Bodnár László - Csapó Beáta - Luspay Miklós

Bankkártyával online vásárol? A 2021 a változások éve

2021. január 1-től jelentősen megváltozott az élete annak, aki bankkártyával interneten szeretne fizetni. Ekkortól kell ugyanis alkalmazni az ún. erős ügyfél-hitelesítést[1], ami alapvetően azzal a céllal született, hogy az ügyfelek védelmét szolgálja.

Az átutalásoknál már korábban megszokott kettő hitelesítési elem (faktor) használata a bankkártyával történő fizetések esetében is kötelezővé vált. E fizetéseknél pedig a kártyán szereplő adat nem használható már fel faktorként. E változással érintett hazai pénzforgalmi szolgáltatók (számlavezetők, jellemzően bankok) számára az MNB az Európai Bankhatóság (EBA) által megadott véghatáridőt megelőzően korábbi megfelelési határidőt írt elő, és ezt a határidőt csak indokolt esetben, egyedileg hosszabbította meg 2020. december 31-ig. Ennek is köszönhetően a hazai szektor végül a felkészültségben kiemelkedő helyet ért el Európai Uniós összehasonlításban, de az átállás nem volt teljesen zökkenőmentes. Az induláskor ugyanis adódtak apró nehézségek, azonban egy komplex változást igénylő átállás esetén ez elfogadható szinten maradt, a pénzforgalom lebonyolítása alapvetően zavartalan volt.

Az MNB számára többféle technikai megvalósítás is ismert, amellyel a számlavezetők megfelelnek a szabályozásnak, azonban az elvárás volt, hogy ezek ügyfélbarát módon kerüljenek kialakításra, továbbá olyan ügyfelek számára is biztosított legyen az erős ügyfél-hitelesítés alkalmazása, akik nem rendelkeznek többfunkciós vagy okoseszközzel. Mindez ugyanis elősegíti, hogy ne egy illetéktelen csaló hitelesítse a tranzakciót, mivel csupán a kártyán szereplő adatok ismerete nem elegendő az interneten keresztüli vásárlás lebonyolításához. A bevezetett új megoldásokat a számlavezetők folyamatosan fejlesztik az ügyfelek visszajelzései és a tapasztalatoknak megfelelően.

Néhány bank már a véghatáridőt megelőzően is lehetővé tette az erős ügyfél-hitelesítést, amit a biztonságtudatos ügyfelek készséggel használtak már annak kötelezővé tétele előtt is. Ezen bankok az általuk kibocsátott fizetési kártyákkal

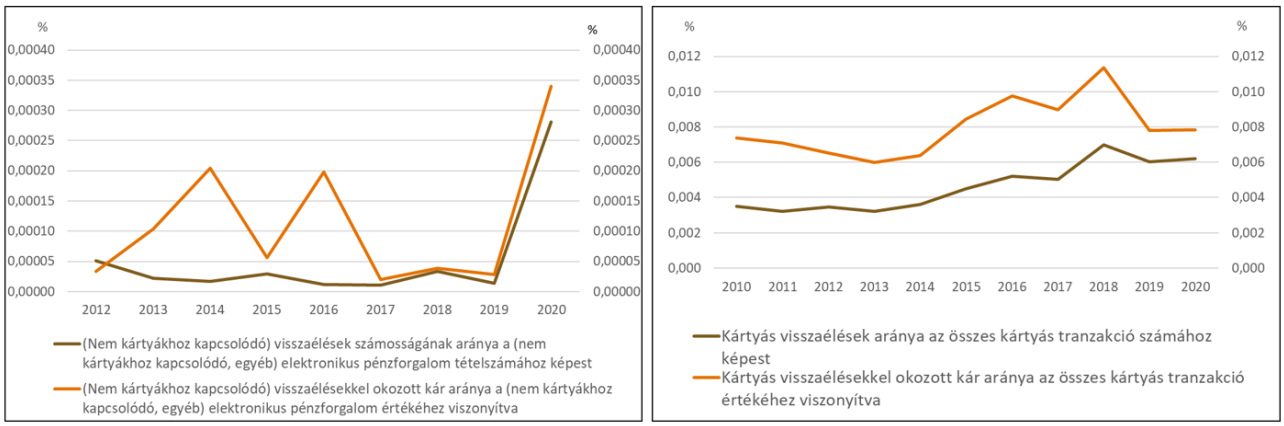
[1] Lásd keretes írás.

kezdeményezett fizetési műveletek 13,9%-ánál már a tavalyi évben alkalmazták az új megoldást.

Mire lehet számítani a visszaélési adatok számosságát tekintve?

Szintén a tavalyi évben volt tapasztalható, hogy megnőtt az elektronikus fizetési műveletek száma, főleg a járványhelyzet következtében. Az átutalások során már korábban is kötelező volt az erős ügyfél-hitelesítés alkalmazása, ami biztonságosabbá teszi a fizetést. A kártyás fizetések biztonságát tekintve hazánk eddig is jó helyen állt uniós viszonylatban is. A visszaélések száma az MNB számára elérhető adatok alapján inkább az internetes vásárlásokhoz kapcsolódik (1. ábra). 2020-ban például összesen 1,5 milliárd forint összegű visszaélés történt a fizetési kártyákhoz kötődően, amely a teljes pénzforgalomhoz képest marginális.

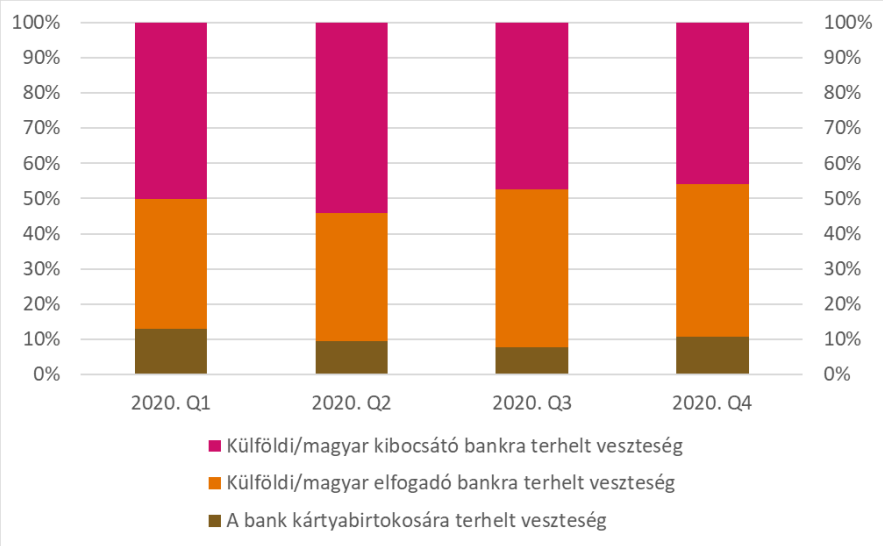
1. ábra: *A visszaélések arányai a nem kártás és kártyás fizetési műveletek összforgalmához képest*



Forrás: MNB

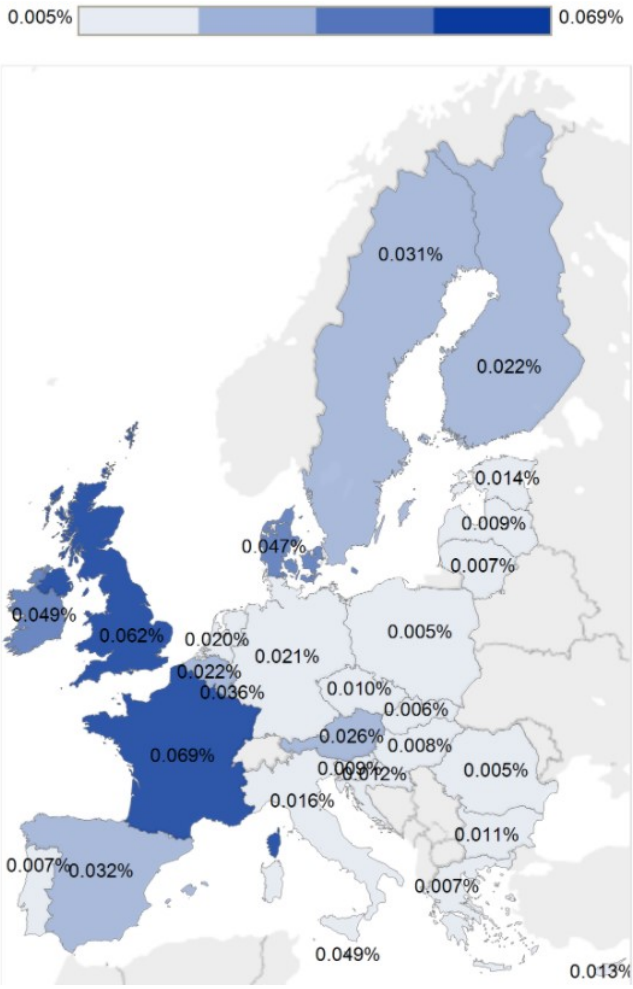
Szintén fontos megemlíteni, hogy a visszaélések jelentős számánál az ügyfelek jelentős hányadát nem érte kár (2. ábra), - többek között - a pénzforgalomhoz kapcsolódó speciális felelősségi szabályoknak köszönhetően. Uniós szinten tehát hazánk egyébként is jó helyezést ért el (3. ábra) a csalásokra és visszaélésekre vonatkozó adatok alapján, azonban **az erős ügyfél-hitelesítés alkalmazásával az MNB arra számít, hogy tovább csökken a visszaélések számossága a fizetési kártyákkal történő internetes vásárlások esetében is.**

***2. ábra**: Fizetési kártyás visszaélések kibocsátó oldali veszteségek megoszlása*



Forrás: MNB

***3. ábra**: A fizetési kártyás visszaélések számának százalékos megoszlása az uniós tagállamok közt*



Forrás: EKB

Mindig kell erős ügyfél-hitelesítést alkalmazni?

A kivételi szabályok alkalmazása miatt az ügyfelek néha azt tapasztalhatták, hogy nem minden esetben hajtja végre az erős ügyfél-hitelesítést a pénzforgalmi szolgáltató. Ezen kivételi szabályok listáját EU-s rendelet tartalmazza, így minden EU tagállamban ugyanolyan kivételi szabályok kerülhetnek alkalmazásra. A kivételi szabályokat az EU-s jogalkotó azért építette be a szabályozásba, hogy egyes alacsony kockázatúnak tartott esetekben gyorsítsa a fizetési folyamatot.

A kivételi szabályok alkalmazásáról a pénzforgalmi szolgáltatók egyedileg dönthetnek, emiatt eltérés mutatkozhat a számlavezetők gyakorlata között. A jogszabály pontosan meghatározza azokat az eseteket, amikor a kivételi szabályok alkalmazására a pénzforgalmi szolgáltatónak lehetősége van. Ilyen például a kisösszegű, azaz 11.000 forintösszeg (30 EUR-nak megfelelő[2])alatti tranzakciók esete. Ebben az esetben a pénzforgalmi szolgáltató ugyanis dönthet úgy, hogy nem alkalmazza az erős ügyfél-hitelesítést. Ugyanakkor fontos megjegyezni, hogyha a pénzforgalmi szolgáltató az erős ügyfél-hitelesítés mellőzése mellett dönt, akkor a pénzforgalmi kárfelelősségi szabályok tovább szigorodnak. Amennyiben bármely okból nem történik a tranzakció során erős ügyfél-hitelesítés, az ennek hiányából fakadóan bekövetkezett károkért a teljeskörű felelősség az ügyfél számlavezetőjét terheli

Maximum 180.000 forintösszegig (500 EUR-nak megfelelő, e fölötti összeg esetében már nem) szintén dönthet úgy a pénzforgalmi szolgáltató, hogy nem alkalmaz erős ügyfél-hitelesítést online fizetések esetében. Ebben az esetben egyéb feltételeknek is teljesülniük kell, például csalás monitoring rendszert kell működtetnie, amellyel valós időben folyamatosan észlelni képes az esetleges visszaéléseket.

További kivételi esetek lehetnek még például az ismétlődő fizetési műveletek (tipikusan ilyenek az előfizetések díjai). Az ügyfeleknek is van továbbá lehetőségük arra, hogy az általuk indított fizetési művelet végső címzettjeit (beleértve azon internetes kereskedőket is, akiknél az ügyfél vásárol) „megbízható”-nak jelöljék meg akár a netbankon vagy mobilalkalmazáson keresztül, így ebben az esetben sem kell erős ügyfél-hitelesítést alkalmazni.

[2] A vonatkozó jogszabály által előírt euro érték forintosításának árfolyamára vonatkozóan nincs kötelezően alkalmazandó jogszabály, az MNB javasolja a számlavezetőknek, hogy a devizaátváltási árfolyam esetében az MNB hivatalos, naponta fixált és publikált devizaárfolyamát vegyék alapul.

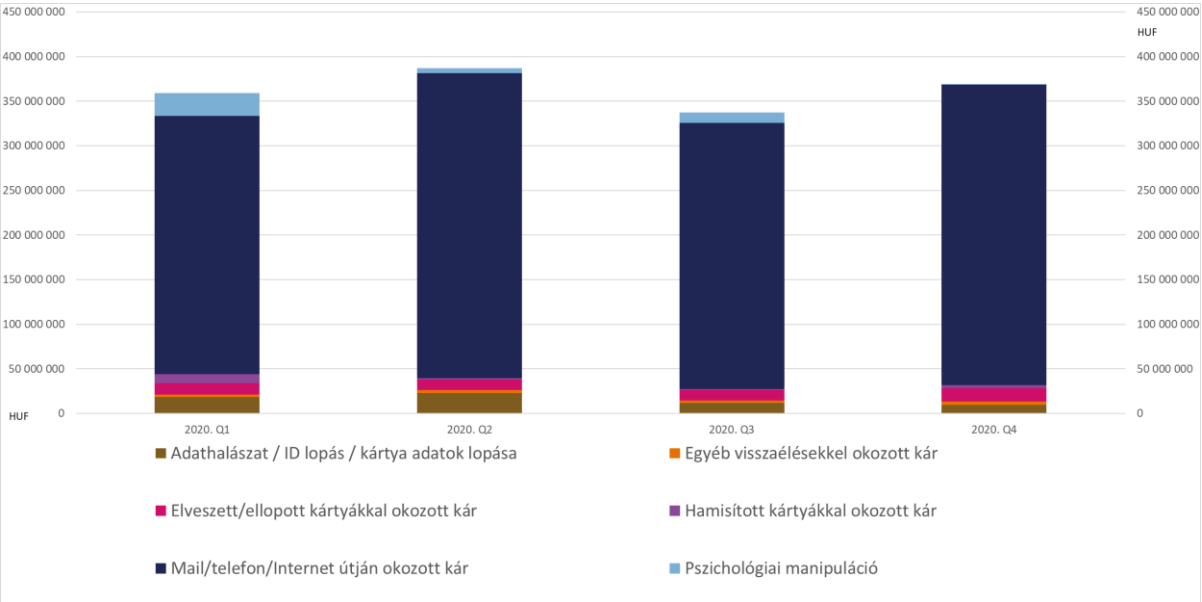
Az MNB a folyamatos felügyelés keretében zajló ellenőrzései során eddig csak kisebb hiányosságokat tapasztalt, a pénzforgalmi ellenőrzések során továbbra is vizsgálni fogja - többek között - a kivételi szabályok jogszerű alkalmazását is.

Mivel fokozható még a biztonság?

Fontos egyúttal azt is hangsúlyozni, hogy az erős ügyfél-hitelesítés nem véd olyan esetek ellen, amikor az ügyfél tévesen (pl. csalás következtében) maga adja ki illetéktelen számára az érzékeny fizetési adatait. Ilyen eset lehet például a gyakorlatban, amikor a csaló a bank nevében telefonon, vagy e-mail-en megkeresi és arra kéri az ügyfelet, hogy adja meg a kártyájának az adatait, valamint a hitelesítéshez szolgáló minden további információt is. Az ügyfél pedig nem is gyanakszik, hogy e-mail, illetve telefon útján a bankja biztosan nem kér el ilyen adatokat, így megteszi azt.

A másik gyakori eset, hogy olyan fizetőoldalra vezet át az internetes vásárlást követően a kereskedő, amely megtévesztésig hasonlít ugyan a megszokott fizetőoldalra, de az az oldal egyáltalán nincs titkosítva és egy csalók által manipulált oldalon megszerezhetővé válnak az adatok. Ezekben az esetekben például hiába is történik erős ügyfél-hitelesítés, a csalás mégis megtörténik. **Fontos tehát, hogy az ügyfél is kellően körültekintő és biztonságtudatos legyen!** A bankkártyákkal érintett visszaélések típus szerinti megoszlását a 4. ábra szemlélteti.

***4. ábra**: A fizetési kártyás visszaélések kibocsátói oldalon visszaélések típusa szerinti csoportosítása*



Forrás: MNB

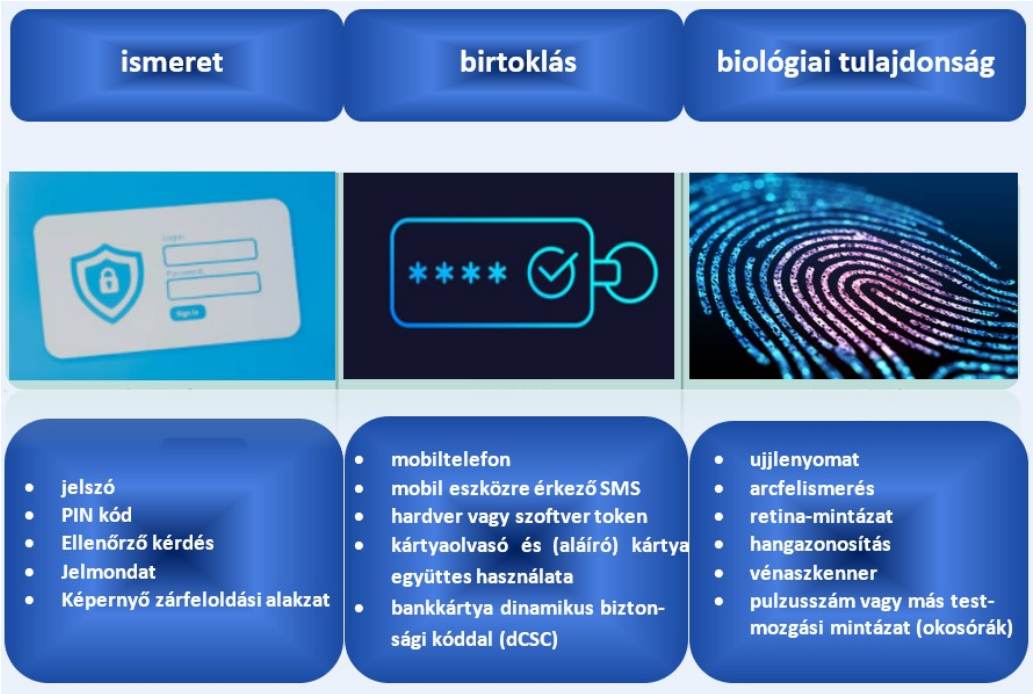
Hogyan fogadták mindezt az ügyfelek?

Ahogy fentebb is már említettük, nem elhanyagolható szempont az sem, hogy a járványhelyzetben jelentősen megnőtt az elektronikus fizetések száma (1. ábra), így a PSD2 által bevezetett szabályok a jövőbeni, magasabb digitalizáltság melletti biztonságos működést is elősegítik. A szabályozás egyik legfontosabb célja a csalások megelőzése és elkerülése, a biztonság rendszer szintű növelésével. Az ügyfelek értékelhették oly módon a változást, hogy kényelmetlenebb lesz az eddig megszokott internetes vásárlásuk, ezért is fogalmazta meg az MNB elvárásként, hogy az erős ügyfél-hitelesítés ügyfélbarát módon történő kialakítását. A bevezetést követően a panaszok egy része mégis inkább ahhoz kapcsolódott, hogy az ügyfelek hiányolták valamelyik hitelesítési faktort, mivel az erős ügyfél-hitelesítés hiányában kevésbé érezték a pénzüket biztonságban. **Az MNB úgy látja, hogy az ügyfelek gyorsan alkalmazkodtak az új biztonsági megoldásokhoz, amelyek a napi gyakorlat részévé váltak.**

keretes írás: *Hány faktor a két faktor többfunkciós eszköz esetében?*

Az erős ügyfél-hitelesítés vagy kétfaktoros azonosítás a pénzforgalmi szolgáltatást igénybe vevők (az ügyfelek) védelmét szolgálja, kettő egymástól független kategóriába eső hitelesítési elem egyidejű használatával (ezek a kategóriák a következők: ismeret, birtoklás, biológiai tulajdonság).

***5. ábra**: A hitelesítési elemek kategóriánként*



Képek forrása: iStock

A hitelesítési elemek függetlenségét biztosítani kell, de ez nem jelenti feltétlenül azt, hogy csak és kizárólag akkor jogszabályi előírásoknak megfelelő a technikai megvalósítás, ha a hitelesítési elemek csakis egy-egy különálló fizikai eszközön valósulnak meg. Megfelelő lehet ugyanis egy többfunkciós eszközön belül telepített applikáció is, amennyiben az egy elkülönített biztonságos környezetben fut az adott eszközön. A gyakorlatban ez azt jelenti, hogy egy mobil készülékkel a Mobilbankba jelszóval történő belépést (ismeret kategóriájú hitelesítési elem) követően lehetőség van ugyanazon mobiltelefonra telepített applikációban, ujjlenyomattal való jóváhagyásra (biometrikus kategóriába eső hitelesítési elem). Ebben az esetben viszont kiemelten fontos, hogy biztosítania kell a

számlavezetőnek olyan védelmi mechanizmusokat is, hogy a mobiltelefonra telepített eszköz esetében felismerhető legyen, ha a telepített szoftvert, vagy applikációt egy csaló manipulálta. Azaz például egy közbenső támadással egy illetéktelen harmadik fél megváltoztatta azt. Az ilyen változtatás bekövetkezésének észlelésére is biztosítani kell megfelelő biztonsági intézkedéseket a számlavezetőnek.

Néhány szakvélemény szerint csakis a fizikailag is teljesen elkülönülő hitelesítési elemek jelenthetik a tényleges szeparációt, azonban ezek függetlensége biztosítható akár egyetlen többfunkciós eszközön is. Valóban az első eset még nagyobb biztonságot nyújthat, így több számlavezető biztosítja ügyfelei számára a különálló fizikai tokeneket, amelyekkel azonosító kód generálható, de a használhatóság és ügyfélélmény szempontjából lehetőség van alternatív megoldások alkalmazására is, természetesen, a megfelelő kockázatmérséklési intézkedésekkel együtt.

Összegzés

A bankkártyás internetes fizetések terén az erős ügyfél-hitelesítésre történő felkészülés jelentős (informatikai) fejlesztést igényelt, továbbá számos más, bankrendszeren kívüli szereplőt is érintett (például az internetes áruházakat működtető kereskedőket is). Az ügyfeleknek ugyan új, a korábbiaktól eltérő fizetési gyakorlatot kellett elsajátítaniuk, de mindez azt a célt szolgálta, hogy a fizetések biztonsága és ezáltal a pénzforgalomba vetett bizalom tovább növekedjen. Fontos továbbá az is, hogy az ügyfelek kellően körültekintően és biztonságtudatosan járjanak el a fizetések során. **Összességében az újonnan bevezetett megoldások még inkább megnövelik tehát a bankkártyás internetes fizetések használatának biztonságát is, továbbá tágabb értelemben a PSD2 elősegíti a digitalizációt és az innovációt egyaránt**.

„Szerkesztett formában megjelent a Világgazdaságban 2021. július 1-én.”