illetve terrorista fenyegetettségét veszik számba, valamint ellenőrzik, hogy az ország nem szerepel-e a nemzetközi szervezetek által kiadott korlátozó és szankciós listák valamelyikén.
- *Termékkockázat:* A pénzintézet egyes termékei különböző kockázatot rejtenek magukban, ezért szükséges az ügyfél termékportfóliójának kockázati értékelése is. Ennek szükségességét fokozza, hogy a napjainkban jellemző piaci dinamizmus és a pénzügyi innovációk mellett egyre komplexebb terméke jönnek létre.[19]

Ezek alapján a szoftver mátrix alapú számítási módszerrel kockázati pontszámokat társít az egyes ügyfelekhez, melyek szerint a pénzintézetek kockázati kategóriákba sorolhatják őket. Az ilyen módszer nagyban segítheti a bankokat a korábban már említett Körültekintő Ügyintézés elvének megvalósításában, hiszen közvetlen az adatok felvételét követően besorolja az ügyfeleket, mely információ ismeretében az ügyintézők az ügyfél kockázati profiljához igazodva tudnak eljárni.

Bár a Magyarországon működő pénzügyi szolgáltatók a vizsgált bűncselekményből fakadó kockázatok felmérésére és értékelésére komoly figyelmet fordítanak, azonban kutatásom eredményei alapján, a bemutatott, rendkívül komplex technológiai megoldások alkalmazása még csak pár nagyobb bank gyakorlatában valósult meg. Ugyanis az igencsak drága, külső fejlesztő cégtől vásárolt CDD/KYC modulok helyett a legtöbben saját fejlesztésű szoftvereket használnak az ilyen típusú kockázatmenedzselésre.

2.1.6. Ügyfél-átvilágítás elvégzésének időpontja

Noha az ügyfél átvilágítását alapesetben az üzleti kapcsolat létesítése, vagy az ügyleti megbízás teljesítése előtt kell elvégezni, azonban a gyakorlatban találhatóak mégis kivételek. Vannak olyan szolgáltatók, amelyek engedélyezik munkatársaik számára, hogy az ügyfél és a tényleges tulajdonos személyazonosságának igazoló ellenőrzését az üzleti kapcsolat létesítése során folytathatssák le, ha azt a rendes üzletmenet megszakításának elkerülése érdekében szükséges vélik és ha a pénzmosás vagy a terrorizmus finanszírozásának valószínűsége csekély. Ilyen esetekben az igazoló okiratok bemutatásáig a számlát zárolni kell, azon pénzügyi műveletek nem végezhetőek.

Az üzleti kapcsolat létesítését követően az ügyfél átvilágítását további szerződéskötések, illetve ügyleti megbízások alkalmával már nem kell elvégezni, ha a szolgáltató munkatársa a megismert adatokat visszakereshető módon a banki rendszerbe rögzítette, az adatokban változás nem következett be, illetve nem áll fent az ügyfél-átvilágítás elvégzését kötelezővé tevő körülmények egyike sem.

Mivel a szolgáltatónak érdeke és egyben kötelezettsége is az ügyfél adatainak naprakészen tartása, ezért ha az ügyfélkapcsolat fennállása során az ügyfél-átvilágításkor megadott adatokban változás következik be – beleértve a tényleges tulajdonosi nyilatkozatot is – akkor az ügyfélnek a tudomásszerzést követő 5 munkanapon belül kötelezettsége erről a pénzintézetet tájékoztatni.

2.1.7. Teendő, ha ügyfél-átvilágítás nem hajtható végre

Előfordulhat olyan eset, hogy az ügyintéző nem tudja az ügyfelet kockázati besorolásának megfelelő mértékben átvilágítani, a szabályzatban meghatározott adatokat felvenni tőle. Ilyenkor az üzleti kapcsolat létesítését, illetve az ügyleti megbízásban foglalt tranzakció végrehajtását meg kell tagadni, és hiánypótlásra kell felszólítani az ügyfelet. Ha a megszabott határidőn belül ennek nem tesz eleget, abban az esetben az érintett ügyféllel fenntartott üzleti kapcsolatot azonnali hatállyal meg kell szüntetni.

2.1.8. Ügyfél-átvilágítás speciális esetei

Más szolgáltató által elvégzett ügyfél-átvilágítási intézkedések átvétele, illetve a bank által elvégzett ügyfél-átvilágítási intézkedések átadása

A szabályozás lehetővé teszi a bankok számára, hogy egy másik szolgáltató[20] által már végrehajtott ügyfél-átvilágítás eredményét elfogadják, amennyiben az érintett ügyféljelölt ezt kéri, és írásbeli meghatalmazást ad a bank részére, hogy bekérhesse a már felvett és rendelkezésre álló adatokat tartalmazó okiratok másolatát. Ilyen esetekben, a kockázatok mérséklésének érdekében, még az üzleti kapcsolat létesítését megelőzően az ügyintéző köteles a Kijelölt személyt írásban tájékoztatni, mellékelni számára az adatokat átadó pénzügyi szolgáltatóról a szükséges információkat. Ha a szolgáltató megfelel a bank belső szabályzatában megszabott feltételeknek és az AML Officer sem értékeli kockázatosnak a korábban elvégzett át-

[18] Megjegyzendő, hogy az itt felsorolt adatok többsége csak ritkán áll a szolgáltatók rendelkezésére, ezért is lenne fontos az azonosítási kötelezettségnél már említett ügyfélprofil kérdőív használatának rendszeresítése.

[19] Rohan Bedi (2006): Anti-Money Laundering Risk Models. Letöltve: Rohan Bedi hivatalos oldala, http://www.rohanbedi.com/AML-RiskModels.pdf, 2012.03.10.

[20] Ez alól kivételt képeznek a készpénzátutalás és pénzváltási tevékenységet folytató szolgáltatók.

világítás adatainak átvételét, akkor pozitív döntésről értesíti az ügyintézőt. A bank munkatársa ezt követően már lekérheti az adatokat, mely a gyakorlatban két módon valósulhat meg:

- bank csoporton belül a bank által használt belső levelezési rendszeren, vagy más, belső kommunikációs csatornán keresztül;
- más magyar, illetve Európai Uniós szolgáltató esetében pedig SWIFT üzeneten keresztül.

Természetesen a bank által elvégzett ügyfél-átvilágítási intézkedések alkalmával megszerzett adatokat más szolgáltató részére is ki lehet adni. Ilyenkor az érintett ügyfél hozzájárulása mellett, a szolgáltató írásbeli megkeresése is szükséges. Ha mindkét feltétel teljesül, akkor a felmerülő igényt jelezni kell az AML osztály vezetője felé, akinek hozzájárulásával az adatok átadása megvalósulhat.

Az effajta információ-tranzakciók mindkét fél részéről kiemelt körültekintést igényelnek, hiszen jelentős kockázatot rejtenek magukban. Míg az átvevő bankot az ügyfél-átvilágítás eredményének elfogadásával járó felelősség terheli, addig az átadó banknak a banktitkot képző ügyféladatok megfelelő és biztonságos kezelésére kell törekednie.

Ügynökök által végzett ügyfél-átvilágítás

A pénzintézetekkel szerződésben álló ügynökök által hozott új üzleti kapcsolatok, illetve ügyleti megbízások esetében az ügyfél-átvilágítás módszere és menete megegyezik a korábban leírtakkal. A folyamatban csupán annyi a különbség, hogy az ügynököknek az ügyfél jóváhagyásával, a szükséges igazoló okiratokról másolatot kell készíteni és azt el kell juttatnia az érintett fiókhoz. Az ügynöki tevékenység során fontosnak tartom továbbá megjegyezni, hogy az általuk végzet átvilágításért a bank teljes körű felelősséggel tartozik.

2.2. Az ügyfél és tranzakcióinak folyamatos figyelemmel kísérése, ügyintézői bejelentés

Manapság a bűnözők a büntetendő cselekményből származó piszkos pénzüket számos módszer segítségével próbálhatják meg legális forrásból származóként feltüntetni. Ebből adódóan a pénzmosás elleni küzdelem során nem lehet normákat előírni, hogy egy tranzakciót mikor kell gyanúsnak ítélni. Ezért a küzdelem legmegfelelőbb módszere a korábban már megismert KYC és CDD elvek szigorú betartása. Vagyis az ügyintézők tevékenysége nem fejeződik be az ügyfél-átvilágítás már eddig ismertetett lépéseinek megtételével. A bank munkatársainak folyamatosan vizsgálniuk kell az ügyfelet, valamint a vele kialakított üzleti kapcsolat fennállása során, a megbízásából végrehajtott tranzakciókat. Ennek érdekében az ügyfél-átvilágításkor begyűjtött adatok, az ügyfél üzleti, pénzügyi és fizetési szokásainak elemzése, valamint kapcsolatainak és pénzforgalmának nyilvántartása alapján ügyfélprofilt hoznak létre. Az effajta adatbázisok a megismert információk mellett tartalmazzák az ügyfél kockázati besorolását, a róla készült pénzintézeti értékeléseket, valamint a külső forrásból beszerzett ismereteket. Az ügyfélprofil esetében fontos, hogy a benne szereplő adatok mindig naprakészek legyenek, hiszen célja, hogy a pénzügyi intézmények ügyfeleikről olyan komplex képet kapjanak, mely alapján értelmezhetőek az ügyfelek ügyletei, illetve üzleti kapcsolatai, valamint megállapíthatóak és kiszűrhetőek gyanús tranzakciói. Ha a bank munkatársai az aktív ügyfélkapcsolat alkalmával szokatlanságot észlelnek az ügyfél számlaforgalmában, olyan ügyletet, mely nincs összhangban az ügyfél szokásaival, nem illeszkedik a róla kialakított profilba, és ez az eltérés nem igazolható könnyen belátható gazdasági, vagy jogszerű céllal, akkor arról bejelentést kell tenniük. Természetesen a bűncselekménynek egyéb jelei is megfigyelhetőek a közvetlen ügyfélkapcsolat folyamán, ezért az ügyintézőknek fokozottan figyelniük kell az ügyfelek viselkedését, illetve megjelenésük körülményeit is. Ha ezekben bármi normálistól eltérőt észlelnek, szintén jelenteniük kell.[21]

A pénzintézeti munkatársnak szokatlan ügyletek észlelésekor, a gyanú jellegétől függően három lehetősége van. A tapasztalt körülményekkel kapcsolatban a tranzakció lebonyolítását megelőzően kikérheti a fióki, illetve adott szervezeti egység vezetőjének véleményét, valamint szükség esetén, konzultációt folytathat az AML Officer-rel is. Ha ezek alapján a gyanú nem bizonyul elégségesnek a megbízás teljesítésének felfüggesztéséhez, illetve visszautasításához, a bank alkalmazottjának a tranzakciót végre kell hajtania. Azonban a konzultációk alapján a Kijelölt személy úgy is dönthet, hogy az eset kapcsán a hatóság azonnali beavatkozását látja szükségesnek és ezért a tranzakció teljesítésének felfüggesztését rendeli el. Ilyenkor a felfüggesztés tényéről szintén bejelentést kell küldeni, melyet a PEII-nek 24, illetve 48 órán[22] belül el kell bírálnia. A hatósági válasz alapján az ügyintézőnek vagy teljesíteni kell az ügyfél felfüggesztett megbízását[23], vagy a PEII további intézkedése esetén visszautasíthatja annak végrehajtását. Bármelyik eset is áll fenn, mivel az ügyintéző az ügylet kapcsán pénzmosásra vagy terrorizmus finanszírozására utaló adat, tény, vagy körülmény felmerülését észlelte, ezért a belső eljárás szerint haladéktala-

[21] Pénzügyi Szervezetek Állami Felügyelete (2008): A PSZÁF Felügyeleti Tanácsának 3/2008. (XI. 20.) számú ajánlása a pénzmosás és a terrorizmus megelőzéséről és megakadályozásáról. Letöltve: PSZÁF, http://www.pszaf.hu/bal_menu/szabalyozo_eszkozok/pszafhu_bt_ajanlirelvutmut/ajanlas_ft/pszaf_ajanlas_3_2008.html, 2012.03.10.

[22] 24 óra belföldi ügyleti megbízás, illetve 48 óra nem belföldi ügyleti megbízás esetén.

[23] Ha a PEII válasza 24/48 órán belül nem érkezik meg, akkor a megbízást a bűncselekmény támogatásának lehetősége ellenére is végre kell hajtani. Mivel az ügyintéző és a bank a hatóság részére jelentett a gyanús esetet, ezért a szolgáltató és munkatársai sem vonhatóak felelősségre, büntetőeljárás a bejelentési kötelezettség elmulasztása miatt nem kezdeményezhető ellenük.

nul bejelentési kötelezettségének eleget kell tennie.

Bár a legtöbb bankban elektronikus formában kell eljuttatni a bejelentéseket az AML osztály felé, azonban ennek belső eljárásrendje és technikai háttere pénzintézettől függően igen változó lehet. A nagyobb bankok esetében három gyakorlati megoldást tapasztaltam. A legegyszerűbb a bejelentési lap szkennelése és elektronikus üzenetben – belső levelezési rendszeren, vagy faxon keresztül – való továbbítása. Bár a rendszer megfelel a követelményeknek, véleményem szerint több szempontból sem nevezhető hatékonynak. Egyrészt mivel az ügyintézőknek nincsen azonnali visszacsatolása arról, hogy helyesen töltötték-e ki a szükséges mezőket, így a fiókvezető kontrollja ellenére is jó esély van a hiányos és hibás dokumentumok beérkezésének. Ráadásul azt adatok manuális rögzítése a hatósági elektronikus bejelentő rendszerbe jelentős időráfordítást igényel az AML részleg munkatársaitól. Ennél hatékonyabb megoldásnak találtam a belső levelező rendszeren belül kialakított, bejelentő modult. Mivel ez az informatikai alkalmazás az ügyintéző számára az elektronikus bejelentő formulához kitöltési opciókat kínál fel, valamint hiányosan, vagy hibásan kitöltött mező esetében nem engedi továbbléptetni felhasználóját, ezért az előző problémafelvetéseimet feloldja. Azonban a rendszer belső adatbázissal való szinkronizálásának hiányából fakadóan a kezelőknek a bejelentő lapok kitöltésével még mindig sokat kell foglalkozniuk. Ezért véleményem szerint az alkalmazottak munkájának egyszerűsítése érdekében a legjobb módszer egy olyan esetrögzítő modul kialakítása és alkalmazása, mely az ügyfél-adatbázissal teljesen szinkronizálva van. Ugyanis ebben az esetben a szoftver a jelentés mezőit automatikusan feltölti az ügyfél adataival, így az ügyintézőknek csupán az ügyfél számla és tranzakció adatait kell kiegészíteniük, valamint a pénzmosás és terrorizmus finanszírozása gyanús eset körülményeit, illetve a hozzá kapcsolódó egyéb információkat kell megadniuk. Ennek elvégzését követően, a fióki vezető jóváhagyásával már továbbítható is a belső dokumentum a Kijelölt személy felé.

Az ügyintézői bejelentésekkel kapcsolatban fontosnak tartom megemlíteni a felfedés tilalmát, melynek személyi hatálya mind a szolgáltatóra, illetve alkalmazottaira, mind pedig a hatóságra kiterjed. Lényege, hogy a törvény szerint a tilalom tárgyául[24] meghatározott információról ügyfélnek, illetve harmadik személynek és szervezetnek[25] nem lehet tájékoztatást adni, illetve az információ titokban maradását biztosítani kell. A szabályozás célja, hogy biztosítsa egyfelől a bejelentő személyének védelmét, másrészt pedig elősegítse a hatósági munka menetét.

[24] Tilalom tárgya: bejelentés és adatszolgáltatás teljesítése, annak tartalma, az ügyleti megbízás teljesítésének felfüggesztése, a bejelentő személye, illetve büntetőeljárás indításának ténye.

[25] A tiltás alóli kivételeket a szabályozó a Pmt. 27. § (2)–(5) bekezdésében határozta meg.

3. Pénzintézetek AML/WLM szűrőrendszereinek működése

3.1. Szűrő és tranzakció-figyelő rendszerek általános bemutatása

Az előzőekben bemutatott körültekintő ügyintézés mellett a gyanús tranzakciók felderítésének másik lehetőségét a szűrő és tranzakció-figyelő informatikai megoldások hatékony használata jelenti. Manapság ugyanis a pénzmosás és terrorizmus finanszírozása során alkalmazott műveletek olyan többszörösen összetett, esetenként több száz tranzakciónak a sorozatát jelentik, melyeket a hagyományos módszerekkel szinte lehetetlen felfedezni. Ezért a szakértők munkáját olyan előre paraméterezett monitoring rendszerekkel támogatják, melyek a pénzintézet által használt belső adatbázisokat, számlaműveleteket és elektronikus tranzakciókat vizsgálva észlelik a gyanúsnak vélt eseteket és erről riasztást küldenek. Ahhoz azonban, hogy egy elektronikus szűrőrendszer hatékonynak bizonyuljon számos feltételnek meg kell felelnie. Egyrészt egy jól kidolgozat szoftver működése során a bank teljes tranzakció-állományát elemzi, és ebből ismeri fel a szokatlan pénzmozgásokat. Ahhoz azonban, hogy ezt eredményesen meg tudja valósítani, vagyis képes legyen az ismerté vált pénzmosás-gyanús technikák és tranzakciók észlelésére, elengedhetetlen a riasztási szabályok megfelelő beállítása. Ugyanis egy rosszul kalibrált rendszer vagy nem fog egyáltalán találatot generálni, vagy pedig olyan mennyiséggel halmozza el a pénzmosás megelőzési szakterület munkatársait, mellyel teljesen megbéníthatja munkájukat. További elvárás a hatékony rendszerekkel kapcsolatban, hogy azok jól kezelhetőek, rugalmasak és jelentős ráfordítások nélkül utólagosan is könnyen fejleszthetőek legyenek. Ugyanis egy ilyen dinamikusan fejlődő területen, mint amilyen a pénzmosás elleni küzdelemé, nem lehet előre látni, hogy 2, 3, vagy 5 év múlva az állandóan változó szabályozás, a bűncselekmény elkövetésének új módszerei, vagy éppen a bank által bevezetett új pénzügyi termékből származó kockázatok milyen megoldásokat és változtatásokat fognak megkövetelni. Ha ennek a kritériumnak nem felel meg a pénzintézet által használt szoftver, akkor az előbb, vagy utóbb szükségessé váló új rendszer beszerzése és üzembe helyezése, valamint kezelésének megismerése komoly időráfordítást és jelentős költségeket igényelhet. Vagyis lehet, hogy egy nagyobb flexibilitást nyújtó szoftver rövidtávon drágább lehet, azonban hosszútávon mégis költséghatékonyabb megoldást biztosíthat. Végül nem lehet elhanyagolni a program kezelhetőségét, az általa kínált funkcionális lehetőségeket sem. Először is fontos, hogy a riasztáso-

kat megfelelő időben és formátumban juttassa el az arra illetékes személynek. Emellett egy felhasználóbarát informatikai megoldás lehetővé teszi például az ad hoc, akár célirányos vizsgálatok elvégzését, a találatok mentését, statisztikai elemzését, vagy éppen a kapcsolati hálók felrajzolását.[26]

3.2. Szűrés a gyakorlatban

A legtöbb nagyobb pénzintézet a fenti kritériumokat szem előtt tartva állandó jelleggel alkalmaz automatizált szűrőszoftvereket, melyeket a gyakorlat alapján két csoportba sorolhatunk. A rendszer pénzmosás elleni modulja – AML[27] modul – paraméterek alapján a tranzakciós adattárházból szűri ki a szokatlan tranzakciókat, míg a listafigyelő modul – WLM[28] modul – a tranzakciós-adattárház, valamint a SWIFT rendszeren keresztül bonyolított nemzetközi átutalások szankciós és korlátozó listás elemzését végzi.

A tranzakció-figyelő rendszer AML modulja a tranzakciós-adattárházból kinyert adatbázisban keresi, és találat esetén jelenti az illetékes személy felé a gyanús belföldi és nemzetközi pénzügyi műveleteket. A program pénzmosás elleni modulja minden bank esetében offline szűrést végez, vagyis az előző napi pénzmozgások és számla információk alapján, éjszakai feldolgozásban végzi el az elemzéseket. A folyamat előre beállított paraméterek alapján megy végbe, melyeket a PSZÁF ajánlásai, a pénzügyi intézmények tapasztalatai, valamint a nemzetközi gyakorlat alapján alakítottak ki. Az analisták által leggyakrabban használt riasztási szabályok a nagy, ismétlődő, illetve kerek összegek, körkörös, vagy oda-vissza utalások, inaktív, alvószámlák hirtelen „ébredése", shell address kedvezményezettek, valamint offshore partnerek, vagy bankok. Természetesen a pénzmosás technikáinak folyamatos fejlődésével új módszerek jelennek meg, melyből adódóan a pénzmosás elleni szakterület rendszeresen felülvizsgálja és aktualizálja a szűrés során alkalmazott szabályokat, illetve feltételeket.

A banki tranzakciós adattárházából származó adatbázis vizsgálatának másik módját a WLM szűrés képezi. Ennek során a terrorista-, illetve egyéb szankciós és embargós listákon szereplő személyekről és szervezetekről, külön erre szakosodott szolgáltatók által készített adatbázist használnak fel.[29] Megfigyeléseim alapján a rendszer által elvégzett listás megfigyelések, a pénzintézet gyakorlatától függően lehetnek real time, vagy offline vizsgálatok egyaránt.

Ha a banknál real time, vagyis valós idejű WLM szűrőrendszert alkalmaznak, abban az esetben szankciós listás találatkor az ügyintézőt már az ügyfél adatainak bevitelekor riasztja a rendszer. Ilyenkor a belső szűrőrendszer kezelőfelületen keresztül értesítést küld a szankciós listás találatról, valamint felhívja a banki alkalmazott figyelmét, hogy a riasztásról haladéktalanul tájékoztassa az AML szakterület munkatársait és a válaszig függessze fel a számlanyitást, illetve az ügyleti megbízás lebonyolítását. Miután az ügyintéző megküldte az ügyfél adatait, a pénzmosás elleni osztály szakemberei a rendelkezésükre bocsátott adatbázisok alapján ellenőrzik a bejelentést, majd a döntésről értesítik az érintett fiókot. A vizsgálat eredményét figyelembe véve a döntésnek két kimenetele lehet. Ha az AML terület munkatársai úgy ítélik meg, hogy nagy valószínűséggel a bankban számlát nyitni, illetve ügyleti megbízást lebonyolítani kívánó személy megegyezik a szankciós, korlátozó listákon szereplő egyénnel, akkor egyrészt bejelentési javaslattal élnek a Kijelölt személy felé, valamint az ügyintézőt tájékoztatják a valós találatról és a rendszer a további ügyintézést megakadályozza. Ellenkező esetben a találatra a „téves riasztás" jelölést alkalmazzák és engedélyezik a számla megnyitását, illetve az ügyleti megbízás teljesítését.

Számos pénzügyi szolgáltatónál azonban a terrorizmus elleni küzdelmet, illetve egyéb korlátozó intézkedések végrehajtását elősegítő listás szűrést az AML szűréshez hasonlóan offline módban végzik. A folyamat során a szűrőrendszer szankciós listák alapján, a tranzakciós adattárházban tárolt előző napi tranzakciók adatait és számla információkat éjszakai műszakban monitorozza. Egyezőség esetén, a keletkezett találatokhoz kapcsolódó személyek, illetve szervezetek tranzakcióit megakadályozza, majd erről a pénzmosás elleni szakterület munkatársának riasztást küld. Ezt követően a találatok ellenőrzése és kezelése a valós idejű ellenőrzéshez hasonlóan történik annyi különbséggel, hogy mivel ebben az esetben a rendszer közvetlenül az AML részleget értesítette, így az ügyleti megbízást, vagy üzleti kapcsolatot intéző fióki kollégát a vizsgálatról nem kell tájékoztatni.

A pénzügyi szolgáltatók a tranzakciós adattárház WLM szűrését akár real time, akár offline módban végzik is el, a kockázatok csökkentése érdekében az ellenőrzéseket változó rendszerességgel és mélységgel későbbi időpontokban is elvégzik. A kutatásom során vizsgált bankok egyikében az a bevált gyakorlat, hogy az új tranzakciók által bekövetkezett változásokat napi, míg a teljes adatbázist heti rendszerességgel vizsgálják.

A bankok a tranzakciós adattárházból nyert adatbázisához hasonlóan a SWIFT rendszerben bonyolított valamennyi tranzakcióra is alkalmazzák a szankciós listákat alapul vevő szűrőrendszereket. Az ilyen típusú ügyletek esetében azonban a szolgáltatók szinte kivétel nélkül valós idejű szűrést alkalmaznak. Abban az esetben, ha a SWIFT üzenetben található adatok egyezőséget mutatnak a listákon szereplő személyekről,

[26] Oracle (2010): Best Practices for Anti Money Laundering (AML): System Selection and Implementation. Letöltve: Oracle hivatalos oldala, http://www.rohanbedi.com/AML-RiskModels.pdf, 2012.03.10.

[27] Anti-Money Laundering

[28] Watchlist Management

[29] A létrehozott adatbázisok számos szervezet listáját tartalmazzák. A bankok ezek közül vásárolják meg az általuk hasznosnak, szükségesnek – illetve megfizethetőnek – tartottakat. Magyarországon leggyakrabban az Európai Unió, valamint az Egyesült Államok Külföldi Eszközök Felügyeltének Irodája (OFAC) által kiadott listákat használják.

illetve szervezetekről nyilvántartott adatokkal, a szoftver azonnali hatállyal blokkolja[30] a SWIFT rendszerben bonyolított tranzakciót és értesíti róla az illetékes személyt. A riasztások további elemzése és kezelése a tranzakciós adattárház valós idejű ellenőrzéséhez hasonlóan alakul.

A 2007. évi pénzmosás és terrorizmus finanszírozása elleni törvény a hatálya alá tartozó szolgáltatók számára legalább egy alkalmazott foglalkoztatása esetén kötelező jelleggel előírja a belső ellenőrző és információs rendszer működtetését. Ez alól a kötelezettség alól a kisebb ügyfélkörrel és forgalommal rendelkező, kevésbé tőkeerős bankok sem képeznek kivételt. Azonban ezeknek a szolgáltatóknak, annak ellenére meg kell felelniük a törvényi előírásoknak, hogy nem áll módjukban a fentiekben bemutatott, alkalmanként több száz millió forintos beruházással és magas fenntartási költségekkel járó szűrőrendszereket alkalmazni. A gyakorlat ezért azt mutatja, hogy ezek a hitelintézetek vagy saját maguk által kidolgozott, a bemutatott rendszerektől fejlettségben jóval elmaradó szoftvereket alkalmaznak, vagy a tranzakciós adatbázisból XLS, vagy XLSX formátumban kinyert adatokat és információkat Microsoft Excel felhasználásával manuálisan elemzik.

4. Pénzintézeti bejelentések

Az eddig megismert folyamatokból kiindulva a hatóság számára megküldött bejelentések alapjául, az ügyfelekkel közvetlen kapcsolatban álló munkatársak észlelései, valamint a szűrő és tranzakció-figyelő rendszerek riasztásai szolgálhatnak. Az így beérkező adatokhoz és információkhoz kapcsolódó bejelentési kötelezettséget két csoportra lehet osztani. A Pmt. értelmében a pénzmosás és terrorizmus finanszírozása szempontjából gyanúsnak vélt eseteket a szolgáltatónak haladéktalanul jelenteni kell a Pénzügyi Hírszerző Egység felé. Emellett a hatályos Kit. alapján a bankok kötelezettsége az olyan adat, tény, vagy körülmény bejelentésére is kiterjed, melyekből arra lehet következtetni, hogy az Európai Unió korlátozó intézkedéseinek alanya Magyarország területén, az intézkedés hatálya alá eső vagyonnal rendelkezik, illetve olyan ügyletet folytat, melyből vagyoni előnye származik.

Bár a Pmt. rendelkezése szerint a Kijelölt személynek minden ügyintézői bejelentést haladéktalanul, mérlegelés nélkül továbbítani kellene a PEII felé, ennek ellenére a bűncselekmény elleni fellépés hatékonyságának növelése érdekében a gyakorlatban ez másképpen működik. Ugyanis a bejelentési kötelezettség elmulasztását követő jogi felelősségre vonás óvatosságra inti az ügyintézőket. Mivel jóhiszeműség esetén, a később megalapozatlannak bizonyuló ügyek jelentése sem jár semmilyen következménnyel, ezért sokszor a fióki alkalmazottak a legkisebb szokatlan körülmény felmerülésekor is automatikusan értesítik a pénzmosás megelőzési csoport kollégáit. Ha azonban a szolgáltatók a törvényt szó szerint értelmeznék, akkor így olyan mennyiségű bejelentéssel halmoznák el a Pénzügyi Hírszerző Egységet, mellyel teljesen ellehetetlenítenék a munkáját. Ezért a hatóság elfogadja, de nem teszi kötelezővé, ha a pénzintézet munkatársai az észlelések megküldése előtt elemzik azok jogosságát. Ezt figyelembe véve, a magyar gyakorlatban az ügyintézői bejelentések kezelésének három típusát különböztetem meg. Egyrészt vannak olyan bankok, melyeknél a pénzmosás elleni osztály a biztonság elvét szem előtt tartva minden beérkezett bejelentést mérlegelés nélkül küld tovább. A legtöbb bank esetében azonban annak ellenére, hogy nem tartozik valós feladatkörükbe a kapott jelentések vizsgálata, mégis egy bizonyos fokú elemző-értékelő munkát végrehajtanak. Ekkor a gyanúsnak talált tranzakcióhoz kapcsolódóan az AML csoport szakértői nyomon követik a pénz útját, vizsgálják a pénzmozgásban érintett partnereket, valamint értelmezik az ügylet hátterét. A folyamat során a bank által létrehozott ügyfélprofil mellett a jogszabályok szerint rendelkezésre bocsátott adatbázisokat, egyéb nyilvántartásokat, valamint külső forrásból beszerezhető információkat is felhasználnak. Az esetek feldolgozása után a valóban gyanúsnak talált ügyleteket haladéktalanul jelentik, míg ellenkező esetben pénzintézeti gyakorlattól függően újabb két lehetőség áll fenn. Vannak olyan szolgáltatók, akik a bejelentést visszaküldik az észlelő személy felé további átgondolásra. Ilyenkor az ügyintéző a gyanú igazolására további adatokkal és információkkal egészítheti ki jelentését, vagy akár vissza is vonhatja azt. Ha utóbbit nem teszi, a Kijelölt személy mérlegelés nélkül továbbítja a dokumentumot. A másik módszer, melyet a pénzügyi intézmények alkalmaznak, hogy az elemző-értékelő munka eredménye alapján a téves riasztásokat irattárba helyezik, míg a valóban gyanúsnak vélt eseteket a hatóság felé továbbküldik. Bár ebben az esetben a büntetőjogi felelősségre vonás kockázata nagyobb, mint az imént bemutatott módszereknél, azonban az AML Officer csakis olyan ügylet jelentését utasítja el, melynek legális voltában maradéktalanul biztos.

A bejelentések másik forrásának a szűrő és tranzakció-figyelő rendszerek AML és WLM modulja által észlelt esetek tekinthetőek. Mivel az automatizált szűrés előre beállított paraméterek, illetve listák megadásával történik, ezért az ilyen riasztások hatóság felé történő továbbítását minden esetben meg kell előznie egy elemző-értékelő munkának. Ezért a programot felügyelő és kezelő analistáknak a rendelkezésre álló adatbázisok és egyéb források alapján vizsgálatot kell végezniük a találat jogosságát illetően.

- *AML modul:* Ha a pénzmosás megelőzési csoport szakértője úgy ítéli meg, hogy az adott ügylet

[30] A VIBER átutalások kivételt képeznek, ugyanis ezeket a riasztás ellenére késlekedés nélkül teljesíteni kell.

pénzmosás szempontjából valóban gyanúsnak tekinthető, akkor az esettel kapcsolatban bejelentési javaslattal kell élnie a Kijelölt személy felé. Ellenkező esetben a program találatát tévesnek minősíti.

- *WLM modul:* Ha a szakterület munkatársának véleménye szerint, a riasztást generáló személy, illetve szervezet nagy valószínűséggel megegyezik a terrorista-, illetve egyéb szankciós és embargós listákon szereplő személyek, illetve szervezetek egyikével, abban az esetben haladéktalanul értesítenie kell erről az AML Officer-t és a gyanúról bejelentést kell készítenie. Ilyenkor a Kijelölt személy kötelezettsége, hogy a hatóságot azonnali hatállyal tájékoztassa és a PEII válaszáig – maximum 24/48 órán keresztül – fenntartsa a tranzakció felfüggesztését. Ha a Pénzügyi Hírszerző Egység vizsgálata megállapítja, hogy a bejelentett személy megegyezik a korlátozó intézkedések alanyával, akkor a szolgáltatónak kötelessége a megbízás végrehajtását elutasítani. Ellenkező esetben, vagyis ha a hatóság, illetve már az AML csoport szakértője is téves riasztásnak értékeli a találatot, akkor a felfüggesztést fel kell oldani és a normális eljárási menet szerint teljesíteni kell a megbízást.

A lefolytatott vizsgálatokat követően gyanúsnak talált esetekről ezután bejelentés készül, melyet 2008. december 15-től minden szolgáltatónak az ABeV PMT08 számú kitöltő program segítségével kell elkészíteni. A hatósági vizsgálat megkönnyítése érdekében a bejelentéseket egységes séma alapján kell megtenni. Eszerint az űrlapoknak tartalmazniuk kell a bejelentő szolgáltatónak, illetve az észlelő szervezeti egységnek általános adatait, az ügyfélről átvilágítása során rögzített információkat, valamint a pénzmosásra vagy terrorizmus finanszírozására utaló adat, tény, körülmény megadását, illetve a hozzá kapcsolódó tényállás leírását. Emellett a bankok, ha szükségesnek találják, lehetőségük van további mellékletek nyomtatványhoz csatolására is. Az így elkészült nyomtatványokat egy végső kontrollt követően a Kijelölt személy ügyfélkapun keresztül, védelemmel ellátott elektronikus üzenet formájában küldi el a hatósági szerv részére. A beérkezett bejelentéseket a Pénzmosás Elleni Információs Iroda munkatársai a munkafolyamat megkönnyítése érdekében a belső adatbázisába rögzítik, majd ellenőrzésüket követően, a vizsgálat eredményének függvényében járnak el.

Bár az ABeV keretprogram bevezetésekor a hatóság törekedett egy igazán hatékony és könnyen használható elektronikus bejelentő rendszert kialakítani, mégis a megoldással kapcsolatban számos kritika fogalmazható meg. Egyrészt a bevezetett szoftver közel sem tekinthető felhasználóbarátnak. Ugyanis amellett, hogy az alkalmazás telepítésekor és üzemeltetésekor gyakran merülnek fel technikai problémák, a kitöltésével járó adminisztrációs feladatok is sokszor túl sok időt igényelnek. A bejelentési folyamat további bírálataként hoznám fel, hogy mivel az elektronikus üzenetek eljuttatása személyi és nem szervezeti szinten történik meg, ezért a művelet jelentős biztonsági kockázatokat rejt magában.

Ezért szakmai körökben egyre többet hallani az ENSZ Kábítószer-ellenőrzési és Bűnmegelőzési Hivatala által külön a FIU-k[31] számára kifejlesztett integrált szoftvermegoldásának, a goAML-nek bevezetéséről. A program átvétele ugyanis a jelenleg használt alkalmazás kapcsán felmerülő problémák nagy részét orvosolná. Az új technológia segítségével létre lehetne hozni egy olyan teljesen biztonságos, mégis igen egyszerűen kezelhető online felületet, melyen a bejelentéseket meg lehetne tenni. Ezzel egyrészt el lehetne kerülni az ABeV telepítésével és működtetésével járó kellemetlenségeket, másrészt az adminisztráció is csökkenne. Továbbá az AML Officer védettségét fokozná, hogy az űrlapokat a szolgáltató, mint jogi személy küldené el a hatóság felé. Végül megjegyezném, hogy nem csak a pénzügyi intézmények, hanem a PEII munkatársainak munkáját is jelentősen egyszerűsíteni. Hiszen egy olyan integrált rendszer jöhetne létre, mely segít az adatok és információk összegyűjtésében, vizsgálatában, jelentésében, illetve ezek menedzselésében. A távlati jövőben pedig ebből egy olyan nemzetközi hálózat is létrejöhetne, mely növelné a különböző országok Pénzügyi Hírszerző Egységeinek összekötöttségét, javítva ezzel a köztük lévő információáramlást.[32]

Ezek alapján egyértelmű, hogy a goAML bevezetése mind szolgáltatói, mind pedig hatósági oldalon, a küzdelem során folytatott munka hatékonyságának jelentős növekedését segítené elő, azonban a hálózat átvételével és kiépítésével járó igen magas költségek miatt feltehetően ez majd csak a hosszabb távon valósulhat meg.

5. Egyéb feladatok

Bár a pénzmosás megelőzési osztály erőforrásainak legnagyobb hányadát minden bank esetében a már bemutatott pénzmosás és terrorizmus finanszírozása gyanús esetek, valamint egyéb szankciós és korlátozó listán szereplő egyének tranzakcióinak kiszűrése, elemzése és bejelentése köti le, azonban ezek mellett a csoport munkatársainak számos egyéb feladatot is el kell látniuk.

5.1. Hatósági kapcsolattartás

A Kijelölt személy feladatai közé tartozik, hogy a Pénzmosás Elleni Információs Irodával állandó jelleggel tartsa a kapcsolatot. Ugyanis a hatósági szerepkört

[31] Financial Intelligence Unit (Pénzügyi Hírszerző Egység)

[32] IMoLIN: goAML – UNODC's Software for Financial Intelligence Units. Letöltve: IMoLIN hivatalos oldala, http://www.imolin.org/imolin/en/goAML-goCASE.html#goaml, 2012.03.10.

betöltő egység munkatársai a beérkezett gyanús bejelentések elemzése során felmerülő adatszükség esetén, információ kiegészítés iránti megkereséssel élhetnek a pénzintézet felé. Ezt a szolgáltató abban az esetben sem tagadhatja meg, ha a kikért adat bank-, értékpapír-, vagy üzleti titkot tartalmaz. Vagyis a FIU felé történő adattovábbítás alkalmával ki kell adni minden olyan, a bejelentett ügyfelekhez, számlákhoz, valamint a bejelentésben nem szereplő, szerződéses kapcsolatokhoz és tranzakciókhoz tartozó információkat, melyek elősegíthetik a hatóság vizsgálatát. A PEII megkeresés három esetben történhet meg. Egyrészt a bejelentést beküldő szolgáltatótól pontosítását, vagy részletezést kér a beérkezett adattal, ténnyel, körülménnyel kapcsolatban, másrészt, ha az adott pénzintézet egy másik szolgáltató bejelentésében megjelent és erre vonatkozó plusz információt igényel. A harmadik esetben további adatok igénylését a külföldi FIU megkeresése teszi szükségessé.[33]

5.2. Magas kockázatú ügyfelek kezelése

Korábban már részletesen kifejtettem, hogy a bankok kockázatérzékenységi alapon értékelik, majd kategorizálják ügyfeleiket. Azokkal a személyekkel, illetve szervezetekkel szemben, akik ez alapján magas kockázati besorolásba kerülnek, szigorúbb biztonsági intézkedéseket foganatosítanak. Egyrészt az ilyen típusú ügyfelek esetében az üzleti kapcsolat létesítéséhez a Kijelölt személy engedélyére is szükség van. Ezen felül a velük fenntartott szerződéses jogviszony alatt pénzügyi tevékenységeik nagyobb figyelmet kapnak, tranzakcióikat gyakrabban ellenőrzik. Ha ezek során az AML csoport szakértői úgy találják, hogy az adott ügyféllel fennálló kapcsolat túl nagy kockázatot rejt magában a bank számára, üzletpolitikai okokra hivatkozva elrendelhetik számláinak zárását.

5.3. Levelezőbanki kapcsolatok kezelése

A fokozott ügyfél-átvilágításnál korábban már említett levelezőbanki szolgáltatással kapcsolatban a pénzmosás megelőzési szakterület munkatársainak több feladatot is el kell látniuk. A Kijelölt személy feladatát képezi, hogy levelezőbanki megkeresés esetén kitöltse a pénzintézet megbízhatóságára vonatkozó kérdőíveket, valamint partnerei számára tájékoztatást adjon a vonatkozó magyar pénzmosás és terrorizmus finanszírozása elleni előírásokról. Emellett a nemzetközi gyakorlatnak megfelelően a szolgáltató honlapján közzéteszi a kitöltött Patriot Act Certification-t. Továbbá az AML csoport feladata, hogy levelezőbanki kapcsolat létesítése előtt, vagy azt követően legalább háromévente felülvizsgálja partnerei megbízhatóságát, valamint pénzmosás és terrorizmus finanszírozása elleni tevékenységét. Ehhez elsősorban a nemzetközi küzdelem meghatározó képviselője, a Wolfsberg csoport által kibocsátott kérdőívet használják fel.

5.4. Nyilvántartási kötelezettség

A pénzintézet pénzmosás elleni csoportjának mindennapi tevékenysége mellett adminisztrációs feladatokat is el kell látnia. A hatályos Pmt. rendelkezése szerint a szolgáltatót nyilvántartási kötelezettség terheli. Ennek értelmében az ügyfél-átvilágítás alkalmával rögzített adatokról, azok valóságtartalmát igazoló okiratokról és másolatukról, a FIU felé tett bejelentésekről, illetve megkeresésük alapján nyújtott adattovábbításról, az ügyleti megbízások felfüggesztését igazoló iratokról, vagy azok másolatáról, valamint a hárommillió-hatszázezer forint összeget elérő, vagy meghaladó készpénzes tranzakciókról nyilvántartást kell vezetnie és az adatrögzítéstől, illetve bejelentéstől számított 8 évig meg kell őriznie. Mivel ezek az információk a banktitok részét képezik, ezért a pénzintézetnek az adatok kezelését és tárolását úgy kell megoldani, hogy azokhoz egyrészt illetéktelen személyek véletlenül sem férhessenek hozzá, másrészt szükség esetén visszakereshetőek legyenek, esetleges módosítások esetén pedig a régi adatokat is egyértelműen ki lehessen olvasni belőlük.

5.5. Statisztikai adatszolgáltatási kötelezettség

Az adminisztrációs feladatok másik csoportját a 45/2008. PM rendeletben, a hitelintézetek számára előírt adatszolgáltatási kötelezettség alkotja. Eszerint a szolgáltatóknak a felügyeletüket ellátó PSZÁF felé statisztikai jelentést kell tenniük, melynek 9D fejezetét a pénzmosással és terrorizmus finanszírozásával kapcsolatos adatok képezik. A negyedéves bejelentéssel a szabályozó célja, hogy megfelelő ismeretek birtokában fel tudja mérni a Pmt. végrehajtásának hatásait.[34]

5.6. Belső szabályzat készítése

A pénzintézet pénzmosás és terrorizmus finanszírozása elleni hatékony fellépésének érdekében az AML Officer-nek belső szabályzatot kell készíteni. Ennek elkészítéséhez a PSZÁF mintaszabályzatot bocsát ki, azonban a szolgáltató belső szabályzatának kötelező elemeit nem ez, hanem a 35/2007. (XII. 29.) PM rendelet határozza meg. Ebből adódóan, bár a bankok

[33] Papp Zsófia – Ujváriné Fejes Renáta – Simonka Gábor (2008): A pénzmosás és terrorizmus finanszírozása megelőzéseiről és megakadályozásáról szóló új törvény. Pénzügyi Szemle. 53. évf. 2. szám. 293–316. o.

[34] Pénzügyi Szervezetek Állami Felügyelete (2010): A Pénzügyi Szervezetek Állami Felügyeletének 1/2010. számú módszertani útmutatója a hitelintézetek adatszolgáltatási kötelezettségéről szóló, a 42/2009. PM rendelettel módosított 45/2008. PM rendeletben előírt felügyeleti jelentések elkészítéséhez. Letöltve: PSZÁF, http://www.pszaf.hu/data/cms2104442/modszertani_utmutato_hitelint_20100521_weblapra.pdf, 2012.03.10.

kapnak egy egységes útmutatást, azonban a belső szabályzatok, főbb tartalmi elemeiket leszámítva eltérhetnek egymástól. Ez egyrészt függ a szolgáltatók pénzmosás megelőzési és megakadályozási gyakorlatának eltéréseitől, másrészt pedig a Kijelölt személytől. Általánosságban a szabályzatok a Pmt. fontosabb rendelkezéseit, az azokhoz tartozó feladatok és belső eljárásrendek részletes ismertetését, a szükséges nyomtatványokat, valamint egyéb, az alkalmazottak eredményes munkáját elősegítő javaslatokat és dokumentumokat tartalmaznak.

5.7. Oktatási kötelezettség

Ugyancsak a bűncselekmény elleni hatékony fellépést szolgálja a bankok részére előírt oktatási kötelezettség. Ugyanis a képzési programokon való részvétel alkalmával, a pénzintézet érintett alkalmazottai[35] részére bemutatásra kerülnek a pénzmosás és terrorizmus finanszírozása megelőzésére és megakadályozására vonatkozó szabályozás, illetve a Büntető Törvénykönyv erre vonatkozó részeinek alapvető rendelkezései, a tanfolyam résztvevői megismerik az illegális tevékenységekhez köthető gyanús esetköröket, valamint elsajátítják a törvényből adódó kötelezettségek teljesítésének belső eljárás rendjét. Emellett az eredményes fellépés érdekében a pénzmosási törvénnyel szoros kapcsolatban álló, az Európai Unió által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvény is ismertetésre kerül. A tréningeket elvégzésük időpontja alapján két csoportba lehet sorolni. Egyrészt a belépő munkatársaknak, a munkaviszony létrejöttét követő 30 napon belül kötelező jelleggel részt kell venniük rajtuk, másrészt minden új, illetve régi alkalmazottnak legalább éves szinten részesülni kell pénzmosás elleni képzésben. Utóbbit további két részre oszthatom fel. Napjaink technikai fejlettsége mellett a pénzintézetek dolgozóinak általános e-learning, másfelől pedig terület specifikus tananyagot is el kell sajátítaniuk. Az oktatással kapcsolatban érdemesnek tartom még megjegyezni, hogy azt a szolgáltatók szervezeti kereteiken belül saját, illetve külső szakértők által kidolgozott tananyag felhasználásával, valamint külön erre specializálódott cégek segítségével is lebonyolíthatják. Azonban fontos, hogy bármelyik megoldást is választják a felelősséget minden esetben az AML Officer viseli.

Természetesen az eddig felsorolt kötelezettségek mellett a pénzintézet gyakorlatától, illetve compliance kultúrájának fejlettségétől függően egyéb feladatokat is elláthat. A legtöbb nagyobb bank esetében a pénzmosás megelőzési csoport tanácsadói és véleményezési funkciókat is ellát, melyek elsődlegesen nem a szabályozásnak való megfelelést, hanem inkább a várható veszteségek minimalizálásán keresztül a menedzseri értékteremtést szolgálják.

[35] Azok a banki alkalmazottak, akik a pénzügyi szolgáltató üzletszerű tevékenysége alkalmával kapcsolatba kerülnek az ügyfelekkel.

6. Záró gondolatok

Az elmúlt közel két évtizedben a hazai pénzmosás elleni küzdelem jelentős fejlődésen ment keresztül, melynek eredményeként mára a nemzetközi elvárásoknak is megfelelő szabályozási rendszer jött létre. Bár a pénzmosás és terrorizmus finanszírozása elleni törvény a személyi hatálya alá tartozók számára általános érvényű kötelezettségeket ír elő és ezen elvárásoknak a szolgáltatók kivétel nélkül igyekeznek is megfelelni, ennek ellenére mégsem lehet kijelenteni, hogy Magyarországon egy egységes pénzintézeti gyakorlat alakult volna ki. Véleményem szerint az eltérések elsősorban a bankok tulajdonosi hátterére, az anyaország pénzügyi kultúrájára, az intézmények tőkeerősségére, piaci részesedésére, ügyfélkörének méretére, illetve minőségére, valamint a pénzmosás elleni részleg bankon belüli presztízsére, alkalmazottainak képzettségére, szaktudására és tapasztalatára vezethetőek vissza. Kutatásom szerint az egyik legmarkánsabb különbség a szolgáltatók által alkalmazott informatikai rendszerekben, valamint az egyes ellátandó feladatokat szoftveres támogatásában fedezhető fel. Láthattuk, hogy a pénzintézetek által használt kockázatértékelő, illetve szűrő és tranzakció-figyelő programok, valamint az ügyintézői bejelentések elküldésének módszerei között gyakran igen jelentős különbségek mutatkoznak. Ugyanis a külső cégek által kínált fejlett rendszerek beszerzése és működtetése hatalmas összegekbe kerül, melyre több szolgáltatónál nincs meg a szükséges keret. Így sok esetben inkább az olcsóbb, de olykor kevésbé hatékony, saját fejlesztésű alkalmazásokkal látják el feladataikat. Emellett további különbségek fedezhetőek fel a jogszabályi kötelezettségek, illetve felügyeleti ajánlások belső eljárásrendbe történő implementálásában, annak gyakorlati megvalósulásában.

Bár az eltérések olykor jelentősek és még a fejlettebb rendszerekkel rendelkező pénzintézeteknek is van hová fejlődniük, ennek ellenére kijelenthető, hogy a szabályozók, illetve a szolgáltatók által meghatározott irány jónak tekinthető. Ha utóbbiak számára rendelkezésre állnak majd a megfelelő erőforrások, akkor az idő előre haladtával a banki AML tevékenység – megfelelő hatósági támogatás mellett – valóban a pénzmosás és terrorizmus finanszírozása elleni fellépés leghatékonyabb eszköze lehet. Az ehhez vezető út azonban még nagyon hosszú és a bűncselekmény fejlődését jellemző dinamizmusból kiindulva talán sosem ér véget.

Irodalomjegyzék[36]

1. FATF (2012): International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – the FATF Recommendations. Letöltve: FATF hivatalos oldala, http://www.fatf-gafi.org/topics/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html, 2012.05.25.
2. *Gál István László* (2009): *Bejelentés vagy feljelentés? A pénzmosással és a terrorizmus finanszírozása elleni küzdelemmel kapcsolatos feladatok és kötelezettségek.* Budapest: Penta Unió Kft.
3. IMoLIN: goAML – UNODC's Software for Financial Intelligence Units. Letöltve: IMoLIN hivatalos oldala, http://www.imolin.org/imolin/en/goAMLgoCASE.html#goaml, 2012.03.10.
4. *Jacsó Judit* (2000): *A pénzmosás elleni nemzetközi fellépés eszközei.* Magyar Jog. 47. évf. 9. szám. 545–556. o.
5. KPMG (2011): Global Anti-Money Laundering Survey. How banks are facing up to the challenge. Letöltve: KPMG hivatalos oldala, http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/anti-money-laundering.pdf, 2012.03.10.
6. *Papp Zsófia – Ujváriné Fejes Renáta – Simonka Gábor* (2008): *A pénzmosás és terrorizmus finanszírozása megelőzéseiről és megakadályozásáról szóló új törvény.* Pénzügyi Szemle. 53. évf. 2. szám. 293–316. o.
7. Pénzügyi Szervezetek Állami Felügyelete (2010): A Pénzügyi Szervezetek Állami Felügyeletének 1/2010. számú módszertani útmutatója a hitelintézetek adatszolgáltatási kötelezettségéről szóló, a 42/2009. PM rendelettel módosított 45/2008. PM rendeletben előírt felügyeleti jelentések elkészítéséhez. Letöltve: PSZÁF, http://www.pszaf.hu/data/cms2104442/modszertani_utmutato_hitelint_20100521_weblapra.pdf, 2012.03.10.
8. Pénzügyi Szervezetek Állami Felügyelete (2008): A PSZÁF Felügyeleti Tanácsának 3/2008. (XI. 20.) számú ajánlása a pénzmosás és a terrorizmus megelőzéséről és megakadályozásáról. Letöltve: PSZÁF, http://www.pszaf.hu/bal_menu/szabalyozo_eszkozok/pszafhu_bt_ajanlirelvutmut/ajanlas_ft/pszaf_ajanlas_3_2008.html, 2012.03.10.
9. Pénzügyi Szervezetek Állami Felügyelete (2004): 1/2004. évi ajánlás a terrorizmus finanszírozása és a pénzmosás megelőzéséről és megakadályozásáról. Letöltve: PSZÁF, http://www.pszaf.hu/intezmenyeknek/biztositok/szabalyozo_eszkozok/ajanlasok/pszafhu_penzmosastrv_20050729_1.html, 2012.03.10.
10. *Peter Lilley* (2001): *Piszkos ügyletek. A pénzmosás világa.* Budapest: Perfekt Gazdasági Tanácsadó, Oktató és Kiadó Rt.
11. *Rohan Bedi* (2006): *Anti-Money Laundering Risk Models.* Letöltve: Rohan Bedi hivatalos oldala, http://www.rohanbedi.com/AML-RiskModels.pdf, 2012.03.10.
12. *Steiner Péter* (2006): *Paradigmaváltás a pénzmosás elleni küzdelemben: Globális rendszer a bűnözés ellen.* Pénzügyi Szemle. 51. évf. 3. szám. 320–335. o.
13. *Tóth Mihály* (2002): *Gazdasági bűnözés és bűncselekmények.* Budapest: KJK-KERSZÖV Jogi és Üzleti Kiadó
14. 1996. évi CXII. törvény a hitelintézetekről és pénzügyi vállalkozásokról
15. 2007. évi CLXXX. törvény az Európai Unió által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról, valamint ehhez kapcsolódóan egyes törvények módosításáról
16. 2007. évi CXXXVI. törvény a pénzmosás és terrorizmus finanszírozása megelőzéséről és megakadályozásáról ■

[36] A banki és üzleti titok védelmét szem előtt tartva, a belső források, valamint a mélyinterjúk során rendelkezésemre bocsátott belső szabályzatok részletes ismertetésétől el kell hogy tekintsek.