Boóc Ádám*

Az online banki csalások egyes magánjogi felelősségi kérdései

1. Bevezetés

A digitális pénzügyi szolgáltatások robbanásszerű fejlődése az elmúlt másfél évtizedben új dimenziókat nyitott meg a lakossági és vállalati bankhasználatban. Ezzel párhuzamosan azonban az online pénzügyi térben tapasztalható visszaélések száma is aggasztó mértékben emelkedett. A Magyar Nemzeti Bank (MNB) adatai szerint 2023-ban összesen körülbelül 23 milliárd forintnyi kár keletkezett online banki csalások következtében, míg 2024 első három negyedévében ez az összeg már elérte a 33,6 milliárd forintot.[1] A számok mögött gyakran súlyos magánéleti és vállalkozási krízisek állnak: a csalók módszerei egyre kifinomultabbá és célzottabbá válnak, miközben az ügyfelek pénzügyi tudatossága nem minden esetben követi ezt a tempót.[2]

A tanulmány célja az online banki csalások felelősségi kérdéseinek átfogó vizsgálata a magyar polgári jog, a pénzforgalmi szabályozás, valamint az új, 2024-ben elfogadott törvényi rendelkezések tükrében. Külön figyelmet fordítunk az MNB által indított „Öt csapás" elnevezésű intézkedéscsomagra, amely a digitális pénzügyi tér fokozott védelmét szolgálja. A tanulmány a gyakorlati tapasztalatok bemutatása mellett jogdogmatikai alapokra építkezve keresi a választ arra a kérdésre, hogy milyen esetekben és milyen mértékben tartozik felelősséggel az ügyfél, illetve a pénzforgalmi szolgáltató az online csalásokból eredő károkért.

* *Dr. Boóc Ádám, intézetvezető egyetemi tanár, Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar, Budapest*

[1] Lásd: Magyar Nemzeti Bank: *Digitális pénzügyi kockázatok – 2023. évi összefoglaló jelentés*, MNB, 2024. január. Elérhető: https://www.mnb.hu

[2] Az Európai Központi Bank 2023-as jelentése szerint a SEPA-övezetben az online csalások okozta veszteség 1,2 milliárd euróra nőtt, főként APP (*Authorised Push Payment*) típusú támadások miatt. Lásd ECB – *Card Fraud Report*, 2023 https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr240801~f21cc4a009.en.html

2. Az online banki csalások tipológiája és fejlődése

Az online banki csalások nem újkeletű jelenségek, ám módszertani sokszínűségük és adaptív természetük miatt az elmúlt években kiemelt figyelmet kaptak mind a hatóságok, mind a szabályozó szervek részéről. A korábbi klasszikus adathalász e-mailek helyét ma már sokkal célzottabb és szofisztikáltabb támadások veszik át, amelyek nem ritkán több csatornát is egyidejűleg használnak az ügyfelek megtévesztésére.[3]

A főbb csalástípusok a következők:

a) Phishing – klasszikus e-mailes adathalászat

A „*phishing*" (az angol *fishing* – horgászat szóból) olyan megtévesztésen alapuló kiberbűnözési forma, amelynek célja, hogy a felhasználót rávegye banki hitelesítési adatainak (pl. felhasználónév, jelszó, SMS-kód) önkéntes megadására. A csaló hitelesnek tűnő e-mailt küld az ügyfélnek (pl. „biztonsági ellenőrzés", „frissítés szükséges" tárggyal). A levél egy **hamis weboldalra** irányítja a felhasználót, amely szinte teljesen megegyezik a bank valódi oldalával.

Példa e módszerre: Egy OTP-re hasonlító e-mail arról tájékoztatja az ügyfelet, hogy „felfüggesztették a fiókját", és az újraaktiváláshoz kattintson egy linkre. A link egy hamis weboldalra visz, ahol a gyanútlan ügyfél megadja az összes belépési adatát. Ez a forma ma már gyakran többcsatornás támadással kombinálódik *(smishing*, *vishing*).[4]

b) Vishing – telefonos megtévesztés

A „*vishing*" (*voice phishing*) során a támadó telefonon keresztül próbálja megszerezni az ügyfél bizalmas banki adatait, miközben banki ügyintézőnek vagy hatósági személynek (pl. NAV-ellenőr, rendőr) adja ki magát. A támadó az ügyfelet felhívja, és pánikkeltéssel (pl. „gond van a számláján") próbálja rávenni, hogy diktálja be a netbanki jelszót, SMS-

[3] Összefoglaló jelleggel lásd: www.kiberpajzs.hu

[4] A „*phishing*" kifejezést az 1990-es évek közepén kezdték használni először olyan csalásokra, ahol megtévesztéssel próbáltak jelszavakat kicsalni e-mailben. Lásd: T. N. JAGATIC – N. A. JOHNSON – M. JAKOBSSON – F. MENCZER*: Social Phishing.* Communications of the ACM Volume 50, Number 10 (2007), 94-100. o. lásd: https://dl.acm.org/doi/fullHtml/10.1145/1290958.1290968

kódot vagy indítson átutalást.

Példa e módszerre: A csaló közli: „a számláját éppen feltörik, gyorsan át kell utalnunk a pénzét egy biztonságos számlára”. Az ügyfél pánikba esik és önként utalja át a megtakarítását a csalónak. Sok esetben a bank nem téríti vissza a kárt, mivel az ügyfél maga indította el a tranzakciót – még ha megtévesztés hatására is.

c) Smishing – SMS-alapú adathalászat

A „*smishing*” az SMS (*Short Message Service*) és phishing összevonásából származik. A támadó **hamis banki SMS-t** küld, amely egy linket tartalmaz a „probléma megoldására”. A csaló bank nevében SMS-t küld, mely szerint „rendellenes mozgást észleltünk fiókján”. A mellékelt linkre kattintva egy hamis netbank oldalra jut az ügyfél, ahol megadja adatait.

Példa e módszerre: A csaló által küldött SMS: „Erste Bank: Gyanús bejelentkezést észleltünk. Ellenőrizze most: https://erste-biztonsag.net”. Egyre gyakoribb, hogy a csalók valódi SMS-szálakba is „beépülnek” úgy, hogy a hamis üzenet ugyanabban az üzenetláncban jelenik meg, mint a bank valódi üzenetei – ez spoofinggal kombinálódhat.

d) Spoofing – hívószám-hamisítás

A „*spoofing*” során a csaló megtévesztő módon **a bank hivatalos telefonszámát tünteti fel** a hívás során, így az ügyfél azt hiszi, hogy a bank hívja. A támadó speciális technológiát használ, amely lehetővé teszi, hogy az ügyfél kijelzőjén a bank valódi számát lássa. Így a hívás hitelesnek tűnik, az ügyfél pedig könnyebben bedől a kéréseknek.

Példa e módszerre: Az ügyfél mobilján a „+36 1 366 6666 OTP Bank” jelenik meg. A hívó azt mondja: „idegen országban történt bejelentkezés, gyorsan szükség van hitelesítő kódra.” A bank gyakran nem tekinti ezt technikai hibának, mivel az ügyfél jóváhagyta a tranzakciót.

e) Evil Twin Phishing – hamis Wi-Fi hálózat

Ez a módszer egy **nyilvános Wi-Fi hálózat** megtévesztő másolatán alapul, amelybe a felhasználó önként kapcsolódik, és így a támadó minden adatforgalmat láthat. A csaló olyan Wi-Fi hálózatot állít be, amely nevét és kinézetét tekintve hasonlít egy ismert hálózatra (pl.

„Starbucks_WiFi" helyett „Starbuks_WiFi"). A kapcsolódás után minden adat, amit az ügyfél beír (jelszó, banki hitelesítés), a támadóhoz kerül.

Példa e módszerre: Egy repülőtéren az ügyfél automatikusan csatlakozik a „Free Airport WiFi" néven futó hálózatra, de az valójában a csaló által létrehozott másolat.

f) Nigériai típusú csalás – érzelmi manipuláció

Ez a klasszikus „*advance-fee scam*" (előrefizetéses csalás), amely során a csaló érzelmekre vagy erkölcsi kötelességre ható történettel pénzt próbál kicsalni. A csaló e-mailben vagy üzenetben keres meg: beteg gyermeket ápol, örökséghez jutna, de szüksége van „adminisztrációs díjra". Gyakran külföldi, egzotikus történet kíséri a kérelmet.

Példa e módszerre: „Drága barátom! Segítsen eljuttatni 10 millió dollárt Magyarországra, 10% jutalékot kínálok. Előre szükségem lenne 3000 euró ügyvédi költségre." Ez a forma mára átalakult: szerelmi csalások, „hamis katona" vagy „gyermekét egyedül nevelő nő" típusú történetek formájában jelenik meg.

g) Hamis befektetési lehetőségek

A csalók nemlétező vagy manipulált pénzügyi termékeket kínálnak, gyakran gyors meggazdagodást ígérve. A „befektetési tanácsadó" megkeresi az ügyfelet (telefonon, e-mailben, közösségi médián), és „exkluzív lehetőséget" ajánl. Gyakoriak a kriptovaluták, forex kereskedés, startup befektetések.

Példa e módszerre: „Most csatlakozhat egy új *blockchain* technológiát alkalmazó céghez, amely a következő évek Tesla-ja lesz!" Az ügyfél pénzt utal át, de sosem látja viszont.

h) Spear phishing – célzott adathalászat

Ez a „klasszikus" *phishing* célzott, személyre szabott változata. A támadó konkrét személyre, cégre, pozícióra szabott üzenetekkel operál.[5]

[5] A „*spear phishing*" különösen veszélyes, mivel célzott és személyre szabott. A támadók gyakran a LinkedIn, Facebook vagy nyilvános cégadatbázisok alapján építik fel az

A támadó előre begyűjt adatokat a célpontról (pl. közösségi médiából). A célzott üzenet úgy van megszerkesztve, hogy hitelesnek tűnjön – gyakran munkahelyi, pénzügyi vagy hivatalos kommunikációra hivatkozva.

Példa e módszerre: Egy pénzügyi osztályvezető e-mailt kap a „vezérigazgatótól": „Kérlek, utald el az alábbi összeget az új partnernek, sürgős." Az aláírás, a megszólítás, a stílus teljesen hiteles – de hamis.

Egyre gyakoribbak az úgynevezett *multi-vector* támadások, ahol az elkövetők e-mail, telefon, közösségi média és hamis weboldalak kombinációját alkalmazzák a siker érdekében.[6] Ezzel párhuzamosan a bűncselekmények határon átnyúló jellege is felerősödött: a pénz gyakran offshore számlákon, kriptovalutában vagy úgynevezett pénzmosó hálózatokon keresztül tűnik el.

A statisztikai adatok mögött nem pusztán pénzösszegek, hanem egyének és vállalkozások drámái húzódnak meg. Egy tipikus csalás során egy magánszemély akár több havi jövedelmét is elveszítheti – gyakran úgy, hogy semmilyen visszatérítési lehetőség nem áll fenn számára. Az MNB 2024 első negyedéves adatai szerint az átlagos kár egy magánszemély esetében 1,3 millió forint, míg egy vállalkozás esetében 31 millió forint volt.

Az online csalások társadalmi hatása messze túlmutat az egyes ügyeken. A digitális pénzügyi szolgáltatásokba vetett közbizalom csökkenése közvetve hat az elektronikus fizetési rendszerek fejlődésére, a pénzügyi rendszerre, valamint az állampolgári jogtudatosságra. Mindez különösen súlyos következményekkel járhat egy olyan országban, ahol a digitális pénzügyi ökoszisztéma fejlődése még mindig jelentős társadalmi rétegek számára új és bizonytalan terület.

3. A releváns jogszabályi háttér áttekintése

Az online banki csalások kapcsán megállapítható felelősség jogi alapjait Magyarországon elsődlegesen a magyar polgári jog, valamint a pénzforgalommal kapcsolatos ágazati szabályozás határozza meg. Emellett az utóbbi években egyre fontosabbá váltak az uniós pénzügyi irányelvek, különösen a PSD2 (*Payment Services Directive 2*) és a GDPR,

---

átverést. Lásd: Symantec Threat Report, 2022. https://docs.broadcom.com/doc/istr-03-jan-en

[66] A „*multi-vector*" támadások egyszerre több csatornán keresztül zajlanak – pl. *phishing* e-mail*, spoof*olt telefonhívás és hamis weboldal kombinálva. Céljuk a megtévesztés maximalizálása.

valamint a fogyasztóvédelmi előírások.[7]

A magyar magánjogi felelősség legfontosabb szabályait tartalmazó Ptk. (2013. évi V. törvény) több rendelkezése is releváns az online csalások jogi megítélésekor:

- 6:142. § [Szerződésszegéssel okozott kár] – Ha a szerződésszegésből kár keletkezik, a károkozó köteles azt megtéríteni, kivéve ha bizonyítja, hogy a szerződésszegés oka rajta kívül álló, elháríthatatlan körülmény volt.
- 6:518. § [Deliktuális felelősség] – Aki jogellenesen másnak kárt okoz, köteles azt megtéríteni, kivéve, ha bizonyítja, hogy magatartása nem volt felróható.

A polgári jogi felelősség megállapításához – mint ismeretes – négy feltétel együttes fennállása szükséges: jogellenes magatartás, kár, okozati összefüggés és felróhatóság.[8] Ennek a feltételrendszernek a banki online csalások vizsgálata esetén különös jelentősége lehet.

Az online banki csalásoknál a helyzet kettős: A bank felelőssége szerződéses, mivel ő a szolgáltató. A csaló felelőssége deliktuális, de ő számos esetben nem perelhető hatékonyan (ismeretlen, eltűnt, külföldi).

A pénzforgalmi szolgáltatásokról szóló 2009. évi LXXXV. törvény az ügyfél és a pénzforgalmi szolgáltató közötti kapcsolatot különös szabályokkal részletezi. E törvény témánk szempontjából releváns rendelkezései az alábbiak:

- 45. § (1) bekezdés kimondja, hogy a pénzforgalmi szolgáltató nem téríti meg a kárt, ha az ügyfél súlyosan gondatlan vagy csalárd módon járt el.
- 45. § (2) alapján az ügyfél a kárt 15.000 forintig köteles viselni, ha bizonyítottan nem ő volt a hibás.
- 45. § (3) szerint ha a pénzforgalmi szolgáltató nem biztosította a megfelelő biztonsági feltételeket, teljes körű kártérítési kötelezettség terheli.

[7] A GDPR (2016/679/EU rendelet) 32. cikk (1) bekezdése előírja az adatkezelők számára az adatok megfelelő technikai és szervezési védelmét – ez kiterjed az online bankolás során kezelt személyes adatokra is.

[8] A legújabb magyar szakirodalomból lásd különösen: SÁRKÖZY T,: Fordulat a magyar kártérítési jogban. Magyar Jog, 2013/9., 535-542. o.; FUGLINSZKY Á.: Kártérítési jog. Budapest, 2015.; MISKOLCZI BODNÁR P.: A kártérítési felelősség közös szabályainak alkalmazási köre. Jogtudományi Közlöny 2019/2. 53-60. o.; VÉKÁS L.: Szerződésszegési kártérítési felelősség a bírói gyakorlatban. Magyar Jog, 2020/10., 557-566. o.

A 2024. évi XVIII. törvény külön rendelkezik az online visszaélések utáni gyors adattovábbításról a pénzforgalmi szolgáltatók között. [9]

A bírósági eljárások fő kérdése: az ügyfél vagy a bank járt-e el nagyobb gondatlansággal?

A bírói gyakorlat (pl. BH2022.116., BH2023.41.) több esetben a „súlyosan gondatlan" ügyféltől megtagadta a kártérítést, ha nyilvánvalóan hamis linkre kattintott, ismeretlen számlára utalt saját döntés alapján vagy megadta a netbanki azonosítót és SMS-kódot harmadik félnek.

Figyelmet érdemel a Kúria igen friss, a Pfv.I.20.685/2024. számú ügyben hozott döntése.

E döntés értelmében - egy online csalással összefüggő ügyben - megállapításra került, hogy a szándékos vagy súlyosan gondatlan magatartás ugyanis olyan vétkességi kategória, amely a károkozással összefüggésben állít fel mércét egy konkrét személlyel szemben.

A Kúria hangsúlyozta, a súlyos gondatlanságnak nem a szabályszegés, hanem a kár bekövetkezése vonatkozásában kell fennállnia, vagyis a súlyos gondatlanság megállapításához nem elegendő a szabályszegés súlyossága, valamennyi körülményt értékelve az érintett fogyasztó tudattartalmát is vizsgálni kell. Értékelni kell, hogy szubjektíve tisztában volt-e magatartása következményével, számolnia kellett-e a kár bekövetkezésével, vagyis a hátrányos következményekkel kapcsolatban megállapítható-e a fogyasztó nagyfokú közömbössége, felelőtlensége. Mindez nagy eséllyel a joggyakorlat jelentős változását idézheti elő a jövőben.[10]

A vonatkozó pénzügyi jogszabályok szerint a szolgáltató köteles biztosítani az ügyfél adatainak védelmét, technikai és szervezési intézkedéseket alkalmazni, olyan rendszert működtetni, amely képes kiszűrni a gyanús tranzakciókat. Ha ez nem történik meg, a bank objektív felelősséggel tartozik. Azonban, ha az ügyfél átadta az adatait vagy jóváhagyta a tranzakciót, a felelősség átszállhat rá – kivéve, ha bizonyítható, hogy csalás történt (pl. telefonos manipulációval, megtévesztéssel).

A jelenlegi magyar szabályozás nem tartalmaz pontos definíciót a „súlyos gondatlanság" fogalmára – ezt a bírói gyakorlat alakítja ki eseti alapon. A bírói gyakorlat értelmezése szerint az „átlagos gondosság" mértéke az online bankhasználat során magasabb, mint általános

[9] A 2024. évi XVIII. törvény 5. §-a külön rendelkezik az adatszolgáltatási határidőkről a pénzforgalmi szolgáltatók között – ezek a csalás észlelése utáni „kritikus első perceket" szabályozzák.

[10] Lásd: https://kuria-birosag.hu/hu/sajto/tajekoztato-kuria-pfvi206852024-szamu-ugyben-hozott-donteserol

jogviszonyokban – különösen, ha az ügyfél már korábban részesült banki oktatásban, figyelmeztetésben.

Fentiek alapján az online banki csalások kapcsán megállapítható felelősség jogi alapjait elsődlegesen a magyar polgári jog, valamint a pénzforgalommal kapcsolatos ágazati szabályozás határozza meg. Emellett az utóbbi években egyre fontosabbá váltak az uniós pénzügyi irányelvek, különösen a PSD2 (*Payment Services Directive 2*) és a GDPR, valamint a fogyasztóvédelmi előírások. Az EU-s PSD2 irányelv alapján a banknak akkor van visszatérítési kötelezettsége, ha a tranzakció nem jóváhagyott, vagy technikai hiba történt. Amennyiben az utalást maga az ügyfél indította el, még ha tévedésből is, a bankot nem terheli felelősség.

4. Rövid nemzetközi kitekintés

Az online banki csalások világszerte jelentős problémát jelentenek, amelyek kezelésére a különböző országok eltérő jogi és intézményi válaszokat dolgoztak ki. Az alábbiakban néhány meghatározó joghatóság szabályozási megközelítését mutatjuk be, különös tekintettel a kártérítési és felelősségi kérdésekre.

Az Egyesült Királyságban az úgynevezett „*Authorised Push Payment*" (APP) csalások kezelésére a szabályozó hatóság, a *Payment Systems Regulator* (PSR) külön visszatérítési modellt vezetett be. A modell célja, hogy az ügyfél ne maradjon teljesen védelem nélkül akkor sem, ha maga indította el a tranzakciót, de ezt megtévesztés hatására tette.

A „*Contingent Reimbursement Model*" (CRM) értelmében a bankok kötelesek visszatérítést biztosítani, amennyiben az ügyfél nem járt el súlyosan gondatlanul, és betartotta a bank által előírt biztonsági intézkedéseket.[11] 2024-től e modell kötelező érvényű lett az Egyesült Királyság legtöbb nagybankja számára. A szabályozás különösen hangsúlyozza a megelőzés, figyelmeztetés és ügyféltámogatás szerepét.

A kontinentális európai országok – így Németország és Franciaország – jogrendszere erőteljesebben támaszkodik a fogyasztóvédelemre és az objektív felelősség elvére. Német bírói gyakorlat például elutasítja azt az érvelést, hogy az ügyfél automatikusan viselje a kockázatot, ha adatot adott meg a csalóknak. A bíróság vizsgálja, hogy a bank nyújtott-

[11] A *Contingent Reimbursement Model* (UK) kifejezetten a lakossági fogyasztók és mikro-vállalkozások védelmét szolgálja, és jelenleg a legtöbb brit bank csatlakozott hozzá önként vagy kötelezően.

e megfelelő figyelmeztetést, és biztosította-e a kellő technikai védelmet. Franciaországban a *Code monétaire et financier* előírja a „*due diligence*" kötelezettséget a bank számára, különösen ismeretlen címzetteknek szóló, nagyösszegű utalások esetén. Ha e kötelezettséget a szolgáltató megszegi, felelőssé válhat akkor is, ha az ügyfél tévedésből indította az utalást.

Hollandiában az *Ombudsman Financiële Dienstverlening* aktív szerepet vállal az online csalások áldozatainak segítésében. Számos esetben javasolt kompromisszumot a bank és az ügyfél között, még akkor is, ha jogilag a felelősség nem volt egyértelműen megállapítható. Ez a gyakorlat a prevenció mellett a pénzügyi bizalom fenntartását is szolgálja.

Az Egyesült Államokban a FinCEN irányelvei mentén a pénzintézetek saját csalásmegelőző mechanizmusokat alkalmaznak, de nincs egységes kártérítési szabályozás. A hangsúly a *real-time fraud detection* rendszerek fejlesztésén van, valamint a közösségi média platformokkal való együttműködésen.

Szingapúrban a *Monetary Authority of Singapore* (MAS) elvárja a bankoktól, hogy AI-alapú csalásdetektáló algoritmusokat vezessenek be, amelyek viselkedésalapú elemzést is alkalmaznak. A gyanús tranzakciókat azonnali riasztás és felfüggesztés követheti. Emellett a „*kill-switch*" funkció lehetőséget ad arra, hogy az ügyfél azonnal zárolja számláját, ha úgy véli, támadás alatt áll.[12]

5. A Magyar Nemzeti Bank Öt csapás elnevezésű intézkedés-csomagja

A digitális pénzügyi tranzakciók térnyerése nemcsak kényelmet, hanem új kockázatokat is magával hozott. A banki átutalásokkal kapcsolatos csalások – különösen az úgynevezett „technikai támadással" vagy „megtévesztéssel" kiváltott, jogilag vitatott utalások – napjaink egyik legkomolyabb kihívásává váltak a kiberbiztonság és a polgári jog határterületén.

A Magyar Nemzeti Bank Öt Csapás elnevezésű intézkedés

[12] Az úgynevezett „*kill-switch*" funkció Szingapúrban már 2022 óta elérhető, lehetővé téve, hogy az ügyfél egy gyanús esemény esetén teljes körűen zárolja a számláját akár mobilon keresztül. Lásd: MAS Singapore – *Fraud Management Framework*, 2022. https://www.mas.gov.sg/regulation/regulations-and-guidance?topics=Risk%20Management%2FFraud%20Risk

csomagjának a lényege az alábbiak szerint foglalható össze.[13] Az **öt „csapás”** öt különböző, de egymással szorosan összefüggő intézkedési területet jelent. Ezek a következők:

1. **Gyanús utalások azonnali zárolása**
2. **Kockázatos utalások figyelmeztetése**
3. **Kockázatos számlák feketelistázása**
4. **Erős ügyfélhitelesítés alkalmazása**
5. **Pénzforgalmi szolgáltatók közötti gyors adattovábbítás**

A még nem kialakult gyakorlat nyilvánvaló hiányában a fentiekkel kapcsolatos észrevételeket az alábbiak szerint foglaljuk össze.

***Ad 1.*: Gyanús utalások azonnali zárolása -** Ennek célja gátat szabni a csalók által indított vagy kicsalt átutalásoknak. Az intézkedés lényege, hogy a bankok kötelesek automatikusan felfüggeszteni a gyanús tranzakciókat, amíg azokat nem ellenőrzik. A gyakorlatban ez percek alatt megelőzheti, hogy a pénz „eltűnjön” offshore vagy kriptoszámlákon keresztül.

***Ad 2.*: Kockázatos utalások figyelmeztetése -** Ennek célja tudatosítani az ügyfelekben, ha veszélyes tranzakciót készülnek végrehajtani. A bank köteles vizuális és szöveges figyelmeztetést küldeni a felhasználónak gyanús vagy szokatlan tranzakció esetén. Példaként utalhatunk arra, ha az ügyfél először utal nagy összeget egy új számlaszámra, felugró üzenet figyelmeztet: *„Figyelem! Győződjön meg róla, hogy nem csalás áldozata!”*

***Ad 3.*: Kockázatos számlák feketelistázása -** Ennek célja megakadályozni, hogy a csalók többször is visszaéljenek ugyanazzal a számlaszámmal. A bankoknak meg kell osztaniuk egymással a csalással összefüggésbe hozható számlaszámokat, melynek eredményeképpen egy ügyféltől pénzt kicsaló számlaszám néhány órán belül „letiltásra kerül” a többi pénzintézetnél is.

***Ad 4.*: Erős ügyfélhitelesítés alkalmazása -** Ennek célja csökkenteni az azonosítási adatokkal való visszaélések lehetőségét. Az intézkedés lényege szeri A bankok kötelesek kétfaktoros hitelesítést (pl. jelszó + SMS-kód vagy biometria) alkalmazni minden érzékeny műveletnél. Ez megfelel az EU PSD2 irányelv erős ügyfélhitelesítési (SCA)

[13] Lásd: Az MNB „Öt csapás” intézkedéscsomagja a 2023-ban indított átfogó csalásmegelőzési stratégia része. Részletezve: MNB sajtóközlemény, 2023. október 19. – *„Digitális védelem: az MNB bevezeti az Öt Csapást”*. Elérhető: https://www.mnb.hu

követelményének.[14]

***Ad 5.*: Pénzforgalmi szolgáltatók közötti gyors adattovábbítás -** Ennek célja lehetővé tenni, hogy a bankok valós időben kommunikáljanak egymással egy gyanús esetben. A 2024. évi XVIII. törvény alapján a bankok kötelezően adatot szolgáltatnak egymásnak visszaélés gyanúja esetén. Fentiek következtében, amennyiben egy ügyfél csalás áldozata, másodperceken belül elindítható a nyomkövetés és a blokkolás.

Az „Öt csapás" célja nem csupán a visszaélések utólagos kezelése, hanem a megelőzés és gyors reagálás rendszerének létrehozása. Ez a rendszer erősíti a pénzügyi biztonságot, növeli a banki szolgáltatók felelősségét, és tudatosabbá teszi az ügyfeleket is. Az intézkedéscsomag nem törli el az ügyfél felelősségét, de jelentősen növeli a bankok technikai és eljárási kötelezettségeit.

6. Összefoglalás

Ismeretes, hogy a jelenlegi jogi rendszer jelenleg nem tud hatékonyan fellépni a kifinomult pszichológiai manipulációk ellen (pl. *social engineering*), ahol az ügyfél maga adja meg a kódokat, maga indítja el az utalást, nem veszi észre, hogy csalás áldozata lett.[15]

A vitarendezési lehetőségek kapcsán lényeges, hogy a Pénzügyi Békéltető Testület eljárása csak korlátozott eredményeket hozhat.[16] Polgári peres eljárásban az ügyfélnek kell bizonyítania, hogy nem adott valós hozzájárulást a megbízáshoz – ez rendkívül nehéz.

Az online csalások technikai háttere is folyamatosan változik, különösen a mesterséges intelligencia (AI) elterjedésével. A következő új fenyegetések figyelhetők meg:

- *Voice cloning*: Telefonhívások során a csalók a mesterséges intelligencia segítségével az ügyfél rokonának, banki ügyintézőnek

[14] Az EU *PSD2* irányelv (2015/2366/EU) célja az elektronikus fizetési szolgáltatások biztonságának növelése, különösen az *erős ügyfél-hitelesítés* (SCA – *Strong Customer Authentication*) bevezetésével.

[1515] Az MNB 2023. évi Pénzügyi stabilitási jelentésében külön fejezetet szentel az online csalások banki kockázatainak és a bankok által alkalmazott kockázatcsökkentő technológiáknak. Forrás: *MNB Pénzügyi stabilitási jelentés – 2023. november.*

[16] A Pénzügyi Békéltető Testület (PBT) alternatív vitarendezési fórumként működik, de határozatai nem kötelező érvényűek, ha az egyik fél az eljárásban nem működik együtt. Részletes tájékoztató: https://www.mnb.hu/bekeltetotestulet

vagy vezető beosztású munkatársnak álcázzák magukat.[17]

- *Deepfake* videók: A jövőben akár banki videóazonosítók manipulálására is alkalmas lehet.[18]
- Automatizált *social engineering*: Chatbotok és AI-modellek használata tömeges megtévesztéshez, különösen e-mailes támadásoknál.
- **„***Behavioral biometrics***"** kijátszása: A gyanús viselkedésminták felismerésére szolgáló rendszereket célzott AI-támadásokkal meg lehet kerülni.[19]

A szabályozók jelenleg nem tudnak lépést tartani e fejlődéssel, különösen, hogy ezek a támadások nem egyszerűen technikaiak, hanem pszichológiai és bizalmi manipulációkra épülnek.

A javasolt szabályozási irány egyértelmű, olyan új jogszabálymódosítások kellenek, amelyek lehetővé tennék a visszautalt összegek automatikus zárolását, a bankok közötti gyors riasztási rendszert, illetve a kockázatos utalásoknál kötelező figyelmeztetést vagy időzített megerősítést.

Az online banki csalások elleni védekezés csak komplex megközelítéssel lehet sikeres. A következő reformjavaslatokat érdemes figyelembe venni a jogalkotók és szabályozók részéről:

- Valós idejű kommunikáció előírása a bankok között a gyanús tranzakciók esetén.
- Automatikus tranzakció-zárolási mechanizmus bevezetése nagy kockázatú megbízások esetén.
- „Második megerősítő lépcső": ismeretlen számlára irányuló utalásoknál időzített megerősítés vagy emberi ügyintéző bevonása.
- Egységes európai kártérítési protokoll kialakítása (hasonlóan az UK CRM modellhez).

---

[17] A „*voice cloning*" technológia lehetővé teszi egy emberi hang szintetikus utánzását néhány percnyi hangminta alapján. Ezzel kapcsolatban a technikai előzményekhez lásd: N. CARLINI – P. MISHRA – T. VAIDYA – Y. ZHANG – M. SHERR – C. SHIELDS – D. WAGNER – W. ZHOU: *Hidden Voice Commands.* Proceedings of the 25th USENIX Security Symposium August 10–12, 2016 Austin, TX. lásd: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_carlini.pdf

[18] Az ENSZ Nemzetközi Távközlési Uniója (ITU) szerint 2024-ben a *deepfake* és *voice cloning* alapú csalások a kibertámadások egyik leggyorsabban növekvő típusa volt a pénzügyi szektorban.

[19] A „*behavioral biometrics*" módszerek a felhasználó gépelési sebességét, egérmozgását, és viselkedési szokásait elemzik, de ezeket mesterséges intelligenciával meg lehet kerülni. L

- Közös adatbázisok és *fraud watchlist* létrehozása a pénzforgalmi szolgáltatók között, GDPR-konform módon.
- Ügyféltudatosság erősítése: kötelező digitális pénzügyi ismeretek bevezetése a banki ügyfél *onboarding* folyamatába.

A digitális bankolás korszakában a megtévesztésen alapuló átutalások komoly problémát jelentenek, amelyre a jelenlegi polgári és büntetőjogi eszköztár csak részben ad választ. A banki szerződéses keretrendszer – az ügyfél felelősségére építve – nem igazodik a kiberbűnözés új típusaihoz.

Az ügyfelek tudatosságának növelését nagy mértékben segítheti az MNB, a Magyar Bankszövetség, az Országos Rendőrfőkapitányság, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, valamint a Nemzeti Média- és Hírközlési Hatóság által 2022 őszén indított KiberPajzs projektje.[20]

A digitális pénzügyi tér fejlődése soha nem látott kényelmet kínál az ügyfeleknek, de ezzel együtt új, eddig ismeretlen típusú kockázatokat is. A jogi szabályozás jelenleg nem képes lépést tartani azzal a sebességgel, ahogy a csalási módszerek fejlődnek.

A Magyarországon 2025. július 1. napjával elinduló, a teljes hazai átutalási forgalmi rendszerre rálátó ún. Központi Visszaélésszűrő Rendszer (röviden: KVR) is az online csalások megelőzését, szűrését hivatott szolgálni.

Az ügyfél felelősségén alapuló jelenlegi szabályozás egyre kevésbé igazságos abban a környezetben, ahol a támadások pszichológiai és technológiai manipulációval, kifinomult *social engineering* stratégiákkal történnek. A jövő szabályozási modelljeinek három alappillére: prevenció, kompenzáció és együttműködés. A bankoknak, a szabályozóknak és a társadalomnak együtt kell fellépnie az ügyfelek védelme érdekében, a digitális pénzügyi ökoszisztéma biztonságának megőrzéséért. A jogalkotás és az igazságszolgáltatás részéről érdemi beavatkozásra van szükség, különösen: a fogyasztóvédelem, a pénzügyi prevenció, és az ügyfelek automatikus visszatérítési jogainak területén.

Felhasznált irodalom:

FUGLINSZKY Á.: *Kártérítési jog.* Budapest, 2015.;
MISKOLCZI BODNÁR P.: *A kártérítési felelősség közös szabályainak*

[20] Részletesen lásd: www.kiberpajzs.hu

alkalmazási köre. Jogtudományi Közlöny 2019/2. 53-60. o.;
SÁRKÖZY T,: *Fordulat a magyar kártérítési jogban.* Magyar Jog, 2013/9., 535-542. o.;
T. N. JAGATIC – N. A. JOHNSON – M. JAKOBSSON – F. MENCZER*: Social Phishing.* Communications of the ACM Volume 50, Number 10 (2007), 94-100. o. lásd: https://dl.acm.org/doi/fullHtml/10.1145/1290958.1290968
VÉKÁS L.: *Szerződésszegési kártérítési felelősség a bírói gyakorlatban*. Magyar Jog, 2020/10., 557-566. o.