A BIZOTTSÁG (EU) 2018/389 FELHATALMAZÁSON ALAPULÓ RENDELETE

(2017. november 27.)

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

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről szóló, 2015. november 25-i (EU) 2015/2366 európai parlamenti és tanácsi irányelvre [1] és különösen annak 98. cikke (4) bekezdésének második albekezdésére,

mivel:

(1) Az elektronikusan kínált pénzforgalmi szolgáltatásokat biztonságos módon kell teljesíteni, olyan technológiák alkalmazásával, amelyekkel szavatolható a szolgáltatást igénybe vevő biztonságos azonosítása, és a lehető legnagyobb mértékben csökkenthető a csalás kockázata. A hitelesítési eljárásnak általánosságban magában kell foglalnia műveletmegfigyelő mechanizmusokat a pénzforgalmi szolgáltatást igénybe vevők esetében az elveszett, ellopott vagy jogosulatlanul használt személyes hitelesítési adatok használatára irányuló kísérletek észlelése érdekében, valamint azt is biztosítania kell, hogy a pénzforgalmi szolgáltatást igénybe vevő legyen a jogos igénybe vevő, és ezért a személyes hitelesítési adatok rendes felhasználásával jóváhagyását adja a pénzátutaláshoz és a számlainformációihoz való hozzáféréshez. Szükséges meghatározni továbbá azon erős ügyfél-hitelesítés követelményeit, amelyet minden alkalommal alkalmazni kell, amikor a fizető fél online fér hozzá a fizetési számlájához, elektronikus fizetési műveletet kezdeményez vagy a műveleteket távoli csatornán keresztül hajtja végre, ami fizetéssel kapcsolatos csalásokra és más visszaélésekre adhat módot, olyan hitelesítési kód generálásának előírásával, amelynek ellenállónak kell lennie az egészében vagy a kód generálásának alapját képező bármely elem közzétételével történő hamisítás kockázatával szemben.

(2) mivel a csalási módszerek állandóan változnak, az erős ügyfél-hitelesítés követelményeinek lehetővé kell tenniük az elektronikus fizetések biztonságára jelentett új fenyegetések megjelenését kezelő technikai megoldások innovációját. A meghatározandó követelmények tényleges folyamatos végrehajtásának biztosítása érdekében indokolt azt is előírni, hogy az erős ügyfél-hitelesítés alkalmazására és az az alóli kivételre vonatkozó biztonsági intézkedéseket, a személyes hitelesítési adatok bizalmasságának és integritásának megóvását szolgáló intézkedéseket és a közös és biztonságos nyílt kommunikációs standardokat létrehozó intézkedéseket az informatikai biztonság és a fizetések terén szakértelemmel rendelkező, valamint függetlenül működő könyvvizsgálók dokumentálják, rendszeres időközönként teszteljék, értékeljék és ellenőrizzék. Annak érdekében, hogy az illetékes hatóságok nyomon követhessék az ilyen intézkedések felülvizsgálatának minőségét, az említett felülvizsgálatokat kérésre a rendelkezésükre kell bocsátani.

(3) mivel az elektronikus távoli fizetési műveletek magasabb csalási kockázatnak vannak kitéve, szükséges az ilyen műveletek esetében az erős ügyfél-hitelesítésre vonatkozó további követelményeket bevezetni, amelyek biztosítják, hogy az elemek dinamikusan összekapcsolják a műveletet a fizető fél által a művelet kezdeményezésekor megadott összeggel és kedvezményezettel.

(4) A dinamikus összekapcsolás hitelesítési kódok generálásán keresztül lehetséges, ami szigorú biztonsági követelményrendszer alá tartozik. A technológiai semlegesség fenntartása érdekében nem írható elő a hitelesítési kódok végrehajtásához egy konkrét technológia. A hitelesítési kódoknak ezért olyan megoldásokon kell alapulniuk, mint például egyszeri jelszavak generálása és validálása, digitális aláírások vagy egyéb, a hitelesítési elemekben tárolt kulcsokat vagy kriptográfiai anyagot felhasználó, kriptográfiailag alátámasztott érvényesség-megállapítások, mindaddig, amíg a biztonsági követelmények teljesülnek.

[1] HL L 337., 2015.12.23., 35. o.

(5) Külön követelményeket szükséges meghatározni arra a helyzetre, amikor a végső összeg nem ismert az elektronikus távoli fizetési művelet fizető fél általi kezdeményezésének pillanatában, annak biztosítása érdekében, hogy az erős ügyfél-hitelesítés azon maximális összeg szempontjából specifikus legyen, amelyet a fizető fél az (EU) 2015/2366 irányelvben említettek szerint jóváhagyott.

(6) Az erős ügyfél-hitelesítés alkalmazásának biztosítása érdekében szükséges megfelelő biztonsági jellemzőket előírni az erős ügyfél-hitelesítés ismeret kategóriába sorolható elemeire (csak a szolgáltatást igénybe vevő által ismert információ) vonatkozóan, mint például hosszúság vagy összetettség, a birtoklás kategóriába sorolható elemeire (csak a szolgáltatást igénybe vevő által birtokolt dolog) vonatkozóan, mint például algoritmus specifikációk, kulcshosszúság és információs entrópia, és a biológiai tulajdonság kategóriába sorolható elemeit (a szolgáltatást igénybe vevő jellemzője) olvasó eszközökre és szoftverekre vonatkozóan, mint például algoritmus specifikációk, biometrikus érzékelők és sablonvédelmi jellemzők, különösen azon kockázat csökkentése céljából, hogy az említett elemeket jogosulatlan felek feltárják, azokat előttük felfedjék, és azokat használják. Szükséges az azt biztosító követelményeket is megállapítani, hogy az említett elemek egymástól függetlenek legyenek, így az egyikük feltörése nem befolyásolja a többi elem megbízhatóságát, különösen amikor ezen elemek bármelyikét többfunkciós eszközök, azaz olyan eszközök, mint a táblagép vagy a mobiltelefon segítségével használják, amelyek a fizetés teljesítésére vonatkozó utasítás adására és a hitelesítési folyamat során egyaránt használhatók.

(7) Az erős ügyfél-hitelesítésre vonatkozó követelmények a fizető fél által kezdeményezett fizetésekre alkalmazandók, tekintet nélkül arra, hogy a fizető fél természetes személy vagy jogi személy.

(8) Sajátos jellegüknél fogva az anonim készpénz-helyettesítő fizetési eszközök használatával végrehajtott fizetésekre nem vonatkozik az erős ügyfél-hitelesítési kötelezettség. Amennyiben az ilyen eszközök anonimitása szerződés vagy jogszabály alapján megszűnik, a fizetések az (EU) 2015/2366 irányelvből és az ebből a szabályozástechnikai standardból eredő biztonsági követelmények hatálya alá tartoznak.

(9) Az (EU) 2015/2366 irányelvnek megfelelően az erős ügyfél-hitelesítés elve alóli kivételek a kockázati szint, az összeg, a gyakoriság és a fizetési művelet végrehajtásához igénybe vett fizetési csatorna alapján kerültek meghatározásra.

(10) A valamely fizetési számla egyenlegéhez és a legutóbbi műveleteihez érzékeny fizetési adatok közzététele nélkül való hozzáférést, a fizető fél által erős ügyfél-hitelesítés igénybevételével korábban meghatározott vagy megerősített ugyanazon kedvezményezettek részére történő ismétlődő fizetéseket, valamint az ugyanannál a pénzforgalmi szolgáltatónál számlával rendelkező ugyanazon természetes személyek vagy jogi személyek részére történő és tőlük eredő fizetéseket magukban foglaló műveletek alacsony kockázati szintet jelentenek, ezért esetükben lehetősége van a pénzforgalmi szolgáltatóknak arra, hogy ne alkalmazzanak erős ügyfél-hitelesítést. Ettől függetlenül az (EU) 2015/2366 irányelv 65., 66. és 67. cikkével összhangban a megbízásos online átutalási szolgáltatók, a kártyaalapú készpénz-helyettesítő fizetési eszközt kibocsátó pénzforgalmi szolgáltatók és a számlainformációkat összesítő szolgáltatók egy adott pénzforgalmi szolgáltatás nyújtása tekintetében kizárólag a pénzforgalmi szolgáltatás igénybe vevőjének jóváhagyásával kérhetik és kaphatják meg a számlavezető pénzforgalmi szolgáltatótól a szükséges és alapvető információkat. Ezt a jóváhagyást meg lehet adni külön minden egyes információkérés esetében vagy minden egyes kezdeményezendő fizetés esetében, vagy megjelölt fizetési számlákra és a kapcsolódó fizetési műveletekre vonatkozó megbízásként a számlainformációkat összesítő szolgáltatók esetében, a pénzforgalmi szolgáltatást igénybe vevővel kötött szerződéses megállapodásban rögzítettek szerint.

(11) Az értékesítési helyeken történő kis összegű érintéses fizetésekre vonatkozó olyan kivételek, amelyek az erős ügyfél-hitelesítés alkalmazása nélküli, egymást követő műveletek maximális számát vagy egymást követő műveletek bizonyos rögzített maximális értékét is figyelembe veszik, lehetővé teszik a felhasználóbarát és alacsony kockázatú pénzforgalmi szolgáltatások kifejlesztését, és ezért azokról rendelkezni kell. Emellett indokolt kivételről rendelkezni a felügyelet nélküli terminálóknál kezdeményezett elektronikus fizetési műveletek esetében, ahol az erős ügyfél-hitelesítés operatív okokból (például a fizetőkapuknál a sorok és az esetleges balesetek elkerülése érdekében, vagy egyéb biztonsági vagy védelmi kockázatok miatt) nem mindig alkalmazható könnyen.

(12) Az értékesítés helyén történő kis összegű érintéses fizetésekre vonatkozó kivételhez hasonlóan megfelelő egyensúlyt kell teremteni a távoli fizetések fokozott biztonságához fűződő érdek és az elektronikus kereskedelem területén a fizetések felhasználóbarát jellege és hozzáférhetősége iránti igény között. Ezen elvekkel összhangban prudens módon kell meghatározni a küszöbértékeket, amelyek alatt nincs szükség az erős ügyfél-hitelesítés alkalmazására, hogy csak a kis összegű online vásárlásokra terjedjenek ki. Az online vásárlásokra vonatkozó küszöbértékeket még körültekintőbben kell meghatározni, figyelembe véve, hogy a személy nincs fizikailag jelen a vásárláskor, ami valamivel nagyobb biztonsági kockázatot jelent.

(13) Az erős ügyfél-hitelesítésre vonatkozó követelmények a fizető fél által kezdeményezett fizetésekre alkalmazandók, tekintet nélkül arra, hogy a fizető fél természetes személy vagy jogi személy. Számos vállalati fizetést célzott folyamatok vagy protokollok segítségével kezdeményeznek, amelyek garantálják azt a magas szintű fizetési biztonságot, amelyet az (EU) 2015/2366 irányelv az erős ügyfél-hitelesítés alkalmazása révén el kíván érni. Amennyiben az illetékes hatóságok megállapítják, hogy a szóban forgó, kizárólag nem fogyasztónak minősülő fizető felek rendelkezésére bocsátott fizetési folyamatok vagy protokollok a biztonság tekintetében megvalósítják az (EU) 2015/2366 irányelv célkitűzéseit, a pénzforgalmi szolgáltatók ezen folyamatok vagy protokollok kapcsán mentesíthetők az erős ügyfél-hitelesítési követelmények alól.

(14) Az olyan valós idejű műveletikockázat-elemzések esetében, amelyek egy fizetési műveletet alacsony kockázatúnak sorolnak be, szintén helyénvaló kivételt bevezetni az erős ügyfél-hitelesítést alkalmazni nem kívánó pénzforgalmi szolgáltató számára, mégpedig olyan hatékony és kockázatalapú követelmények elfogadása révén, amelyek biztosítják a pénzforgalmi szolgáltatást igénybe vevő pénzeszközeinek és személyes adatainak biztonságát. Az említett kockázatalapú követelményeknek a távoli fizetésekre vonatkozóan kiszámított csalási arányokon alapuló pénzbeli küszöbértékekkel kell kombinálniuk a kockázatelemzés azt megerősítő eredményeit, hogy a fizető fél esetében nem azonosítottak a normálistól eltérő költési vagy viselkedési mintát, figyelembe véve egyéb kockázati tényezőket is, beleértve a fizető fél és a kedvezményezett elhelyezkedésére vonatkozó információkat. Amennyiben a valós idejű műveletikockázat-elemzés alapján egy fizetés nem minősíthető alacsony kockázati szintet jelentőnek, a pénzforgalmi szolgáltatónak vissza kell térnie az erős ügyfél-hitelesítéshez. Az ilyen kockázatalapú kivétel maximális értékét nagyon alacsony kapcsolódó csalási arányt biztosító módon kell meghatározni, többek között a pénzforgalmi szolgáltató összes fizetési műveletének csalási arányával egy bizonyos időszakon belül és gördülő alapon történő összehasonlítás révén, beleértve az erős ügyfél-hitelesítés segítségével hitelesített műveleteket is.

(15) A hatékony végrehajtás biztosítása céljából az erős ügyfél-hitelesítés alóli kivételeket kihasználni kívánó pénzforgalmi szolgáltatóknak rendszeresen meg kell figyelniük és az illetékes hatóságok és az Európai Bankhatóság (EBH) rendelkezésére kell bocsátaniuk azok kérésére minden egyes fizetésiművelet-típus esetében a csalárd vagy nem engedélyezett fizetési műveletek értékét és az összes fizetési műveletük esetében megfigyelt csalási arányokat, függetlenül attól, hogy erős ügyfél-hitelesítés segítségével hitelesített vagy egy vonatkozó kivétel alapján végrehajtott műveletről van-e szó.

(16) Az elektronikus fizetési műveletek csalási arányaira vonatkozó ezen új historikus bizonyíték gyűjtése hozzá fog járulni ahhoz is, hogy az EBH hatékonyan felülvizsgálhassa az erős ügyfél-hitelesítés alóli, valós idejű műveleti-kockázat-elemzésen alapuló kivételre vonatkozó küszöbértékeket. Az (EU) 2015/2366 irányelv 98. cikkének (5) bekezdésével és az 1093/2010/EU európai parlamenti és tanácsi rendelet ([1]) 10. cikkével összhangban az EBH-nak ezeket a szabályozástechnikai standardokat felül kell vizsgálnia és adott esetben az azok aktualizálására vonatkozó tervezeteket kell benyújtania a Bizottságnak, új küszöbértékekre és a kapcsolódó csalási arányokra vonatkozó javaslatok előterjesztésével, amelyek célja az elektronikus távoli fizetések biztonságának javítása.

(17) A meghatározandó kivételek bármelyikét igénybe venni kívánó pénzforgalmi szolgáltatók számára lehetővé kell tenni, hogy a szóban forgó rendelkezésekben említett műveletek és fizetési műveletek esetében bármikor dönthessenek az erős ügyfél-hitelesítés alkalmazása mellett.

(18) Indokolt, hogy a személyes hitelesítési adatok bizalmasságának és integritásának, valamint a hitelesítési eszközöknek és szoftvereknek a védelmét szolgáló intézkedések korlátozzák a készpénz-helyettesítő fizetési eszközök nem engedélyezett vagy csalárd használatán és a fizetési számlákhoz való jogosulatlan hozzáférésen keresztüli csaláshoz kapcsolódó kockázatokat. E célból szükséges a személyes hitelesítési adatok biztonságos létrehozására és kézbesítésére, valamint a pénzforgalmi szolgáltatást igénybe vevővel való társítására vonatkozó követelmények bevezetése, továbbá a hitelesítési adatok megújítására és deaktiválására vonatkozó feltételek előírása.

(19) A számlainformációkat összesítő szolgáltatások, a megbízásos online átutalási szolgáltatások és a fedezet rendelkezésre állásának megerősítése keretében az érintett szereplők között folytatott hatékony és biztonságos kommunikáció biztosítása érdekében szükséges meghatározni a közös és biztonságos nyílt kommunikációs standardokra vonatkozó, az összes érintett pénzforgalmi szolgáltató által teljesítendő követelményeket. Az (EU) 2015/2366 irányelv a számlainformációkat összesítő szolgáltatók fizetésiszámla-információkhoz való hozzáféréséről és az információk felhasználásáról rendelkezik. Ez a rendelet ezért nem módosítja a fizetési számlától eltérő számlákhoz való hozzáférésre vonatkozó szabályokat.

([1]) Az Európai Parlament és a Tanács 1093/2010/EU rendelete (2010. november 24.) az európai felügyeleti hatóság (Európai Bankhatóság) létrehozásáról, a 716/2009/EK határozat módosításáról és a 2009/78/EK bizottsági határozat hatályon kívül helyezéséről (HL L 331., 2010.12.15., 12. o.).

(20) Minden számlavezető pénzforgalmi szolgáltatónak, amely online hozzáférhető számlákkal rendelkezik, legalább egy olyan hozzáférési interfészt kell kínálnia, amely lehetővé teszi a számlainformációkat összesítő szolgáltatókkal, megbízásos online átutalási szolgáltatókkal és kártyaalapú készpénz-helyettesítő fizetési eszközt kibocsátó pénzforgalmi szolgáltatókkal való biztonságos kommunikációt. Az interfésznek lehetővé kell tennie a számlainformációkat összesítő szolgáltatók, a megbízásos online átutalási szolgáltatók és a kártyaalapú készpénz-helyettesítő fizetési eszközt kibocsátó pénzforgalmi szolgáltatók számára, hogy azonosítsák magukat a számlavezető pénzforgalmi szolgáltató felé. Az interfésznek lehetővé kell tennie továbbá a számlainformációkat összesítő szolgáltatók és a megbízásos online átutalási szolgáltatók számára, hogy azokra a hitelesítési eljárásokra hagyatkozzanak, amelyeket a számlavezető pénzforgalmi szolgáltató a pénzforgalmi szolgáltatást igénybe vevő számára biztosít. A technológiai és üzletimodell-semlegesség biztosítása céljából a számlavezető pénzforgalmi szolgáltatók szabadon kell, hogy dönthessenek arról, hogy egy, a számlainformációkat összesítő szolgáltatókkal, megbízásos online átutalási szolgáltatókkal és kártyaalapú készpénz-helyettesítő eszközöket kibocsátó pénzforgalmi szolgáltatókkal való kommunikáció céljára rendelt interfészt kínálnak-e, vagy e kommunikáció céljára lehetővé teszik a számlavezető pénzforgalmi szolgáltató pénzforgalmi szolgáltatást igénybe vevőinek azonosítására és a velük való kommunikációra szolgáló interfész használatát.

(21) Annak érdekében, hogy a számlainformációkat összesítő szolgáltatók, a megbízásos online átutalási szolgáltatók és a kártyaalapú készpénz-helyettesítő fizetési eszközt kibocsátó pénzforgalmi szolgáltatók ki tudják fejleszteni saját technikai megoldásaikat, az interfész technikai specifikációját megfelelően dokumentálni kell és nyilvánosan elérhetővé kell tenni. Ezenfelül a számlavezető pénzforgalmi szolgáltatónak egy olyan eszközt kell kínálnia, amely lehetővé teszi a pénzforgalmi szolgáltatók számára a technikai megoldások tesztelését legalább hat hónappal ezen szabályozási standardok alkalmazásának dátuma előtt, vagy ha az interfész elindítása e standardok alkalmazási dátuma után történik, akkor azon dátum előtt, amikor az interfész megjelenik a piacon. A különböző kommunikációs technológiai megoldások interoperabilitásának biztosítása céljából az interfésznek a nemzetközi vagy európai szabványügyi szervezetek által kidolgozott kommunikációs standardokat kell alkalmaznia.

(22) A számlainformációkat összesítő szolgáltatók és a megbízásos online átutalási szolgáltatók által nyújtott szolgáltatások minősége a számlavezető pénzforgalmi szolgáltatók által létrehozott vagy kiigazított interfészek megfelelő működésétől fog függeni. Ezért fontos, hogy amennyiben az ilyen interfészek nem felelnek meg az ezen standardokban foglalt előírásoknak, akkor az üzletmenet-folytonosságot az említett szolgáltatások igénybe vevői részére garantáló intézkedésekre kerüljön sor. A nemzeti illetékes hatóságok felelőssége annak biztosítása, hogy a számlainformációkat összesítő szolgáltatókat és a megbízásos online átutalási szolgáltatókat ne blokkolja vagy akadályozza semmi a szolgáltatásaik nyújtásában.

(23) Amennyiben a fizetési számlákhoz célra rendelt interfészen keresztül kínálnak hozzáférést, akkor elő kell írni, hogy a célra rendelt interfészeknek ugyanolyan szintű elérhetősége és teljesítménye legyen, mint a pénzforgalmi szolgáltatást igénybe vevő rendelkezésére álló interfésznek, a pénzforgalmi szolgáltatást igénybe vevők azon jogának biztosítása érdekében, hogy igénybe vegyék a megbízásos online átutalási szolgáltatókat és a számlával kapcsolatos információkhoz való hozzáférést lehetővé tevő szolgáltatásokat, az (EU) 2015/2366 irányelvben előírtak szerint. A számlavezető pénzforgalmi szolgáltatóknak a célra rendelt interfészek elérhetőségére és teljesítményére vonatkozóan átlátható fő teljesítménymutatókat és a szolgáltatás szintjére vonatkozó célokat is meg kell határozniuk, amelyek legalább olyan szigorúak, mint a pénzforgalmi szolgáltatást igénybe vevőik esetében használt interfészekre vonatkozóak. Az említett interfészeket ezért tesztelniük kell azon pénzforgalmi szolgáltatóknak, akik használni fogják azokat, valamint az illetékes hatóság általi stressztesztnek és megfigyelésnek lesznek alávetve.

(24) Annak biztosítására, hogy a célra rendelt interfészre hagyatkozó pénzforgalmi szolgáltatók az elérhetőséggel vagy a nem megfelelő teljesítménnyel kapcsolatos problémák esetén is folytatni tudják szolgáltatásaik nyújtását, szükséges előírni – szigorú feltételek mellett – egy tartalékmechanizmust, amely lehetővé teszi az érintett szolgáltatók számára, hogy a számlavezető pénzforgalmi szolgáltató által a saját pénzforgalmi szolgáltatásokat igénybe vevőinek azonosítására és a velük való kommunikációra fenntartott interfészt használják. Bizonyos számlavezető pénzforgalmi szolgáltatók mentesülnek azon előírás alól, hogy az ügyféloldali interfészen keresztül ilyen tartalékmechanizmust biztosítsanak, amennyiben az illetékes hatóságaik megállapítják, hogy a célra rendelt interfészek megfelelnek az akadálytalan versenyt biztosító meghatározott feltételeknek. Abban az esetben, ha a mentesített célra rendelt interfészek nem felelnek meg az előírt feltételeknek, az érintett illetékes hatóságoknak vissza kell vonniuk a megadott mentességeket.

(25) Annak érdekében, hogy az illetékes hatóságok hatékonyan felügyelhessék és nyomon követhessék a kommunikációs interfészek végrehajtását és kezelését, a számlavezető pénzforgalmi szolgáltatóknak weboldalukon elérhetővé kell tenniük a releváns dokumentáció összefoglalóját, és kérésre az illetékes hatóságok rendelkezésére kell bocsátaniuk a sürgős helyzetekre vonatkozó megoldások dokumentációját. A számlavezető pénzforgalmi szolgáltatóknak emellett nyilvánosan elérhetővé kell tenniük a szóban forgó interfész elérhetőségére és teljesítményére vonatkozó statisztikákat is.

(26) Az adatok bizalmasságának és integritásának a megóvása érdekében szükséges biztosítani a számlavezető pénzforgalmi szolgáltatók, a számlainformációkat összesítő szolgáltatók, a megbízásos online átutalási szolgáltatók és a kártyaalapú készpénz-helyettesítő eszközöket kibocsátó pénzforgalmi szolgáltatók közötti

kommunikációs munkamenetek biztonságát. Mindenekelőtt szükséges előírni, hogy a számlainformációkat összesítő szolgáltatók, a megbízásos online átutalási szolgáltatók, a kártyaalapú készpénz-helyettesítő fizetési eszközöket kibocsátó pénzforgalmi szolgáltatók és a számlavezető pénzforgalmi szolgáltatók az adatcsere során biztonságos titkosítást alkalmazzanak.

(27) A felhasználói bizalom javítása és az erős ügyfél-hitelesítés biztosítása érdekében figyelembe kell venni a 910/2014/EU európai parlamenti és tanácsi rendeletben ([1]) meghatározott elektronikus azonosítási eszközök és bizalmi szolgáltatások használatát, különös tekintettel a bejelentett elektronikus azonosítási rendszerekre.

(28) Az összehangolt alkalmazási dátumok biztosítása érdekében ezt a rendeletet ugyanattól a dátumtól kell alkalmazni, mint amelyiktől a tagállamoknak biztosítaniuk kell az (EU) 2015/2366 irányelv 65., 66., 67. és 97. cikkében említett biztonsági intézkedések alkalmazását.

(29) Ez a rendelet az Európai Bankhatóság (EBH) által a Bizottsághoz benyújtott szabályozástechnikai standardtervezeten alapul.

(30) Az EBH nyílt és átlátható nyilvános konzultációt folytatott az e rendelet alapját képező szabályozástechnikai standardtervezetről, elemezte az esetleges kapcsolódó költségeket és hasznot, továbbá kikérte az 1093/2010/EU rendelet 37. cikkével összhangban létrehozott banki érdekképviseleti csoport véleményét,

ELFOGADTA EZT A RENDELETET:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy

Ez a rendelet meghatározza a pénzforgalmi szolgáltatók által azon biztonsági intézkedések végrehajtása céljából teljesítendő követelményeket, amelyek lehetővé teszik számukra a következők megtételét:

a) az (EU) 2015/2366 irányelv 97. cikkével összhangban az erős ügyfél-hitelesítési eljárás alkalmazása;

b) az erős ügyfél-hitelesítés biztonsági követelményeinek alkalmazása alóli kivétel, a kockázati szinten, az összegen és a fizetési művelet gyakoriságán, valamint a végrehajtásához igénybe vett fizetési csatornán alapuló meghatározott és korlátozott feltételek függvényében;

c) a pénzforgalmi szolgáltatást igénybe vevők esetében a személyes hitelesítési adatok bizalmasságának és integritásának megóvása;

d) az (EU) 2015/2366 irányelv IV. címének alkalmazásában a pénzforgalmi szolgáltatások nyújtásával és igénybevételével kapcsolatban a számlavezető pénzforgalmi szolgáltatók, a megbízásos online átutalási szolgáltatók, a számlainformációkat összesítő szolgáltatók, a fizető felek, a kedvezményezettek és az egyéb pénzforgalmi szolgáltatók közötti közös és biztonságos nyílt kommunikációs standardok meghatározása.

2. cikk

Általános hitelesítési követelmények

(1) A pénzforgalmi szolgáltatóknak olyan műveletmegfigyelő mechanizmusokkal kell rendelkezniük, amelyek lehetővé teszik számukra a nem engedélyezett vagy csalárd fizetési műveletek észlelését, az 1. cikk a) és b) pontjában említett biztonsági intézkedések végrehajtása céljából.

([1]) Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (HL L 257., 2014.8.28., 53. o.).

Ezeknek a mechanizmusoknak a fizetési műveletek elemzésén kell alapulniuk olyan elemeket figyelembe véve, amelyek a személyes hitelesítési adatok rendes használatának körülményei között jellemzőek a pénzforgalmi szolgáltatást igénybe vevőre.

(2) A pénzforgalmi szolgáltatók biztosítják, hogy a műveletmegfigyelő mechanizmusok figyelembe vegyék legalább a következő kockázatalapú tényezők mindegyikét:

a) a már nem biztonságos vagy ellopott hitelesítési elemek jegyzéke;

b) az egyes fizetési műveletek összege;

c) a pénzforgalmi szolgáltatások nyújtása során ismert csalási forgatókönyvek;

d) a hitelesítési eljárás bármely munkamenete során a rosszindulatú szoftverrel való fertőzöttség jelei;

e) amennyiben a hozzáférést biztosító eszközt vagy szoftvert a pénzforgalmi szolgáltató bocsátja rendelkezésre, a pénzforgalmi szolgáltatást igénybe vevő rendelkezésére bocsátott, hozzáférést biztosító eszköz vagy szoftver használatának naplója és a hozzáférést biztosító eszköz vagy szoftver normálistól eltérő használata.

3. cikk

A biztonsági intézkedések felülvizsgálata

(1) Az 1. cikkben említett biztonsági intézkedések végrehajtását a pénzforgalmi szolgáltatóra alkalmazandó jogi kerettel összhangban az informatikai biztonság és a fizetések terén szakértelemmel rendelkező, valamint a pénzforgalmi szolgáltatón belül vagy kívül függetlenül működő könyvvizsgálóknak dokumentálni, rendszeres időközönként tesztelni, értékelni és ellenőrizni kell.

(2) Az (1) bekezdésben említett ellenőrzések közötti időtartamot a pénzforgalmi szolgáltatóra alkalmazandó számviteli és kötelező könyvvizsgálati keret figyelembevételével kell meghatározni.

Mindazonáltal a 18. cikkben említett kivételt alkalmazó pénzforgalmi szolgáltatók esetében legalább évente kell ellenőrizni a módszertant, a modellt és a jelentett csalási arányokat. Az ezt az ellenőrzést végző könyvvizsgálónak szakértelemmel kell rendelkeznie az informatikai biztonság és a fizetések területén, és a pénzforgalmi szolgáltatón belül vagy kívül függetlenül kell működnie. Ezt az ellenőrzést a 18. cikk szerinti kivétel alkalmazásának első évében és azt követően legalább háromévente, vagy az illetékes hatóságok kérésére gyakrabban egy független és szakképesítéssel rendelkező külső könyvvizsgálónak kell elvégeznie.

(3) Ezen ellenőrzés során egy értékelést és egy jelentést kell készíteni a pénzforgalmi szolgáltató biztonsági intézkedéseinek az ebben a rendeletben meghatározott követelményeknek való megfeleléséről.

Az illetékes hatóságok kérésére a teljes jelentést a rendelkezésükre kell bocsátani.

II. FEJEZET

AZ ERŐS ÜGYFÉL-HITELESÍTÉS ALKALMAZÁSÁRA VONATKOZÓ BIZTONSÁGI INTÉZKEDÉSEK

4. cikk

Hitelesítési kód

(1) Amennyiben a pénzforgalmi szolgáltatók az (EU) 2015/2366 irányelv 97. cikke (1) bekezdésének megfelelően erős ügyfél-hitelesítést alkalmaznak, a hitelesítésnek kettő vagy több olyan elemen kell alapulnia, amelyek az ismeret, a birtoklás és a biológiai tulajdonság kategóriába sorolhatók, és egy hitelesítési kód generálását kell eredményeznie.

A hitelesítési kódot csak egyszer fogadhatja el a pénzforgalmi szolgáltató, amikor a fizető fél a hitelesítési kódot használja a fizetési számlájához való online hozzáféréshez, elektronikus fizetési művelet kezdeményezéséhez vagy műveletek távoli csatornán keresztüli végrehajtásához, ami fizetéssel kapcsolatos csalásokra vagy más visszaélésekre adhat módot.

(2) Az (1) bekezdés alkalmazásában a pénzforgalmi szolgáltatóknak olyan biztonsági intézkedéseket kell elfogadniuk, amelyek biztosítják, hogy a következő követelmények mindegyike teljesül:

a) nem állítható elő semmilyen, az (1) bekezdésben említett elemek bármelyikére vonatkozó információ a hitelesítési kód közzététele esetén;

b) a korábban generált bármely egyéb hitelesítési kód ismerete alapján nem lehetséges új hitelesítési kódot generálni;

c) a hitelesítési kód nem hamisítható.

(3) A pénzforgalmi szolgáltatók biztosítják, hogy a hitelesítési kód generálásával történő hitelesítés magában foglalja a következő intézkedések mindegyikét:

a) amennyiben a távoli hozzáférés, elektronikus távoli fizetések és fizetéssel kapcsolatos csalásokra vagy más visszaélésekre esetleg módot adó, távoli csatornán keresztüli egyéb műveletek céljából történő hitelesítés során nem sikerült hitelesítési kódot generálni az (1) bekezdés alkalmazásában, nem lehetséges azonosítani, hogy az adott bekezdésben említett elemek melyike volt helytelen;

b) azon sikertelen hitelesítési kísérletek száma, amelyek egymást követhetik, és amelyeket követően az (EU) 2015/2366 irányelv 97. cikkének (1) bekezdésében említett műveleteket ideiglenesen vagy tartósan le kell tiltani, egy adott időtartamon belül nem haladhatja meg az ötöt;

c) a kommunikációs munkamenetek védettek a hitelesítés során továbbított hitelesítési adatok elfogásával szemben és a jogosulatlan felek általi manipulációval szemben az V. fejezet követelményeivel összhangban;

d) az a maximális idő, amelyet a fizető fél a fizetési számlájához való online hozzáférés céljából történt hitelesítése után tétlenül eltölthet, nem haladhatja meg az öt percet.

(4) Amennyiben a (3) bekezdés b) pontjában említett letiltás ideiglenes, a letiltás időtartamát és az újbóli próbálkozások számát a fizető félnek nyújtott szolgáltatás jellemzői és a kapcsolódó összes releváns kockázat alapján kell megállapítani, figyelembe véve legalább a 2. cikk (2) bekezdésében említett tényezőket.

A fizető felet figyelmeztetni kell a letiltás tartóssá tétele előtt.

Amennyiben a letiltás tartóssá vált, egy biztonságos eljárást kell létrehozni, amely lehetővé teszi a fizető fél számára, hogy újból használhassa a letiltott elektronikus készpénz-helyettesítő fizetési eszközöket.

5. cikk

Dinamikus összekapcsolás

(1) Amennyiben a pénzforgalmi szolgáltatók az (EU) 2015/2366 irányelv 97. cikkének (2) bekezdésével összhangban alkalmaznak erős ügyfél-hitelesítést, akkor az e rendelet 4. cikkének követelményei mellett olyan biztonsági intézkedéseket is el kell fogadniuk, amelyek a következő követelmények mindegyikének megfelelnek:

a) a fizető fél tisztában van a fizetési művelet összegével és a kedvezményezettel;

b) a generált hitelesítési kód egyedi a fizetési művelet azon összege és azon kedvezményezett vonatkozásában, amelyet a fizető fél a művelet kezdeményezésekor jóváhagyott;

c) a pénzforgalmi szolgáltató által elfogadott hitelesítési kód megfelel a fizetési művelet eredeti egyedi összegének és a kedvezményezett kilétének, amelyet a fizető fél jóváhagyott;

d) az összeg vagy a kedvezményezett bármely változása a generált hitelesítési kód érvénytelenítését eredményezi.

(2) Az (1) bekezdés alkalmazásában a pénzforgalmi szolgáltatóknak olyan biztonsági intézkedéseket kell elfogadniuk, amelyek biztosítják a következők mindegyikének bizalmasságát, hitelességét és integritását:

a) a művelet összege és a kedvezményezett a hitelesítés minden szakasza során;

b) a fizető fél számára kijelzett információ a hitelesítés minden szakasza során, beleértve a hitelesítési kód generálását, továbbítását és használatát.

(3) Az (1) bekezdés b) pontja alkalmazásában, és amennyiben a pénzforgalmi szolgáltatók az (EU) 2015/2366 irányelv 97. cikkének (2) bekezdésével összhangban alkalmaznak erős ügyfél-hitelesítést, a hitelesítési kódra vonatkozóan a következő követelmények alkalmazandók:

a) olyan kártyaalapú fizetési művelet kapcsán, amely esetében a fizető fél az említett irányelv 75. cikkének (1) bekezdése értelmében jóváhagyta a zárolandó pénzösszeg pontos nagyságát, a hitelesítési kódnak egyedinek kell lennie azon összeg vonatkozásában, amelynek zárolását a fizető fél jóváhagyta, és amelyet a fizető fél a művelet kezdeményezésekor jóváhagyott;

b) olyan fizetési műveletek kapcsán, amelyek esetében a fizető fél jóváhagyta az elektronikus távoli fizetési műveletek egy csoportjának egy vagy több kedvezményezett részére történő végrehajtását, a hitelesítési kódnak egyedinek kell lennie a fizetési műveletek csoportjának teljes összege és a meghatározott kedvezményezettek vonatkozásában.

6. cikk

Az ismeret kategóriába sorolható elemekre vonatkozó követelmények

(1) A pénzforgalmi szolgáltatók intézkedéseket fogadnak el azon kockázat mérséklésére, hogy az erős ügyfél-hitelesítés ismeret kategóriába sorolható elemeit jogosulatlan felek feltárják vagy azokat előttük felfedjék.

(2) Az említett elemeknek a fizető fél általi használatára kockázatmérséklési intézkedéseket kell alkalmazni annak megakadályozása érdekében, hogy az elemeket jogosulatlan felek előtt felfedjék.

7. cikk

A birtoklás kategóriába sorolható elemekre vonatkozó követelmények

(1) A pénzforgalmi szolgáltatók intézkedéseket fogadnak el azon kockázat mérséklésére, hogy az erős ügyfél-hitelesítés birtoklás kategóriába sorolható elemeit jogosulatlan felek felhasználják.

(2) Az említett elemeknek a fizető fél általi használatára az elemek lemásolásának megakadályozását célzó intézkedéseket kell alkalmazni.

8. cikk

A biológiai tulajdonság kategóriába sorolható elemekhez kapcsolódó eszközökre és szoftverekre vonatkozó követelmények

(1) A pénzforgalmi szolgáltatók intézkedéseket fogadnak el azon kockázat mérséklésére, hogy a biológiai tulajdonság kategóriába sorolható és a fizető fél rendelkezésére bocsátott hozzáférési eszközök és szoftverek által olvasott hitelesítési elemeket jogosulatlan felek feltárják. A pénzforgalmi szolgáltatóknak legalább azt biztosítaniuk kell, hogy az említett hozzáférési eszközök és szoftverek esetében nagyon alacsony legyen a valószínűsége annak, hogy jogosulatlan felet hitelesítenek fizető félként.

(2) Az említett elemeknek a fizető fél általi használatára olyan intézkedéseket kell alkalmazni, amelyek biztosítják, hogy az említett eszközök és szoftverek garantált védelmet nyújtsanak az elemeknek az eszközökhöz és a szoftverekhez való hozzáférés révén történő jogosulatlan felhasználásával szemben.

9. cikk

Az elemek függetlensége

(1) A pénzforgalmi szolgáltatók biztosítják, hogy az erős ügyfél-hitelesítés 6., 7. és 8. cikkben említett elemeinek használatára olyan intézkedések legyenek alkalmazandók, amelyet biztosítják, hogy a technológia, az algoritmusok és a paraméterek tekintetében az elemek egyikének feltörése nem befolyásolja a többi elem megbízhatóságát.

(2) A pénzforgalmi szolgáltatók biztonsági intézkedéseket fogadnak el arra az esetre, ha az erős ügyfél-hitelesítés bármely elemét vagy magát a hitelesítési kódot többfunkciós eszköz segítségével használják, hogy mérsékeljék az esetlegesen abból eredő kockázatot, hogy a többfunkciós eszköz már nem biztonságos.

(3) A (2) bekezdés alkalmazásában a kockázatmérséklési intézkedéseknek magukban kell foglalniuk a következők mindegyikét:

a) a többfunkciós eszközön belül telepített szoftveren keresztül elkülönített biztonságos végrehajtási környezetek alkalmazása;

b) azt biztosító mechanizmusok, hogy a szoftvert vagy eszközt nem változtatta meg a fizető fél vagy harmadik fél;

c) ha változtatásokra került sor, az ezek következményeit mérséklő mechanizmusok.

III. FEJEZET

AZ ERŐS ÜGYFÉL-HITELESÍTÉS ALÓLI KIVÉTELEK

10. cikk

Fizetési számlára vonatkozó információk

(1) A pénzforgalmi szolgáltatók számára lehetővé kell tenni, hogy ne alkalmazzanak erős ügyfél-hitelesítést, amennyiben megfelelnek a 2. cikkben meghatározott követelményeknek és az e cikk (2) bekezdésének, valamint ha a pénzforgalmi szolgáltatást igénybe vevőre olyan korlátozás vonatkozik, hogy a következő információk egyikéhez vagy mindkettőhöz érzékeny fizetési adatok közzététele nélkül férhet hozzá:

a) egy vagy több megjelölt fizetési számla egyenlege;

b) az elmúlt 90 napban egy vagy több megjelölt fizetési számlán keresztül végrehajtott fizetési műveletek.

(2) Az (1) bekezdés alkalmazásában a pénzforgalmi szolgáltatók számára nem biztosítható kivétel az erős ügyfél-hitelesítés alkalmazása alól, ha a következő feltételek valamelyike teljesül:

a) a pénzforgalmi szolgáltatást igénybe vevő az (1) bekezdésben meghatározott információhoz első alkalommal fér hozzá online;

b) több mint 90 nap eltelt azóta, hogy a pénzforgalmi szolgáltatást igénybe vevő utoljára online hozzáfért az (1) bekezdés b) pontjában meghatározott információhoz, és erős ügyfél-hitelesítésre került sor.

11. cikk

Az értékesítés helyén történő érintéses fizetés

A pénzforgalmi szolgáltatók számára lehetővé kell tenni, hogy ne alkalmazzanak erős ügyfél-hitelesítést, amennyiben megfelelnek a 2. cikkben meghatározott követelményeknek, amikor a fizető fél érintéses elektronikus fizetési műveletet kezdeményez, feltéve, hogy teljesülnek a következő feltételek:

a) az érintéses elektronikus fizetési művelet egyedi összege nem haladja meg az 50 EUR-t; valamint

b) az erős ügyfél-hitelesítés utolsó alkalmazásának dátuma óta az érintéses funkcióval rendelkező készpénz-helyettesítő eszköz használatával kezdeményezett előző érintéses elektronikus fizetési műveletek kumulált összege nem haladja meg a 150 EUR-t; vagy

c) az erős ügyfél-hitelesítés utolsó alkalmazása óta az érintéses funkciót kínáló készpénz-helyettesítő eszköz használatával kezdeményezett egymást követő érintéses elektronikus fizetési műveletek száma nem haladja meg az ötöt.

12. cikk

Közlekedési viteldíjakhoz és parkolási díjakhoz használt felügyelet nélküli terminálok

A pénzforgalmi szolgáltatók számára lehetővé kell tenni, hogy ne alkalmazzanak erős ügyfél-hitelesítést, amennyiben megfelelnek a 2. cikkben meghatározott követelményeknek, amikor a fizető fél egy felügyelet nélküli fizetési terminálnál közlekedési viteldíj vagy parkolási díj megfizetése céljából elektronikus fizetési műveletet kezdeményez.

13. cikk

Megbízható kedvezményezettek

(1) A pénzforgalmi szolgáltatók erős ügyfél-hitelesítést alkalmaznak, amikor a fizető fél a számlavezető pénzforgalmi szolgáltatóján keresztül a megbízható kedvezményezettek egy listáját összeállítja vagy módosítja.

(2) A pénzforgalmi szolgáltatók számára lehetővé kell tenni, hogy ne alkalmazzanak erős ügyfél-hitelesítést, amennyiben megfelelnek az általános hitelesítési követelményeknek, ha a fizető fél fizetési műveletet kezdeményez és a kedvezményezett szerepel a fizető által előzőleg összeállított, megbízható kedvezményezettek listáján.

14. cikk

Ismétlődő műveletek

(1) A pénzforgalmi szolgáltatók erős ügyfél-hitelesítést alkalmaznak, amikor egy fizető fél ugyanazon összegű és ugyanazon kedvezményezett részére történő ismétlődő műveletek sorozatát létrehozza, módosítja vagy első alkalommal kezdeményezi.

(2) A pénzforgalmi szolgáltatók számára lehetővé kell tenni, hogy ne alkalmazzanak erős ügyfél-hitelesítést, amennyiben megfelelnek az általános hitelesítési követelményeknek, az (1) bekezdésben említett fizetésiművelet-sorozatba tartozó összes későbbi fizetési művelet kezdeményezése esetében.

15. cikk

Ugyanazon természetes vagy jogi személy által tartott számlák közötti átutalások

A pénzforgalmi szolgáltatók számára lehetővé kell tenni, hogy ne alkalmazzanak erős ügyfél-hitelesítést, amennyiben megfelelnek a 2. cikkben meghatározott követelményeknek, ha a fizető fél olyan körülmények között kezdeményez átutalást, ahol a fizető fél és a kedvezményezett ugyanaz a természetes vagy jogi személy, és mindkét fizetési számlát ugyanazon számlavezető pénzforgalmi szolgáltatónál tartják.

16. cikk

Kis összegű műveletek

A pénzforgalmi szolgáltatók számára lehetővé kell tenni, hogy ne alkalmazzanak erős ügyfél-hitelesítést, amikor a fizető fél távoli elektronikus fizetési műveletet kezdeményez, feltéve, hogy teljesülnek a következő feltételek:

a) a távoli elektronikus fizetési művelet összege nem haladja meg a 30 EUR-t; valamint

b) az erős ügyfél-hitelesítés utolsó alkalmazása óta a fizető fél által kezdeményezett előző távoli elektronikus fizetési műveletek kumulált összege nem haladja meg a 100 EUR-t; vagy

c) az erős ügyfél-hitelesítés utolsó alkalmazása óta a fizető fél által kezdeményezett előző távoli elektronikus fizetési műveletek száma nem haladja meg az 5 egymást követő egyedi távoli elektronikus fizetési műveletet.

17. cikk

Biztonságos vállalati fizetési folyamatok és protokollok

A pénzforgalmi szolgáltatók számára lehetővé kell tenni, hogy ne alkalmazzanak erős ügyfél-hitelesítést olyan jogi személyek kapcsán, amelyek erre a célra kijelölt, kizárólag nem fogyasztónak minősülő fizető felek rendelkezésére bocsátott fizetési folyamatok vagy protokollok használatával kezdeményeznek elektronikus fizetési műveleteket, amennyiben az illetékes hatóságok meggyőződtek arról, hogy a szóban forgó folyamatok vagy protokollok az (EU) 2015/2366 irányelvben előírtakkal legalább egyenértékű szintű biztonságot garantálnak.

18. cikk

Műveletikockázat-elemzés

(1) A pénzforgalmi szolgáltatók számára lehetővé kell tenni, hogy ne alkalmazzanak erős ügyfél-hitelesítést, ha a fizető fél olyan távoli elektronikus fizetési műveletet kezdeményez, amelyet a pénzforgalmi szolgáltató a 2. cikkben és az e cikk (2) bekezdésének c) pontjában említett műveletmegfigyelő mechanizmusok alapján alacsony kockázatúként azonosít.

(2) Az (1) bekezdésben említett elektronikus fizetési műveletet alacsony kockázatúnak kell tekinteni, ha az összes következő feltétel teljesül:

a) a pénzforgalmi szolgáltató által jelentett és a 19. cikknek megfelelően kiszámított csalási arány e művelettípus esetében a mellékletben a „távoli elektronikus kártyaalapú fizetések", illetve a „távoli elektronikus átutalások" táblázatban meghatározott referencia csalási arányokkal egyenlő vagy azok alatti;

b) a művelet összege nem haladja meg a melléklet táblázatában meghatározott vonatkozó kivételi küszöbértéket;

c) a pénzforgalmi szolgáltatók valós idejű kockázatelemzés elvégzését követően nem azonosították a következők egyikét sem:

   i. a fizető fél normálistól eltérő költési vagy viselkedési mintája;

   ii. a fizető fél eszköz-/szoftverhozzáférésére vonatkozó szokatlan információ;

   iii. a hitelesítési eljárás bármely munkamenete során rosszindulatú szoftverrel való fertőzöttség;

   iv. a pénzforgalmi szolgáltatások nyújtása során ismert csalási forgatókönyv;

   v. a fizető fél normálistól eltérő elhelyezkedése;

   vi. a kedvezményezett magas kockázatú elhelyezkedése.

(3) A távoli elektronikus fizetési műveleteket azok alacsony kockázata okán az erős ügyfél-hitelesítés alól mentesíteni szándékozó pénzforgalmi szolgáltatók figyelembe veszik legalább a következő kockázatalapú tényezőket:

a) a pénzforgalmi szolgáltatást igénybe vevő egyén korábbi költési mintái;

b) a pénzforgalmi szolgáltató minden egyes pénzforgalmi szolgáltatást igénybe vevőjének a fizetésiművelet-története;

c) a fizető fél és a kedvezményezett elhelyezkedése a fizetési művelet időpontjában abban az esetben, ha a hozzáférési eszközt vagy szoftvert a pénzforgalmi szolgáltató bocsátja rendelkezésre;

d) a pénzforgalmi szolgáltatást igénybe vevőnek a fizetésiművelet-történetéhez képest a normálistól eltérő fizetési mintáinak azonosítása.

A pénzforgalmi szolgáltató által végzett értékelés az összes említett kockázatalapú tényezőt egy kockázatpontozássá kombinálja minden egyes művelet esetében, annak meghatározása céljából, hogy egy adott fizetés engedélyezhető-e erős ügyfél-hitelesítés nélkül.

19. cikk

A csalási arányok kiszámítása

(1) A pénzforgalmi szolgáltató a mellékletben meghatározott táblázatban említett minden művelettípus esetében biztosítja, hogy a mind az erős ügyfél-hitelesítés segítségével hitelesített fizetési műveletekre, mind a 13–18. cikkben említett kivételek bármelyike alapján végrehajtott műveletekre kiterjedő átfogó csalási arányok a mellékletben meghatározott táblázatban az ugyanazon fizetésiművelet-típusra vonatkozóan feltüntetett referencia csalási aránnyal egyenlők, vagy annál alacsonyabbak legyenek.

Az egyes művelettípusokra vonatkozó átfogó csalási arányok kiszámításához gördülő negyedévi (90 napos) alapon a nem engedélyezett vagy csalárd távoli műveletek összértékét – függetlenül attól, hogy a pénzösszegeket visszaszerezték vagy sem – el kell osztani az ugyanolyan művelettípusokat érintő összes távoli művelet összértékével, függetlenül attól, hogy a műveleteket erős ügyfél-hitelesítés alkalmazásával hitelesítették vagy a 13–18. cikkben említett bármely kivétel alapján hajtották végre.

(2) A csalási arányok kiszámítását és az abból eredő számadatokat a 3. cikk (2) bekezdésében említett könyvvizsgálói ellenőrzés során értékelni kell, aminek biztosítania kell az adatok teljességét és pontosságát.

(3) A pénzforgalmi szolgáltató által a csalási arányok kiszámításához használt módszertant és modelleket, valamint magukat a csalási arányokat megfelelően dokumentálni kell és teljeskörűen az illetékes hatóságok és az EBH rendelkezésére kell bocsátani, az érintett illetékes hatóság/hatóságok előzetes értesítése mellett, azok kérésére.

20. cikk

A műveletikockázat-elemzésen alapuló kivételek alkalmazásának megszüntetése

(1) A 18. cikkben említett kivételeket alkalmazó pénzforgalmi szolgáltatók azonnal jelentik az illetékes hatóságoknak, ha a mellékletben meghatározott táblázatban feltüntetett fizetésiművelet-típusok bármelyike esetében a megfigyelt csalási arányok egyike meghaladja az alkalmazandó referencia csalási arányt, és az illetékes hatóságok rendelkezésére bocsátják azon intézkedések leírását, amelyeket el kívánnak fogadni annak érdekében, hogy helyreállítsák a megfigyelt csalási arányuknak az alkalmazandó referencia csalási aránynak való megfelelését.

(2) A pénzforgalmi szolgáltatók azonnal megszüntetik a 18. cikkben említett kivétel alkalmazását a mellékletben lévő táblázatban az adott kivételi küszöbértéknél feltüntetett minden olyan fizetésiművelet-típus esetében, amelynél a megfigyelt csalási arányuk két egymást követő negyedévben meghaladja az adott készpénz-helyettesítő eszköz vagy fizetésművelet-típus esetében a szóban forgó kivételi küszöbérték-tartományban alkalmazandó referencia csalási arányt.

(3) A 18. cikkben említett kivétel alkalmazásának az e cikk (2) bekezdésével összhangban történő megszüntetését követően a pénzforgalmi szolgáltatók nem alkalmazhatják újra azt a kivételt, amíg a kiszámított csalási arányuk a szóban forgó fizetésiművelet-típusra vonatkozóan az adott kivételi küszöbérték-tartományban alkalmazandó referencia csalási arányokkal egy negyedévben egyenlő, vagy azoknál alacsonyabb nem lesz.

(4) Ha a pénzforgalmi szolgáltatók újra alkalmazni kívánják a 18. cikkben említett kivételt, észszerű időn belül tájékoztatniuk kell az illetékes hatóságokat, és a kivétel újbóli alkalmazása előtt bizonyítaniuk kell, hogy a megfigyelt csalási arányuk megfelel az adott kivételi küszöbérték-tartományban alkalmazandó referencia csalási aránynak, e cikk (3) bekezdésével összhangban.

21. cikk

Megfigyelés

(1) A 10–18. cikkben meghatározott kivételek alkalmazása érdekében a pénzforgalmi szolgáltatók a fizetési műveletek minden típusa esetében legalább negyedévente rögzítik és megfigyelik a következő adatokat, távoli és nem távoli fizetési műveletek szerinti bontásban:

a) Az (EU) 2015/2366 irányelv 64. cikkének (2) bekezdésével összhangban a nem engedélyezett vagy csalárd fizetési műveletek összértéke, az összes fizetési művelet összértéke és az ezekből következő csalási arány, beleértve az erős ügyfél-hitelesítés segítségével és az egyes kivételek alapján kezdeményezett fizetési műveletek szerinti bontást;

b) az átlagos műveleti érték, beleértve az erős ügyfél-hitelesítés segítségével és az egyes kivételek alapján kezdeményezett fizetési műveletek szerinti bontást;

c) azon fizetési műveletek száma, amelyeknél az egyes kivételeket alkalmazták, valamint a fizetési műveletek teljes számához viszonyított százalékos arányuk.

(2) A pénzforgalmi szolgáltatók az (1) bekezdésnek megfelelő megfigyelés eredményeit az illetékes hatóságok és az EBH rendelkezésére bocsátják, az érintett illetékes hatóság/hatóságok előzetes értesítése mellett, azok kérésére.

IV. FEJEZET

A PÉNZFORGALMI SZOLGÁLTATÁST IGÉNYBE VEVŐK SZEMÉLYES HITELESÍTÉSI ADATAINAK BIZALMASSÁGA ÉS INTEGRITÁSA

22. cikk

Általános követelmények

(1) A pénzforgalmi szolgáltatók a hitelesítés minden szakaszában biztosítják a pénzforgalmi szolgáltatást igénybe vevő személyes hitelesítési adatainak bizalmasságát és integritását, beleértve a hitelesítési kódokat.

(2) Az (1) bekezdés alkalmazásában a pénzforgalmi szolgáltatók biztosítják, hogy a következő követelmények mindegyike teljesül:

a) a személyes hitelesítési adatokat a megjelenítés során kitakarják, és azok nem olvashatók teljes terjedelmükben a hitelesítés során a pénzforgalmi szolgáltatást igénybe vevő általi bevitelkor;

b) az adatformátumú személyes hitelesítési adatokat, valamint a személyes hitelesítési adatok titkosításához kapcsolódó kriptográfiai anyagokat nem tárolják egyszerű szövegként;

c) a titkos kriptográfiai anyagok védettek a nem engedélyezett felfedéssel szemben.

(3) A pénzforgalmi szolgáltatók teljeskörűen dokumentálják a személyes hitelesítési adatok titkosításához vagy más módon történő olvashatatlanná tételéhez használt kriptográfiai anyagok kezeléséhez kapcsolódó folyamatot.

(4) A pénzforgalmi szolgáltatók biztosítják, hogy a személyes hitelesítési adatok és a II. fejezettel összhangban generált hitelesítési kódok feldolgozása és továbbítása biztonságos környezetben, erős és széles körben elismert ágazati szabványoknak megfelelően történjen.

23. cikk

A hitelesítési adatok előállítása és továbbítása

A pénzforgalmi szolgáltatók biztosítják, hogy a személyes hitelesítési adatok előállítása biztonságok környezetben történjen.

Mérsékelniük kell a személyes hitelesítési adatok és a hitelesítési eszközök és szoftverek jogosulatlan használatának kockázatát a fizető félnek való kézbesítésük előtti elvesztésük, ellopásuk, vagy lemásolásuk esetén.

24. cikk

Társítás a pénzügyi szolgáltatást igénybe vevővel

(1) A pénzforgalmi szolgáltatók biztosítják, hogy kizárólag a pénzforgalmi szolgáltatás igénybe vevőjét társítsák – biztonságos módon – a személyes hitelesítési adatokkal, a hitelesítési eszközökkel és szoftverekkel.

(2) Az (1) bekezdés alkalmazásában a pénzforgalmi szolgáltatók biztosítják, hogy a következő követelmények mindegyike teljesül:

a) a pénzforgalmi szolgáltatást igénybe vevő személyazonosságának a személyes hitelesítési adatokkal, hitelesítési eszközökkel és szoftverekkel való társítása a pénzforgalmi szolgáltató felelőssége mellett biztonságos környezetben zajlik, amely magában foglalja legalább a pénzforgalmi szolgáltató helyiségeit, a pénzforgalmi szolgáltató által biztosított internetes környezetet vagy a pénzforgalmi szolgáltató által használt egyéb hasonló biztonságos weboldalakat, és annak bankjegykiadó automatákat érintő szolgáltatásait, valamint figyelembe veszi a társítási folyamat során használt olyan eszközökhöz és mögöttes komponensekhez kapcsolódó kockázatokat, amelyek nem a pénzforgalmi szolgáltató felelősségébe tartoznak;

b) a pénzforgalmi szolgáltatást igénybe vevő személyazonosságának a személyes hitelesítési adatokkal és a hitelesítési eszközökkel vagy szoftverekkel való, távoli csatornán keresztül történő társítását erős ügyfél-hitelesítés alkalmazásával végzik.

25. cikk

A hitelesítési adatok, hitelesítési eszközök és szoftverek kézbesítése

(1) A pénzforgalmi szolgáltatók biztosítják, hogy a személyes hitelesítési adatoknak, hitelesítési eszközöknek és szoftvereknek a pénzforgalmi szolgáltatást igénybe vevő részére történő kézbesítése biztonságos, az elvesztésükből, ellopásukból vagy másolásukból eredő nem engedélyezett használathoz kapcsolódó kockázatok kezelésére alkalmas módon menjen végbe.

(2) Az (1) bekezdés alkalmazásában a pénzforgalmi szolgáltatók legalább a következő intézkedések mindegyikét alkalmazzák:

a) hatékony és biztonságos kézbesítési mechanizmusok, amelyek biztosítják, hogy a személyes hitelesítési adatokat, a hitelesítési eszközöket és szoftvereket a jogos pénzforgalmi szolgáltatást igénybe vevőnek kézbesítsék;

b) a pénzforgalmi szolgáltató számára azt lehetővé tevő mechanizmusok, hogy a pénzforgalmi szolgáltatást igénybe vevő részére az interneten keresztül kézbesített hitelesítési szoftver hitelességét ellenőrizze;

c) azt biztosító intézkedések, hogy amennyiben a személyes hitelesítési adatok kézbesítése a pénzforgalmi szolgáltató helyiségein kívül vagy távoli csatornán keresztül történik:

   i. jogosulatlan felek ne szerezhessék meg a személyes hitelesítési adatok, a hitelesítési eszközök vagy szoftverek egynél több jellemzőjét, amikor a kézbesítés ugyanazon a csatornán keresztül történik;

   ii. a kézbesített személyes hitelesítési adatokat, hitelesítési eszközöket vagy szoftvereket a használat előtt aktiválni kell;

d) azt biztosító intézkedések, hogy amennyiben a személyes hitelesítési adatokat, hitelesítési eszközöket vagy szoftvereket az első használatuk előtt aktiválni kell, az aktiválás a 24. cikkben említett társítási eljárásoknak megfelelő biztonságos környezetben történjen.

26. cikk

A személyes hitelesítési adatok megújítása

A pénzforgalmi szolgáltatók biztosítják, hogy a személyes hitelesítési adatok megújítása vagy újbóli aktiválása a 23., 24. és 25. cikkel összhangban a hitelesítési adatok és a hitelesítési eszközök előállítására, társítására és kézbesítésére vonatkozó eljárások szerint történjen.

27. cikk

Megsemmisítés, deaktiválás és visszavonás

A pénzforgalmi szolgáltatók gondoskodnak arról, hogy hatékony eljárásokkal rendelkezzenek a következő biztonsági intézkedések mindegyikének alkalmazására:

a) a személyes hitelesítési adatok, hitelesítési eszközök és szoftverek biztonságos megsemmisítése, deaktiválása vagy visszavonása;

b) amennyiben a pénzforgalmi szolgáltató újrafelhasználható hitelesítési eszközöket és szoftvereket ad ki, sor kerül az eszköz vagy szoftver biztonságos újrafelhasználásának kidolgozására, dokumentálására és végrehajtására, mielőtt az eszközt vagy szoftvert egy másik, pénzforgalmi szolgáltatást igénybe vevő rendelkezésére bocsátják;

c) a pénzforgalmi szolgáltató rendszereiben és adatbázisaiban, és adott esetben nyilvános adattárakban tárolt, személyes hitelesítési adatokhoz kapcsolódó információk deaktiválása vagy visszavonása.

V. FEJEZET

KÖZÖS ÉS BIZTONSÁGOS NYÍLT KOMMUNIKÁCIÓS STANDARDOK

1. szakasz

A kommunikációra vonatkozó általános követelmények

28. cikk

Az azonosításra vonatkozó követelmények

(1) A pénzforgalmi szolgáltatók gondoskodnak a biztonságos azonosításról a fizető fél eszköze és a kedvezményezett elektronikus fizetést fogadó eszköze közötti kommunikáció során, beleértve többek között a fizetési terminálokat.

(2) A pénzforgalmi szolgáltatók biztosítják, hogy az elektronikus pénzforgalmi szolgáltatásokat kínáló mobilalkalmazásokban és a pénzforgalmi szolgáltatást igénybe vevők egyéb interfészeiben a kommunikáció jogosulatlan felekhez történő eltérítésének kockázatát hatékonyan mérsékeljék.

29. cikk

Visszakövethetőség

(1) A pénzforgalmi szolgáltatók azt biztosító eljárásokkal rendelkeznek, hogy a pénzforgalmi szolgáltatás nyújtása keretében a pénzforgalmi szolgáltatást igénybe vevővel, más pénzforgalmi szolgáltatókkal és egyéb szervezetekkel, köztük kereskedőkkel folytatott minden fizetési művelet és egyéb interakció visszakövethető legyen, biztosítva, hogy az elektronikus művelet szempontjából lényeges minden eseményről az összes különböző szakaszban utólag ismeretekhez lehessen jutni.

(2) Az (1) bekezdés alkalmazásában a pénzforgalmi szolgáltatók biztosítják, hogy a pénzforgalmi szolgáltatást igénybe vevővel, más pénzforgalmi szolgáltatókkal és egyéb szervezetekkel, köztük kereskedőkkel létrehozott minden kommunikációs munkamenet a következők mindegyikén alapuljon:

a) a munkamenet egyedi azonosítója;

b) a művelet részletes naplózásának biztonsági mechanizmusai, beleértve a műveletszámot, időbélyegzőket és minden releváns műveleti adatot;

c) olyan időbélyegzők, amelyek egységesített időreferencia-rendszeren alapulnak, és amelyeket egy hivatalos időjel alapján kell szinkronizálni.

2. szakasz

A közös és biztonságos nyílt kommunikációs standardokra vonatkozó egyedi követelmények

30. cikk

A hozzáférési interfészekre vonatkozó általános kötelezettségek

(1) Azon számlavezető pénzforgalmi szolgáltatóknak, akik a fizető félnek online hozzáférhető fizetési számlát kínálnak, legalább egy olyan interfésszel kell rendelkezniük, amely teljesíti a következő követelmények mindegyikét:

a) a számlainformációkat összesítő szolgáltatók, a megbízásos online átutalási szolgáltatók és a kártyaalapú készpénz-helyettesítő fizetési eszközt kibocsátó pénzforgalmi szolgáltatók képesek magukat a számlavezető szolgáltató felé azonosítani;

b) a számlainformációkat összesítő szolgáltatók képesek biztonságosan kommunikálni egy vagy több megjelölt fizetési számlára és a kapcsolódó fizetési műveletekre vonatkozó információk kérése és fogadása céljából;

c) a megbízásos online átutalási szolgáltatók képesek biztonságosan kommunikálni abból a célból, hogy fizetési megbízást kezdeményezzenek a fizető fél fizetési számlájáról, és fogadjanak a fizetési művelet kezdeményezésére vonatkozó minden információt, valamint a fizetési művelet végrehajtását illetően a számlavezető pénzforgalmi szolgáltató rendelkezésére álló minden információt.

(2) A pénzforgalmi szolgáltatást igénybe vevő hitelesítése céljából az (1) bekezdésben említett interfész lehetővé teszi a számlainformációkat összesítő szolgáltatók és a megbízásos online átutalási szolgáltatók számára, hogy mindazokra a hitelesítési eljárásokra hagyatkozzanak, amelyeket a számlavezető pénzforgalmi szolgáltató a pénzforgalmi szolgáltatást igénybe vevő számára biztosít.

Az interfésznek teljesítenie kell legalább a következő követelmények mindegyikét:

a) a megbízásos online átutalási szolgáltató vagy a számlainformációkat összesítő szolgáltató utasíthatja a számlavezető pénzforgalmi szolgáltatót, hogy kezdje meg a hitelesítést a pénzforgalmi szolgáltatást igénybe vevő jóváhagyása alapján;

b) a hitelesítés során kommunikációs munkameneteket kell létrehozni és fenntartani a számlavezető pénzforgalmi szolgáltató, a számlainformációkat összesítő szolgáltató, a megbízásos online átutalási szolgáltató és bármely, pénzforgalmi szolgáltatást igénybe vevő között;

c) biztosítani kell a megbízásos online átutalási szolgáltató vagy a számlainformációkat összesítő szolgáltató által vagy rajta keresztül továbbított személyes hitelesítési adatok és hitelesítési kódok integritását és bizalmasságát.

(3) A számlavezető pénzforgalmi szolgáltatók biztosítják, hogy interfészeik kövessék a nemzetközi vagy európai szabványügyi szervezetek által kibocsátott kommunikációs standardokat.

A számlavezető pénzforgalmi szolgáltatók azt is biztosítják, hogy bármely interfész technikai specifikációjának dokumentációja meghatározza azokat a rutinokat, protokollokat és eszközöket, amelyekre a megbízásos online átutalási szolgáltatóknak, számlainformációkat összesítő szolgáltatóknak és a kártyaalapú készpénz-helyettesítő fizetési eszközt kibocsátó pénzforgalmi szolgáltatóknak szükségük van ahhoz, hogy szoftvereik és alkalmazásaik együtt tudjanak működni a számlavezető pénzforgalmi szolgáltató rendszereivel.

A számlavezető pénzforgalmi szolgáltatók legalább hat hónappal a 38. cikk (2) bekezdésében említett alkalmazási dátum előtt, vagy a hozzáférési interfész piaci megjelenésének céldátuma előtt, ha ez a megjelenés a 38. cikk (2) bekezdésében említett dátum után következik be, legalább a dokumentációt díjmentesen rendelkezésre bocsátják azon engedélyezett megbízásos online átutalási szolgáltatók, számlainformációkat összesítő szolgáltatók és kártyaalapú készpénz-helyettesítő fizetési eszközt kibocsátó pénzforgalmi szolgáltatók, vagy olyan pénzforgalmi szolgáltatók kérésére, amelyek illetékes hatóságuknál kérelmezték a vonatkozó engedélyt, valamint a dokumentáció összefoglalóját nyilvánosan elérhetővé teszik a weboldalukon.

(4) A (3) bekezdés mellett a számlavezető pénzforgalmi szolgáltatók biztosítják, hogy – sürgős helyzetek kivételével – az interfészük technikai specifikációjának bármely változását előzetesen a lehető leghamarabb, és legalább 3 hónappal a változás végrehajtása előtt az engedélyezett megbízásos online átutalási szolgáltatók, számlainformációkat összesítő szolgáltatók és kártyaalapú készpénz-helyettesítő fizetési eszközt kibocsátó pénzforgalmi szolgáltatók, vagy olyan pénzforgalmi szolgáltatók rendelkezésére bocsátják, amelyek illetékes hatóságuknál kérelmezték a vonatkozó engedélyt.

A pénzforgalmi szolgáltatók dokumentálják azokat a sürgős helyzeteket, amelyekben változtatásokat hajtottak végre, és a dokumentációt kérésre az illetékes hatóságok rendelkezésére bocsátják.

(5) A számlavezető pénzforgalmi szolgáltatók a kapcsolat és a működés tesztelése céljából támogatással együtt rendelkezésre bocsátanak egy tesztelési eszközt, hogy az engedélyezett megbízásos online átutalási szolgáltatók, a kártyaalapú készpénz-helyettesítő fizetési eszközt kibocsátó pénzforgalmi szolgáltatók és a számlainformációkat összesítő szolgáltatók, vagy olyan pénzforgalmi szolgáltatók, amelyek illetékes hatóságuknál kérelmezték a vonatkozó engedélyt, tesztelni tudják a pénzforgalmi szolgáltatás felhasználóknak történő nyújtásához használt szoftvereiket és alkalmazásaikat. Ezt a tesztelési eszközt legkésőbb hat hónappal a 38. cikk (2) bekezdésében említett alkalmazási dátum előtt, vagy a hozzáférési interfész piaci megjelenésének céldátuma előtt rendelkezésre kell bocsátani, ha ez a megjelenés a 38. cikk (2) bekezdésében említett dátum után következik be.

Érzékeny információkat azonban nem szabad megosztani a tesztelési eszközön keresztül.

(6) Az illetékes hatóságok biztosítják, hogy a számlavezető pénzforgalmi szolgáltatók az általuk létrehozott interfésszel/interfészekkel kapcsolatosan mindenkor teljesítsék az ezekben a standardokban foglalt kötelezettségeket. Amennyiben egy számlavezető pénzforgalmi szolgáltató nem teljesíti az interfészekre vonatkozóan ezekben a standardokban meghatározott követelményeket, az illetékes hatóságok biztosítják, hogy a megbízásos online átutalási szolgáltatások és a számlainformációkat összesítő szolgáltatások nyújtása ne ütközzön akadályba vagy ne szakadjon meg, amennyiben az ilyen szolgáltatások érintett szolgáltatói megfelelnek a 33. cikk (5) bekezdésében meghatározott feltételeknek.

31. cikk

A hozzáférési interfész opciói

A számlavezető pénzforgalmi szolgáltatók a 30. cikkben említett interfészt/interfészeket egy célra rendelt interfész segítségével vagy úgy hozzák létre, hogy engedélyezik a 30. cikk (1) bekezdésében említett pénzforgalmi szolgáltatók számára azon interfészek igénybevételét, amelyeket a számlavezető pénzforgalmi szolgáltató pénzforgalmi szolgáltatást igénybe vevőinek hitelesítésére és a velük való kommunikációra használnak.

32. cikk

A célra rendelt interfészre vonatkozó kötelezettségek

(1) A 30. és 31. cikknek való megfelelés függvényében azon számlavezető pénzforgalmi szolgáltatók, amelyek célra rendelt interfészt hoztak létre, biztosítják, hogy a célra rendelt interfész mindenkor ugyanolyan szintű elérhetőséget és teljesítményt kínáljon, beleértve a támogatást, mint a pénzforgalmi szolgáltatást igénybe vevő számára a fizetési számlájához való közvetlen hozzáférés céljából rendelkezésre bocsátott interfészek.

(2) A számlavezető pénzforgalmi szolgáltatók, amelyek célra rendelt interfészt hoztak létre, átlátható fő teljesítménymutatókat és a szolgáltatás szintjére vonatkozó célokat határoznak meg, amelyek mind az elérhetőség, mind a 36. cikkel összhangban rendelkezésre bocsátott adatok tekintetében legalább olyan szigorúak, mint a pénzforgalmi szolgáltatást igénybe vevőik által használt interfészekre vonatkozóan meghatározottak. A szóban forgó interfészeket, mutatókat és célokat az illetékes hatóságok nyomon követik és stressztesztelik.

(3) Azon számlavezető pénzforgalmi szolgáltatók, amelyek célra rendelt interfészt hoztak létre, biztosítják, hogy ez az interfész ne akadályozza a megbízásos online átutalási és a számlainformációkat összesítő szolgáltatások nyújtását. Az akadályozás körébe tartozhat többek között annak meggátolása, hogy a 30. cikk (1) bekezdésében említett pénzforgalmi szolgáltatók használják a számlavezető pénzforgalmi szolgáltatók által az ügyfeleiknek kibocsátott hitelesítési adatokat, ezáltal kénytelenek lennének a számlavezető pénzforgalmi szolgáltató hitelesítési vagy egyéb funkcióit igénybe venni, amihez az (EU) 2015/2366 irányelv 11., 14. és 15. cikkében előírtakon túl további engedélyekre és nyilvántartásba vételekre lenne szükség, vagy többször kellene ellenőrizni a pénzforgalmi szolgáltatást igénybe vevők által a megbízásos online átutalási szolgáltatóknak és a számlainformációkat összesítő szolgáltatóknak adott jóváhagyást.

(4) Az (1) és (2) bekezdés alkalmazásában a számlavezető pénzforgalmi szolgáltatók nyomon követik a célra rendelt interfész elérhetőségét és teljesítményét. A számlavezető pénzforgalmi szolgáltatók weboldalukon negyedéves statisztikákat tesznek közzé a célra rendelt interfész és a pénzforgalmi szolgáltatást igénybe vevői által használt interfész elérhetőségéről és teljesítményéről.

33. cikk

A célra rendelt interfészre vonatkozó rendkívüli intézkedések

(1) A számlavezető pénzforgalmi szolgáltatók a célra rendelt interfész kialakításába belefoglalják a rendkívüli intézkedésekre vonatkozó stratégiát és terveket arra az esetre, ha az interfész nem a 32. cikknek megfelelően teljesít, ha az interfész nem tervezetten elérhetetlen, vagy ha a rendszer összeomlik. A nem tervezett elérhetetlenség vagy a rendszerösszeomlás bekövetkezése akkor feltételezhető, ha a megbízásos online átutalási szolgáltatások vagy számlainformációkat összesítő szolgáltatások nyújtása céljából való információ-hozzáférés iránti öt egymást követő kérésre 30 másodpercen belül nem érkezik válasz.

(2) A rendkívüli intézkedések közé tartoznak a célra rendelt interfészt igénybe vevő pénzforgalmi szolgáltatóknak a rendszer helyreállítását célzó intézkedésekről való tájékoztatására irányuló kommunikációs tervek, valamint azoknak az azonnal elérhető alternatív lehetőségeknek a leírása, amelyek ezen idő alatt esetleg a pénzforgalmi szolgáltatók rendelkezésére állnak.

(3) Mind a számlavezető pénzforgalmi szolgáltató, mind a 30. cikk (1) bekezdésében említett pénzforgalmi szolgáltatók haladéktalanul jelentik az érintett illetékes hatóságaiknak az (1) bekezdésben leírt, a célra rendelt interfészekkel kapcsolatos problémákat.

(4) Egy tartalékmechanizmus részeként a 30. cikk (1) bekezdésében említett pénzforgalmi szolgáltatók számára lehetővé kell tenni azon interfészek igénybevételét, amelyeket hitelesítés és a számlavezető pénzforgalmi szolgáltatójukkal való kommunikáció céljából a pénzforgalmi szolgáltatásokat igénybe vevők rendelkezésére bocsátottak, mindaddig, amíg helyre nem állítják a célra rendelt interfész 32. cikkben előírt elérhetőségi szintjét és teljesítményét.

(5) E célból a számlavezető pénzforgalmi szolgáltatók biztosítják, hogy a 30. cikk (1) bekezdésében említett pénzforgalmi szolgáltatók azonosíthatók legyenek és a számlavezető pénzforgalmi szolgáltató által a pénzforgalmi szolgáltatást igénybe vevő számára biztosított hitelesítési eljárásokra támaszkodhassanak. Amennyiben a 30. cikk (1) bekezdésében említett pénzforgalmi szolgáltatók a (4) bekezdésben említett interfészt igénybe veszik:

a) meg kell tenniük az annak biztosításához szükséges intézkedéseket, hogy az adatokhoz ne férjenek hozzá, azokat ne tárolják vagy dolgozzák fel a pénzforgalmi szolgáltatást igénybe vevő által kért szolgáltatás nyújtásától eltérő célból;

b) továbbra is meg kell felelniük az (EU) 2015/2366 irányelv 66. cikkének (3) bekezdéséből, illetve 67. cikkének (2) bekezdéséből eredő kötelezettségeknek;

c) a számlavezető pénzforgalmi szolgáltató által a pénzforgalmi szolgáltatást igénybe vevői számára működtetett interfészen keresztül elért adatokat naplózniuk kell, és kérésre haladéktalanul az illetékes nemzeti hatóságuk rendelkezésére kell bocsátaniuk a naplófájlokat;

d) kérésre haladéktalanul megfelelően indokolniuk kell az illetékes nemzeti hatóságuk felé a pénzforgalmi szolgáltatást igénybe vevők számára a fizetési számlájukhoz való közvetlen hozzáférés céljából rendelkezésre bocsátott interfészek igénybevételét;

e) megfelelően tájékoztatniuk kell a számlavezető pénzforgalmi szolgáltatót.

(6) Az illetékes hatóságok a következő feltételek következetes alkalmazásának biztosítása céljából az EBH-val folytatott konzultációt követően azokat a számlavezető pénzforgalmi szolgáltatókat, amelyek a célra rendelt interfész mellett döntöttek, mentesíti a (4) bekezdésben leírt tartalékmechanizmus létrehozása alól, amennyiben a célra rendelt interfész megfelel a következő feltételek mindegyikének:

a) a 32. cikkben a célra rendelt interfészekre vonatkozóan meghatározott összes kötelezettségnek megfelel;

b) a 30. cikk (5) bekezdésének megfelelően, az ott említett pénzforgalmi szolgáltatók megelégedésére alakították ki és tesztelték;

c) a pénzforgalmi szolgáltatók széleskörűen, legalább három hónapja használják számlainformációkat összesítő szolgáltatások, megbízásos online átutalási szolgáltatások nyújtására, valamint a kártyaalapú fizetések esetében a fedezet rendelkezésre állásának megerősítésére;

d) a célra rendelt interfésszel kapcsolatos problémákat indokolatlan késedelem nélkül megoldották.

(7) Az illetékes hatóságok visszavonják a (6) bekezdésben említett mentességet, ha a számlavezető pénzforgalmi szolgáltatók az a) és d) feltételeket több mint két egymást követő naptári héten át nem teljesítik. Az illetékes hatóságok tájékoztatják az EBH-t a visszavonásról és biztosítják, hogy a számlavezető pénzforgalmi szolgáltató a lehető legrövidebb idő alatt, de legkésőbb két hónapon belül létrehozza a (4) bekezdésben említett tartalékmechanizmust.

34. cikk

Tanúsítványok

(1) A 30. cikk (1) bekezdésének a) pontjában említett azonosítás céljából a pénzforgalmi szolgáltatók a 910/2014/EU rendelet 3. cikkének 30. pontjában említett, az elektronikus bélyegző minősített tanúsítványára, vagy ugyanazon rendelet 3. cikkének 39. pontjában említett minősített weboldal-hitelesítő tanúsítványra hagyatkoznak.

(2) E rendelet alkalmazásában a 910/2014/EU rendelet III. melléklete c) pontjának vagy IV. melléklete c) pontjának megfelelően a hivatalos nyilvántartásban említett nyilvántartási szám a kártyaalapú készpénz-helyettesítő fizetési eszközt kibocsátó pénzforgalmi szolgáltató, a számlainformációkat összesítő szolgáltató és megbízásos online átutalási szolgáltató – beleértve az ilyen szolgáltatásokat nyújtó számlavezető pénzforgalmi szolgáltatókat is – engedélyszáma, amely az (EU) 2015/2366 irányelv 14. cikke értelmében elérhető a székhely szerinti tagállam nyilvánosság számára hozzáférhető nyilvántartásában, vagy amely a 2013/36/EU európai parlamenti és tanácsi irányelv ([1]) 8. cikke alapján megadott minden engedélynek az említett irányelv 20. cikkével összhangban történő értesítéséből következik.

(3) E rendelet alkalmazásában az (1) bekezdésben említett, az elektronikus bélyegző minősített tanúsítványa vagy a minősített weboldal-hitelesítő tanúsítvány a nemzetközi pénzügyi körökben szokásos nyelven a következők mindegyikéhez kapcsolódóan további specifikus attribútumokat foglal magában:

a) a pénzforgalmi szolgáltató szerepe, amely a következők közül egy vagy több lehet:

   i. számlavezetés;

   ii. megbízásos online átutalás;

   iii. számlainformációk összesítése;

   iv. kártyaalapú készpénz-helyettesítő fizetési eszközök kibocsátása;

b) azon illetékes hatóságok neve, ahol a pénzforgalmi szolgáltatót nyilvántartásba vették.

(4) A (3) bekezdésben említett attribútumok nincsenek hatással az elektronikus bélyegző minősített tanúsítványának vagy a minősített weboldal-hitelesítő tanúsítványnak az interoperabilitására és elismerésére.

([1]) Az Európai Parlament és a Tanács 2013/36/EU irányelve (2013. június 26.) a hitelintézetek tevékenységéhez való hozzáférésről és a hitelintézetek és befektetési vállalkozások prudenciális felügyeletéről, a 2002/87/EK irányelv módosításáról, a 2006/48/EK és a 2006/49/EK irányelv hatályon kívül helyezéséről (HL L 176., 2013.6.27., 338. o.).

35. cikk

A kommunikációs munkamenetek biztonsága

(1) A számlavezető pénzforgalmi szolgáltatók, kártyaalapú készpénz-helyettesítő fizetési eszközöket kibocsátó pénzforgalmi szolgáltatók, számlainformációkat összesítő szolgáltatók és megbízásos online átutalási szolgáltatók biztosítják, hogy az adatok interneten keresztüli cseréjekor az adatok bizalmasságának és integritásának a megóvása érdekében biztonságos titkosítást alkalmazzanak a kommunikáló felek között a kapcsolódó kommunikációs munkamenet egésze során, erős és széles körben elismert titkosítási technikák igénybevételével.

(2) A kártyaalapú készpénz-helyettesítő fizetési eszközt kibocsátó pénzforgalmi szolgáltatók, számlainformációkat összesítő szolgáltatók és megbízásos online átutalási szolgáltatók a számlavezető pénzforgalmi szolgáltatók által kínált hozzáférési munkameneteket a lehető legrövidebbre korlátozzák, és aktívan megszüntetnek minden ilyen munkamenetet, amint a kívánt művelet befejeződött.

(3) Amikor a számlavezető pénzforgalmi szolgáltatóval párhuzamos hálózati munkamenetek folynak, a számlainformációkat összesítő szolgáltatók és a megbízásos online átutalási szolgáltatók biztosítják, hogy a szóban forgó munkamenetek biztonságosan kapcsolódjanak a pénzforgalmi szolgáltatást igénybe vevővel/vevőkkel létrehozott vonatkozó munkamenetekhez azon lehetőség megakadályozása érdekében, hogy a közöttük átadott bármely üzenetet vagy információt el lehessen téríteni.

(4) A számlainformációkat összesítő szolgáltatók, a megbízásos online átutalási szolgáltatók és a kártyaalapú készpénz-helyettesítő fizetési eszközöket kibocsátó pénzforgalmi szolgáltatók számlavezető pénzforgalmi szolgáltatóval folytatott kommunikációjának egyértelmű hivatkozásokat kell tartalmaznia a következő elemek mindegyikére:

a) a pénzforgalmi szolgáltatást igénybe vevő vagy vevők és a kapcsolódó kommunikációs munkamenet, az ugyanattól/ugyanazoktól a pénzforgalmi szolgáltatást igénybe vevőtől vagy vevőktől származó több kérés megkülönböztetése érdekében;

b) a megbízásos online átutalási szolgáltatások esetében az egyedileg azonosított kezdeményezett fizetési művelet;

c) a fedezet rendelkezésre állásának megerősítése esetében a kártyaalapú fizetési művelet végrehajtásához szükséges összeghez kapcsolódó egyedileg azonosított kérés.

(5) A számlavezető pénzforgalmi szolgáltatók, a számlainformációkat összesítő szolgáltatók, a megbízásos online átutalási szolgáltatók és a kártyaalapú készpénz-helyettesítő fizetési eszközöket kibocsátó pénzforgalmi szolgáltatók biztosítják, hogy amennyiben személyes hitelesítési adatokat és hitelesítési kódokat közölnek, azok semmikor ne legyenek sem közvetlenül, sem közvetetten bármely személyzet által olvashatóak.

Személyes hitelesítési adatok bizalmasságának az illetékességi körükben történő elvesztése esetén az érintett szolgáltatók indokolatlan késedelem nélkül tájékoztatják az adatokkal társított pénzforgalmi szolgáltatást igénybe vevőt, valamint a személyes hitelesítési adatok kibocsátóját.

36. cikk

Adatcsere

(1) A számlavezető pénzforgalmi szolgáltatók megfelelnek a következő követelmények mindegyikének:

a) a megjelölt fizetési számlákra és a kapcsolódó fizetési műveletekre vonatkozóan ugyanazokat az információkat bocsátják a számlainformációkat összesítő szolgáltatók rendelkezésére, mint amelyeket a pénzforgalmi szolgáltatást igénybe vevő rendelkezésére bocsátanak, amikor az közvetlenül kér hozzáférést a számlainformációkhoz, feltéve, hogy ez az információ nem tartalmaz érzékeny fizetési adatokat;

b) a fizetési megbízás kézhezvétele után azonnal a megbízásos online átutalási szolgáltató rendelkezésére bocsátják a fizetési művelet kezdeményezésére és végrehajtására vonatkozó ugyanazon adatokat, mint amelyeket a pénzforgalmi szolgáltatást igénybe vevő számára rendelkezésre bocsátanak vagy elérhetővé tesznek, amikor ez utóbbi közvetlenül kezdeményezi a műveletet;

c) kérésre azonnal, egyszerű „igen” vagy „nem” formátumban a pénzforgalmi szolgáltatók rendelkezésére bocsátják annak megerősítését, hogy egy fizetési művelet végrehajtásához szükséges összeg rendelkezésre áll-e a fizető fél fizetési számláján.

(2) Az azonosítás, hitelesítés vagy az adatelemek cseréje során bekövetkező váratlan esemény vagy hiba esetében a számlavezető pénzforgalmi szolgáltató értesítő üzenetet küld a megbízásos online átutalási szolgáltatónak vagy a számlainformációkat összesítő szolgáltatónak és a kártyaalapú készpénz-helyettesítő eszközöket kibocsátó pénzforgalmi szolgáltatónak, amelyben ismerteti a váratlan esemény vagy hiba okait.

Amennyiben a számlavezető pénzforgalmi szolgáltató célra rendelt interfészt kínál a 32. cikkel összhangban, az interfésznek biztosítania kell, hogy a váratlan eseményt vagy hibát észlelő pénzforgalmi szolgáltatók az eseményekkel vagy hibákkal kapcsolatos értesítő üzenetet tudjanak küldeni a kommunikációs munkamenetben részt vevő többi pénzforgalmi szolgáltatónak.

(3) A számlainformációkat összesítő szolgáltatók olyan alkalmas és hatékony mechanizmusokkal rendelkeznek, amelyek megakadályozzák a megjelölt fizetési számlákkal és a kapcsolódó fizetési műveletekkel kapcsolatos információktól eltérő információkhoz való hozzáférést, a felhasználó kifejezett jóváhagyásának megfelelően.

(4) A megbízásos online átutalási szolgáltatók ugyanazt az információt bocsátják a számlavezető pénzforgalmi szolgáltató rendelkezésére, mint amelyet a fizetési művelet közvetlen kezdeményezésekor a pénzforgalmi szolgáltatást igénybe vevőtől kérnek.

(5) A számlainformációkat összesítő szolgáltatóknak képeseknek kell lenniük hozzáférni a megjelölt fizetési számlákra és a kapcsolódó fizetési műveletekre vonatkozó, a számlavezető pénzforgalmi szolgáltatóknál lévő információkhoz a számlainformációkat összesítő szolgáltatásnak a következő körülmények valamelyikében történő teljesítése céljából:

a) minden esetben, amikor a pénzforgalmi szolgáltatást igénybe vevő aktívan kéri az említett információt;

b) amennyiben a pénzforgalmi szolgáltatást igénybe vevő nem kéri aktívan az említett információt, legfeljebb négy alkalommal egy 24 órás időszakon belül, kivéve, ha a számlainformációkat összesítő szolgáltató és a számlavezető pénzforgalmi szolgáltató a pénzforgalmi szolgáltatást igénybe vevő jóváhagyásával ennél nagyobb gyakoriságban állapodott meg.

VI. FEJEZET

ZÁRÓ RENDELKEZÉSEK

37. cikk

Felülvizsgálat

Az (EU) 2015/2366 irányelv 98. cikke (5) bekezdésének sérelme nélkül, az EBH 2021. március 14-ig felülvizsgálja az e rendelet mellékletében említett csalási arányokat, valamint a 33. cikk (6) bekezdésében a célra rendelt interfészekkel kapcsolatban megadott mentességeket, és ha indokolt, az 1093/2010/EU rendelet 10. cikkével összhangban benyújtja a Bizottságnak az ezek aktualizálására irányuló tervezeteket.

38. cikk

Hatálybalépés

(1) Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon lép hatályba.

(2) Ezt a rendeletet 2019. szeptember 14-től kell alkalmazni.

(3) A 30. cikk (3) és (5) bekezdését azonban 2019. március 14-től kell alkalmazni.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, 2017. november 27-én.

a Bizottság részéről

az elnök

Jean-Claude JUNCKER

MELLÉKLET

	Referencia csalási arány (%) a következők esetében:	
Kivételi küszöbérték	Távoli elektronikus kártyaalapú fizetések	Távoli elektronikus átutalások
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015