EBA/GL/2014/12_Rev1

2014. december 19.

Végleges iránymutatások

az internetes fizetések biztonságáról

Tartalom

Iránymutatások az internetes fizetések biztonságáról **3**

I. cím – Alkalmazási kör és fogalommeghatározások 4

Alkalmazási kör 4
Fogalommeghatározások 6

II. cím – Iránymutatások az internetes fizetések biztonságáról 8

Általános ellenőrzési és biztonsági környezet 8
Az internetes fizetésekre vonatkozó különleges ellenőrzési és biztonsági intézkedések 12
Ügyféltudatosság, az ügyfelek felvilágosítása és az ügyfelekkel folytatott kommunikáció 19

III. cím – Záró rendelkezések és végrehajtás 21

1. melléklet: Bevált gyakorlati példák 22

Általános ellenőrzési és biztonsági környezet 22
Az internetes fizetésekre vonatkozó különleges ellenőrzési és biztonsági intézkedések 22

Iránymutatások az internetes fizetések biztonságáról

Az iránymutatás jogállása

Az e dokumentumban szereplő iránymutatást az EBH az európai felügyeleti hatóság (Európai Bankhatóság) létrehozásáról, a 716/2009/EK határozat módosításáról és a 2009/78/EK bizottsági határozat hatályon kívül helyezéséről szóló, 2010. november 24-i 1093/2010/EU európai parlamenti és tanácsi rendelet (a továbbiakban: EBH-rendelet) 16. cikkének rendelkezéseivel összhangban adta ki. Az EBH-rendelet 16. cikkének (3) bekezdése szerint az illetékes hatóságok és pénzügyi intézmények minden erőfeszítést megtesznek azért, hogy megfeleljenek az iránymutatásnak.

Az iránymutatás rögzíti az EBH álláspontját azzal kapcsolatban, hogy mi a megfelelő felügyeleti gyakorlat a Pénzügyi Felügyeletek Európai Rendszerében, és miként kell alkalmazni az uniós jogot egy adott területen belül. Az EBH ezért elvárja, hogy minden pénzügyi intézmény és illetékes hatóság betartsa a neki címzett iránymutatásokat. Az iránymutatások hatálya alá tartozó, illetékes hatóságok azzal tesznek eleget az iránymutatásnak, hogy megfelelően beépítik azt saját felügyeleti gyakorlataikba (pl. saját jogi kereteik vagy felügyeleti folyamataik módosításával), beleértve azokat az eseteket is, ahol az iránymutatás elsősorban intézményekre vonatkozik.

Adatszolgáltatási követelmények

Az EBH-rendelet 16. cikkének (3) bekezdése értelmében az egyes illetékes hatóságok 2015. május 5-ig kötelesek értesíteni a Hatóságot arról, hogy megfelelnek-e vagy meg kívánnak-e felelni ennek az iránymutatásnak, és ha nem, úgy tájékoztatniuk kell a Hatóságot a meg nem felelés indokairól. Amennyiben a fenti határidőig ilyen értesítés nem érkezik, a Hatóság úgy tekinti, hogy a szóban forgó illetékes hatóság nem felel meg az iránymutatásnak. Az értesítéseket „EBA/GL/2014/12” hivatkozással az V. fejezetben szereplő formanyomtatványon kell megküldeni a compliance@eba.europa.eu címre. Az értesítéseket olyan személyek nyújthatják be, akik megfelelő felhatalmazással rendelkeznek arra nézve, hogy illetékes hatóságuk nevében nyilatkozzanak annak megfeleléséről.

Az értesítéseket a 16. cikk (3) bekezdésével összhangban közzéteszik az EBH honlapján.

I. cím – Alkalmazási kör és fogalommeghatározások

Alkalmazási kör

1. Ezek az iránymutatások az internetes fizetések biztonságára vonatkozó minimumkövetelményeket határozzák meg. Az iránymutatások a 2007/64/EC [1] irányelv („pénzforgalmi szolgáltatásokról szóló irányelv", PSD) pénzforgalmi szolgáltatásokra vonatkozó tájékoztatási követelményekre és a pénzforgalmi szolgáltatók pénzforgalmi szolgáltatások nyújtásával kapcsolatos kötelezettségeire vonatkozó szabályaira épülnek. Az irányelv 10. cikkének (4) bekezdése előírja továbbá, hogy a pénzforgalmi intézményeknek megbízható vállalatirányítási rendszerrel és megfelelő belső ellenőrzési mechanizmusokkal kell rendelkezniük.

2. Az iránymutatások az irányelv 1. cikkében meghatározott pénzforgalmi szolgáltatók interneten keresztül nyújtott pénzforgalmi szolgáltatásaira alkalmazandók.

3. Az iránymutatások címzettjei az 1093/2010/EU rendelet 4. cikkének (1) bekezdésében meghatározott pénzügyi intézmények és az 1093/2010/EU rendelet 4. cikkének (2) bekezdésében meghatározott hatáskörrel rendelkező hatóságok. Az Európai Unió 28 tagállamában a hatáskörrel rendelkező hatóságoknak kell biztosítaniuk azt, hogy a pénzforgalmi szolgáltatásokról szóló irányelv 1. cikkében meghatározott, felügyeletük alá tartozó pénzforgalmi szolgáltatók alkalmazzák ezeket az iránymutatásokat.

4. Emellett a hatáskörrel rendelkező hatóságok előírhatják a pénzforgalmi szolgáltatóknak, hogy a hatáskörrel rendelkező hatóságnak beszámoljanak az iránymutatásoknak való megfelelésükről.

5. Ezek az iránymutatások nem érintik az Európai Központi Bank által kiadott „internetes fizetések biztonságára vonatkozó ajánlások (az „Ajánlás")[2] érvényességét. Különösen azért, mert továbbra is az Ajánlás marad az a dokumentum, amely alapján a központi bankoknak a fizetési rendszerek és eszközök felvigyázása során értékelniük kell az internetes fizetések biztonságára vonatkozó előírásoknak való megfelelést.

6. Az iránymutatások a minimum elvárásokat alkotják. Nem érintik a pénzforgalmi szolgáltatók felelősségét azért, hogy a pénzforgalmi tevékenységükkel kapcsolatos kockázatokat figyelemmel kísérjék és értékeljék, saját részletes biztonsági szabályzatot dolgozzanak ki, és az általuk nyújtott pénzforgalmi szolgáltatásokkal járó kockázatokkal arányos, megfelelő biztonsági, vészhelyzeti, esetkezelési és az üzletmenet folytonosságát biztosító intézkedéseket foganatosítsanak.

[1] Az Európai Parlament és a Tanács 2007/64/EK irányelve (2007. november 13.) a belső piaci pénzforgalmi szolgáltatásokról és a 97/7/EK, a 2002/65/EK, a 2005/60/EK és a 2006/48/EK irányelv módosításáról és a 97/5/EK irányelv hatályon kívül helyezéséről, HL L 319, 2007.12.05.

[2] http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

7. Az iránymutatások célja az alább felsorolt internetes fizetésekre vonatkozó egységes, a használt belépési eszköztől független minimumkövetelmények meghatározása:

    - [kártyák] kártyás fizetési műveletek végrehajtása az interneten, ideértve a virtuális kártyával végrehajtott fizetési műveleteket, valamint a kártyás fizetési adatok „elektronikus tárca szolgáltatások” használata céljára történő rögzítését;

    - [átutalások] átutalások lebonyolítása az interneten;

    - [elektronikus meghatalmazások] beszedés elektronikus felhatalmazásának megadása és módosítása;

    - [elektronikus pénz] interneten keresztül történő, két elektronikuspénz-számla közötti elektronikuspénz-utalás.

8. Ahol az iránymutatások valamilyen eredményre utalnak, ott az eredményt különböző eszközökkel lehet elérni. Ezek az iránymutatások az alábbiakban meghatározott követelmények mellett olyan legjobb gyakorlat szerinti megoldásokat is bemutatnak (az 1. mellékletben), amelyek követése a pénzforgalmi szolgáltatók számára javasolt, de nem előírás.

9. Fizetési modellen (például kártyás fizetési, átutalási vagy beszedési modelleken, stb.) keresztül kínált pénzforgalmi szolgáltatások és fizetési eszközök esetében az illetékes hatóságoknak és a fizetési eszközök feletti felvigyázást ellátó központi banknak együtt kell működniük annak biztosítása érdekében, hogy a rendszer működéséért felelős szereplők következetesen alkalmazzák az iránymutatásokat.

10. A fizetéskezdeményezési szolgáltatásokat kínáló fizetésiszolgáltatás-integrátorok[3] vagy az internetes fizetési szolgáltatások elfogadójának (és így pénzforgalmi szolgáltatóknak), vagy az adott rendszerek, illetve pénzforgalmi szolgáltatók külső technikai szolgáltatóinak tekinthetők. Az utóbbi esetben a fizetési integrátorokat szerződésben kell kötelezni az iránymutatásoknak való megfelelésre.

11. Az iránymutatások alkalmazási köre nem terjed ki a következőkre:

    - a pénzforgalmi szolgáltató fizetési oldalán nyújtott egyéb internetes szolgáltatások (például elektronikus brókeri tevékenység, online szerződések);

    - olyan fizetési műveletek, ahol a fizetési megbízás megadása postai úton, telefonon, hangpostán keresztül vagy sms alapú technológia használatával történik;

    - nem böngésző alapú mobiltelefonos fizetési műveletek;

[3] A fizetési integrátorok a kedvezményezett (vagyis az internetes kereskedő) részére egy szabványosított kapcsolódási felületet biztosítanak a pénzforgalmi szolgáltatók által nyújtott fizetéskezdeményezési szolgáltatásokhoz.

- olyan átutalások, ahol harmadik fél fér hozzá az ügyfél fizetési számlájához;

- vállalkozás által dedikált hálózaton keresztül lebonyolított fizetési műveletek;

- anonim és nem újratölthető, fizikai vagy virtuális előre fizetett kártyával végrehajtott kártyás fizetési műveletek, ahol nincs folyamatos kapcsolat a kibocsátó és a kártyabirtokos között;

- fizetési műveletek elszámolása és kiegyenlítése.

Fogalommeghatározások

12. Ezen iránymutatások alkalmazásában a pénzforgalmi szolgáltatásokról szóló irányelvben foglalt fogalommeghatározások mellett a következő fogalommeghatározások érvényesek:

- *Hitelesítés*: olyan eljárás, amely lehetővé teszi a pénzforgalmi szolgáltatónak az ügyfél személyazonosságának az ellenőrzését.

- *Erős ügyfél-hitelesítés*: ezen iránymutatások alkalmazásában olyan eljárás, amely a következő – tudásnak, tulajdonnak és egyedi jellemzőnek minősíthető – elemek közül legalább kettő használatán alapul: i) valami, amit csak a felhasználó tud, például statikus jelszó, kód, személyi azonosító szám; ii) valami, amit csak a felhasználó birtokol, például token, intelligens kártya, mobiltelefon; iii) valami, ami a felhasználó maga, például olyan biometriai jellemző, mint az ujjlenyomat. A kiválasztott elemeknek továbbá egymástól függetlennek kell lenniük, vagyis az egyikkel való visszaélés nem veszélyeztetheti a másikat (többit). Legalább az egyik elem nem lehet újrafelhasználható és megismételhető (az egyedi jellemző kivételével), valamint nem lehet titokban ellopható az interneten keresztül. Az erős ügyfél-hitelesítési eljárást úgy kell kialakítani, hogy védje a hitelesítési adatok bizalmas jellegét.

- *Engedélyezés*: az ügyfél vagy a pénzforgalmi szolgáltató bizonyos művelet elvégzésére – például pénzátutalásra vagy érzékeny adatokhoz való hozzáférésre – való jogának az ellenőrzésére szolgáló eljárás.

- *Hitelesítő adatok*: azok az – általában bizalmas – információk, amelyeket az ügyfél hitelesítés céljából megad a pénzforgalmi szolgáltatónak. Jelenthetik továbbá az ügyfél birtokában lévő, az adatokat tartalmazó fizikai eszközt (például egyszer használatos jelszót előállító eszköz, intelligens kártya) vagy valamit, amit a felhasználó megjegyez vagy képvisel (például biometriai jellemzők).

- *Jelentős fizetésbiztonsági incidens:* olyan esemény, ami jelentős hatást gyakorol vagy gyakorolhat a pénzforgalmi szolgáltató fizetési műveletekkel kapcsolatos rendszereinek biztonságára, sértetlenségére vagy folyamatos működésére és/vagy az érzékeny fizetési adatok vagy a pénzeszközök biztonságára. A jelentőség értékelése során figyelembe kell venni a potenciálisan érintett ügyfelek számát, a kockáztatott összeget és a más pénzforgalmi szolgáltatókra vagy más fizetési infrastruktúrákra gyakorolt hatást.

- *Tranzakciókockázat-elemzés:* egy adott tranzakcióhoz kapcsolódó kockázat értékelése olyan szempontok figyelembevételével, mint például az ügyfél fizetési szokásai (viselkedése), a kapcsolódó tranzakció értéke, a termék típusa és a kedvezményezetti profil.

- *Virtuális kártyák*: olyan kártya alapú fizetési megoldás, amelyhez egy internetes vásárlás céljára használható alternatív, ideiglenes kártyaszám kerül létrehozásra, amely csökkentett érvényességi idővel, korlátozottan használható, és előre meghatározott költési limittel rendelkezik.

- *Tárca szolgáltatások*: olyan szolgáltatás, amely lehetővé teszi az ügyfélnek egy vagy több fizetési eszköz adatainak a regisztrálását annak érdekében, hogy több internetes kereskedő felé hajtson végre fizetési műveleteket.

II. cím – Iránymutatások az internetes fizetések biztonságáról

Általános ellenőrzési és biztonsági környezet

Irányítási rend

1. A pénzforgalmi szolgáltatóknak az internetes pénzforgalmi szolgáltatásokra vonatkozó hatályos biztonsági politikát kell alkalmazniuk, és azt rendszeresen felül kell vizsgálniuk.

1.1 A biztonsági politikát megfelelően dokumentálni kell, rendszeresen felül kell vizsgálni (a 2.4. iránymutatás szerint), és a felső vezetésnek jóvá kell hagynia. Tartalmaznia kell a biztonsági célkitűzések és a kockázatvállalási hajlandóság meghatározását.

1.2 A biztonsági szabályozásnak meg kell határoznia a feladat- és felelősségi köröket, beleértve a kockázatkezelési funkciót, melynek közvetlen jelentési kötelezettsége van az igazgatótanács felé, valamint az internetes pénzforgalmi szolgáltatások jelentési kötelezettségeit, beleértve az érzékeny adatok kezelésével kapcsolatos kockázatelemzést, kontrollokat és kockázatcsökkentést.

Kockázatértékelés

2. A pénzforgalmi szolgáltatóknak a szolgáltatás(ok) bevezetése előtt és azt követően rendszeresen alapos kockázatelemzést kell végezniük az internetes fizetések és az azokhoz kapcsolódó szolgáltatások biztonságára vonatkozóan, és dokumentálniuk kell ezeket..

2.1 A pénzforgalmi szolgáltatóknak a kockázatkezelési feladatkört ellátó szervezeti egységükkel el kell végeztetniük és dokumentáltatniuk kell az internetes fizetések és az azokhoz kapcsolódó szolgáltatások részletes kockázatelemzését. A pénzforgalmi szolgáltatóknak a már nyújtott vagy nyújtani kívánt internetes pénzforgalmi szolgáltatásokkal kapcsolatos biztonsági fenyegetések folyamatos monitorozása során az alábbiakat kell figyelembe venniük: t: i) az alkalmazott technológiai megoldások, ii) a külső szolgáltatókhoz kiszervezett szolgáltatások és iii) az ügyfelek technikai környezete. A pénzforgalmi szolgáltatóknak meg kell vizsgálniuk mind a saját oldalukon[4], mind az ügyfeleik oldalán[5] a választott technológiai platformokkal, alkalmazás architektúrával, programozási technikákkal és eljárásokkal kapcsolatban jelentkező kockázatokat, valamint a biztonsági incidensek nyomon követésének eredményeit (lásd a 3. iránymutatást).

2.2 A kockázatelemzés alapján a pénzforgalmi szolgáltatóknak meg kell határozniuk, hogy vajon szükséges-e, és ha igen, milyen mértékben szükséges változtatni a

[4] Úgymint a rendszer fogékonysága olyan támadásokra, mint a fizetési munkamenet eltérítése, a kódbeszúrás, az oldalközi szkriptelés, a puffer túlcsordulás, stb.

[5] Ezek a kockázatok a multimédia alkalmazások, böngészőbe beépülő modulok, keretek, külső hivatkozások, stb. használatához kapcsolódnak.

meglévő biztonsági intézkedéseken, az alkalmazott technológiákon és a kínált eljárásokon vagy szolgáltatásokon. A pénzforgalmi szolgáltatóknak figyelembe kell venniük, hogy mennyi időt vesz igénybe a változtatások végrehajtása (az ügyfelek körében történő bevezetést beleértve), és megfelelő ideiglenes intézkedéseket kell hozniuk a biztonságot befolyásoló események és a csalás, valamint a potenciális zavaró események előfordulásának minimalizálása érdekében.

2.3 A kockázatértékelésnek ki kell terjednie az érzékeny pénzforgalmi adatok védelmére.

2.4 A pénzforgalmi szolgáltatónak felül kell vizsgálniuk a kockázati forgatókönyveket és a meglévő biztonsági intézkedéseket a szolgáltatást érintő minden jelentős incidens után, az infrastruktúrát vagy eljárást érintő minden jelentős módosítás előtt, valamint a kockázatok monitorozása révén azonosított új fenyegetések esetén. Ezen felül a kockázatelemzés átfogó felülvizsgálatát évente el kell végezni. A kockázatelemzés és a felülvizsgálat eredményét jóváhagyás céljából a felső vezetés elé kell terjeszteni.

Incidensek figyelemmel kísérése és jelentése

3. A pénzforgalmi szolgáltatóknak biztosítaniuk kell a biztonságot befolyásoló események – az ügyfelek biztonsággal kapcsolatos panaszait is ideértve – következetes és integrált módon történő figyelemmel kísérését, kezelését és utánkövetését. A pénzforgalmi szolgáltatóknak ki kell alakítaniuk az ilyen eseményekkel kapcsolatos felsővezetői tájékoztatást, illetve a fizetés biztonságát befolyásoló jelentős esemény bekövetkezése esetén az illetékes hatóságok értesítésére szolgáló eljárást.

3.1 A pénzforgalmi szolgáltatóknak kidolgozott folyamattal kell rendelkezniük a biztonsági incidensek és a biztonsággal kapcsolatos ügyfélpanaszok figyelemmel kísérésére, kezelésére és nyomon követésére, valamint a vezetőség felé történő jelentésére.

3.2 A pénzforgalmi szolgáltatóknak kidolgozott eljárással kell rendelkezniük az illetékes hatóságok (vagyis a felügyeleti, felvigyázási és az adatvédelmi hatóságok) azonnali értesítésére az általuk nyújtott pénzforgalmi szolgáltatásokat érintő, fizetés biztonságát befolyásoló jelentős esemény bekövetkezése esetén.

3.3 A pénzforgalmi szolgáltatóknak eljárással kell rendelkezniük a megfelelő bűnüldöző szervekkel való együttműködésre jelentős fizetésbiztonsági incidensek esetén, beleértve az érzékeny adatok illetéktelen kezekbe jutását is.

3.4 Az elfogadó pénzforgalmi szolgáltatóknak szerződésben kell kötelezniük az internetes kereskedőket, melyek érzékeny fizetési adatokat tárolnak, dolgoznak fel és továbbítanak, hogy jelentős fizetésbiztonsági incidensek esetén, beleértve az érzékeny

adatok illetéktelen kezekbe jutását is, mind velük, mind a bűnüldöző szervekkel együttműködjenek. Amennyiben a pénzforgalmi szolgáltató tudomására jut, hogy az internetes kereskedő nem működik együtt a szerződésben előírt módon, lépéseket kell tennie e szerződéses kötelezettség betartatása érdekében, vagy fel kell bontania a szerződést.

A kockázatok kezelése és mérséklése

4. A pénzforgalmi szolgáltatóknak a saját biztonsági politikájukkal összhangban álló biztonsági intézkedéseket kell hozniuk az azonosított kockázatok mérséklése érdekében. Ezekbe az intézkedésekbe többrétegű biztonságvédelmet kell beépíteni, ami azt jelenti, hogy az egyik védelmi vonalon átjutott támadót a következő védelmi vonal feltartóztatja („mélységi védelem").

4.1 Az internetes pénzforgalmi szolgáltatások kialakítása, fejlesztése és működtetése során a pénzforgalmi szolgáltatóknak különös figyelmet kell fordítaniuk az információtechnológiai (IT) környezeteken (például a fejlesztési, tesztelési és éles üzemi környezeteken) belüli feladatok megfelelő elkülönítésére és a megbízható személyazonosság- és hozzáférés-kezelés alapját képező "legkisebb jogosultság" elvének megfelelő érvényesítésére.[6]

4.2 A pénzforgalmi szolgáltatóknak megfelelő biztonsági megoldásokat kell alkalmazniuk, amelyek lehetővé teszik a hálózatok, weboldalak, szerverek és kommunikációs kapcsolatok visszaélések vagy támadások elleni védelmét. A szerverek felesleges funkcióit le kell tiltani, ezáltal erősítve a szerverek védelmét és csökkentve vagy megszűntetve a sebezhetőségüket. A különféle alkalmazások szükséges adatokhoz és erőforrásokhoz való hozzáférését a "legkisebb jogosultság" elvét követve a lehető legnagyobb mértékben korlátozni kell. A „hamis" (a pénzforgalmi szolgáltatók jogszerűen üzemeltetett weboldalaihoz hasonló) weboldalak használatának a korlátozása érdekében az internetes pénzforgalmi szolgáltatásokat kínáló fizetési oldalaknak a pénzforgalmi szolgáltató nevére kiállított kiterjesztett ellenőrzésű (EV) tanúsítványt vagy ahhoz hasonló egyéb hitelesítési módszert kell használniuk.

4.3 A pénzforgalmi szolgáltatóknak megfelelő folyamatokat kell működtetniük, amelyek révén figyelemmel kísérhetik, nyomon követhetik és korlátozhatják a hozzáférést i) az érzékeny fizetési adatokhoz és ii) a kritikus logikai és fizikai erőforrásokhoz, így például a hálózatokhoz, rendszerekhez, adatbázisokhoz, biztonsági modulokhoz, stb. A pénzforgalmi szolgáltatóknak megfelelő naplókat és eseménynaplókat kell létrehozniuk, tárolniuk és elemezniük.

[6] "A rendszerben minden programnak és a minden jogosultsággal rendelkező felhasználónak a feladat ellátásához szükséges legalacsonyabb jogosultsággal kell működnie." Lásd J.H. Saltzer (1974), „Protection and the Control of Information Sharing in Multics", Communications of the ACM, 17. évfolyam, 7. szám, 388. o.

4.4 A pénzforgalmi szolgáltatóknak biztosítaniuk kell a lehető legkevesebb személyes adat összegyűjtését (data minimisation) az internetes fizetési szolgáltatások tervezése[7], fejlesztése és üzemeltetése során: az alaptevékenység elengedhetetlen részeként minimalizálni kell a bizalmas fizetési adatok[8] gyűjtését, továbbítását, feldolgozását, tárolását, archiválását és megjelenítését.

4.5 Az internetes pénzforgalmi szolgáltatásokra vonatkozó biztonsági intézkedéseket a kockázatkezelési feladatkört ellátó szervezeti egység felügyelete alatt tesztelni kell annak érdekében, hogy megbízhatók és hatékonyak legyenek. Minden változást a hivatalos változáskezelési eljárás keretében kell végrehajtani, amely biztosítja a változások megfelelő módon történő megtervezését, tesztelését, dokumentálását és engedélyezését. A végrehajtott változások és a figyelembe vett biztonsági veszélyek alapján a teszteket rendszeres időközönként meg kell ismételni, amelynek során figyelembe kell venni a lényeges és ismert lehetséges támadások forgatókönyveit.

4.6 A pénzforgalmi szolgáltató internetes pénzforgalmi szolgáltatásokra vonatkozó biztonsági intézkedéseit megbízhatóságuk és hatékonyságuk biztosítása érdekében időszakosan ellenőrizni kell. Az internetes pénzforgalmi szolgáltatások megvalósítását és működését ugyancsak ellenőrizni kell. Az ellenőrzések gyakoriságát és fókuszát az érintett biztonsági kockázatok figyelembevételével, azokkal arányosan kell meghatározni. Az ellenőrzéseket megbízható és független (belső vagy külső) szakértőknek kell elvégezni. A szakértők semmilyen módon nem vehetnek részt a pénzforgalmi szolgáltató által nyújtott internetes pénzforgalmi szolgáltatások fejlesztésében, megvalósításában vagy operatív irányításában.

4.7 Amennyiben a pénzforgalmi szolgáltató kiszervezi az internetes fizetési szolgáltatások biztonságával kapcsolatos feladatköröket, a szerződésnek az ezen iránymutatásokban foglalt elvek és útmutatások betartását előíró rendelkezéseket is tartalmaznia kell.

4.8 Az elfogadói tevékenységet folytató pénzforgalmi szolgáltatóknak szerződésben kell kötelezniük az érzékeny fizetési adatokat kezelő (vagyis tároló, feldolgozó vagy továbbító) internetes kereskedőket arra, hogy a 4.1–4.7. iránymutatásokkal összhangban az IT infrastruktúrájukra vonatkozó biztonsági intézkedéseket hozzanak az érzékeny fizetési adatok rendszereiken keresztül történő ellopásának az elkerülése érdekében. Amennyiben a pénzforgalmi szolgáltató tudomására jut, hogy az internetes kereskedő nem hozta meg az előírt biztonsági intézkedéseket, lépéseket kell tennie a szerződéses kötelezettség betartatása érdekében, vagy fel kell bontania a szerződést.

[7] Beépített adatvédelem.

[8] Az adatminimalizálás az adott feladat elvégzéséhez szükséges lehető legkevesebb személyes adat gyűjtésének az elvére utal.

Nyomon követhetőség

5. A pénzforgalmi szolgáltatóknak rendelkezniük kell olyan folyamatokkal, amelyek egyaránt biztosítják valamennyi művelet, valamint az elektronikus csatornán benyújtott meghatalmazás nyomon követhetőségét.

    5.1 A pénzforgalmi szolgáltatóknak gondoskodniuk kell arról, hogy az általuk nyújtott szolgáltatás magába foglalja a tranzakciókra és az elektronikus csatornán benyújtott meghatalmazásokra (*e-mandate*) vonatkozó adatok részletes naplózásával kapcsolatos biztonsági mechanizmusokat, ideértve a tranzakciók egymásutániságát jelző számsorozatot, a tranzakciós adatok keletkezési idejét bizonyító időbélyegeket, a meghatározott paraméterek változásait, valamint a tranzakciókra és az elektronikus csatornán benyújtott meghatalmazásokra vonatkozó adatokhoz való hozzáférést.

    5.2 A pénzforgalmi szolgáltatók által megvalósított naplózásnak lehetővé kell tennie a tranzakciós adatok és az elektronikus felhatalmazások felvitelének, módosításának vagy törlésének nyomon követését.

    5.3 A pénzforgalmi szolgáltatóknak képesnek kell lenniük hozzáférni és elemezni a tranzakciós és elektronikus felhatalmazási adatokat, és rendelkezniük kell olyan eszközzel, amellyel képesek a naplóadatok elemezni. Ezekhez az eszközökhöz csak a felhatalmazott munkavállalók férjenek hozzá.

Az internetes fizetésekre vonatkozó különleges ellenőrzési és biztonsági intézkedések

Előzetes ügyfél-azonosítás, tájékoztatás

6. Az ügyfeleket a pénzmosás elleni európai jogszabályokkal [9] összhangban megfelelően azonosítani kell, és a szolgáltatásokhoz való hozzáférés biztosítását megelőzően megerősítést kell kérni tőlük arra vonatkozóan, hogy a szolgáltatások igénybevételével internetes fizetési műveleteket kívánnak végrehajtani. A pénzforgalmi szolgáltatóknak kielégítő „előzetes”, „rendszeres” vagy adott esetben „eseti” tájékoztatást kell adniuk az ügyfélnek a biztonságos internetes fizetési műveletek végrehajtásához szükséges feltételekről (például berendezés, eljárások) és a kapcsolódó kockázatokról.

[9] Például az Európai Parlament és a Tanács 2005/60/EK irányelve (2005. október 26.) a pénzügyi rendszereknek a pénzmosás, valamint terrorizmus finanszírozása céljára való felhasználásának megelőzéséről. Hl L 309, 2005.11.25., 15-36. o. Lásd még a Bizottság 2006/70/EK irányelvét (2006. augusztus 1.) a „politikai közszereplők” fogalmát, valamint az egyszerűsített ügyfél-átvilágítási eljárások és az alkalmi vagy nagyon korlátozott alapon folytatott pénzügyi tevékenység alapján nyújtott mentesség technikai követelményeit illetően a 2005/60/EK európai parlamenti és tanácsi irányelvre vonatkozó végrehajtási intézkedések megállapításáról. HL L 214, 2006.8.4., 29-34. o.

6.1 A pénzforgalmi szolgáltatóknak gondoskodniuk kell arról, hogy az internetes pénzforgalmi szolgáltatásokhoz való hozzáférés biztosítását megelőzően az ügyfél átessen az ügyfél-átvilágítási eljáráson, és benyújtsa a személyazonosságát igazoló megfelelő dokumentumokat[10] és a kapcsolódó információkat.[11]

6.2 A pénzforgalmi szolgáltatóknak gondoskodniuk kell arról, hogy az ügyfélnek adott előzetes tájékoztatás[12] tartalmazza az internetes fizetési szolgáltatások konkrét részleteit. Ezeknek adott esetben a következőket kell magukban foglalniuk:

- egyértelmű tájékoztatás az ügyfél által használt berendezésre, szoftverre vagy egyéb szükséges eszközre (például vírusirtó szoftver, tűzfal) vonatkozó követelményekről;

- a személyre szóló biztonsági hitelesítő adatok helyes és biztonságos használatára vonatkozó útmutatás;

- tranzakciók ügyfél általi kezdeményezésére és jóváhagyására és/vagy a tájékoztatáskérésre szolgáló eljárás lépésről lépésre történő ismertetése, az egyes lépések megtételének a következményeit is beleértve;

- az ügyfél rendelkezésére bocsátott valamennyi hardver és szoftver helyes és biztonságos használatára vonatkozó útmutatás;

- a személyre szabott biztonsági azonosító adatok vagy a bejelentkezéshez illetve a tranzakciók végrehajtásához szükséges hardverek vagy szoftverek elvesztése vagy ellopása esetén követendő eljárások leírása;

- a visszaélés észlelése vagy gyanújának felmerülése esetén követendő eljárások;

- a pénzforgalmi szolgáltató és az ügyfél internetes fizetési szolgáltatás használatával kapcsolatos köztelezettségeinek és felelősségeinek az ismertetése.

6.3 A pénzforgalmi szolgáltatóknak olyan keretszerződést kell kötniük az ügyféllel, amely kimondja, hogy a pénzforgalmi szolgáltató biztonsági aggályokra hivatkozva letilthat egy adott műveletet vagy a fizetési eszközt[13]. A szerződésben a pénzforgalmi szolgáltatásokról szóló irányelvben foglaltakkal összhangban meg kell

[10] Például útlevél, személyazonosító igazolvány vagy fokozott biztonságú elektronikus aláírás.

[11] Az ügyfél-azonosítási eljárást a hatályos pénzmosás elleni jogszabályokban meghatározott kivételek sérelme nélkül kell végrehajtani. A pénzforgalmi szolgáltatóknak nem kell külön ügyfél-azonosítási folyamatot alkalmazni az internetes pénzforgalmi szolgáltatások esetében, amennyiben az adott ügyfél azonosítását már elvégezték, például más meglévő, fizetéssel kapcsolatos szolgáltatások céljára vagy számlanyitáskor.

[12] Ez a tájékoztatás kiegészíti a pénzforgalmi szolgáltatásokról szóló irányelv 42. cikkét, amely meghatározza, hogy a pénzforgalmi szolgáltatónak milyen tájékoztatást kell adnia a pénzforgalmi szolgáltatást igénybe vevőnek a pénzforgalmi szolgáltatások nyújtására vonatkozó szerződés megkötése előtt.

[13] Lásd a pénzforgalmi szolgáltatásokról szóló irányelv fizetési eszköz használatára vonatkozó korlátozásokról szóló 55. cikkét.

határozni az ügyfél értesítésének a módját és feltételeit, valamint azt, hogy az ügyfél hogyan léphet kapcsolatba a pénzforgalmi szolgáltatóval az internetes fizetési művelet vagy a szolgáltatás letiltásának a feloldása végett.

Erős ügyfél-hitelesítés

7. Az internetes fizetések kezdeményezésének, valamint az érzékeny fizetési adatokhoz való hozzáférésnek a védelme érdekében erős ügyfél-hitelesítést kell használni. A pénzforgalmi szolgáltatóknak az ezen iránymutatásokban szereplő meghatározásnak megfelelő erős ügyfél-hitelesítési eljárással kell rendelkezniük.

7.1 [CT/elektronikus meghatalmazás/elektronikus pénz] A pénzforgalmi szolgáltatóknak erős ügyfél-hitelesítést kell végezniük az internetes fizetések ügyfél általi jóváhagyása (a kötegelt CT-ket is beleértve), és az elektronikus beszedési megbízások („direct debit" automatikus terhelés) kiadása vagy módosítása során. A pénzforgalmi szolgáltatók a következők esetében fontolóra vehetik alternatív ügyfél-hitelesítési intézkedések elfogadását:

- az ügyfél korábban létrehozott fehér listáin szereplő megbízható kedvezményezettek felé irányuló kimenő tranzakciók;
- ugyanazon ügyfél ugyanannál a pénzforgalmi szolgáltatónál vezetett két számlája közötti tranzakciók;
- ugyanazon a pénzforgalmi szolgáltatón belüli átutalások, melyeket a tranzakciókockázat-elemzés megengedhetőnek tart;
- a pénzforgalmi szolgáltatásokról szóló irányelvben említett kis összegű fizetési műveletek.[14]

7.2 Az érzékeny fizetési adatokhoz történő hozzáférés vagy azok módosítása (beleértve a fehér listák készítését és módosítását is) esetén erős ügyfél-hitelesítés szükséges. Amennyiben egy pénzforgalmi szolgáltató tisztán tanácsadói szolgáltatásokat nyújt, melyekben nem érintettek érzékeny ügyfél és fizetési adatok - mint pl. a kártyaadatok, melyekkel könnyen lehet csalást elkövetni -, a pénzforgalmi szolgáltató kockázatelemzés alapján saját hitelesítési követelményeit módosíthatja.

7.3 [kártyák] A kártyával végrehajtott tranzakciókhoz minden kártyakibocsátó pénzforgalmi szolgáltatónak biztosítania kell a kártyabirtokos erős hitelesítésének a támogatását. Minden kibocsátott kártyának technikailag alkalmasnak (regisztrálva) kell lennie az erős hitelesítéssel való használatra.

[14] Lásd a kis összegű fizetésekre szolgáló fizetési eszközök pénzforgalmi szolgáltatásokról szóló irányelv 34. cikke (1) bekezdésében és 53. cikke (1) bekezdésében szereplő meghatározását.

7.4 [kártyák] Az elfogadási szolgáltatásokat kínáló pénzforgalmi szolgáltatóknak biztosítaniuk kell azoknak a technikai megoldásoknak a támogatását, amelyek lehetővé teszik a kibocsátó számára a kártyabirtokosok erős hitelesítésének az elvégzését azokban a kártyás fizetési rendszerekben, amelyekben az elfogadó részt vesz.

7.5 [kártyák] Az elfogadói szolgáltatást kínáló pénzforgalmi szolgáltatók írják elő az internetes kereskedőik számára, hogy támogassák azoknak a technikai megoldásokat, amelyek lehetővé teszik a kártyakibocsátó számára a kártyabirtokos erős hitelesítését kártyás tranzakciók interneten keresztül történő végrehajtásához. Olyan előre meghatározott tranzakciók esetében, amelyek – például kockázatelemzés alapján vagy a pénzforgalmi szolgáltatásokról szóló irányelvben meghatározott kis értékű fizetési műveletek miatt – alacsony kockázattal járnak, fontolóra vehető alternatív hitelesítési intézkedések elfogadása.

7.6 [kártyák] A tárca szolgáltatásokat nyújtó szolgáltatóknak a szolgáltatás keretében elfogadott kártyás fizetési rendszerekre vonatkozóan elő kell írniuk, hogy a kártyakibocsátó erős hitelesítést végezzen, amikor a jogos birtokos első alkalommal regisztrálja a kártyaadatokat.

7.7 A tárca szolgáltatást nyújtó szolgáltatóknak erős ügyfél-hitelesítést kell alkalmazniuk, amikor az ügyfél bejelentkezik a tárca fizetési szolgáltatásba vagy kártyatranzakciót hajt végre az interneten. Alternatív ügyfél-hitelesítési eljárást előre meghatározott alacsony kockázati kategóriába eső tranzakciók esetében alkalmazhatnak, pl. tranzakció alapú kockázatelemzés alapján, vagy a pénzforgalmi szolgáltatásokról szóló irányelvben meghatározott kis értékű tranzakciók esetében.

7.8 [kártyák] A virtuális kártyák esetében az első regisztrációnak biztonságos és megbízható környezetben kell történnie.[15] Az interneten kibocsátott virtuális kártyák adatainak generálása erős ügyfél-hitelesítés mellett történjen. .

7.9 A pénzforgalmi szolgáltatóknak biztosítani kell a megfelelő kétoldalú hitelesítést az internetes kereskedőkkel történő kommunikáció során, amikor a fizetés kezdeményezése és az érzékeny fizetési adatokhoz való hozzáférés megtörténik.

[15] A következőket foglalják magukba azok a pénzforgalmi szolgáltató felelősségi körébe tartozó környezetek, ahol az ügyfél és a szolgáltatást kínáló pénzforgalmi szolgáltató megfelelő hitelesítése, valamint a bizalmas/különleges adatok védelme biztosított: i) a pénzforgalmi szolgáltató helyiségei; ii) internetes banki műveletek végzésére szolgáló vagy egyéb biztonságos weboldal, például ahol a kártyás fizetési rendszer irányító szerve többek között a 4. iránymutatásban meghatározottakhoz hasonló biztonsági jellemzőket kínál; vagy iii) bankautomata (ATM) szolgáltatások. (Az ATM-ek esetében erős ügyfél-hitelesítés szükséges. Ilyen hitelesítést tesz lehetővé a chipkártya és a PIN-kód vagy a chipkártya és a biometriai azonosítás együttes alkalmazása).

Az ügyfélnek átadott azonosító eszközök és/vagy szoftverek igénylése és biztosítása

8. A pénzforgalmi szolgáltatóknak gondoskodniuk kell arról, hogy az internetes fizetési szolgáltatás igénybevételéhez szükséges hitelesítési eszközök ügyfelek általi igénylése és az eszközök első alkalommal történő biztosítása és/vagy a fizetéssel kapcsolatos szoftverek ügyfeleknek történő átadása biztonságosan történjen.

8.1 A hitelesítő eszközök és/vagy fizetéshez kapcsolódó szoftverek ügyfelek általi igénylésének és az ügyfelekhez történő eljuttatásának követelményei:

- A kapcsolódó eljárásokat biztonságos és megbízható környezetben kell végrehajtani, figyelembe véve a nem a pénzforgalmi szolgáltató ellenőrzése alatt álló eszközökhöz kapcsolódó lehetséges kockázatokat.

- A személyhez kapcsolt biztonsági hitelesítő adatok, a fizetéssel kapcsolatos szoftverek és az internetes fizetéssel kapcsolatos valamennyi személyre szabott eszköz átadása során hatékony és biztonságos eljárásokat kell alkalmazni. Az interneten keresztül rendelkezésre bocsátott szoftvereket a pénzforgalmi szolgáltatónak digitális aláírással kell ellátnia, hogy az ügyfél számára lehetővé tegye azok eredetiségének és sértetlenségének az ellenőrzését.

- [kártyák] Kártyás tranzakciók esetében az ügyfélnek meg kell adni a lehetőséget, hogy erős hitelesítést igényelhessen az adott internetes vásárlástól függetlenül. Ha van lehetőség az erős hitelesítés igénybe vételére internetes vásárlás során, akkor az azonosítás aktiválása az ügyfél biztonságos és megbízható környezetbe irányításával történjen meg.

8.2 [kártyák] A kibocsátóknak aktívan ösztönözniük kell a kártyabirtokosokat az erős hitelesítés igénylésére, és az igénylés megkerülését csak néhány olyan kivételes esetben engedhetik meg a kártyabirtokosoknak, amikor azt az adott kártyás fizetési művelethez kapcsolódó kockázat indokolja.

Bejelentkezési kísérletek, időtúllépés, a hitelesítés érvényessége

9. A pénzforgalmi szolgáltatóknak korlátozniuk kell a belépési vagy hitelesítési kísérletek számát, meg kell határozniuk az időtúllépés internetes pénzforgalmi szolgáltatásokra vonatkozó szabályait, valamint a hitelesítés érvényességének időbeli korlátját.

9.1 A hitelesítési célra használt egyszer használatos jelszavak (OTP) esetében a pénzforgalmi szolgáltatóknak gondoskodniuk kell arról, hogy a jelszó érvényességi időtartama a szükséges minimumra korlátozódjon.

9.2 A pénzforgalmi szolgáltatóknak meg kell határozniuk a sikertelen belépési vagy hitelesítési kísérletek maximális számát, amelyek túllépése esetén az internetes fizetési szolgáltatáshoz való hozzáférés (ideiglenesen vagy véglegesen) letiltásra

kerül. A letiltott internetes pénzforgalmi szolgáltatások újbóli aktiválására biztonságos eljárást kell alkalmazniuk.

9.3 A pénzforgalmi szolgáltatóknak meg kell határozniuk azt a maximális időtartamot, amely túllépése esetén automatikusan megszakad az internetes fizetési szolgáltatás inaktív munkamenete.

Tranzakciók figyelemmel kísérése

10. A pénzforgalmi szolgáltató végleges engedélyének a megadása előtt a tranzakciók figyelemmel kísérésére szolgáló mechanizmusokat kell működtetni a csalárd fizetési tranzakciók megelőzése, észlelése és letiltása céljából; a gyanús vagy nagy kockázatú tranzakciókat egyedi átvilágítási és ellenőrzési eljárásnak kell alávetni. Az elektronikus csatornán adott megbízásokra vonatkozóan is ugyanilyen biztonsági monitoring és engedélyező mechanizmusokkal kell rendelkezni.

10.1 A pénzforgalmi szolgáltatók alkalmazzanak csalásfelderítésre és -megelőzésre alkalmas rendszereket a gyanús tranzakciók vagy elektronikus meghatalmazások azonosítására, mielőtt az adott tranzakciót a pénzforgalmi szolgáltató véglegesen jóváhagyná. Ezek a rendszerek alapulhatnak például paraméterezett szabályokon (például a nyilvánosságra került vagy lopott kártyaadatok fekete listája), valamint monitorozniuk kell az ügyfelek vagy az ügyfelek által használt belépési eszközök rendellenes viselkedésmintáit (például az internetprotokoll- (IP-) cím[16] vagy az IP-címtartomány internetes fizetési szolgáltatás munkamenete során történő megváltozását, ami néha az IP-cím szerinti földrajzi hely ellenőrzésével meghatározható,[17] az adott ügyfélre jellemzőtől eltérő internet kereskedői kategóriákat vagy a szokásostól eltérő tranzakciós adatokat, stb.). Ezeknek a rendszereknek képesnek kell lenniük továbbá a munkamenet során bekövetkező, rosszindulatú szoftver által okozott fertőzés jeleinek az észlelésére (pl. ha a felhasználó helyett egy script végzi a hitelesítést), valamint az ismert csalási forgatókönyvek felismerésére. A monitorozó rendszer terjedelmét, összetettségét és rugalmasságát úgy kell meghatározni, hogy összhangban álljon a kockázatértékelés eredményével, és a vonatkozó adatvédelmi jogszabályoknak is megfeleljen.

10.2 Az elfogadó pénzforgalmi szolgáltatóknak a csalások észlelésére és megelőzésére szolgáló rendszereket kell működtetniük abból a célból, hogy figyelemmel kísérjék az internetes kereskedők tevékenységét.

[16] Az IP-cím az internethez csatlakozó számítógépek azonosítására szolgáló egyedi numerikus kód.

[17] A GeoIP cím ellenőrzés a kibocsátó ország és a műveletet kezdeményező felhasználó IP-címe közötti megfelelés ellenőrzésére szolgál.

10.3 A pénzforgalmi szolgáltatóknak megfelelő időn belül kell elvégezniük a tranzakció-átvilágítási és –értékelési eljárásokat, nehogy indokolatlanul késleltessék az érintett fizetési szolgáltatás kezdeményezését és/vagy végrehajtását.

10.4 Amennyiben a pénzforgalmi szolgáltató kockázatokra vonatkozó szabályzata alapján úgy dönt, hogy letilt egy esetlegesen csalárdnak minősített fizetési műveletet, a letiltást csak a biztonsági probléma lehető legrövidebb időn belüli megoldásáig tarthatja fenn.

Az érzékeny fizetési adatok védelme

11. Érzékeny fizetési adatok tárolása, kezelése vagy továbbítása során biztosítani kell azok védelmét.

11.1 Az ügyfelek azonosítására és hitelesítésére (például belépéskor, internetes fizetési művelet kezdeményezésekor és elektronikus csatornán benyújtott meghatalmazás kibocsátása, módosítása vagy törlése esetén) szolgáló adatok teljes körét, valamint az ügyfelek által használt felhasználói felületet (a pénzforgalmi szolgáltató vagy az internetes kereskedő weboldalát) megfelelő módon kell védeni az adatlopás és a jogosulatlan hozzáférés vagy módosítás ellen.

11.2 Érzékeny fizetési adatok interneten történő cseréje során az adatok bizalmas jellegének és sértetlenségének a védelme érdekében a pénzforgalmi szolgáltatóknak a kommunikációs munkamenet egésze alatt biztosítaniuk kell a végpontok közötti titkosítást[18] a kommunikáló felek között, amelyhez erős és széles körben elismert titkosítási technikákat kell alkalmazniuk.

11.3 Az elfogadó szolgáltatásokat kínáló pénzforgalmi szolgáltatóknak ösztönözniük kell a velük szerződésben álló internetes kereskedőket arra, hogy ne tároljanak érzékeny fizetési adatokat. Abban az esetben, ha az internetes kereskedők kezelnek, tárolnak, feldolgoznak vagy továbbítanak érzékeny fizetési adatokat, a pénzforgalmi szolgáltatóknak szerződésben kell kötelezniük őket arra, hogy tegyék meg a szükséges intézkedéseket ezeknek az adatoknak a védelmére. A pénzforgalmi szolgáltatóknak rendszeres ellenőrzéseket kell végezniük, és amennyiben a tudomásukra jut, hogy egy érzékeny fizetési adatokat kezelő internetes kereskedő nem hozta meg az előírt biztonsági intézkedéseket, lépéseket kell tenniük a szerződéses kötelezettség betartatása érdekében, vagy fel kell bontaniuk a szerződést.

[18] A végpontok közötti titkosítás azt jelenti, hogy a titkosítás a forrásvégpontot alkotó rendszernél vagy azon belül, a titkosítás feloldása pedig csak a célvégpontot alkotó rendszernél vagy azon belül történik. ETSI EN 302 109 V1.1.1. (2003-06).

Ügyféltudatosság, az ügyfelek felvilágosítása és az ügyfelekkel folytatott kommunikáció

Ügyféltudatosság és az ügyfelekkel folytatott kommunikáció

12. A pénzforgalmi szolgáltatóknak szükség esetén segítséget és útmutatást kell nyújtaniuk az ügyfeleknek az internetes pénzforgalmi szolgáltatások biztonságos használatához. A pénzforgalmi szolgáltatóknak úgy kell kommunikálniuk az ügyfeleikkel, hogy az ügyfelek biztosak lehessenek a kapott üzenetek hitelességében.

12.1 A pénzforgalmi szolgáltatóknak legalább egy biztonságos csatornát kell biztosítaniuk[19] arra a célra, hogy az ügyfelekkel folyamatos kommunikációt folytassanak az internetes fizetési szolgáltatás helyes és biztonságos használatáról. A pénzforgalmi szolgáltatóknak tájékoztatniuk kell az ügyfeleket erről a csatornáról, és el kell magyarázniuk, hogy a pénzforgalmi szolgáltató nevében az internetes fizetési szolgáltatás helyes és biztonságos használatáról más módon, például e-mailen küldött üzenetek nem megbízhatók. A pénzforgalmi szolgáltatónak felvilágosítást kell adniuk a következőkről:

- az ügyfelek által követendő eljárás abban az esetben, ha (gyaníthatóan) csalárd fizetéseket, az internetes fizetési szolgáltatás munkamenete során tapasztalt gyanús eseményeket vagy rendellenességeket és/vagy a pszichológiai manipulációra[20] irányuló esetleges kísérleteket kívánnak jelenteni a pénzforgalmi szolgáltatónak;

- a következő lépések, vagyis hogyan válaszol a pénzforgalmi szolgáltató az ügyfélnek;

- hogyan értesíti a pénzforgalmi szolgáltató az ügyfelet az (esetlegesen) csalárd tranzakciókról vagy azok kezdeményezésének a megakadályozásáról, illetve hogyan figyelmezteti az ügyfelet a támadások (például adathalász e-mailek) előfordulásáról.

12.2 A pénzforgalmi szolgáltatóknak biztonságos csatornán keresztül kell tájékoztatniuk az ügyfeleket az internetes fizetési szolgálatokkal kapcsolatos biztonsági eljárásokban végrehajtott fejlesztésekről. Minden felmerülő jelentős kockázat esetén (például pszichológiai manipulációra vonatkozó figyelmeztetések) a riasztás céljára is a biztonságos csatornát kell használni.

12.3 A pénzforgalmi szolgáltatóknak ügyfélszolgálatot kell működtetniük az internetes fizetési műveletekkel és a kapcsolódó szolgáltatásokkal kapcsolatos kérdések, panaszok, támogatásra irányuló kérések és rendellenességekre vagy incidensekre

[19] Ilyen például a pénzforgalmi szolgáltató honlapján erre a célra létrehozott postafiók vagy egy biztonságos weboldal.

[20] A pszichológiai manipuláció jelentése ebben a kontextusban: az emberek információszerzés céljából történő (például e-mailen vagy telefonon keresztüli) manipulálására szolgáló technikák vagy közösségi hálózatokról való információgyűjtés csalás vagy számítógéphez vagy hálózathoz való jogosulatlan hozzáférés céljából.

vonatkozó bejelentések fogadására, és az ügyfeleket megfelelően tájékoztatniuk kell arról, hogy az ügyfélszolgálatot hogyan vehetik igénybe.

12.4 A pénzforgalmi szolgáltatóknak az ügyfelek felvilágosítását és tudatosságának növelését célzó programokat kell indítaniuk annak biztosítása érdekében, hogy az ügyfelek tisztában legyenek legalább a következők szükségességével:

- jelszavaik és más bizalmas adataik, biztonsági tokenjeik, személyes és egyéb bizalmas adataik védelme;
- megfelelő gondoskodás a személyes eszközök (például számítógép) biztonságáról biztonsági elemek (vírusirtó, tűzfal, biztonsági javítócsomagok) telepítése és frissítése révén;
- az internetről letöltött szoftverekhez fűződő jelentős veszélyek és kockázatok mérlegelése abban az esetben, ha az ügyfél nem lehet eléggé biztos abban, hogy a szoftver eredeti és nem lett módosítva;
- a pénzforgalmi szolgáltató internetes fizetésre szolgáló hiteles weboldalának a használata.

12.5 Az elfogadó pénzforgalmi szolgáltatóknak meg kell követelniük az internetes kereskedőktől, hogy a fizetéshez kapcsolódó folyamatokat egyértelműen elkülönítsék az online vásárlástól annak érdekében, hogy az ügyfél számára világossá váljon, hogy mikor kommunikál a kereskedővel és mikor a pénzforgalmi szolgáltatóval (ennek lehetséges módja például az ügyfél átirányítása és egy külön ablak megnyitása annak érdekében, hogy a fizetési folyamat elkülönüljön az internetes kereskedő rendszerétől)).

Értesítések, értékhatárok meghatározása

13. A pénzforgalmi szolgáltatóknak meg kell határozniuk az internetes fizetési szolgáltatások értékhatárait, és lehetőségeket biztosíthatnak az ügyfeleknek a kockázatok további korlátozására ezeken az értékhatárokon belül. Ezenkívül figyelmeztetési és ügyfélprofil kezelési szolgáltatásokat is nyújthatnak.

13.1 Mielőtt egy ügyfélnek internetes fizetési szolgáltatásokat nyújtanak, a pénzforgalmi szolgáltatóknak meg kell határozniuk a szolgáltatásokra vonatkozó értékhatárokat[21] (például az egyes fizetési műveletek maximális összegét vagy egy bizonyos időtartamon belüli összesített összeget), és azokról tájékoztatniuk kell az ügyfelet. A pénzforgalmi szolgáltatóknak lehetővé kell tenniük az ügyfelek számára az internetes fizetési funkció letiltását.

[21] Az értékhatárok alkalmazhatók általánosan (vagyis az internetes fizetési műveleteket lehetővé tévő valamennyi fizetési eszközön) vagy egyéni alapon.

Az ügyfél hozzáférése a fizetéskezdeményezés és -végrehajtás státuszára vonatkozó információkhoz

14. A pénzforgalmi szolgáltatóknak vissza kell igazolniuk az ügyfeleik számára a tranzakciók kezdeményezését, és kellő időben az ügyfelek rendelkezésére kell bocsátaniuk a tranzakciók helyes kezdeményezésének, illetve végrehajtásának az ellenőrzéséhez szükséges információkat.

    14.1 [átutalás/ elektronikus csatornán adott megbízás] A pénzforgalmi szolgáltatóknak közel valós idejű lehetőséget kell biztosítaniuk az ügyfeleknek arra, hogy a tranzakciók végrehajtási státuszát és a számlaegyenlegeket bármikor [22] ellenőrizhessék, és ehhez biztonságos és megbízható környezetet kell biztosítaniuk.

    14.2 A részletes elektronikus számlakivonatokat biztonságos és megbízható környezetben kell elérhetővé tenni. Amennyiben a pénzforgalmi szolgáltató arról tájékoztatja az ügyfelet, hogy az elektronikus számlakivonat (például a rendszeres időközönként vagy eseti alapon, művelet végrehajtását követően kibocsátott elektronikus számlakivonatok) más csatornán, például SMS-ben, e-mailen vagy levélben is rendelkezésre áll, érzékeny fizetési adatokat nem, vagy csak olvashatatlan formában közölhet.

III. cím – Záró rendelkezések és végrehajtás

15. Ezeket az iránymutatásokat 01.08.2015-jétől kell alkalmazni.

[22] Kivéve azokat a kivételes alkalmakat, amikor a szolgáltatás műszaki karbantartás miatt vagy jelentős esemény következtében szünetel.

1. melléklet: Bevált gyakorlati példák

A fenti követelmények mellett ezek az iránymutatások bemutatnak néhány bevált gyakorlati példát, amelyek követése a pénzforgalmi szolgáltatók és az érintett piaci szereplők számára javasolt, de nem előírás. A hivatkozás megkönnyítése érdekében egyértelműen meghatározzuk, hogy a példák melyik fejezetekhez tartoznak.

Általános ellenőrzési és biztonsági környezet

Vállalatirányítás

1. bevált gyakorlat: A biztonsági szabályzatot önálló dokumentumba kell foglalni.

A kockázatok kezelése és mérséklése

2. bevált gyakorlat: Az ügyfelek által használt felhasználói felület jogellenes használattal vagy támadásokkal (például böngészőbe közbeékelődő un. „man int he browser” (MitB) típusú támadásokkal) szembeni védelme érdekében a pénzforgalmi szolgáltatók biztonsági eszközöket (például megfelelő védelemmel ellátott eszközöket és/vagy egyedi kialakítású böngészőket) biztosíthatnak.

Nyomon követhetőség

3. bevált gyakorlat: Az elfogadási szolgáltatásokat kínáló pénzforgalmi szolgáltatók szerződésben kötelezhetik a fizetési adatokat tároló internetes kereskedőket arra, hogy a nyomon követhetőséget támogató, megfelelő folyamatokkal rendelkezzenek.

Az internetes fizetésekre vonatkozó különleges ellenőrzési és biztonsági intézkedések

Előzetes ügyfél-azonosítás, tájékoztatás

4. bevált gyakorlat: A feltételek pénzforgalmi szolgáltató általános szolgáltatási szerződésébe való belefoglalása helyett az ügyfél külön szolgáltatási szerződést köthet az internetes fizetési műveletek végzésére vonatkozóan.

5. bevált gyakorlat: A pénzforgalmi szolgáltatók arról is gondoskodhatnak, hogy az ügyfelek megfelelő eszközök útján (például hírlevélben, weboldalon) folyamatosan vagy adott esetben alkalmanként világos és egyértelmű útbaigazítást kapjanak arról, hogy mit kell tenniük a szolgáltatás biztonságos használata érdekében.

Erős ügyfél-hitelesítés

6. bevált gyakorlat: [kártyák] Az internetes kereskedők támogassák a kártyabirtokos kibocsátó általi erős hitelesítését az internetes kártyatranzakciók esetén.

7. bevált gyakorlat: Az ügyfelek kényelme érdekében a pénzforgalmi szolgáltatók fontolóra vehetik azt, hogy egyetlen erős ügyfél-hitelesítési eszközt használjanak minden internetes fizetési szolgáltatáshoz.

8. bevált gyakorlat: Az erős ügyfél-hitelesítés tartalmazhat olyan elemeket, amelyek egy adott összeghez és kedvezményezetthez kötik a hitelesítést. Ez fokozott biztonságot jelenthet az ügyfelek számára a fizetési műveletek engedélyezése során. Az erős hitelesítéshez használt adatok és a tranzakciós adatok összekapcsolását módosításbiztos technológiai megoldással kell lehetővé tenni.

Az érzékeny fizetési adatok védelme

9. bevált gyakorlat: Kívánatos, hogy az érzékeny fizetési adatokat kezelő internetes kereskedők megfelelő képzést biztosítsanak a csalások elleni védekezésért felelős munkatársaik számára, és a képzést rendszeresen naprakésszé tegyék annak érdekében, hogy tartalma érvényes maradjon az állandóan változó biztonsági környezetben.

Az ügyfelek felvilágosítása és az ügyfelekkel folytatott kommunikáció

10. bevált gyakorlat: Kívánatos, hogy az elfogadási szolgáltatásokat kínáló pénzforgalmi szolgáltatók felvilágosító programokat szervezzenek a csalásmegelőzés témakörében a velük szerződésben álló internetes kereskedők számára.

Értesítések, értékhatárok meghatározása

11. bevált gyakorlat: A pénzforgalmi szolgáltatók lehetővé tehetik ügyfeleiknek, hogy a meghatározott értékhatárokon belül beállítsák az internetes fizetési szolgáltatásokra vonatkozó értékhatárokat, amelyhez biztonságos és megbízható környezetet biztosítanak.

12. bevált gyakorlat: A kockázatkezelési szabályzatuk alapján gyanúsnak vagy nagy kockázatúnak minősülő tranzakciók esetén a pénzforgalmi szolgáltatók figyelmeztethetik ügyfeleiket, például telefonhívás vagy sms útján.

13. bevált gyakorlat: A pénzforgalmi szolgáltatók tegyék lehetővé ügyfeleik számára, hogy általános érvényű, személyre szabott szabályokat tudjanak beállítani online fizetési viselkedésük és az ahhoz kapcsolódó szolgáltatásokat illetően például azt, hogy fizetéseiket csak bizonyos előre meghatározott országokból fogják kezdeményezni, és a máshonnan történő tranzakció

indítást blokkolni kell, vagy, hogy meghatározott kedvezményezetteket ún. fehér vagy fekete listára tesznek.