**MNB azonosító kód: P14**

**Módszertani segédlet**

**A fizetési kártya kibocsátói és elfogadói üzletágban felmerült kár, leírt veszteség és visszaélés adatai**

**I. Általános előírások**

1. Jelen adatszolgáltatás a fizetési kártya üzletágban mind a kibocsátói, mind pedig az elfogadói oldalon felmerült károkat és az ezekből keletkező veszteségeket tartalmazza.

2. A bankoktól, mint adatszolgáltatóktól teljes körű szolgáltatást igénybe vevő szövetkezeti hitelintézetek adatait - összesített formában - a rendszert üzemeltető adatszolgáltató (bank) gyűjti ki a rendszerből és összesíti, valamint küldi az MNB-nek. Szponzorbanki kapcsolat esetén a szponzorált bank adatait maga a szponzorált bank vagy a szponzorbank küldi meg az MNB-nek, de ez utóbbi esetben a saját adataitól elkülönítve, a szponzorált bank GIRO kódjával, illetve törzsszámával.

3. Nem magyarországi székhelyű adatszolgáltatók, határon átnyúló szolgáltatásnyújtás jelentésére vonatkozó előírások:

* 01. tábla: Kibocsátói üzletág: Jelenteni kell az összes olyan a szolgáltató által kibocsátott fizetési kártyát érintő visszaélést, amelyek birtokosa magyarországi lakhellyel vagy székhellyel rendelkezik.
* 02. tábla: Elfogadói üzletág: Jelenteni kell az összes olyan visszaélést, amely az adatszolgáltató által
* Magyarország területén található fizikai elfogadóhelyeknek nyújtott kártyaelfogadói szolgáltatás során, valamint
* az adatszolgáltató által magyarországi székhellyel rendelkező vállalkozásoknak nyújtott internetes (card not present) elfogadói szolgáltatás során, továbbá
* Magyarország területén működtetett ATM berendezések elfogadói üzemeltetése során merült fel.

4. A határon átnyúló fizetési szolgáltatást Magyarországon nyújtó adatszolgáltatóknak a „CROSSB” kódot kell alkalmazniuk a „Pénzforgalmi szolgáltató típusa” oszlopban.

5. A kitöltéshez szükséges kódokat az e rendelet 3. mellékletének 4.8. pontja szerinti, az MNB honlapján közzétett technikai segédletek tartalmazzák.

**II . Az adatszolgáltatáshoz tartozó fogalmi meghatározások**

1. Felmerült kár: A tárgyidőszakban az adatszolgáltató kibocsátói vagy elfogadói üzletágában az adatszolgáltató tudomására jutott visszaélés, amely még ugyanabban a tárgyidőszakban leírt veszteségként megjelenik a kártyaüzletág valamely szereplőjénél, vagy végleges rendezése áthúzódik egy következő tárgyidőszakra.
2. A kártyaüzletág valamely szereplőjénél jelentkező veszteség: Az adott, vagy egy korábbi tárgyidőszakban, az adatszolgáltató kibocsátói vagy elfogadói üzletágában felmerült kár veszteségként történő leírása, kárviselőként bontva.
3. On-us forgalomban felmerült kár: Az adatszolgáltató saját hálózatában, a saját kártyái használatához kapcsolódó kár.
4. Belföldi bankközi forgalomban felmerült kár: A kibocsátói üzletágban: az adatszolgáltató kártyáihoz kapcsolódóan más hazai bankok hálózatában felmerült kár. Az elfogadói üzletágban: az elfogadó bank hálózatában más hazai bank által kibocsátott kártyák használatához tapadó kár.

A következő meghatározásokban, zárójelben szerepelnek a kártyatársaságok által használt fogalmak is:

1. Határon átnyúló (Cross-border) forgalomban felmerült kár: A kibocsátói üzletágban: az adatszolgáltató kártyáinak külföldi használatához kapcsolódó kár. Az elfogadói üzletágban: az elfogadó bank hálózatában a külföldi kibocsátású kártyák használatához kapcsolódó kár.
2. Elveszett/ellopott kártyákkal okozott kár (Lost/Stolen): azon káresemény és leírt veszteség, amelyet a kártya jogos birtokosa által elvesztett, vagy a tőle ellopott kártyákkal követtek el.
3. Meg nem kapott kártyákkal okozott kár (Card not received): a kibocsátó bank által a kártyabirtokos részére postai úton továbbított, de a jogos birtokoshoz meg nem érkezett azon kártya, amellyel illetéktelen személy jogtalan tranzakciókat bonyolít le.
4. Hamis adatokkal igényelt kártyával okozott kár (Fraudulent application): a kártyabirtokos hamis adatokkal kér és kap kártyát a kibocsátótól és ezzel jogtalan műveleteket bonyolít le.
5. Hamisított kártyákkal okozott kár (Counterfeit): a kártyahamisítás minden formája ideértendő (pl. duplikált – skimming – kártyákkal elkövetett visszaélések, valódi kártyák megszemélyesítési adatainak megváltoztatása).
6. Egyéb visszaélésekkel okozott kár (Other): mindazon visszaélések ide tartoznak, amelyek a fenti pontok egyikébe sem sorolhatók. Nem tartozik azonban ide a kártyabirtokos ügyfél számlaegyenleg túllépéséből eredő kár, valamint azok a visszaélések, amikor a kártyabirtokos saját maga él vissza a saját kártyájával. Ez utóbbi esetben, abban a kár kategóriában kell szerepeltetni az összeget, amelybe az ügyfél bejelentése alapján besorolható. A veszteségek között azonban egyik esetben sem kell szerepeltetni a tételt (függetlenül attól, hogy a kár értéke az ügyféltől behajtható-e vagy sem), ugyanis az ilyen esetek a hitelezési veszteség kategóriájába és nem a fizetési kártyás veszteségek közé tartoznak.
7. Kártya adatszerzés (Card Skimming): a fizetési kártya használatához szükséges bármely adat (pl. mágnescsík vagy chip adatai, PIN) jogosulatlan megszerzése ATM és POS berendezéseknél, valamint interneten abból a célból**,** hogy az adatok birtokában hamisított kártyát gyártsanak és azzal jogosulatlan műveleteket hajtsanak végre.
8. Kártya megszerzése (Card Trapping): az ATM-művelet végrehajtása során a kártya és a hozzá tartozó PIN kód fizikai megszerzése, majd a kártya készpénzfelvételre való jogosulatlan használata.
9. Készpénz illetéktelen megszerzése (Cash Trapping): az ATM-művelet során a kártyabirtokos nem jut hozzá a készpénzhez, annak ellenére, hogy a bizonylat szerint az ATM kiadta azt. Miután a kártyabirtokos a berendezés meghibásodását feltételezve távozik, a csaló megszerzi az általa „manipulált” gépbe ragadt pénzt.

**III. A táblák kitöltésével kapcsolatos részletes tudnivalók, az adatok összeállításának módja**

1. **01. tábla: A fizetési kártya kibocsátói és elfogadói üzletágban a tárgyidőszakban felmerült kár és leírt veszteség**

Az ATM tulajdonosa ellen elkövetett visszaéléseket annak az adatszolgáltatónak kell jelentenie, amely az ATM berendezésen a szolgáltatást nyújtja (acquiring institution ID), akár saját, akár más szervezet által üzemeltetett ATM hálózatot vesz igénybe.

Az adatszolgáltatás egyes oszlopaiban jelentendő adatok:

* „a” oszlop: Ebben az oszlopban kell jelölni, hogy az adatszolgáltató pénzforgalmi szolgáltató, pénzforgalmi szolgáltatást nem nyújtó elektronikuspénz-kibocsátó intézmény, határon átnyúló (cross-border) szolgáltató, vagy hitelintézet-e.
* „b” oszlop: Ebben az oszlopban kell jelölni, ha a kibocsátott kártyához tartozó fizetési számlát nem az adatszolgáltató vezeti. Ez az oszlop csak a kibocsátói oldali adatoknál töltendő.
* „PENZ” kód: Ezt a kódot kell megadni, ha a visszaélés olyan kártyához kapcsolódik, amelyet az adatszolgáltató pénzforgalmi szolgáltató más pénzforgalmi szolgáltatónál vezetett fizetési számlához kapcsolódó kártyát bocsátott ki harmadik fél szolgáltatóként.
* „EGYEB” kód: Ezt a kódot kell megadni, ha a visszaélés olyan kártyához kapcsolódik, amelyet az adatszolgáltató fizetési számlát vezető pénzforgalmi szolgáltató bocsát ki a nála vezetett számlához kapcsolódóan.
* „TPP” kód: Ezt a kódot kell megadni, ha a visszaélés olyan kártyához kapcsolódik, amelyet az adatszolgáltató számlavezető pénzforgalmi szolgáltató által vezetett számlához más – harmadik fél – pénzforgalmi szolgáltató bocsátott ki.
* „c” oszlop: itt kell jelölni, hogy a jelentett adat visszaélésekre (esetszám és felmerült kár), a visszaélések miatt leírt kárra, vagy kártyás adatszerzésekre, egyéb incidensekre, illetve berendezések elleni támadásokra vonatkozik.
* „d” oszlop: Ebben az oszlopban kell jelölni, hogy a jelentett adat kibocsátói oldali visszaélésekre vagy elfogadói oldali visszaélésekre vonatkozik. Az elfogadói oldalon felmerülő károkat a nemzetközi védjeggyel ellátott kártyák esetén a kártyatársaságoktól kapott adatokhoz igazodva kell kitölteni. Az adatszolgáltató elfogadói hálózatában történt, a tárgyidőszakban az adatszolgáltató tudomására jutott káreseményeket kell jelenteni (függetlenül attól, hogy a visszaélés a tárgyidőszakban vagy azt megelőzően történt). Azokat az eseteket is szerepeltetni kell, amelyeket a kibocsátó bank visszaélésként lejelentett, de a későbbiek során nem jelenik meg veszteségként.
* „e” oszlop: Ebben az oszlopban kell jelölni a mellékelt kódlisták alapján a kártyatársasági kódokat.
* „f” oszlop: Ebben az oszlopban kell jelenteni a kártyák funkcióját. Azon kártyák esetében, amelyek a credit, debit és delayed debit funkciók közül többel is rendelkeznek, a forgalmi adatokat a funkciók szerint egyértelműen szét kell választani
* „g” oszlop: Itt kell jelenteni, hogy az adott visszaélés milyen típusú kártyás forgalomhoz kapcsolódóan merült fel.
* „h” oszlop: Ebben az oszlopban kell jelölni, hogy a jelentett visszaélést milyen berendezésen követték el. Nem tekintjük INAPP tranzakciónak azokat a fizetéseket, amikor egy mobiltárcába digitalizált kártyával POS terminálnál fizetnek, vagy akár ATM-nél vesznek fel készpénzt, ezen esetekben POS és ATM kódon kell jelenteni. Új típusú, innovatív POS megoldások alatt azon okoseszközöket (pl. mobiltelefonokat, tableteket) kell érteni, amelyek egy szoftveres frissítésnek köszönhetően képesek a fizetési kártyás tranzakciókhoz kapcsolódó folyamatok tekintetében a tranzakciók feldolgozására. Ebben a kategóriában 3 megoldás különíthető el: okoseszköz kommunikációs csatornájának és kijelzőjének használata, de adatátadás (pl. kártya chip beolvasás) és PIN magadás egy különálló eszközön (MPOS); PIN magadás is az okos eszközön, de az adatátadás (pl. kártya chip beolvasás) egy különálló eszközön (SPOS); adatátadás (pl. kártya chip beolvasás) és PIN megadás is az okos eszközön (Tap-on-Phone). Az új típusú, innovatív eszközökhöz kapcsolódó tételeket a megfelelő kategória és nem a „POS” kódérték alatt kell jelenteni.
* „i” oszlop: Itt kell jelölni, ha a visszaélést érintéses tranzakcióval összefüggésben követték el.
* „j” oszlop: Ebben az oszlopban kell jelölni, hogy a jelentett visszaélés milyen irányú forgalomhoz kapcsolódott
* „k” oszlop: Ebben az oszlopban kell jelölni, hogy a jelentett kibocsátói oldali visszaélés esetében hol volt az elfogadó pénzforgalmi szolgáltató székhelye, elfogadói oldali visszaélés esetén pedig a kártya kibocsátásának helyét kell megadni.
* „l” oszlop: Ebben az oszlopban kell jelölni a visszaélés által érintett tranzakció helyét. Elfogadói oldalon azon belföldi visszaéléseket, amelyek esetében az érintett külföldi szolgáltató közvetlenül (cross-border) nyújt elfogadói szolgáltatást Magyarországon, belföldi visszaélésként, „HU” kóddal kell jelenteni. Itt kell jelölni a magyarországi adatszolgáltató külföldi elfogadó hálózatában történt visszaéléseket is, a megfelelő kódértékkel, amennyiben azt a szolgáltatást nem leányvállat vagy fióktelep útján nyújtja.
* „m” oszlop: Itt kell jelölni kibocsátói oldali visszaélés esetén, hogy az adott kártya, amivel a forgalmat lebonyolították mobiltárcába regisztrált-e. Mobiltárcába regisztrált kártyának azokat a kártyákat kell jelölni, amelyeket a kártyakibocsátó pénzforgalmi szolgáltató vagy vele szerződésben álló szolgáltató által nyújtott, fizikai elfogadóhelyen történt fizetésnél (pl. NFC vagy QR-kód alkalmazásával) használható mobiltelefonos fizetési alkalmazásba regisztráltak, és amelyeket fizikai formában is kibocsáthatnak
* „n” oszlop: itt kell jelölni, hogy az adott forgalom a pénzforgalmi szolgáltatás nyújtásáról szóló 2009. évi LXXXV. törvény (továbbiakban Pft.) 2. § 27a. pontja alapján távoli („remote”) fizetési műveletnek minősül-e.
* „o” oszlop: itt kell jelölni, hogy a Pft. 2. §. 4a. pontjában meghatározott erős ügyfél-hitelesítésre (strong customer authentication – SCA) sor került-e a tranzakció indításánál.
* „p” oszlop: amennyiben az adott forgalom esetében nem került sor erős ügyfél-hitelesítésre, akkor ebben az oszlopban kell jelölni ennek okát az (EU) 2015/2366 európai parlamenti és tanácsi irányelvnek az erős ügyfél-hitelesítésre, valamint a közös és biztonságos nyílt kommunikációs standardokra vonatkozó szabályozástechnikai standardok tekintetében történő kiegészítéséről szóló 2017. november 27-i (EU) 2018/389 felhatalmazáson alapuló bizottsági rendelet alapján.
* „q” oszlop: itt kell jelenteni a visszaélés eredetére vonatkozó adatokat.
* Csaló által kezdeményezett fizetési megbízás: olyan jóvá nem hagyott fizetési művelet, amikor a csaló hamis fizetési megbízást kezdeményez, miután a fizető fél érzékeny fizetési adatait csalárd módon megszerezte, illetve valamilyen csalárd módon hozzáférést szerzett az ügyfél által használt készpénzhelyettesítő fizetési eszközhöz. Ide tartoznak azok az esetek is, mikor a csaló az ügyfél eszközét megszerezve, vagy távoli elérést biztosító programmal az ügyfél eszközéről indítja a megbízást.
* Csaló által módosított fizetési megbízás: olyan jóvá nem hagyott fizetési művelet, amikor a csaló a fizető fél és a pénzforgalmi szolgáltató közötti elektronikus kommunikáció során módosítja a jogszerű fizetési megbízást (közbeékelődéses támadás), vagy a tranzakció feldolgozásában résztvevő valamely szolgáltató rendszerében módosítja a fizetési megbízást annak elszámolása és kiegyenlítése előtt.
* Fizető fél által kezdeményezett fizetési megbízás: olyan jóváhagyott fizetési művelet, amikor a fizető fél tudatosan indítja a tranzakciót például egy megtévesztés vagy pszichológiai manipuláció hatására.
* Fieztő fél hozzátartozója által kezdeményezett fizetési megbízás: olyan jóvá nem hagyott fizetési művelet, amikor nem egy csalárd módon eljáró fél, hanem a fizető fél hozzátartozója kezdeményezi a megbízást a fizető fél jóváhagyása nélkül.
* „r” oszlop: Itt kell jelölni a fizetési kártyás visszaélés fajtáját.
  + Adathalászat / ID lopás / kártya adatok lopása: a fizető fél érzékeny fizetési adatainak / személyi azonosságát igazoló dokumentumainak / kártyaadatainak megszerzése a csaló által, amelyek birtokában kártyás fizetés indítható az ügyfél nevében. Adathalászat / ID lopás esetén töltendő a „v” oszlop az adathalászat módjának megjelölése érdekében.
  + Pszichológiai manipuláció / megtévesztés fizetési tranzakció kezdeményezésére / jóváhagyására. Ebbe a kategóriába tartozik többek között:
    - fiktív vásárlásra való rábeszélés: amikor a fizető felet ráveszik arra – jellemzően valamilyen fiktív hirdetésen vagy webshopon keresztül –, hogy előre fizessen egy termékért vagy szolgáltatásért, amelyet azonban soha nem kap kézhez, illetve az soha nem teljesül;
    - fiktív befektetéshez kapcsolódó rászedés: amikor a csalárd módon eljáró fél meggyőzi a fizető felet, hogy pénzét egy, a valóságban nem létező befektetési eszközbe (pl. valamilyen befektetési alap, nemesfém, ingatlan vagy kriptovaluta) helyezze, de a befektetés a pénz csaló részére történő átadását követően azonban soha nem történik meg a valóságban;
    - érzelmi alapra épített átverés / manipuláció: amikor a fizető felet ráveszik, hogy fizetést teljesítsen valamilyen problémára hivatkozva (pl. megromlott egészségi állapothoz kapcsolódó kezelések vagy személyes találkozás megvalósítása érdekében felmerülő költségek fedezése) olyan személynek, akivel korábban (jellemzően online térben, valamilyen közösségi média felületen keresztül) ismerkedett meg és úgy véli, hogy érzelmi kapcsolatban áll vele;
    - nagy értékű tárgyak, illetve összegek hozzáférhetővé tételéhez kacsolódó átverés (pl. ún. „nigériai típusú átverés”): amikor a csalárd módon eljáró fél meggyőzi a fizető felet olyan díj megfizetéséről, amely állítása szerint egy nagyobb összegű fizetés vagy különösen nagy értékű áruk szabadon bocsátásához szükséges (pl. sorsoláson nyert nagy értékű nyeremény kifizetéséhez, illetve megküldéséhez kapcsolódó adminisztratív költségek előre történő megtérítése; ajándékba küldött áruk vámkezeléséhez kapcsolódó költségek megtérítése; örökléshez kapcsolódó költségek megtérítése);
    - számlafizetéshez kapcsolódó átverés: amikor a fizető fél megkísérel kifizetni egy számlát egy törvényes kedvezményezettnek, de a csalárd módon eljáró fél beavatkozik és meggyőzi a fizető felet arról, hogy a fizetést az általa ellenőrzött számlára teljesítse;
    - megszemélyesítéshez kapcsolódó átverés: amikor a csalárd módon eljáró fél valamilyen, jellemzően hivatalos személynek (pl. hatósági, jellemzően rendőrségi állományhoz tartozó fél; állami vagy önkormányzati tisztviselő), banki alkalmazottnak, fizető fél munkáltatója magas beosztású képviselőjének, közüzemi vagy telekommunikációs szolgáltató alkalmazottjának, adománygyűjtést megvalósító civil szervezet képviselőjének kiadva magát meggyőzi a fizető felet, hogy teljesítsen egy fizetést az általa kontrollált számlára.
  + Fizető fél jár el csalárd módon: öncsalás, amikor a fizető fél csalás áldozatának színleli magát, ezzel megkísérelve azt, hogy a pénzforgalmi szolgáltatója térítse meg a színlelt kárt.
  + Készpénzhelyettesítő fizetési eszközhöz történő közvetlen hozzáférés: Kereskedőnél vagy szolgáltatónál tárolt kártyaadatokkal vagy tokenizált kártyával az adott kereskedő vagy szolgáltató rendszerében fizetés indítása, az adatok kimásolása nélkül. Ide értendő az eltulajdonított mobiltelefonnal érintéses fizetés végrehajtása is.
* „s” oszlop: Itt kell jelölni, hogy az elfogadói és kibocsátói visszaélésekből származó leírt károkat a fizetési tranzakcióban résztvevő melyik szereplőre terhelték. Amennyiben a bekövetkezett káron több szereplő osztozik, úgy meg kell azt osztani a releváns kódértékek sorai között. Ha a visszaélés valamilyen formában megtérül vagy sikerül a visszaéléssel érintett kárösszeg részleges vagy teljes visszaszerzése, akkor azt a részt a „MEGTER” kódérték alatt kell jelenteni. Ebben az esetben ezzel az összeggel csökkenteni kell az ügyfélre vagy a kereskedőre terhelt, illetve a szolgáltató által viselt kárt. Ha a megtérülés a tényleges kárleírástól eltérő időszakban történt, úgy a rendelkezésre álló új információk alapján visszamenőleges módosítást kell végrehajtani. Ugyanakkor alap esetben csak akkor kell jelenteni a kárleírást, ha lezárult az érintett ügy, és már megtörtént a számviteli rendezés is minden oldalon, tehát visszamenőleges pontosításra csak akkor van szükség, ha egy lezárt, és ennek megfelelően jelentett ügy kapcsán történt egy új információ hatására változás.
* „t” oszlop: Itt kell jelölni az adatszerzések és támadások típusát.
* Kártya megszerzésére irányuló incidensek: Azoknak a fizetési kártyáknak a darabszámát kell megadni, amelyek esetében a kártyát eltulajdonítottak a kártyabirtokostól.
* Jogtalan tranzakció reverzálást eredményező incidensek: Azoknak az incidenseknek a számát kell megadni, amelyek esetében az ATM működését úgy befolyásolják, hogy az a műveletet sikertelennek minősíti, holott a pénz kiadásra kerül.
* Készpénz illetéktelen megszerzésére irányuló incidensek: azoknak az incidenseknek a számát kell megadni, amelyek esetében a pénz kiadásra kerül, de nem a kártya jogos birtokosa számára (pl. ragasztás).
* ATM elleni fizikai és elektronikus támadások (kivéve a robbantást): azoknak az eseményeknek a számát és a ténylegesen eltulajdonított vagy értékét vesztett készpénz összegét kell megadni, amelyek esetében az ATM berendezést, vagy az azt kiszolgáló hálózatot fizikai vagy elektronikus támadás éri (kivéve a robbantást). Jelenteni kell azokat az eseteket is, amikor csak a gépben keletkezik kár, és azokat is, amelyeknél a gépben tárolt készpénz is eltulajdonításra kerül vagy megsemmisül (pl. kitépik az ATM-et a falból vagy megfúrják azt a széfes kazetta megszerzése érdekében).
* Robbantással együttjáró ATM elleni támadások: azoknak az eseményeknek a számát és a ténylegesen eltulajdonított vagy értékét vesztett készpénz összegét kell megadni, amelyek esetében az ATM berendezést felrobbantják.
* ATM-et kiszolgáló személyzet elleni támadások: azoknak az incidenseknek (alkalmaknak) a számát és a támadások során ténylegesen eltulajdonított vagy értékét vesztett készpénz összegét kell megadni, amelyeket az ATM-et kiszolgáló személyzet ellen indítottak, azokat az eseteket is jelenteni kell, amikor nem sikerül ellopni a készpénzt.
* Kártya adatszerzésre irányuló incidensek: Azoknak az incidensek a számát kell megadni, amelyek esetében a kártyaadatok megszerzése a cél.
* „u” oszlop: itt kell jelölni, hogy sikeres volt-e a visszaélési kísérlet. Azokat a sikertelen visszaélési kísérleteket, amelyek esetében az eltulajdonítani kívánt összeg nem állapítható meg, 0 összeggel kell jelenteni.
  + Összes eset: Pénzforgalmi visszaélésnek kell tekinteni azokat az eseteket is, amikor a fizető fél hozzátartozója a fizető fél jóváhagyása nélkül kezdeményez egy tranzakciót, valamint a fizető fél önmaga ad egy fizetési megbízást egy csalárd módon eljáró fél felé valamilyen megtévesztés vagy pszichológiai manipuláció hatására. Ugyanakkor csak azon eseteket szükséges jelenteni, amelyeket az adatszolgáltató is visszaélésnek minősít, és a megfelelő szervezeti egysége (pl. bankbiztonság, belső ellenőrzés) ennek megfelelően kezeli.
  + Sikertelen eset: Sikertelen visszaélési kísérletnek minősül minden olyan eset, amelynél a fizetési megbízás teljesítésére nem kerül sor. Ezek közé tartoznak azok az esetek, amikor a fizető fél pénzforgalmi szolgáltatója – jellemzően az alkalmazott visszaélésszűrési mechanizmusok eredményeként – még a fizetési megbízás jóváhagyása előtt közbeavatkozik, függetlenül a visszaélés eredetétől, illetve fő motívumától. Nem minősülnek sikertelen visszaélési kísérletnek mindazon esetek, amelyeknél a készpénzhelyettesítő fizetési eszköz felett rendelkező authorizációja hiúsul meg, így például mobiltárcás alkalmazásnál a jelszó többszöri elrontása. Ugyanakkor sikertelen visszaélésnek minősül az is, ha a csalárd módon eljáró fél megszerzi a fizető fél érzékeny fizetési adatait vagy hozzáférést szerez a készpénzhelyettesítő fizetési eszközhöz, de nem jut el fizetési megbízás megadásának megkezdéséig (pl. a pénzforgalmi szolgáltató a visszaélésszűrési mechanizmusai révén rosszindulatú, adott esetben távoli hozzáférést biztosító szoftver közbeavatkozását érzékeli, ezért korlátozza a fizetési megbízások megadását). Ezekben az esetekben a sikertelen visszaélés értékeként 0 forintot kell megadni. A sikertelen visszaélések jelentése kapcsán az ügyféljelzéseket is figyelembe kell venni, de jelentési kötelezettség csak akkor társul hozzájuk, ha az adatszolgáltató megfelelő szervezeti egysége is visszaélésnek minősíti ezeket az eseteket.
  + Sikeres eset: Sikeres visszaélésnek minősül minden olyan eset, ahol a megbízást az adatszolgáltató teljesíti, akkor is, ha az eltulajdonított összeget az adatszolgáltató később visszakapja.
* „v” oszlop: itt kell jelölni, hogy az „r” oszlopban megjelölt adathalászathoz / ID lopáshoz / kártya adatok lopásához köthető visszaéléseknél pontosan mi volt az elkövetés módja.
  + Rosszindulatú szoftver általi adatszerzés: Ügyfél eszközére telepített szoftver által személyes vagy kártya adatok megszerzése. Ide értendő a legális szoftverek (pl távoli hozzáférést nyújtó programok) rosszindulatú felhasználása is.
  + IT rendszer feltöréséből adódó jogosulatlan adatszerzés: Nem ügyfél által birtokolt rendszer feltöréséből származó adatszerzés. Ez lehet a fizetési lánc vármely szereplője, de akár azon kívüli harmadik fél, aki egyéb okból tárolta az ügyfél személyes adatait.
  + Amennyiben adatszerzés módja nem ismert „Egyéb” kód jelentendő
* „w” oszlop: itt kell jelölni, hogy az „r” oszlopban megjelölt készpénzhelyettesítő fizetési eszközhöz történő közvetlen hozzáférés esetében pontosan mi volt a hozzáférés módja. Amennyiben a csalók a felhasználó csalásban használt fiókjának adatait fizető fél által telepített szoftver vagy IT rendszer feltörése nélkül szerezték meg, „Egyéb” kód jelentendő (Pl. adatszerzés ügyféltől, pszichológiai manipuláció útján)
* „x” oszlop: itt jelentendő a visszaélések és adatszerzések darabszáma.
* „y” oszlop: itt jelentendő a visszaélésekkel kapcsolatban felmerült és leírt kár értéke egységnyi forintban megadva. A devizában keletkező adatok forint értékét az adatszolgáltatónak a tranzakció napján érvényes saját árfolyamán vagy a tárgyidőszakra vonatkozó MNB tárgyidőszaki deviza átlagárfolyamon átszámítva kell megadni.

**02. A fizetési kártya kibocsátói üzletágban a tárgyidőszakra vonatkozó csalási arány statisztika**

Az adatszolgáltatás egyes oszlopaiban jelentendő adatok:

* „a” oszlop: Ebben az oszlopban kell jelölni, hogy az adatszolgáltató pénzforgalmi szolgáltató, pénzforgalmi szolgáltatást nem nyújtó elektronikuspénz-kibocsátó intézmény, határon átnyúló (cross-border) szolgáltató, vagy hitelintézet-e.
* „b” oszlop: Ebben az oszlopban kell jelölni, ha a kibocsátott kártyához tartozó fizetési számlát nem az adatszolgáltató vezeti.
* „c” oszlop: Ebben az oszlopban kell jelölni az „f” oszlopban jelentett értékhez kapcsolódó csalási arányt és az SCAr. szerinti referencia csalási aránytól való eltérést, azaz azt az esetet, amikor a számított csalási arány eltér az SCAr. szerinti referencia csalási aránytól. Itt kell jelölni továbbá a műveletikockázat-elemzésen alapuló – az erős ügyfél-hitelesítés alóli – kivételek alkalmazásának megszüntetését, azaz azt az esetet, amikor a tranzakció típusok bármelyike esetében két egymást követő negyedévben (180 nap) a számított csalási arány meghaladta az SCAr. szerinti referencia csalási arányt, és ez alapján az adatszolgáltató megszüntette a műveletikockázat-elemzésen alapuló kivételek alkalmazását.
* „d” oszlop: Itt kell jelenteni a tranzakció típusát, hogy az adott visszaélés kártyás forgalomhoz kapcsolódóan merült fel.
* „e” oszlop: Itt kell jelenteni a tranzakció típushoz kapcsolódó SCAr. szerinti referencia csalási arányhoz tartozó küszöbértéket csalásarány, csaláseltérés esetén.
* „f” oszlop: Itt jelentendő a számított csalási arány százalékos értéke, valamint az SCAr. szerinti referencia csalási aránytól való eltérés is. Az SCAr. szerinti referencia csalási aránytól való eltérést úgy kell kiszámítani, hogy a számított csalási arányból ki kell vonni az SCAr. szerinti referencia csalási arányt. Az érték adatokat egységnyi értékben, 3 tizedesjegy pontossággal kell megadni. Az SCAr. szerinti referencia csalási aránytól való eltérés esetén negatív érték is jelenthető, míg a csalási arány, valamint a műveletikockázat-elemzésen alapuló – az erős ügyfél-hitelesítés alóli – kivételek alkalmazásának megszüntetése esetén csak pozitív érték jelenthető.