Csapó Beáta-Luspay Miklós:

2021 az év, amikor már nem úgy használjuk a bankkártyánkat, ahogy eddig

Jelen cikkünkben röviden összefoglaljuk, hogy mi indokolja a 2021 január 1.-től megvalósuló online bankkártyás fizetések esetében várható változásokat és hogy mire számíthatnak az ügyfelek. Mindezek mellett bemutatjuk, milyen feladataik vannak a számlavezetőknek, pl. bankoknak, valamint a kártyatársaságoknak a gördülékeny átállás érdekében.

Már megint a PSD2, de mit is jelent ez pontosan?

A PSD2 egy Európai Uniós irányelv, amely az EU-n belüli elektronikus pénzforgalmat (pl. bankszámlavezetés, átutalások, bankkártyák) szabályozza. A PSD2 egyik kiemelt célja volt, hogy erősítse a versenyt a pénzforgalmi szolgáltatók piacán, az új innovatív technológiákat is alkalmazó szereplők megjelenésének elősegítésével, aminek köszönhetően az ügyfelek jobb, gyorsabb és nem mellesleg olcsóbb elektronikus pénzforgalmi szolgáltatásokat tudnak igénybe venni. A jogszabály lehetővé tette az új pénzforgalmi szereplők szabályozott és ellenőrzött körülmények (felügyeleti ernyő alatt) közötti piacra lépését és megteremtette a pénzforgalmi szolgáltatások terén a verseny lehetőségét a „klasszikus" szereplők (pl. a bankok) és az új szereplők között. Mindezek mellett alapvető fontosságú az elektronikus pénzforgalomba vetett bizalom fenntartása.

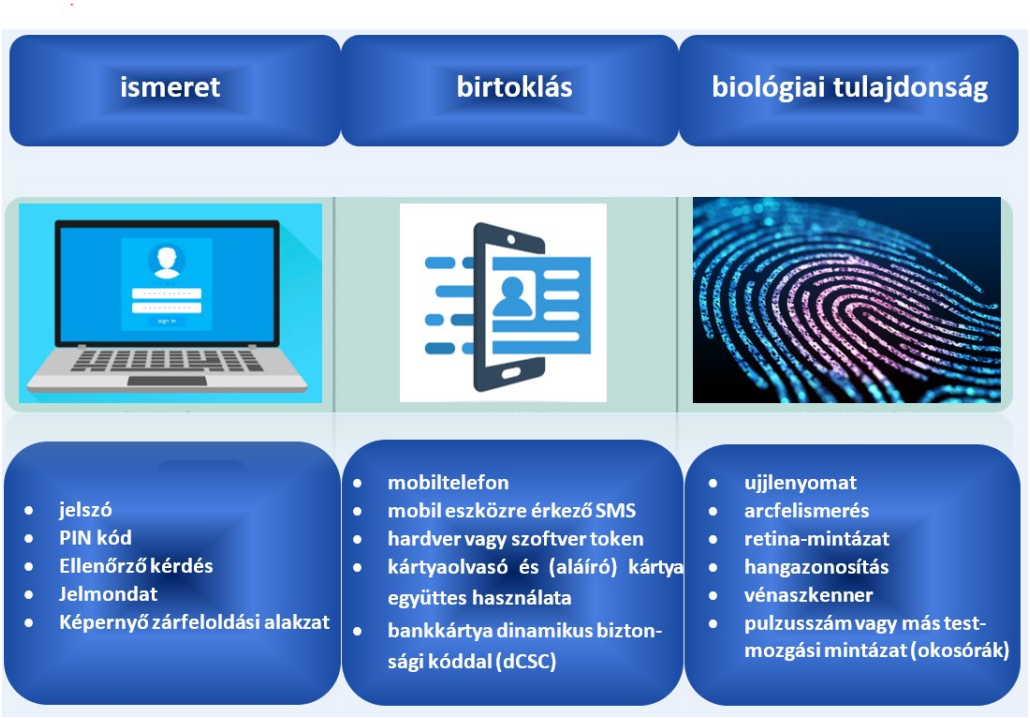
A fentieket szem előtt tartva a PSD2 számos felelősségi és biztonsággal kapcsolatos szabályt vezetett be nem csak az új, hanem a már jelenleg is piacon lévő szereplők számára is. A pénzforgalmi felelősségi szabályok közül kiemelendő a kártyás tranzakciókkal kapcsolatos 15.000 forintos maximális kárviselési összeg, vagy az, hogy a bankkártya letiltásáért nem lehet díjat felszámítani. Emellett megemlítendő, hogy amennyiben az ügyfél egy általa jóvá nem hagyott tranzakció miatt a pénzforgalmi szolgáltatójához fordul, akkor a számlavezetőnek főszabályként vissza kell adnia a vitatott összeget és vita esetén a számlavezetőnek kell bizonyítani az ügyfél csalárd vagy súlyosan gondatlan magatartását. Mindezen szabályok hátterében az a megfontolás állt, hogy elsősorban a számlavezető az, amely - többek között az informatikai fejlesztéseivel - képes biztosítani, hogy az ügyfelek számára a pénzforgalmi szolgáltatás ne csak gyors és kényelmes, hanem biztonságos is legyen. Természetesen fontos, hogy az ügyfél is kellően biztonságtudatos legyen.

A felelősségi szabályok mellett a PSD2 több biztonsági előírást is megfogalmazott a pénzforgalmi szolgáltatókra vonatkozóan. Ezek között kell említeni a csalásmonitoring rendszer bevezetését, valamint egy kockázatértékelés rendszeres elkészítését és annak a felügyeleti hatóságokkal történő megosztását. Mindezek azonban eltörpülnek az úgynevezett erős ügyfél-hitelesítésnek nevezett eljárás mellett, amellyel szavatolható az ügyfél biztonságos hitelesítése, továbbá nagy mértékben csökkenthető a csalás kockázata.

Erős ügyfél-hitelesítés

Az erős ügyfél-hitelesítés a pénzforgalmi szolgáltatást igénybe vevők (az ügyfelek) védelmét szolgálja, kettő egymástól független kategóriába (ismeret, birtoklás, biológiai tulajdonság) eső hitelesítési elem egyidejű használatával. Ez a gyakorlatban azt jelenti, hogy például egy elektronikus tranzakcióhoz kapcsolódó hitelesítéshez egyidejűleg szükség van egy statikus jelszó ismeretére, továbbá például egy mobiltelefonra érkező SMS-ben vagy felugró (push) üzenetben kapott egyszer felhasználható kódra.

1. ábra: A hitelesítési elemek kategóriánként



Képek forrása: iStock

Mindezek használata a biztonságot jelentősen megemeli és segítheti a visszaélések megelőzését, hiszen ezen elemeknek egymástól függetlennek kell lenniük, azaz az egyik feltörése nem befolyásolja a másik elem megbízhatóságát. Ha például adathalászat során sikerül is megszerezni az ügyfél jelszavát, az önmagában még nem elegendő egy fizetés kezdeményezéséhez, mert még egy másik kategóriában sorolt hitelesítési faktor (pl. ujjlenyomat használata, vagy SMS-ben kapott egyszer használatos kód) is szükséges hozzá.

A 2019. szeptember 14. előtt alkalmazandó szabályok alapján elegendő volt az ügyfél hitelesítéséhez mindössze egy hitelesítési elem használata valamennyi fizetés estében. Azaz például átutaláskor az internetbankon egy, az ügyfél által ismert (statikus), jelszóval történő belépést követően indítható volt egy tranzakció még egy további hitelesítési elem (például egyszeri SMS-ben küldött vagy token által generált jelszó) használata nélkül.

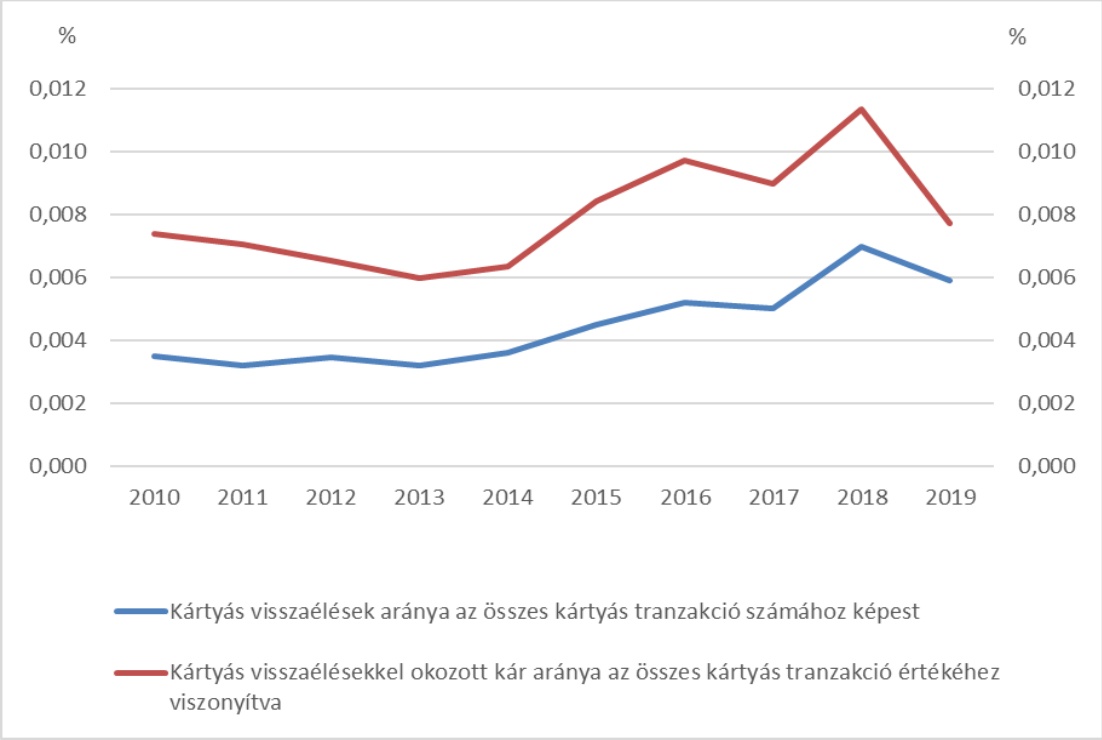
Az új szabályok értelmében azonban a pénzforgalmi szolgáltatóknak már pl. a jelszótól eltérő hitelesítést is kérniük kell egy fizetés elindításához, ami ráadásul már nem tartozhat az ismeret kategóriába.

Az erős ügyfél-hitelesítés bevezetési kötelezettség minden elektronikusan indított (pl. internetbanki felületen, mobilbankon) tranzakciók esetében kötelező, a 2020. december 31.-i véghatáridő letelte után az online bankkártyás vásárlások (pl. internetes vásárlás) esetében is!

Ok, de mi a helyzet visszaélésekkel, ekkora lenne a gond?

2019-ben Magyarországon mintegy 1,4 Mrd darab elektronikus fizetési tranzakció volt, amiből 1 Mrd bankkártyás fizetés. Az MNB által a bankoktól gyűjtött statisztika alapján a visszaélések száma és az ezekkel okozott kár aránya a kártyakibocsátók oldalán az összes bankkártyás forgalomhoz képest elhanyagolható mértékű, mindössze a 0,008 %-át teszi ki értékben és 0,006%-át darabszámban.

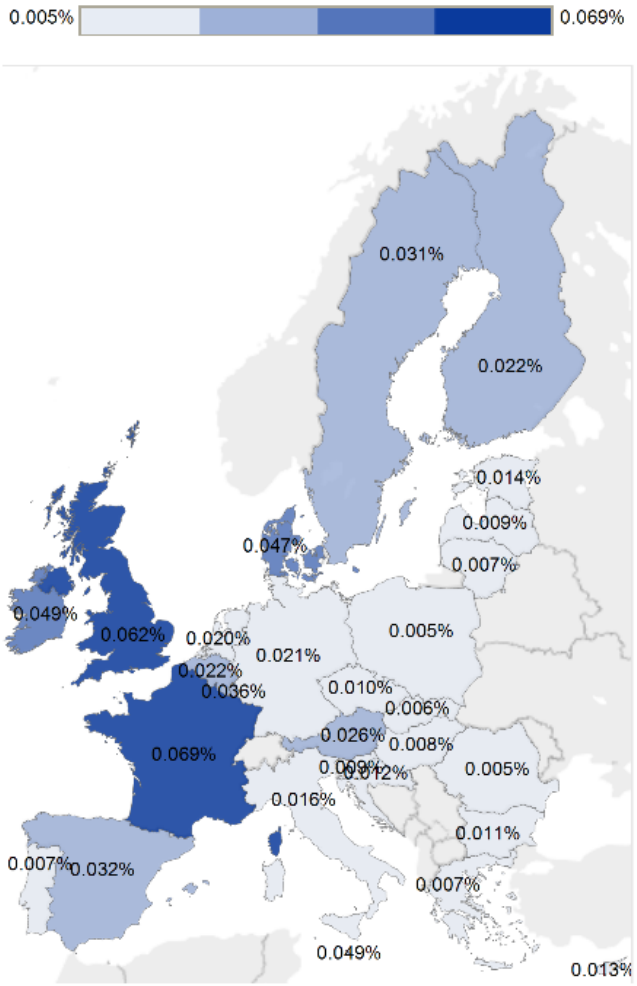
2. ábra: A visszaélések száma és az ezekkel okozott kár aránya a kártyakibocsátók oldalán



Forrás: MNB

Az MNB a rendelkezésére álló jelenlegi adatok alapján úgy látja, hogy ezen rendkívül alacsony visszaélési számokban a PIN-kód nélküli érintéses fizetési limit 15 ezer forintra történő emelése sem változtatott. Az Európai Központi Bank csalásra vonatkozó statisztikai adatai alapján Magyarország az egyik legbiztonságosabb ország az uniós tagállamok között, a bankkártyás fizetések terén.

3. ábra: A bankkártyás visszaélések százalékos megoszlása az uniós tagállamok között



Forrás: EKB

A visszaélési statisztikákhoz kapcsolódóan fontos még megemlíteni azt a tényt is, hogy a fogyasztók érdekeit előtérbe helyező pénzforgalmi felelősségi szabályoknak köszönhetően a ténylegesen bekövetkezett kár túlnyomó többségét, 93%-ot 2019-ben a számlavezetőknek kellett viselniük!

Amennyiben azonban alaposabban megnézzük a statisztikai adatokat, azt is látjuk, hogy főként a kártya jelenlétét nem igényló fizetési helyzetekben (pl. internetes vásárlások) fordulnak elő visszaélések nagyobb arányban. Éppen ezen helyzetet felismerve írta elő a PSD2 egyik technikai részletszabálya az erős ügyfél-hitelesítés alkalmazását 2019. szeptember 14.-től a számlavezető számára minden fizetési helyzetben.

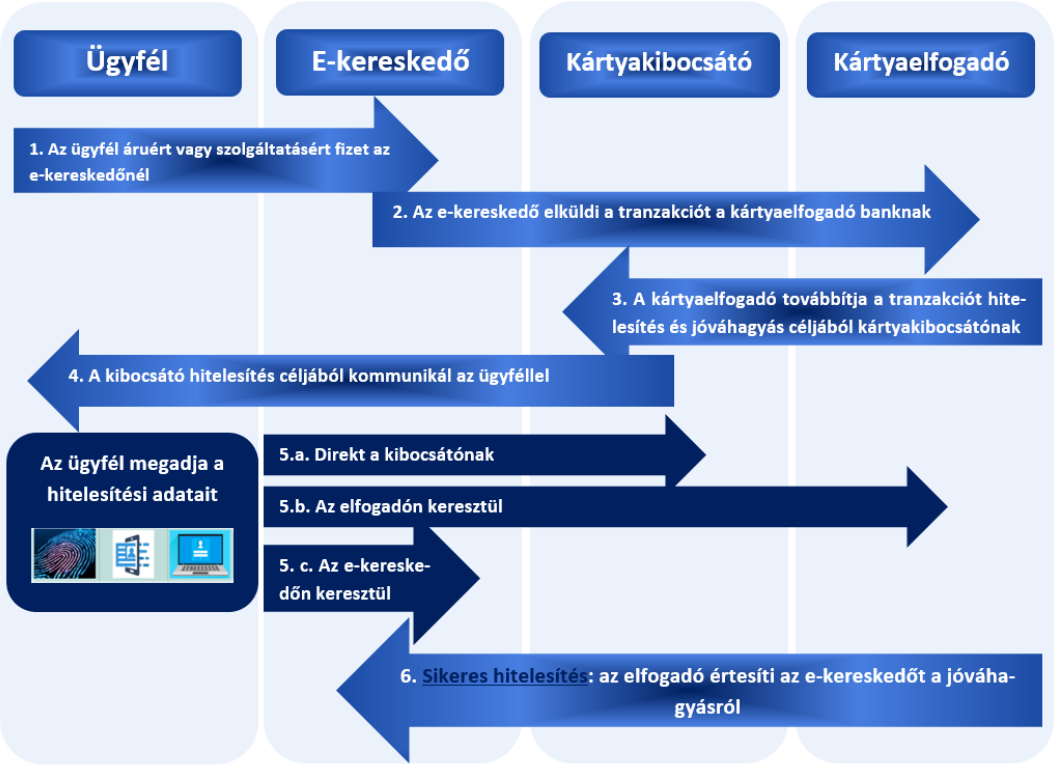
<u>De mit is jelent az erős ügyfél-hitelesítés az online bankkártyás fizetések esetében?!</u>

A szabályozás értelmében az interneten keresztül indított bankkártyás vásárlások során jelenleg alkalmazott megoldás, vagyis a kártyán szereplő adatok: kártyaszám, az ügyfél neve, kártya lejárati

dátuma, a bankkártya hátoldalán, a fehér aláírósávban található 3 jegyű kód (CVV/CVC kód), mint hitelesítési elemek nem sorolhatóak egyik hitelesítési elem kategóriába sem. Az sem teljes mértékben megfelelő, amennyiben például a kártyán szereplő adatok megadása mellett egy egyszer használatos kód kerül kiküldésre az ügyfél telefonjára, ez ugyanis még mindig csak egy hitelesítési elemnek tekinthető.

Mindez azt jelenti tehát, hogy a jövőben, ha egy internetes áruházban vásárolunk, akkor az eddig megszokott módon, csupán a bankkártyánkon lévő információk nem lesznek elégségesek a vásárlás lebonyolításához.

4. ábra: Az online bankkártyás fizetés sematikus folyamata



Míg az elektronikus banki átutalások terén sok esetben részben vagy teljesen már a szabályozás hatályba lépése előtt is megvalósult az erős ügyfél-hitelesítés (SMS, vagy token segítségével) addig a kártyás vásárlások esetén ilyen nem volt. Ahhoz, hogy ez a kártyás vásárlások esetében is megvalósítható legyen, a kártyakibocsátóknak, a kártyaelfogadóknak, a kártyatársaságoknak, valamint az internetes kereskedőknek is komoly fejlesztéseket kell végrehajtaniuk. Amennyiben ezen szereplők közül bármelyik nem képes a szükséges adatokat kezelni a teljes fizetési láncban, akkor a tranzakció sikertelenné válhat.

Jól mutatja ezt a kockázatot, hogy a szereplőknek nem sikerült felkészülni az eredetileg megszabott 2019. szeptember 14.-i határidőre, ezért az Európai Bankhatóság új határidőként 2020. december 31.-t állapította meg.

Az MNB azt az álláspontot képviselte, hogy a szabályozás bevezetése csak Európában egységesen és egy időben lehetséges, így alkalmazkodott az egységes, kötelező, európai véghatáridőhöz.

Milyen változásra lehet számítani?

A változás alapvetően azt jelenti majd, hogy míg 2020. december 31.-ig az esetek döntő hányadában elégséges a bankkártyán lévő adatok megadása egy online bankkártyás tranzakció lebonyolításához, a jövőben erre már nincsen lehetőség. 2021-től a bankkártyán lévő információ nem tekinthető hitelesítő elemnek, azaz azok megadása nem tekinthető erős ügyfél-hitelesítésnek.

A gyakorlatban számos megoldási lehetőség kínálkozik a számlavezetők számára: kellően gyors megoldás lehet például egyedi SMS kód küldése a mobiltelefonra, az online tranzakciókra rendszeresített PIN kód, a biometrikus azonosítás bevezetése (például a mobiltelefonon keresztül történő ujjlenyomat), vagy akár az internetbankon keresztül kimondottan erre a célra megadható jelszó alkalmazása is. A megoldások számlavezetőnként változhatnak, de alapvető cél olyan megoldás megalkotása és megvalósítása, amely az ügyfél számára kényelmes és gyors.

Fontos tudni, hogy már jelenleg is van olyan hazai számlavezető, amely megfelel az erős ügyfél-hitelesítésre vonatkozó előírásoknak bizonyos tranzakciók esetében, ugyanakkor az ügyfelek nagy részénél érdemben meg fog változni az online kártyás fizetés folyamata. Az MNB a változásokkal kapcsolatban elvárja a piaci szereplőktől, hogy olyan ügyfélbarát hitelesítési megoldásokat alakítsanak ki, amelyek nem akadályozzák az elektronikus fizetési módok használatát és támogatják az online fizetések további térnyerését! Az MNB támogatta az egységes európai véghatáridő alkalmazását, ugyanakkor elvárásként fogalmazta mega a hazai számlavezetőkkel szemben, hogy 2020. szeptember 14.-ig készüljenek el a szükséges fejlesztések, lehetőleg még abban az esetben is, ha a tényleges alkalmazásukra 2020. december 31.-én kerül csak sor. Tette mindezt azért, hogy a számlavezetők még nagyobb biztonsággal készüljenek el a 2020. december 31.-i véghatáridőre és a fejlesztések ne az amúgy is igen terhelt év végi időszakra essenek. További alapvető elvárás, hogy időben megvalósuljon az ügyfelek és más érintettek megfelelő módon történő tájékoztatása és amennyiben szükséges, megfelelő oktatása az új technikai megoldások használatára.

Az ügyfelek azonban az újítások bevezetése után sem fognak feltétlenül minden egyes online bankkártyás tranzakció esetén találkozni az erős-ügyfél hitelesítéssel, hiszen a jogszabály bizonyos esetekben ez alól mentességet adhat. Ilyen mentességi kritérium lehet például, ha a parkolás vagy egyéb közlekedés viteldíját szeretnénk megfizetni. A jövőben például lehetőségünk lesz arra is, hogy ha egy online vásárlás során rendszeres időközönként, például ugyanazon összeggel terhelnék be a számlánk, akkor a kártyakibocsátó alkalmazhatja az ismétlődő fizetésekre vonatkozó kivételi szabályt, így elegendő az erős ügyfél-hitelesítést alkalmazni az első terhelésnél.

Összességében elmondható tehát, hogy egy alapvetően biztonságos fizetési megoldás a jövőben még biztonságosabbá válik. A szükséges banki fejlesztésekre és az ügyfelek számára kényelmes és gyors megoldások kidolgozására a számlavezetőknek elégséges idő állt rendelkezésére. A 2021-től alkalmazandó változtatásokkal ugyan meg fog változni az a gyakorlat, ahogy a kártyánkat használjuk az internetes vásárlások során, ugyanakkor ennek hatására még biztonságosabbá válnak az online tranzakcióink.

„Szerkesztett formában megjelent az Infostart.hu oldalon 2020. november 11-én.”